Disquisicions Aritmètiques

Carl Friedrich Gauss

Disquisicions Aritmètiques

traducció i pròleg de

Griselda Pascual Xufré

BARCELONA

1996

Biblioteca de Catalunya. Dades CIP

Gauss, Carl Friedrich
Disquisicions aritmètiques
Trad. de: Disquisitiones arithmeticæ. 1801, 1968
ISBN 84-7283-313-5
I. Pascual Xufré, Griselda
II. Societat Catalana de Matemàtiques
III. Títol 1. Aritmètica 2. Nombres, Teoria dels
511

Traducció i pròleg: Dra. Griselda Pascual Xufré, professora titular d'Àlgebra de la Facultat de Matemàtiques de la Universitat de Barcelona.

Amb la col·laboració científica del Seminari de Teoria de Nombres (UB–UAB–UPC) i el suport de la DGICYT i del Departament d'Ensenyament de la Generalitat de Catalunya.

Traducció de l'edició llatina: *Disquisitiones Arithmeticæ,* Lipsiæ, Gerh. Fleischer, 1801; edició anastàtica: *Disquisitiones Arithmeticæ,* Brussel·les, Culture et Civilisation, 1968.

Text compost amb macros de TEX dissenyades especialment per a aquesta edició.

© de la traducció i el pròleg: Griselda Pascual Xufré

Editat per la Societat Catalana de Matemàtiques
(filial de l'Institut d'Estudis Catalans)
Carme, 47. 08001 Barcelona

Imprès a Impremta Altés, s. l.,
Caballero, 87. 08027 Barcelona

ISBN: 84-7283-313-5
Dipòsit Legal: B. 13575-1996

PRÒLEG DE LA TRADUCTORA

L'obra *Disquisitiones Arithmeticæ* de Carl Friedrich Gauss (Brunswick, 1777 - Göttingen, 1855) apareix citada sovint en llibres i treballs especialitzats; però, dissortadament, fins ara a casa nostra no es trobava a l'abast del públic. En especial, era lamentable que el jovent que s'iniciava en els estudis de l'aritmètica no tingués un accés fàcil a la lectura i la consulta d'aquesta obra cabdal. Sens dubte, les *Disquisitiones Arithmeticæ* són fonamentals en el desenvolupament de l'aritmètica i justifiquen plenament la necessitat i l'esforç que suposa la seva traducció a la nostra llengua.

La idea de realitzar una versió catalana de les *Disquisitiones* sorgí, fa uns quants anys, arran d'una conversa amb la Dra. Pilar Bayer. Vàrem pensar que disposar d'aquest text en català podria ser un ajut inestimable per a aquelles persones que, atretes pel fet matemàtic, volguessin gaudir, mitjançant les primeres fonts, de la genialitat de Gauss.

Partírem de la informació següent: Gauss començà a escriure les *Disquisitiones Arithmeticæ* a l'edat de dinou anys en llengua llatina. Es publicaren per primera vegada l'any 1801 i es reeditaren l'any 1968. L'any 1807 se n'edità la versió francesa, que es reedità el 1979. El 1870 aparegué una segona edició llatina que modificava la primera en la distribució tipogràfica. Aquesta es traduí a l'alemany i s'edità l'any 1889, amb una reedició el 1965. La primera traducció a l'anglès és d'aquesta segona edició; es portà a terme el 1965 i es reedità l'any 1985.

La llengua catalana, per la seva condició de romànica, permet apropar-se fidelment al text de Gauss. La traducció que presentem procura ajustar-se al màxim a l'edició de l'any 1968 de la primera versió llatina.

Recordem que Gauss anomena *Arithmeticæ Sublimior* la matèria que considera en el tractat, per tal de distingir-la dels estudis elementals que, amb el nom d'aritmètica, es portaven a terme a la seva època.

Les *Disquisitiones* consten de set seccions, encara que la persona que les llegeixi observarà que Gauss fa referència diverses vegades a una vuitena secció, que no inclou.

Les tres primeres seccions contenen un tractament força complet de congruències numèriques que, per primera vegada, s'exposava sistemàticament i amb una notació adequada.

La secció quarta és molt peculiar. És dedicada íntegrament als residus quadràtics. S'hi troba la primera demostració de la llei de reciprocitat quadràtica. Malgrat que aquesta demostració és prou senzilla, val a dir que ha passat a l'oblit, en part per la seva laboriositat. El fet que sigui tan àrdua rau en la simplicitat del seu utillatge; que resulti de lectura complexa és, entre d'altres raons, per la manca de flexibilitat de les notacions que fa servir.

La secció cinquena és el nucli de l'obra. Conté un estudi profund de les formes quadràtiques binàries enteres i una introducció a l'estudi de les ternàries. Gauss considera sempre formes quadràtiques binàries del tipus $ax^2 + 2bxy + cy^2$, però, amb un xic d'atenció, es pot aplicar el seu estudi a formes quadràtiques binàries enteres qualssevol. Entre d'altres coses, Gauss classifica les formes quadràtiques binàries, fa la composició de classes, i introdueix el concepte de gènere.

La secció sisena és dedicada a aplicacions de les qüestions tractades en les seccions anteriors. Per exemple, hi utilitza les formes quadràtiques com un mitjà d'atac del problema de la factorització dels enters. Assenyala que aquest és un dels grans problemes que té plantejats l'aritmètica (una visió, certament, ben actual).

La secció setena tracta de les seccions circulars. Hi estudia polinomis ciclotòmics i els seus períodes, i aplica aquesta teoria a la constructibilitat dels polígons regulars amb regle i compàs.

M'agradaria rememorar aquí també el meu encontre personal amb les *Disquisitiones* en un seminari, dirigit pel Dr. Pascual Llorente, a la Universitat Autònoma de Barcelona, durant el curs 1979-1980. Un dels aspectes que, des del primer moment, em va fascinar més de Gauss fou el seu mètode de treball. Càlculs precisos portats a terme en nombrosos casos particulars, degudament seleccionats, seguits de l'examen acurat i intel·ligent dels resultats obtinguts, el porten a la descoberta de lleis generals, que demostra amb tot rigor i exposa magistralment. Així mateix, és destacable la seva notable capacitat de sistematització. Aquesta manera de treballar, que es reflecteix completament en l'obra, em sembla un model ben escaient per a la nostra tasca de recerca avui, sobretot si es té en compte la tecnologia de què disposem, que tant ens pot facilitar alguns càlculs i l'elaboració d'exemples.

No voldria acabar sense fer palès el meu agraïment a tot un equip de treball que ha col·laborat intensament en la versió final de la traducció. A ell es deu el fet que aquesta es presenti d'una manera que, espero, serà prou gratificant per a qui la llegeixi. Dono les gràcies, en primer lloc, a la Dra. Pilar Bayer, matemàtica, que ha coordinat les tasques de l'equip i m'ha encoratjat en tot moment; al Dr. Artur Travesa, matemàtic; a la Sra. Mercè Otero, llicenciada en filologia clàssica i romànica; al Sr. Albert Violant, llicenciat en matemà-

tiques, i a la Sra. M. Teresa Sucarrats, llicenciada en filologia catalana. La lectura, íntegra i acurada, que han realitzat de successives versions de la traducció, i també les nombroses aportacions des dels seus respectius camps de treball, han estat fonamentals i han tingut un gran valor per a mi.

També vull que consti el meu agraïment al Dr. Manuel Castellet, matemàtic i president de l'Institut d'Estudis Catalans, que ha proporcionat els mitjans perquè l'edició d'aquesta traducció s'hagi pogut dur a terme.

Griselda Pascual

Barcelona, abril, 1996

DISQUISICIONS
ARITMÈTIQUES

PER L'AUTOR

SR. CARLES FREDERIC GAUSS

LEIPZIG

1801

AL SERENÍSSIM

PRÍNCEP I SENYOR

CARLES GUILLEM FERRAN

DUC DE BRUNSWICK I LUNEBOURG

PRÍNCEP SERENÍSSIM

És, sens dubte, una gran satisfacció per a mi que em permetis dedicar al *Teu* Excel·lentíssim nom aquesta obra que em sento obligat a oferir-*Te* com a respectuosa mostra de reconeixement. Perquè, si la *Teva* protecció, Príncep Sereníssim, no m'hagués obert les portes a les ciències, si els *Teus* constants favors no haguessin sustentat contínuament els meus estudis, no hauria pogut dedicar-me completament a la ciència matemàtica a la qual sempre m'he abocat amb amor vehement. Encara més, la *Teva* sola benvolença ha fet possible de donar a conèixer aquestes meditacions, de les quals aquest volum en mostra una part, de continuar-les durant molts anys i de posar-les per escrit, i ha procurat que, lliure d'altres preocupacions, jo pogués dedicar-me de ferm a aquesta obra. Quan finalment desitjava donar-les a la llum, la *Teva* generositat ha remogut tots els obstacles que en retardaven l'edició. Aquests favors *Teus*, tan grans i tan dignes d'agraïment, vers la meva persona i els meus afanys, els puc evocar més amb la ment i amb callada admiració que celebrar amb justes i dignes lloances. Perquè, d'una banda, no em sento capaç de

complir un tal deure d'honor i, de l'altra, penso que ningú no ignora que és habitual en *Tu* una tan insigne liberalitat vers tots els que sembla que es dediquen a cultivar les millors disciplines, i que no són excloses del *Teu* patrocini aquelles ciències que són considerades per la gent més abstruses i més allunyades de la utilitat de la vida comuna, perquè *Tu* mateix t'adones fins a l'arrel de l'íntim i necessari vincle de totes les ciències entre elles, amb una ment molt sàvia i molt coneixedora de totes les coses que interessen per tal d'augmentar la prosperitat de la societat humana. Per això *Tu*, Príncep Sereníssim, amb aquell insigne favor amb el qual tantes vegades m'has acollit, no jutgis indigne aquest llibre, testimoni del més gran agraïment vers *Tu* i dels esforços dedicats a la més noble ciència, i jo em felicitaré de no haver col·locat la meva obra inútilment i de gaudir d'aquest honor, que he desitjat per sobre de tot,

PRÍNCEP SERENÍSSIM

Brunsvic, mes de juliol de 1801

Súbdit molt fervent
de la Teva Excel·lència
C. F. Gauss

PREFACI

Les Disquisicions contingudes en aquesta obra pertanyen a la part de les Matemàtiques que tracta dels nombres enters, excloent-ne sovint els fraccionaris, sempre els irracionals. L'Anàlisi indeterminada que anomenen Diofàntica, que ensenya a seleccionar, de les infinites solucions que satisfan un problema indeterminat, les que s'expressen per nombres enters, o almenys racionals (sovint afegida també la condició que siguin positius), no és pròpiament la disciplina, sinó que més aviat n'és una part molt especial i gairebé es conté en ella, així com l'art de reduir i resoldre equacions (Àlgebra) en l'Anàlisi universal. En efecte, de la mateixa manera que totes les disquisicions que es poden establir a propòsit dels aspectes generals de les quantitats es refereixen al domini de l'*Anàlisi*, així els nombres enters (i els fraccionaris en tant que es determinen per enters) constitueixen l'objecte propi de l'Aritmètica. Però com que el que vulgarment es transmet amb el nom d'Aritmètica amb prou feines s'estén més enllà de l'art de numerar i calcular (és a dir, de presentar els nombres mitjançant signes idonis, per exemple, segons el sistema decimal, i d'efectuar operacions aritmètiques), amb l'afegit d'algunes coses que, o bé no pertanyen en absolut a l'Aritmètica (com la doctrina dels logaritmes), o bé ni tan sols no són pròpies dels nombres enters, sinó que apareixen

en totes les quantitats, per això sembla que s'han de distingir dues parts en l'Aritmètica, i que aquelles coses es refereixen a l'Aritmètica elemental, mentre que totes les disquisicions generals dels aspectes propis dels nombres enters es reivindiquen per a una *Aritmètica Superior;* només d'aquesta tractarà aquest discurs.

Pertany a l'Aritmètica Superior allò que Euclides va transmentre en els Elements, L. VII i s., amb l'elegància i el rigor habituals en les obres dels antics; no obstant això, es limita als primers inicis d'aquesta ciència. La cèlebre obra de Diofant, que és íntegrament dedicada a problemes indeterminats, conté moltes qüestions que, per causa de la seva dificultat i per la subtilitat dels artificis, susciten una no gens mediocre estimació pel que fa a l'enginy i l'agudesa de l'autor, sobretot si consideres la migradesa dels mitjans que va poder utilitzar. Però com que aquests problemes demanen més aviat una certa destresa i un tractament experimentat que no pas uns principis més profunds, i, d'altra banda, són massa especials, i rarament condueixen a conclusions més generals, per això sembla que aquest llibre fa època en la història de les Matemàtiques, més perquè posa els primers fonaments d'un art característic i de l'Àlgebra, que perquè faci progressar l'Aritmètica Superior amb nous descobriments. Molt més es deu als moderns, entre els quals uns homes, certament pocs però de glòria immortal, com P. de Fermat, L. Euler, L. La Grange, A. M. Le Gendre (encara que en passi per alt alguns altres) varen obrir la porta al santuari d'aquesta divina ciència i varen mostrar l'abundància de les seves riqueses. Aquí m'abstinc d'enumerar, però, quines coses descobertes per cadascun d'aquests geòmetres són útils, perquè poden ser conegudes mitjançant els

prefacis dels Annexos amb els quals l'il·lm. La Grange va enriquir l'Àlgebra d'Euler, i el de l'obra tot seguit famosa editada recentment per l'il·lm. Le Gendre, i, a més a més, la majoria seran lloades en el seu lloc en aquestes Disquisicions Aritmètiques.

El propòsit d'aquesta obra, de l'edició de la qual ja fa cinc anys havia donat garantia pública, fou de divulgar les disquisicions de l'Aritmètica Superior que vaig confegir, en part, abans d'aquest període de temps i, en part, després. Però que ningú no se sorprengui que aquí s'hagi repetit la ciència des dels seus inicis i s'hagin reprès de nou moltes disquisicions en les quals altres ja havien esmerçat el seu esforç; he valorat que s'ha de tenir present que jo, quan al començament del 1795 vaig dedicar la meva ment a aquest tipus de disquisicions, desconeixia totes les que havien estat elaborades pels més moderns en aquest camp i estava privat de tots els recursos mitjançant els quals hauria pogut assabentar-me una mica d'aquestes qüestions. Sens dubte, ocupat aleshores per casualitat en una altra feina, vaig anar a parar a una extraordinària veritat aritmètica (fou efectivament, si no m'equivoco, el teorema de l'article 108), que, com que, d'una banda, vaig considerar-la bellíssima per ella mateixa i, de l'altra, vaig sospitar que estava connectada amb coses més grans, m'hi vaig dedicar amb el màxim esforç que vaig poder per tal de copsar els principis sobre els quals es basava i d'obtenir-ne una demostració rigorosa. Finalment, després que això hagués sortit segons el desig, vaig quedar lligat pels atractius d'aquestes qüestions de tal manera que no podia deixar-les; així, mentre que les altres qüestions sempre obrien el camí a d'altres, les que es transmeten en les quatre primeres Seccions d'aquesta obra quedaven

acabades, en la seva major part, abans de veure res dels treballs semblants dels altres geòmetres. Després em vaig adonar, fullejant els escrits d'aquests grans genis, que, sens dubte, la major part de les meves meditacions s'havia malgastat en coses conegudes feia temps; però, més esperonat per això, seguint les passes d'aquells, em vaig obstinar a fer avançar l'Aritmètica més enllà; així varen ser establertes diverses disquisicions, part de les quals es transmeten en les Seccions V, VI i VII. Després d'un interval de temps, vaig celebrar consell sobre l'edició pública dels fruits de les meves vetlles; així, de bon grat, vaig deixar-me persuadir pel desig de la majoria que no suprimís res de les altres investigacions prèvies, perquè en aquell temps no hi havia cap llibre mitjançant el qual poguessin ser apresos els treballs dels altres geòmetres sobre aquestes coses, esparsos en els Comentaris de les Acadèmies; perquè moltes [investigacions] eren completament noves i, la majoria, havien estat tractades amb nous mètodes; i, finalment, perquè totes estaven lligades, tant entre elles com amb les disquisicions posteriors, amb un nexe tan estret que, sens dubte, les noves no podien explicar-se prou fàcilment sense repetir les altres des de l'inici.

Mentrestant, va sortir l'obra egrègia d'un home, anteriorment digne de gran mèrit en el camp de l'Aritmètica Superior, *Le Gendre, Essai d'une theorie des nombres, Paris a. VI,* en què no només va recollir escrupolosament i va resumir per ordre el que s'havia elaborat fins aleshores en aquesta ciència, sinó que també va afegir-hi, a més a més, moltes coses noves de la seva pròpia collita. Com que aquest llibre seriós em va arribar a les mans després que la major part de l'obra ja estigués transcrita a la impremta, no fou possible

mencionar-lo en cap lloc on l'analogia dels plantejaments podia donar-hi peu; només, respecte a uns quants punts, semblava necessari incorporar als Apèndixs algunes observacions que l'autor, molt culte i molt brillant, interpretarà, confio, benèvolament.

En el temps de la impressió d'aquesta obra, que fou interrompuda moltes vegades i ajornada fins a quatre anys per diversos impediments, no només vaig continuar més enllà les investigacions, que, certament, ja abans havia emprès, però la publicació de les quals havia decidit deixar per a un altre moment, perquè el llibre no resultés massa extens, sinó que també vaig abordarne moltes altres de noves. També en varen ser represes moltes que, per la mateixa raó, només vaig tractar més per sobre, perquè una visió més aprofundida semblava menys necessària (per exemple, les que es transmeten en els articles 37, 82 i següents, i en altres llocs), i varen donar lloc a disquisicions més generals que semblen molt dignes de la llum pública (Vegeu també les que s'anomenen en els Apèndixs de l'article 306). Finalment, quan el llibre, sobretot per l'extensió de la Secció V, havia crescut de volum molt més del que havia previst, va semblar oportú retallar moltes coses que en un principi li havien estat assignades, i, entre aquestes, tota la Secció *vuitena* (que sobre la marxa ja s'esmenta en aquest volum i que conté el tractat general de les congruències algebraiques de qualsevol grau). Tot això, que omplirà fàcilment un volum igual a aquest, es farà públic a la primera ocasió que es presenti.

El fet que en moltes qüestions difícils hagi utilitzat demostracions sintètiques i hagi suprimit l'anàlisi mitjançant la qual s'han descobert s'ha d'atribuir, prin-

cipalment, a l'afany de brevetat que calia adoptar tant com es pogués.

La teoria de la divisió del cercle, o sigui, dels polígons regulars, que es tracta en la Secció VII, certament no pertany *per si mateixa* a l'Aritmètica; no obstant això, els seus *principis* únicament s'han de cercar en l'Aritmètica Superior; la qual cosa potser serà tan inesperada per als geòmetres com grates espero que els siguin les noves veritats que s'han pogut extreure d'aquesta font.

D'això he volgut advertir el lector. Els continguts, no em toca a mi jutjar-los. Certament, només desitjo que plaguin a aquells que estimen els avenços de les ciències que, o bé satisfan els actuals desitjos, o bé obren nous camins.

CONTINGUT

Secció primera. De les congruències numèriques en general p. 1

Nombres congrus, mòduls, residus, i no-residus, article 1 i següents. Residus mínims, 4. Proposicions elementals de congrus, 5. Algunes aplicacions, 12.

Secció segona. De les congruències de primer grau p. 8

Teoremes preliminars dels nombres primers, dels factors, etc., 13. Solució de les congruències de primer grau, 26. De la recerca d'un nombre congru a residus donats segons mòduls donats, 32. Congruències lineals que impliquen moltes incògnites, 37. Teoremes diversos, 38.

Secció tercera. Dels residus de potències p. 43

Els residus dels termes d'una progressió geomètrica que comença per la unitat constitueixen una sèrie periòdica, 45. *Es consideren primer mòduls que són nombres primers.* Posant el mòdul = p, la quantitat de termes del

període divideix el nombre $p - 1$, article 49. Teorema de Fermat, 50. Quants nombres corresponen als períodes en els quals la quantitat de termes és un divisor donat del nombre $p - 1$, article 52. Arrels primitives, bases, índexs, 57. Algoritme de l'índex, 58. De les arrels de la congruència $x^n \equiv A$, article 60. Nexe per als índexs en sistemes diferents, 69. Bases apropiades per a usos peculiars, 72. Mètode per a assignar arrels primitives, 72. Diversos teoremes de períodes i arrels primitives, 75. (Teorema de Wilson, 76). *Dels mòduls que són potències de nombres primers*, 82. *Mòduls que són potències binàries*, 90. *Mòduls compostos de molts primers*, 92.

Secció quarta. De les congruències de segon grau p. 93

Residus i no-residus quadràtics, article 94. Quan el mòdul és un nombre primer, la quantitat de residus menors que ell és igual que la quantitat de no-residus, 96. La qüestió, un nombre compost és residu o no-residu d'un nombre primer donat? depèn de la naturalesa dels factors, 98. Dels mòduls que són nombres compostos, 100. Criteri general de si un nombre donat és residu o no-residu d'un nombre primer donat, 106. *Disquisicions dels nombres primers dels quals nombres donats són residus o no-residus*, 107 i següents. El residu -1, article 108. Residus $+2$ i -2, article 112. Residus $+3$ i -3, article 117. Residus $+5$ i -5, article 121. De ± 7, article 124. Preparació a la disquisició general, 125. S'estableix per indici el teorema general (*fonamental*), i se'n dedueixen conclusions, 130. Demostració rigorosa d'aquest teorema, 135. Mètodes anàlegs per a demostrar el teorema de l'article 114, 145. Solució del problema general, 146. De les formes lineals que contenen tots els nombres primers dels quals un nombre qualsevol donat és residu o no-

residu, 147. Dels treballs d'altres sobre aquestes investigacions, 151. De les congruències de segon grau no pures, 152.

Secciò cinquena. De les formes i equacions indeterminades de segon grau p. 162

Propòsit de la disquisició; definició de formes i signes, 153. Representació de nombres; determinants, 154. Valors de l'expressió $\sqrt{bb-ac}\,(\text{mòd. }M)$ als quals pertany la representació del nombre M per la forma $(a,\ b,\ c)$, 155. Forma que implica una altra, o sigui, continguda en una altra; transformació, pròpia i impròpia, 157. Equivalència, pròpia i impròpia, 158. Formes oposades, 159, contigües, 160. Divisors comuns dels coeficients de les formes, 161. Connexió de totes les transformacions similars d'una forma donada en una forma donada, 162. Formes ambigües, 163. Teorema sobre el cas en què una forma està continguda en una altra simultàniament pròpiament i impròpiament, 164. Generalitats de les representacions de nombres per formes, i la seva connexió amb les transformacions, 166. *De les formes de determinant negatiu*, 171. Aplicacions especials a la descomposició de nombres en dos quadrats, en un quadrat simple i un de doble, en un simple i un de triple, 182. *De les formes de determinant positiu no quadrat*, 183. *De les formes de determinant quadrat*, 206. Formes contingudes en altres, però que no equivalen a aquestes, 213. *Formes de determinant* 0, article 215. Solució general per nombres enters de totes les equacions indeterminades de segon grau que impliquen dues incògnites, 216. Notes històriques, 222.

Disquisicions ulteriors de les formes. Distribució de les formes de determinant donat en classes, 223; de les

classes en ordres, 226. Partició dels ordres en gèneres, 228. *De la composició de formes*, 238. Composició d'ordres, 245, de gèneres, 246, de classes, 249. Per a un determinant donat, en cadascun dels gèneres d'un mateix ordre es contenen el mateix nombre de classes, 252. Es comparen les quantitats de classes contingudes en cadascun dels gèneres d'ordres diferents, 253. De la quantitat de classes ambigües, 257. Certament, la meitat de tots els caràcters assignables per a un determinant donat no poden correspondre a gèneres pròpiament primitius (positius per a determinants negatius), 261. Segona demostració del teorema fonamental i dels teoremes restants que corresponen als residus -1, $+2$, -2, 262. Es determina més pròpiament la meitat de caràcters als quals no pot correspondre cap gènere, 263. Mètode peculiar per a descompondre nombres primers en dos quadrats, 265. DIGRESSIÓ QUE CONTÉ UN TRACTAT DE FORMES TERNÀRIES, 266 i següents. *Algunes aplicacions a la teoria de les formes binàries.* De la recerca d'una forma de la duplicació de la qual s'origina una forma binària donada del gènere principal, 286. A tots els caràcters, excepte aquells que en els articles 262, 263, s'han trobat impossibles, corresponen realment gèneres, 287, III. Teoria de la descomposició tant de nombres com de formes binàries en tres quadrats, 288. Demostració dels teoremes de Fermat: qualsevol enter es pot descompondre en tres nombres triangulars o bé en quatre quadrats, 293. Solució de l'equació $axx + byy + czz = 0$, article 294. Del mètode pel qual l'il·lm. Le Gendre va tractar el teorema fonamental, 296. Representació de zero per formes ternàries qualssevol, 299. Solució general, per quantitats racionals, de les equacions indeterminades de segon grau que impliquen dues incògnites, 300. De la quantitat mitjana de gèneres, 301, de classes, 302. Algoritme singular

de les classes pròpiament primitives; determinants regulars i irregulars, etc., article 305.

Secció sisena. Aplicacions diverses de les disquisicions precedents p. 525

Descomposició de fraccions en més simples, 309. Conversió de fraccions comunes en decimals, 312. Solució de la congruència $xx \equiv A$ pel mètode d'exclusió, 319. Solució de l'equació indeterminada $mxx + nyy = A$ per exclusions, 323. Un altre mètode per a resoldre la congruència $xx \equiv A$ per al cas en què A és negatiu, 327. Dos mètodes per a distingir nombres compostos de primers, i per a investigar els seus factors, 329.

Secció setena. De les equacions que defineixen les seccions del cercle p. 574

Es redueix la disquisició al cas més simple, en què la quantitat de parts en què convé seccionar el cercle és un nombre primer, 336. Equacions per a les funcions trigonomètriques dels arcs que són part o bé parts de tota la circumferència; reducció de les funcions trigonomètriques a les arrels de l'equació $x^n - 1 = 0$, article 337. *Teoria de les arrels d'aquesta equació* (on se suposa que n és un nombre primer). Ometent l'arrel 1, les restants (Ω) es contenen en l'equació $X = x^{n-1} + x^{n-2} + etc. + x + 1 = 0$. La funció X no es pot descompondre en factors inferiors en els quals tots els coeficients siguin racionals, 341. Es declara el propòsit de les disquisicions següents, 342. Es distribueixen totes les arrels de Ω en certes classes (períodes), 343. Diversos teoremes d'aquests períodes, 344 i següents. Es construeix, per aquestes disquisicions, la solució de l'equació $X = 0$, article 352. Exemples per a

$n = 19$, on la feina es redueix a dues equacions cúbiques i una de quadràtica, i per a $n = 17$, on [es redueix] a quatre de quadràtiques, articles 353, 354. *Disquisicions ulteriors d'aquest argument.* Les sumes en què la quantitat de termes és parella són quantitats reals, 355. De les equacions per les quals es defineix la distribució de les arrels de Ω en *dos* períodes, 356. Demostració dels teoremes mencionats en la secció IV, 357. De les equacions per a la distribució de les arrels de Ω en *tres* períodes, 358. Reducció a pures de les equacions per les quals es troben les arrels de Ω, 359. *Aplicació de les disquisicions precedents a les funcions trigonomètriques.* Mètode per a discernir els angles a què corresponen cada una de les arrels de Ω, 361. Tangents, cotangents, secants i cosecants es deriven sense divisió dels sinus i els cosinus, 362. Mètode per a rebaixar successivament equacions per a funcions trigonomètriques, 363. Seccions del cercle que es poden dur a terme per equacions quadràtiques, o sigui, per construccions geomètriques, 365.

Afegiments p. 645

Taules

DISQUISICIONS ARITMÈTIQUES

Secció Primera

de les

CONGRUÈNCIES NUMÈRIQUES EN GENERAL

1. Si el nombre a divideix la diferència dels nombres b, c, es diu que b i c són *congrus segons* a, si no, *incongrus;* anomenem *mòdul* aquest a. En el primer cas, cadascun dels nombres b, c, és anomenat un *residu* de l'altre; en el segon, un *no-residu*.

Aquestes nocions són vàlides per a tots els nombres enters, tant els positius com els negatius,* però

* Evidentment, el mòdul s'ha de prendre sempre *absolut*; és

no s'han d'estendre a les fraccions. *Per exemple*, -9 i $+16$ són congrus segons el mòdul 5; -7 és un residu de $+15$ segons el mòdul 11, però un no-residu segons el mòdul 3. D'altra banda, com que qualsevol nombre divideix zero, tot nombre s'ha de considerar congru amb si mateix segons qualsevol mòdul.

2. Tots els residus d'un nombre donat a segons el mòdul m estan continguts en la fórmula $a + km$, on k designa un nombre enter indeterminat. De les proposicions que transmetrem després, les més fàcils es poden demostrar sense dificultat a partir d'aquí; però, sens dubte, qualsevol que s'hi fixi podrà copsar la veritat d'aquestes de manera igualment fàcil.

D'ara endavant, denotarem les congruències numèriques amb el símbol $\equiv$, afegint el mòdul entre parèntesis on sigui necessari; $-16 \equiv 9\,(\text{mòd. } 5)$, $-7 \equiv 15\,(\text{mòd. } 11)$.*

3. Teorema. *Proposats m nombres enters consecutius, a, $a+1$, $a+2$, $\cdots$, $a+m-1$, i un altre A, un i solament un d'aquells serà congru amb aquest segons el mòdul m.*

En efecte, si $\dfrac{a-A}{m}$ és enter, serà $a \equiv A$; si és una fracció, sigui $= k$ l'enter més pròxim més gran que ella

---

a dir, sense cap signe.

* Hem adoptat aquest signe per la gran analogia que es troba entre la igualtat i la congruència. Per la mateixa causa l'il·lm. Le Gendre, en els comentaris que cal citar molt sovint més avall, ha conservat per a la congruència el mateix signe d'igualtat, cosa que nosaltres hem dubtat d'imitar perquè no es produeixi ambigüitat.

(o bé, quan és negativa, el més pròxim *més petit* si no es té en compte el signe) i $A + km$ caurà entre a i $a + m$; per tant, serà el nombre cercat. I és evident que tots els quocients $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, $\frac{a+2-A}{m}$, etc., estan situats entre $k-1$ i $k+1$; per tant, només pot ser enter un d'ells.

4. Cada nombre tindrà, doncs, un residu tant en la successió $0, 1, 2, \cdots, m-1$ com en la $0, -1, -2, \cdots, -(m-1)$, els quals anomenarem els *residus mínims;* i és clar que, llevat que el residu fos 0, sempre se'n donen dos, un *positiu*, l'altre *negatiu*. Si, no tenint respecte al signe, les magnituds són diferents, un serà $< \frac{m}{2}$; si d'altra manera, tots dos $= \frac{m}{2}$. D'on és clar que qualsevol nombre té un residu que no supera la meitat del mòdul, que s'anomenarà *[residu] mínim absolut*.

Per exemple, -13, segons el mòdul 5, té residu mínim positiu 2, que a la vegada és el [residu] mínim absolut, però residu mínim negatiu -3; $+5$, segons el mòdul 7, és el seu propi residu mínim positiu, -2 el negatiu i, simultàniament, el [residu] mínim absolut.

5. Establertes aquestes nocions, recopilem aquelles propietats dels nombres congrus que es presenten a primera vista.

Aquells nombres que són congrus segons un mòdul compost, també són congrus segons qualsevol dels seus divisors.

Si uns quants nombres són congrus a un mateix nombre segons un mateix mòdul, seran congrus entre si (segons el mateix mòdul).

Aquesta identitat dels mòduls també s'ha de sobreentendre en tot el que segueix.

Nombres congrus tenen els mateixos residus mínims; incongrus, diferents.

6. *Si es tenen tants nombres A, B, C, etc., com tants altres a, b, c, etc., congrus a aquells segons un mòdul qualsevol, $A \equiv a$, $B \equiv b$, etc., serà $A + B + C + \text{etc.} \equiv a + b + c + \text{etc.}$*

Si $A \equiv a$, $B \equiv b$, serà $A - B \equiv a - b$.

7. *Si $A \equiv a$, també serà $kA \equiv ka$.*

Si k és un nombre positiu, això només és un cas particular de la proposició de l'article precedent, posant allà $A = B = C$ etc., $a = b = c$ etc. Si k és negatiu, $-k$ serà positiu, de manera que $-kA \equiv -ka$, d'on $kA \equiv ka$.

Si $A \equiv a$, $B \equiv b$, serà $AB \equiv ab$. Efectivament, $AB \equiv Ab \equiv ba$.

8. *Si es tenen tants nombres A, B, C, etc., com tants altres a, b, c, etc., congrus a aquests, $A \equiv a$, $B \equiv b$, etc., els productes dels uns i dels altres seran congrus; $ABC\,\text{etc.} \equiv abc\,\text{etc.}$*

De l'article precedent, $AB \equiv ab$ i, per la mateixa raó, $ABC \equiv abc$; i de la mateixa manera es poden afegir qualssevol altres factors.

Si tots els nombres A, B, C, etc., es prenen iguals, i també els corresponents a, b, c, etc., es té aquest teorema: *Si $A \equiv a$ i k és un enter positiu, serà $A^k \equiv a^k$.*

9. *Sigui X una funció algebraica de la indeterminada x de la forma $Ax^a + Bx^b + Cx^c +$ etc., on A, B, C, etc., designen nombres enters qualssevol, però a, b, c, etc., enters no negatius. Llavors, si s'atribueixen a la indeterminada x valors congrus segons un mòdul qualsevol, els valors de la funció X produïts per això seran congrus.*

Siguin f, g, valors de x congrus. Llavors, de l'article precedent, $f^a \equiv g^a$ i $Af^a \equiv Ag^a$, i de la mateixa manera $Bf^b \equiv Bg^b$, etc. D'aquí, $Af^a + Bf^b + Cf^c +$ etc. $\equiv Ag^a + Bg^b + Cg^c +$ etc. *Q. E. D.*

D'altra banda, s'entén fàcilment de quina manera es podria estendre aquest teorema a funcions de més indeterminades.

10. Així, doncs, si per x se substitueixen tots els nombres enters consecutius i els valors de la funció X es redueixen als residus mínims, aquests formaran una sèrie en la qual, després d'un interval de m termes (on m designa el mòdul), es repetiran de nou els mateixos termes; o sigui, aquesta sèrie estarà formada d'un *període* de m termes repetit una infinitat de vegades. Per exemple, sigui $X = x^3 - 8x + 6$ i $m = 5$; llavors els valors de X

per a $x = 0$, 1, 2, 3, etc., donen aquests residus mínims positius, 1, 4, 3, 4, 3, 1, 4, etc., on els cinc primers 1, 4, 3, 4, 3, es repeteixen infinites vegades; també si la sèrie es continua en sentit contrari, és a dir, si s'atribueixen valors negatius a x, es produeix el mateix període amb l'ordre dels termes invertit; d'on és evident que no poden tenir lloc en tota la sèrie altres termes que els que constitueixin aquest període.

11. Així, doncs, en aquest exemple, X no pot resultar ni $\equiv 0$ ni $\equiv 2\,(\text{mòd. } 5)$, ni encara menys $= 0$ o bé $= 2$. D'on se segueix que les equacions $x^3 - 8x + 6 = 0$ i $x^3 - 8x + 4 = 0$ no es poden resoldre per nombres enters ni per tant, com és sabut, tampoc per nombres racionals. Generalment, és copsat que l'equació $X = 0$, quan X és una funció de la incògnita x de la forma $x^n + Ax^{n-1} + Bx^{n-2} + \text{etc.} + N$, on A, B, C, etc., són enters i n és un enter positiu (forma a la qual se sap que es poden reduir totes les equacions algebraiques), no té cap arrel racional si la congruència $X \equiv 0$ no es pot satisfer segons algun mòdul. Però aquest criteri, que ens apareix aquí espontàniament, serà tractat detalladament en la *secció VIII.* Certament, a partir d'aquesta mostra, qualsevol podrà formar-se una petita idea de la utilitat d'aquestes recerques.

12. Moltíssimes [proposicions] que se solen ensenyar en aritmètica es recolzen en els teoremes transmesos en aquest capítol; per exemple, regles per a examinar la divisibilitat de nombres proposats per 9, 11, o bé altres nombres. *Segons el mòdul* 9, totes les potències del nombre 10 són còngrues a la unitat; per tant, si el nombre proposat té la forma $a + 10b + 100c + \text{etc.}$, donarà el

mateix residu mínim que $a+b+c+$etc. segons el nombre 9. D'aquí és evident que si se sumen cada un dels dígits d'un nombre expressat en notació decimal sense [tenir] respecte del lloc que ocupen, aquesta suma i el nombre proposat tenen el mateix residu mínim; de manera que aquest es pot dividir per 9 si aquella és divisible per 9, i recíprocament. També cal entendre el mateix per al divisor 3. Com que, *segons el mòdul* 11, $100 \equiv 1$, en general serà $10^{2k} \equiv 1$, $10^{2k+1} \equiv 10 \equiv -1$, i un nombre de la forma $a+10b+100c+$etc. donarà el mateix residu mínim que $a-b+c$ etc. segons el mòdul 11; d'on es deriva directament la regla coneguda. Del mateix principi es dedueixen fàcilment totes les receptes similars.

Del que precedeix també s'ha d'arribar a la raó de les regles a les quals es confia habitualment la verificació de les operacions aritmètiques. Això és, si d'uns nombres donats se n'han de deduir altres per addició, subtracció, multiplicació o bé elevació a potències, se substitueixen en lloc dels donats els seus residus mínims segons un mòdul arbitrari (habitualment 9 o bé 11, perquè en el nostre sistema decimal, tal com hem mostrat fa un moment, els residus segons aquests es poden trobar tan fàcilment). Els nombres que resulten d'aquí han de ser congrus als que han estat deduïts dels nombres proposats; si això no fos així, es conclou que s'ha infiltrat un error en el càlcul.

Però com que aquestes [proposicions], i similars a aquestes, són ben conegudes, seria superflu detenir-s'hi més estona.

Secció Segona

de les

CONGRUÈNCIES DE PRIMER GRAU

13. Teorema. *El producte de dos nombres positius menors que un nombre primer donat no es pot dividir per aquest primer.*

Sigui p un primer, i a positiu $< p$; llavors, no es donarà cap nombre positiu b menor que p de manera que sigui $ab \equiv 0 \,(\text{mòd.}\, p)$.

Dem. Sempre que algú ho negui, suposem que es donen nombres b, c, d, etc., tots $< p$, de manera que $ab \equiv 0$, $ac \equiv 0$, $ad \equiv 0$, etc. (mòd. p). Sigui b el mínim de tots, de manera que tots els nombres menors que b siguin desproveïts d'aquesta propietat. Evidentment serà $b > 1$: en efecte, si $b = 1$, seria $ab = a < p$ (*per hipòtesi*), de manera que no divisible per p. Per tant, p, com a primer, no podrà ser dividit per b, sinó que caurà entre dos múltiples consecutius de b, mb i $(m+1)b$. Sigui $p - mb = b'$, i b' serà un nombre positiu i $< b$. Ara, com

que hem suposat que $ab \equiv 0\,(\text{mòd.}\,p)$, també es tindrà $mab \equiv 0$ (article 7) i, d'aquí, restant de $ap \equiv 0$, serà $a(p - mb) = ab' \equiv 0$; és a dir, b' s'ha de trobar entre els nombres b, c, d, etc., malgrat que sigui menor que el mínim de tots, b. *Q. E. A.*

14. *Si ni a ni b no es poden dividir per un nombre primer p, el producte ab tampoc no es podrà dividir per p.*

Siguin α, β, els residus mínims positius dels nombres a, b, segons el mòdul p, dels quals cap no serà 0 (*per hipòtesi*). Ara, si fos $ab \equiv 0\,(\text{mòd.}\,p)$, com que $ab \equiv \alpha\beta$, també seria $\alpha\beta \equiv 0$, que no pot ser consistent amb el teorema precedent.

Una demostració d'aquest teorema ja fou transmesa per Euclides, *El. VII.* 32. No obstant això, nosaltres no l'hem volguda ometre; d'una banda, perquè molts dels moderns, o bé han tractat de vendre raonaments vagues com a demostracions, o bé han omès completament el teorema, i de l'altra, perquè la naturalesa del mètode aplicat aquí, que usarem més avall en haver d'aclarir [proposicions] molt profundes, es podrà descobrir més fàcilment del cas més simple.

15. *Si cap dels nombres a, b, c, d, etc., no es pot dividir per un nombre primer p, el producte abcd etc. tampoc no es podrà dividir per p.*

Segons l'article precedent, ab no es pot dividir per p; en conseqüència, tampoc abc; d'aquí $abcd$, etc.

16. Teorema. *Un nombre compost qualsevol només es pot descompondre en factors primers d'una sola manera.*

Dem. És sabut dels rudiments que qualsevol nombre compost es pot descompondre en factors primers, però que això no es pot fer de moltes maneres diferents, se suposa, sovint per error, tàcitament. Imaginem que un nombre compost A, el qual sigui $= a^\alpha b^\beta c^\gamma$ etc., on a, b, c, etc., designen nombres primers diferents, es pot descompondre en factors primers encara d'una altra manera. És evident, en primer lloc, que en aquest segon sistema de factors no poden entrar-hi altres primers que a, b, c, etc., ja que qualsevol altre primer no pot dividir el nombre A, compost d'aquests. Similarment, que en aquest segon sistema de factors tampoc no pot mancar cap dels primers a, b, c, etc., ja que, altrament, aquell no dividiria A (article precedent). Per tant, aquestes dues descomposicions en factors només poden diferir en què en una d'elles es tingui algun primer més vegades que en l'altra. Sigui p un tal primer que en una descomposició aparegui m vegades, i en l'altra, n, i sigui $m > n$; ara, s'esborra n vegades de cada sistema el factor p, perquè resulti que en un encara romangui $m - n$ vegades però hagi desaparegut completament de l'altre. És a dir, es tenen dues descomposicions en factors del nombre $\dfrac{A}{p^n}$, una de les quals és lliure completament del factor p però l'altra el conté $m - n$ vegades, contra el que hem demostrat fa un moment.

17. I així, si un nombre compost A és producte de B, C, D, etc., és clar que entre els factors primers dels nombres B, C, D, etc., no pot haver-n'hi d'altres que

no estiguin entre els factors del nombre A, i qualsevol d'aquests factors ha d'aparèixer conjuntament en B, C, D, etc., tantes vegades com en A. D'aquí es conclou un criteri [per a decidir si] un nombre B divideix o no un altre A. Esdevindrà allò si B no involucra altres factors primers que A ni cap d'ells més vegades; si alguna d'aquestes condicions falla, B no dividirà A.

D'aquí es pot derivar fàcilment, amb l'ajut del càlcul de combinacions, que, si $A = a^\alpha b^\beta c^\gamma$ etc., on a, b, c, etc., designen com més amunt nombres primers diferents, A té $(\alpha+1)(\beta+1)(\gamma+1)$ etc. divisors diferents, incloent-hi també 1 i A.

18. Doncs, si $A = a^\alpha b^\beta c^\gamma$ etc., $K = k^\kappa l^\lambda m^\mu$ etc., i els primers a, b, c, etc., k, l, m, etc., són tots diferents, és clar que A i K no tenen cap divisor comú excepte 1, o sigui, que són primers entre si.

Proposats més nombres A, B, C, etc., *el màxim divisor de tots els comuns* es determina així. Es descomponen tots en els seus factors primers i s'extreuen d'aquests els que són comuns a tots els nombres A, B, C, etc. (si tals no es presenten, cap divisor no serà comú de tots). Llavors s'anota quantes vegades cadascun d'aquests factors primers és contingut en cada un dels A, B, C, etc., o sigui, la *dimensió* que cadascun té en cada un dels A, B, C. Finalment, s'atribueix a cada factor primer la dimensió mínima de totes les que té en A, B, C, etc., i es forma el producte d'aquests, que serà el divisor comú buscat.

Quan es desitja el *mínim comú múltiple* dels nombres A, B, C, etc., cal procedir així. S'agrupen tots els

nombres primers que divideixen algun dels nombres A, B, C, etc.; s'atribueix a cadascun la dimensió màxima de totes les que té en els nombres A, B, C, etc., i es forma d'aquesta manera el producte de tots, que serà el múltiple buscat.

Exemple. Sigui $A = 504 = 2^3 \cdot 3^2 \cdot 7$, $B = 2880 = 2^6 \cdot 3^2 \cdot 5$, $C = 864 = 2^5 \cdot 3^3$. Per a trobar el màxim comú divisor, es tenen els factors primers 2, 3, als quals cal atribuir dimensions 3, 2; d'on resulta $= 2^3 \cdot 3^2 = 72$; el mínim comú múltiple serà $2^6 \cdot 3^3 \cdot 5 \cdot 7 = 60480$.

Ometem les demostracions a causa de la seva simplicitat. D'altra banda, és coneguda dels rudiments de quina manera caldria resoldre aquests problemes quan no es doni la descomposició dels nombres A, B, C, etc., en factors primers.

19. *Si els nombres a, b, c, etc., són primers amb un altre k, el seu producte abc etc. també és primer amb k.*

En efecte, com que cap factor primer dels nombres a, b, c, etc., no és comú amb k i el producte *abc* etc. no pot tenir altres factors primers que els que són factors d'algun dels nombres a, b, c, etc., el producte *abc* etc. tampoc no tindrà cap factor primer comú amb k. Per tant, per l'article precedent, k és primer amb *abc* etc.

Si els nombres a, b, c, etc., són primers entre si i cadascun divideix algun k, el seu producte també dividirà el nombre k.

Això es deriva de manera igualment fàcil dels articles 17 i 18. En efecte, sigui p un divisor primer qualsevol

del producte abc etc., el qual el contingui π vegades; és evident que algun dels nombres a, b, c, etc., ha de contenir π vegades aquest mateix divisor. Per tant, també k, que és divisible per aquest nombre, conté π vegades el divisor p. Similarment per als restants divisors del producte abc etc.

D'aquí, *si dos nombres m, n, són congrus segons uns quants mòduls a, b, c, etc., primers entre si, també seran congrus segons el seu producte.* En efecte, quan $m-n$ sigui divisible per cadascun dels a, b, c, etc., també es podrà dividir pel seu producte.

Finalment, *si a és primer amb b i ak és divisible per b, també k serà divisible per b.* Efectivament, com que ak és divisible tant per a com per b, també es podrà dividir per ab; és a dir, $\dfrac{ak}{ab} = \dfrac{k}{b}$ serà enter.

20. *Quan $A = a^\alpha b^\beta c^\gamma$ etc., on a, b, c, etc., designen nombres primers diferents, és alguna potència, posem $= k^n$, tots els exponents α, β, γ, etc., seran divisibles per n.*

En efecte, el nombre k no involucra altres factors primers que a, b, c, etc. Si conté el factor a α' vegades, k^n, o sigui A, contindrà aquest factor $n\alpha'$ vegades; per tant, $n\alpha' = \alpha$ i $\dfrac{\alpha}{n}$ és enter. Similarment es demostra que $\dfrac{\beta}{n}$, etc., són enters.

21. *Quan a, b, c, etc., són primers entre si i el producte abc etc. és alguna potència, posem $= k^n$, cadascun dels nombres a, b, c, etc., serà una potència similar.*

Sigui $a = l^\lambda m^\mu p^\pi$ etc., on l, m, p, etc., designen nombres primers diferents, cap dels quals no és un factor dels nombres b, c, etc., *per hipòtesi*. Per tant, el producte *abc* etc. contindrà λ vegades el factor l, μ vegades el factor m, etc.; d'aquí (*article precedent*) λ, μ, π, etc., són divisibles per n, de manera que $\sqrt[n]{a} = l^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} p^{\frac{\pi}{n}}$ etc. és enter. Similarment per als restants b, c, etc.

Calia enunciar prèviament aquestes proposicions dels nombres primers; tornem ja a les que atenyen més pròpiament la finalitat del nostre propòsit.

22. *Si els nombres a, b, divisibles per un altre k, són congrus segons un mòdul m primer amb k,* $\frac{a}{k}$ *i* $\frac{b}{k}$ *eren congrus segons el mateix mòdul.*

En efecte, és clar que $a - b$ serà divisible per k, i també per m (*per hipòtesi*); per tant (*article* 19), $\frac{a-b}{k}$ serà divisible per m; és a dir, serà $\frac{a}{k} \equiv \frac{b}{k} \,(\text{mòd.}\, m)$.

Però, si mantingudes les restants [hipòtesis], m i k tenen màxim comú divisor e, serà $\frac{a}{k} \equiv \frac{b}{k} \left(\text{mòd.}\, \frac{m}{e}\right)$. Efectivament, $\frac{k}{e}$ i $\frac{m}{e}$ són primers entre si. Però $a - b$ és divisible tant per k com per m, de manera que també $\frac{a-b}{e}$, tant per $\frac{k}{e}$ com per $\frac{m}{e}$ i, d'aquí, per $\frac{km}{ee}$; és a dir, $\frac{a-b}{k}$ per $\frac{m}{e}$, o sigui $\frac{a}{k} \equiv \frac{b}{k} \left(\text{mòd.}\, \frac{m}{e}\right)$.

23. *Si a és primer amb m, i e, f, nombres incongrus segons un mòdul m, també ae, af, seran incongrus segons m.*

Aquest només és el contrarecíproc del teorema de l'article precedent.

D'aquí és evident que, si a es multiplica per tots els nombres enters des de 0 fins a $m-1$ i els productes es redueixen als seus residus mínims segons el mòdul m, tots aquests seran diferents. I com que el nombre d'aquests residus, dels quals cap no és $> m$, és m, i se'n dóna la mateixa quantitat que nombres des de 0 fins a $m-1$, és clar que entre aquells residus no pot mancar cap d'aquests nombres.

24. *L'expressió $ax+b$,* on a, b, denoten nombres donats, x un nombre indeterminat, o sigui, una variable, *pot resultar còngrua, segons un mòdul m primer amb a, a qualsevol nombre donat.*

Sigui c el nombre al qual ha de resultar còngrua, i e el residu mínim positiu de $c-b$ segons el mòdul m. Per l'article precedent, es dóna necessàriament un valor de $x < m$ tal que el residu mínim del producte ax segons el mòdul m resulti e; sigui v aquest valor, i serà $av \equiv e \equiv c-b$; d'on $av+b \equiv c\,(\text{mòd.}\, m)$. *Q. E. F.*

25. Una expressió que contingui dues quantitats còngrues a manera d'equació, l'anomenem *congruència*; si aquesta conté una incògnita, s'anomena *resolta* quan es troba per a aquesta un valor (*arrel*) que satisfà la congruència. A més a més, d'aquí s'entén què és *con-*

gruència resoluble i congruència irresoluble. Finalment, es copsa fàcilment que aquí poden tenir lloc distincions similars com en les equacions. Apareixeran més avall exemples de congruències *transcendents;* les *algebraiques* es distribueixen, segons la màxima potència de la incògnita, en congruències de primer, segon i *graus* més alts. També es poden proposar més congruències que involucrin més incògnites, de les quals s'ha d'investigar *l'eliminació.*

26. I així, per l'article 24, una congruència de primer grau $ax + b \equiv c$ sempre és resoluble quan el mòdul és primer amb a. Si v fos un valor idoni de x, o sigui, una arrel de la congruència, és palès que tots els nombres congrus a v segons el mòdul de la congruència proposada també seran arrels (article 9). Es copsa no menys fàcilment que totes les arrels han de ser còngrues a v; en efecte, si t fos alguna altra arrel, serà $av + b \equiv at + b$; d'on $av \equiv at$ i, d'aquí, $v \equiv t$ (article 22). D'aquí es conclou que la congruència $x \equiv v\,(\text{mòd.}\,m)$ exhibeix la resolució completa de la congruència $ax + b \equiv c$.

Com que les solucions de la congruència per valors congrus a x són òbvies, i com que, a aquest respecte, cal considerar com a equivalents els nombres congrus, tindrem tals solucions de la congruència per una i la mateixa. Per la qual cosa, quan la nostra congruència $ax + b \equiv c$ no admeti altres solucions, direm que és resoluble només d'una manera, o sigui, que només té una arrel. Així, *per exemple*, la congruència $6x + 5 \equiv 13\,(\text{mòd.}\,11)$ no admet altres arrels que les que són $\equiv 5\,(\text{mòd.}\,11)$. No es té res així en congruències de grau més alt ni tampoc en congruències de primer grau on la incògnita

és multiplicada per un nombre amb el qual el mòdul no és primer.

27. Resta que afegim quelcom de com cal trobar la solució d'una congruència d'aquest tipus. Observem, en primer lloc, que una congruència de la forma $ax + t \equiv u$, el mòdul de la qual suposem primer amb a, depèn de la $ax \equiv \pm 1$; en efecte, si $x \equiv r$ satisfà aquesta, $x \equiv \pm(u - t)r$ satisfarà aquella. Però la congruència $ax \equiv \pm 1$, designat el mòdul per b, equival a l'equació indeterminada $ax = by \pm 1$, i, certament, la manera en què aquesta s'hauria de resoldre és prou coneguda actualment; per tant, ens serà suficient transcriure aquí l'algoritme de càlcul.

Si les quantitats A, B, C, D, E, etc., depenen de α, β, γ, δ, etc., de manera que es tingui $A = \alpha$, $B = \beta A + 1$, $C = \gamma B + A$, $D = \delta C + B$, $E = \varepsilon D + C$, etc., les designem, per abreujar, $A = [\alpha]$, $B = [\alpha, \beta]$, $C = [\alpha, \beta, \gamma]$, $D = [\alpha, \beta, \gamma, \delta]$, etc.* Sigui ara proposada l'equació indeterminada $ax = by \pm 1$, on a, b, són positius. Suposem, la qual cosa és lícita, que a no és $< b$. Llavors, a la manera del conegut algoritme segons el

* Aquesta relació es pot considerar molt més generalment, feina que potser reprendrem en una altra ocasió. Aquí només hi afegim dues proposicions que tenen el seu ús en la investigació present, a saber,

1. $[\alpha, \beta, \gamma, \cdots, \lambda, \mu] \cdot [\beta, \gamma, \cdots, \lambda] - [\alpha, \beta, \gamma, \cdots, \lambda] \cdot [\beta, \gamma, \cdots, \lambda, \mu] = \pm 1$, on cal agafar el signe superior quan la quantitat dels nombres α, β, γ, $\cdots$, λ, μ, sigui parella, i l'inferior quan sigui imparella.

2. Es pot invertir l'ordre dels nombres α, β, γ, etc., $[\alpha, \beta, \cdots, \lambda, \mu] = [\mu, \lambda, \cdots, \beta, \alpha]$. Suprimim aquí les demostracions, que no són difícils.

qual s'investiga el màxim comú divisor de dos nombres, es formen, mitjançant la divisió ordinària, les equacions

$a = \alpha b + c,$
$b = \beta c + d,$
$c = \gamma d + e,$ etc.,

de manera que α, β, γ, etc., c, d, e, etc., siguin enters positius i b, c, d, e, etc., decreixents contínuament, fins que s'arriba a $m = \mu n + 1$, la qual cosa és sabut que finalment ha d'esdevenir. I així serà $a = [n, \mu, \cdots, \gamma, \beta, \alpha]$, $b = [n, \mu, \cdots, \gamma, \beta]$. Llavors resulta $x = [\mu, \cdots, \gamma, \beta]$, $y = [\mu, \cdots, \gamma, \beta, \alpha]$ i serà $ax = by + 1$ quan la quantitat de nombres α, β, γ, $\cdots$, μ, n, és parella, o bé $ax = by - 1$ quan és imparella. *Q. E. F.*

28. L'il·lm. Euler va ser el primer d'ensenyar la resolució general d'equacions indeterminades d'aquest tipus, *Comment. Petrop., T. VII, p.* 46. El mètode que és usual consisteix en la substitució d'altres incògnites en lloc de les x, y; i, certament, és bastant conegut actualment. L'il·lm. La Grange va atacar la qüestió de manera un xic diferent: a saber, és sabut de la teoria de les fraccions contínues que si la fracció $\dfrac{b}{a}$ es convertís en la fracció contínua

$$\cfrac{1}{\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \cfrac{1}{\text{etc.} + \cfrac{1}{\mu + \cfrac{1}{n}}}}}}$$

i aquesta, esborrada la seva última part $\frac{1}{n}$, es restituís en la fracció comuna $\frac{x}{y}$, fóra $ax = by \pm 1$, suposat que a fos primer amb b. D'altra banda, de cada un dels dos mètodes es deriva el mateix algoritme. Les investigacions de l'il·lm. La Grange apareixen en *Hist. de l'Ac. de Berlin, Année* 1767*, p.* 175 i, amb altres, en *Supplementis versioni gallicæ Algebræ Eulerianæ adiectis.*

29. Una congruència $ax + t \equiv u$, el mòdul de la qual no és primer amb a, es redueix fàcilment al cas precedent. Sigui m el mòdul i δ el màxim comú divisor dels nombres a, m. En primer lloc, és clar que qualsevol valor de x que satisfaci la congruència segons el mòdul m també la satisfarà segons el mòdul δ (article 5). Però sempre $ax \equiv 0\,(\text{mòd.}\,\delta)$, ja que δ divideix a. Per tant, llevat que $t \equiv u\,(\text{mòd.}\,\delta)$, és a dir, $t - u$ divisible per δ, la congruència proposada no és resoluble.

I així, posem $a = \delta e$, $m = \delta f$, $t - u = \delta k$, i e serà primer amb f. Llavors, la congruència proposada $\delta ex + \delta k \equiv 0\,(\text{mòd.}\,\delta f)$ equivaldrà a la $ex + k \equiv 0\,(\text{mòd.}\,f)$; és a dir, qualsevol valor de x que satisfaci aquesta, també satisfarà aquella i recíprocament. En efecte, evidentment, $ex + k$ podrà dividir-se per f quan $\delta ex + \delta k$ es pugui dividir per δf i recíprocament. Però més amunt hem ensenyat a resoldre la congruència $ex + k \equiv 0\,(\text{mòd.}\,f)$; d'on és clar simultàniament que si v és un dels valors de x, $x \equiv v\,(\text{mòd.}\,f)$ exhibeix la resolució completa de la congruència proposada.

30. Quan el mòdul és compost, algunes vegades és preferible usar el mètode següent.

Sigui el mòdul $= mn$ i $ax \equiv b$ la congruència proposada. Primer, es resol aquesta congruència segons el mòdul m, i suposem que aquesta se satisfà si $x \equiv v \left(\text{mòd.}\, \frac{m}{\delta}\right)$, on δ designa el màxim comú divisor dels nombres m, a. Ara és evident que qualsevol valor de x que satisfaci la congruència $ax \equiv b$ segons el mòdul mn també l'ha de satisfer segons el mòdul m, de manera que està contingut en la forma $v + \frac{m}{\delta}x'$, on x' designa un nombre indeterminat, mentre que, recíprocament, no tots els nombres continguts en la forma $v + \frac{m}{\delta}x'$ satisfarien la congruència segons el mòdul mn. Ara bé, de quina manera s'hagi de determinar x' perquè $v + \frac{m}{\delta}x'$ resulti arrel de la congruència $ax \equiv b\,(\text{mòd.}\, mn)$ es pot deduir de la solució de la congruència $\frac{am}{\delta}x' + av \equiv b\,(\text{mòd.}\, mn)$, a la qual equival $\frac{a}{\delta}x' \equiv \frac{b - av}{m}\,(\text{mòd.}\, n)$. D'aquí es conclou que la solució de qualsevol congruència de primer grau segons el mòdul mn es pot reduir a la solució de dues congruències segons els mòduls m i n. Però es copsa fàcilment que sempre que m sigui de nou producte de dos factors, la solució de la congruència segons el mòdul n depèn de les solucions de dues congruències els mòduls de les quals siguin aquells factors. En general, la solució d'una congruència segons un mòdul compost qualsevol depèn de la solució d'altres congruències els mòduls de les quals són factors d'aquell nombre, i, si sembla convenient, aquests es poden agafar sempre de manera que siguin nombres primers.

Exemple. Si es proposa la congruència $19x \equiv 1$ $(\text{mòd.}\, 140)$, es resol primer segons el mòdul 2, i serà

$x \equiv 1\,(\text{mòd. } 2)$. Es posa $x = 1 + 2x'$, i resultarà $38x' \equiv -18\,(\text{mòd. } 140)$, a la qual equival $19x' \equiv -9\,(\text{mòd. } 70)$. Si aquesta és resolta novament segons el mòdul 2, resulta $x' \equiv 1\,(\text{mòd. } 2)$, i, posat $x' = 1 + 2x''$, resulta $38x'' \equiv -28\,(\text{mòd. } 70)$, o sigui $19x'' \equiv -14\,(\text{mòd. } 35)$. Resolta aquesta segons 5, dóna $x'' \equiv 4\,(\text{mòd. } 5)$, i, substituït $x'' = 4 + 5x'''$, resulta $95x''' \equiv -90\,(\text{mòd. } 35)$, o sigui $19x''' \equiv -18\,(\text{mòd. } 7)$. Finalment, d'aquesta se segueix $x''' \equiv 2\,(\text{mòd. } 7)$, i, posat $x''' = 2 + 7x^{IV}$, es conclou que $x = 59 + 140x^{IV}$; per tant, $x \equiv 59\,(\text{mòd. } 140)$ és la solució completa de la congruència proposada.

31. De manera similar a com l'arrel de l'equació $ax = b$ s'expressa per $\frac{b}{a}$, també designarem per $\frac{b}{a}$ qualsevol arrel de la congruència $ax \equiv b$, adjuntant el mòdul de la congruència per fer distinció. Així, per exemple, $\frac{19}{17}\,(\text{mòd. } 12)$ denota qualsevol nombre que és $\equiv 11\,(\text{mòd. } 12)$.* En general, és clar del que precedeix que $\frac{b}{a}\,(\text{mòd. } c)$ no significa res real (o si algú ho prefereix, quelcom d'imaginari) sempre que a, c, tinguin un divisor comú que no divideixi b. Exceptuant-ne aquest cas, l'expressió $\frac{b}{a}\,(\text{mòd. } c)$ tindrà sempre valors reals i, certament, infinits; tots seran congrus a aquest segons c quan a sigui primer amb c, o segons $\frac{c}{\delta}$ quan δ sigui el màxim comú divisor dels nombres c, a.

Aquestes expressions tenen un algoritme més o menys semblant al de les fraccions ordinàries. Aquí

* Cosa que, per analogia, es pot designar per $\frac{11}{1}\,(\text{mòd. } 12)$.

afegim algunes propietats que es poden deduir fàcilment del que precedeix.

1. Si segons el mòdul c, $a \equiv \alpha$, $b \equiv \beta$, les expressions $\frac{a}{b}\,(\text{mòd.}\,c)$ i $\frac{\alpha}{\beta}\,(\text{mòd.}\,c)$ són equivalents.

2. $\frac{a\delta}{b\delta}\,(\text{mòd.}\,c\delta)$ i $\frac{a}{b}\,(\text{mòd.}\,c)$ són equivalents.

3. $\frac{ak}{bk}\,(\text{mòd.}\,c)$ i $\frac{a}{b}\,(\text{mòd.}\,c)$ són equivalents quan k és primer amb c.

Es podrien citar moltes altres proposicions similars, però, com que no estarien subjectes a cap dificultat, ni tampoc no són tan necessàries per al que segueix, passem de pressa a altres.

32. El problema, que tindrà un gran ús en el que segueix, de *trobar tots els nombres que presenten residus donats segons mòduls donats qualssevol* es pot resoldre fàcilment a partir del que precedeix. En primer lloc, siguin A, B, dos mòduls segons els quals el nombre cercat, z, hauria de ser congru als nombres a, b, respectivament. Així, tots els valors de z estan continguts en la forma $Ax + a$, on x és indeterminat però tal que resulti $Ax + a \equiv b\,(\text{mòd.}\,B)$. Ara, si δ és el màxim comú divisor dels nombres A i B, la resolució completa d'aquesta congruència tindrà la forma $x \equiv v\left(\text{mòd.}\,\frac{B}{\delta}\right)$, o sigui, el que és el mateix, $x = v + \frac{kB}{\delta}$, on k denota un nombre enter arbitrari. Aquí, la fórmula $Av + a + \frac{kAB}{\delta}$ comprèn

tots els valors de z; és a dir, $z \equiv Av + a \left(\text{mòd. } \frac{AB}{\delta}\right)$ serà la solució completa del problema. Si als mòduls A, B, s'afegeix un tercer C segons el qual el nombre cercat z ha de ser $\equiv c$, cal procedir, evidentment, de la mateixa manera, perquè les dues primeres condicions ja s'haurien fos en una. És a dir, si el màxim comú divisor dels nombres $\frac{AB}{\delta}$, C és $= \varepsilon$ i la resolució de la congruència $\frac{AB}{\delta}x + Av + a \equiv c\,(\text{mòd. } C)$ és $x \equiv w \left(\text{mòd. } \frac{C}{\varepsilon}\right)$, el problema serà resolt completament per la congruència $z \equiv \frac{ABw}{\delta} + Av + a \left(\text{mòd. } \frac{ABC}{\delta\varepsilon}\right)$. Per a tots els mòduls que es proposin cal procedir similarment. Convé observar que $\frac{AB}{\delta}$, $\frac{ABC}{\delta\varepsilon}$, són els mínims comuns múltiples dels nombres A, B, i A, B, C, respectivament; d'això es copsa fàcilment que, per a tots els mòduls A, B, C, etc., que es tinguin, sempre que el seu mínim comú múltiple sigui M, la resolució completa té la forma $z \equiv r\,(\text{mòd. } M)$. D'altra banda, quan alguna de les congruències auxiliars és irresoluble, s'ha de concloure que el problema comporta una impossibilitat. Es copsa que això no pot esdevenir quan tots els nombres A, B, C, etc., siguin primers entre si.

Exemple. Siguin A, B, C; a, b, c, els nombres 504, 35, 16; 17, -4, 33; aquí les dues condicions que z sigui $\equiv 17\,(\text{mòd. } 504)$ i $\equiv -4\,(\text{mòd. } 35)$ equivalen a una única, que sigui $z \equiv 521\,(\text{mòd. } 2520)$; de la qual, conjuntament amb la $z \equiv 33\,(\text{mòd. } 16)$, en surt $z \equiv 3041\,(\text{mòd. } 5040)$.

33. Quan tots els nombres A, B, C, etc., són primers entre si, se sap que el seu producte és el mínim

comú múltiple de tots. En aquest cas, és evident que totes les congruències $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, etc., equivalen del tot a l'única $z \equiv r \pmod{R}$, on R denota el producte dels nombres A, B, C, etc. Inversament, d'aquí se segueix que l'única condició $z \equiv r \pmod{R}$ es pot descompondre en més d'una; això és, si R es descompon de qualsevol manera en factors A, B, C, etc., primers entre si, les condicions $z \equiv r \pmod{A}$, $z \equiv r \pmod{B}$, $z \equiv r \pmod{C}$, etc., exhaureixen la proposada. Aquesta observació ens obre no solament un mètode per a detectar immediatament la impossibilitat [de resolució], si de cas les condicions proposades la impliquen, sinó que proporciona també un mètode per a organitzar el càlcul més còmodament i més elegantment.

34. Siguin com més amunt les condicions proposades, o sigui, $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, $z \equiv c \pmod{C}$. Es descomponen tots els mòduls en factors primers entre si: A en $A'A''A'''$ etc.; B en $B'B''B'''$ etc.; etc., i, encara més, de manera que els nombres A', A'', etc., B', B'', etc., etc., siguin o bé primers o bé potències de primers. Si algun dels nombres A, B, C, etc., ja és un primer o una potència d'un primer, no és necessària, per a aquest, cap descomposició en factors. Llavors es fa palès del que precedeix que les condicions proposades es poden substituir per les $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, $z \equiv a \pmod{A'''}$, etc.; $z \equiv b \pmod{B'}$, $z \equiv b \pmod{B''}$, etc.; etc. Ara, si tots els nombres A, B, C, etc., no fossin primers entre si, per exemple, si A no fos primer amb B, és evident que tots els divisors primers de A, B, no poden ser diferents, sinó que entre els factors A', A'', A''', etc., n'hi ha d'haver algun que en tingui un d'igual, o bé un múltiple, o bé un submúltiple entre els B', B'', B''', etc. *En primer lloc*, si $A' = B'$,

les condicions $z \equiv a\,(\text{mòd. } A')$, $z \equiv b\,(\text{mòd. } B')$, han de ser idèntiques, o sigui $a \equiv b\,(\text{mòd. } A'$ o bé $B')$; per tant, l'altra es podrà rebutjar. Però si no és $a \equiv b\,(\text{mòd. } A')$, el problema implica impossibilitat. *En segon lloc*, si B' és un múltiple de A', la condició $z \equiv a\,(\text{mòd. } A')$ ha d'estar continguda en la $z \equiv b\,(\text{mòd. } B')$; o sigui, la $z \equiv b\,(\text{mòd. } A')$, que es dedueix de la darrera, ha de ser idèntica a la primera. D'on se segueix que la condició $z \equiv a\,(\text{mòd. } A')$ es pot rebutjar llevat que sigui incompatible amb alguna altra (cas en el qual el problema és impossible). Així, quan totes les condicions supèrflues s'han rebutjat, és clar que tots els mòduls que queden entre els A', A'', A''', etc.; B', B'', B''' etc.; etc., seran primers entre si; llavors, doncs, podem estar segurs de la possibilitat del problema i procedir d'acord amb els preceptes donats abans.

35. *Exemple.* Si, com més amunt, ha de ser $z \equiv 17$ (mòd. 504), $\equiv -4$ (mòd. 35) i $\equiv 33$ (mòd. 16), aquestes condicions es poden reduir a les següents: $z \equiv 17$ (mòd. 8), $\equiv 17$ (mòd. 9), $\equiv 17$ (mòd. 7); $\equiv -4$ (mòd. 5), $\equiv -4$ (mòd. 7); $\equiv 33$ (mòd. 16). D'aquestes condicions, es poden rebutjar $z \equiv 17$ (mòd. 8), $z \equiv 17$ (mòd. 7), ja que la primera està continguda en la condició $z \equiv 33$ (mòd. 16) i la darrera és idèntica a $z \equiv -4$ (mòd. 7); d'aquesta manera romanen

$$z \equiv \begin{cases} 17 & (\text{mòd. } 9) \\ -4 & (\text{mòd. } 5) \\ -4 & (\text{mòd. } 7) \\ 33 & (\text{mòd. } 16) \end{cases}$$

d'on es conclou $z \equiv 3041\,(\text{mòd. } 5040)$. D'altra banda, és palès que sovint serà més convenient si, de les condicions

que queden, es recullen aquelles que havien sortit d'una mateixa condició, quan això pugui fer-se sense cap esforç; *per exemple*, quan han desaparegut algunes de les condicions $z \equiv a\,(\text{mòd.}\,A')$, $z \equiv a\,(\text{mòd.}\,A'')$, etc., la que es restitueix de les restants serà la $z \equiv a$, segons el mòdul que és producte de tots els mòduls romanents dels A', A'', A''', etc. Així, en el nostre exemple, de les condicions $z \equiv -4\,(\text{mòd.}\,5)$, $z \equiv -4\,(\text{mòd.}\,7)$, es restitueix espontàniament aquella de la qual ja havien sortit, $z \equiv -4\,(\text{mòd.}\,35)$. A més a més, d'aquí se segueix que, pel que fa a la brevetat del càlcul, no és completament igual quines es rebutgin d'entre les condicions supèrflues, però no és la nostra intenció transmetre aquí aquests i altres artificis pràctics que s'aprenen molt més fàcilment de l'ús que dels preceptes.

36. Quan tots els mòduls A, B, C, D, etc., són primers entre si, molt sovint és preferible el mètode següent. Es determina un nombre α congru a la unitat segons A, a zero segons el producte dels restants mòduls; o sigui, sigui α un valor qualsevol de l'expressió $\frac{1}{BCD\,\text{etc.}}\,(\text{mòd.}\,A)$ (sovint és preferible agafar el *mínim*) multiplicat per $BCD\,\text{etc.}$ (vegeu l'article 32); similarment, sigui $\beta \equiv 1\,(\text{mòd.}\,B)$ i $\equiv 0\,(\text{mòd.}\,ACD\,\text{etc.})$, $\gamma \equiv 1\,(\text{mòd.}\,C)$ i $\equiv 0\,(\text{mòd.}\,ABDetc.)$, etc. Llavors, si es desitja un nombre z que, segons els mòduls A, B, C, D, etc., sigui congru als nombres a, b, c, d, etc., respectivament, es podrà posar $z \equiv \alpha a + \beta b + \gamma c + \delta d\,\text{etc.}\,(\text{mòd.}\,ABCD\,\text{etc.})$. En efecte, evidentment $\alpha a \equiv a\,(\text{mòd.}\,A)$; en canvi, els membres restants, βb, γc, etc., són tots $\equiv 0\,(\text{mòd.}\,A)$; per tant, $z \equiv a\,(\text{mòd.}\,A)$. La demostració per als mòduls restants es disposa similarment. Aquesta solució s'ha de preferir a l'anterior quan

s'han de resoldre uns quants problemes d'aquest tipus per als quals els mòduls A, B, C, etc., retenen els seus valors; en efecte, llavors els nombres α, β, γ, etc., assoleixen valors constants. Això ve al cas en el problema cronològic on se cerca quin és l'any del període julià del qual es donen la indicció, el nombre auri i el cicle solar. Aquí $A = 15$, $B = 19$, $C = 28$; per tant, com que el valor de l'expressió $\frac{1}{19 \cdot 28}$ (mòd. 15), o sigui $\frac{1}{532}$ (mòd. 15), és 13, α serà $= 6916$. Similarment, es troba 4200 per a β i 4845 per a γ; per tant, el nombre cercat serà el residu mínim del nombre $6916a + 4200b + 4845c$, on a denota la indicció, b el nombre auri, c el cicle solar.

37. Siguin suficients aquestes [proposicions] per a les congruències de primer grau que contenen una única incògnita. Resta que ens ocupem de les congruències en què hi ha més incògnites barrejades. Com que, si volem exposar cada una amb tot rigor, aquest capítol no es pot acabar sense fer-lo massa extens, i com que no és el nostre propòsit exhaurir-les totes en aquest lloc, sinó només transmetre les que es vegin més dignes d'atenció, aquí restringim la investigació a unes quantes observacions i ens reservem per a una altra ocasió una exposició més extensa d'aquesta qüestió.

1) De manera similar es copsa que aquí, com en les equacions, també s'han de tenir tantes congruències com incògnites s'hagin de determinar.

2) Siguin, doncs, proposades les congruències

$$ax + by + cz \cdots \equiv f \,(\text{mòd.}\, m) \qquad (A)$$
$$a'x + b'y + c'z \cdots \equiv f' \qquad (A')$$

$a''x + b''y + c''z \cdots \equiv f''$ $\qquad (A'')$
etc.,

tantes en nombre com incògnites x, y, z, etc., hi hagi.

Ara es determinen nombres ξ, ξ', ξ'', etc., de manera que sigui

$b\xi + b'\xi' + b''\xi'' + \text{etc.} = 0,$
$c\xi + c'\xi' + c''\xi'' + \text{etc.} = 0,$
etc.,

i encara més, de manera que tots siguin enters i no tinguin cap factor comú, la qual cosa consta que es pot fer per la teoria de les equacions lineals. De manera similar, es determinen ν, ν', ν'', etc.; ζ, ζ', ζ'', etc.; etc., de manera que sigui

$a\nu + a'\nu' + a''\nu'' + \text{etc.} = 0,$
$c\nu + c'\nu' + c''\nu'' + \text{etc.} = 0,$
etc.
$a\zeta + a'\zeta' + a''\zeta'' + \text{etc.} = 0,$
$b\zeta + b'\zeta' + b''\zeta'' + \text{etc.} = 0,$
etc. etc.

3) És evident que si es multipliquen les congruències A, A', A'', etc., per ξ, ξ', ξ'', etc.; després, per ν, ν', ν'', etc.; etc., i després se sumen, s'han de produir les congruències

$(a\xi + a'\xi' + a''\xi'' + \text{etc.})x \equiv f\xi + f'\xi' + f''\xi'' + \text{etc.},$
$(b\nu + b'\nu' + b''\nu'' + \text{etc.})y \equiv f\nu + f'\nu' + f''\nu'' + \text{etc.},$
$(c\zeta + c'\zeta' + c''\zeta'' + \text{etc.})z \equiv f\zeta + f'\zeta' + f''\zeta'' + \text{etc.},$
etc.

que, per a abreujar, escrivim així

$\Sigma(a\xi)x \equiv \Sigma(f\xi)$,
$\Sigma(b\nu)y \equiv \Sigma(f\nu)$,
$\Sigma(c\zeta)z \equiv \Sigma(f\zeta)$,
etc.

4) Ara, s'han de distingir més casos. *Primer,* quan tots els coeficients $\Sigma(a\xi)$, $\Sigma(b\nu)$, etc., de les incògnites són primers amb el mòdul m de les congruències, aquestes congruències es poden resoldre segons els preceptes transmesos anteriorment, i la solució completa del problema s'expressarà per congruències de la forma $x \equiv p\,(\text{mòd.}\,m)$, $y \equiv q\,(\text{mòd.}\,m)$, etc.* Per exemple, si es proposen les congruències $x+3y+z \equiv 1$, $4x+y+5z \equiv 7$, $2x+2y+z \equiv 3\,(\text{mòd.}\,8)$, es trobarà $\xi = 9$, $\xi' = 1$, $\xi'' = -14$, d'on resulta $-15x \equiv -26$; per tant, $x \equiv 6\,(\text{mòd.}\,8)$; de la mateixa manera, es troba $15y \equiv -4$, $15z \equiv 1$, i, d'aquí, $y \equiv 4$, $z \equiv 7\,(\text{mòd.}\,8)$.

5) *Segon*, quan no tots els coeficients $\Sigma(a\xi)$, $\Sigma(b\nu)$, etc., són primers amb el mòdul, siguin α, β, γ, etc., els màxims comuns divisors de m amb $\Sigma(a\xi)$, $\Sigma(b\nu)$, $\Sigma(c\zeta)$, etc., respectivament; és clar que el problema és impossible llevat que aquells divideixin els nombres $\Sigma(f\xi)$, $\Sigma(f\nu)$, $\Sigma(f\zeta)$, etc., respectivament. Però quan aquestes condicions tenen lloc, les congruències de 3) seran completament resoltes per les semblants $x \equiv p\left(\text{mòd.}\,\frac{m}{\alpha}\right)$,

* Convé observar que aquesta conclusió requereix una demostració que, en canvi, aquí hem suprimit. En efecte, de la nostra anàlisi, només se'n segueix pròpiament que les congruències proposades no poden ser resoltes per altres valors de les incògnites *x, y,* etc.; però no se'n segueix que aquests les satisfacin. Fins i tot podria resultar que no es donés cap solució en absolut. Un paralogisme similar es presenta també sovint en l'explicació de les equacions lineals.

$y \equiv q \left(\text{mòd. } \frac{m}{\beta}\right)$, $z \equiv r \left(\text{mòd. } \frac{m}{\gamma}\right)$, etc., o bé, si es prefereix, es donaran α valors diferents de x (és a dir, incongrus segons m, posem p, $p+\frac{m}{\alpha}$, …, $p+\frac{(\alpha-1)m}{\alpha}$), β valors diferents de y, etc., que satisfan aquelles congruències; i, evidentment, totes les solucions de les congruències proposades (si n'hi ha alguna) es trobaran entre aquelles. No obstant això, no és lícit invertir aquesta conclusió; efectivament, sovint no totes les combinacions de tots els α valors de x amb tots els de y, amb tots els de z, etc., satisfan el problema, sinó només aquelles el nexe de les quals és lícit posar de manifest per una o més congruències condicionals. Però com que la resolució completa d'aquest problema no és necessària per a allò que segueix, no prosseguim la difusió d'aquest argument en aquest lloc i en tenim prou de donar-ne alguna idea mitjançant un exemple.

Siguin proposades les congruències $3x+5y+z \equiv 4$, $2x+3y+2z \equiv 7$, $5x+y+3z \equiv 6$ (mòd. 12). Aquí resulten ξ, ξ', ξ''; ν, ν', ν''; ζ, ζ', ζ'', respectivament $= 1, -2, 1$; $1, 1, -1$; $-13, 22, -1$; d'on $4x \equiv -4$, $7y \equiv 5$, $28z \equiv 96$. D'aquí s'obtenen quatre valors de x, posem $\equiv 2, 5, 8, 11$; un valor de y, posem $\equiv 11$; quatre valors de z, posem $\equiv 0, 3, 6, 9$ (mòd. 12). Ara, perquè sapiguem a quines combinacions dels valors de x amb valors de z és lícit recórrer, substituïm en les congruències proposades x, y, z, per $2+3t$, 11, $3u$, respectivament, d'on es transformen en les $57+9t+3u \equiv 0$, $30+6t+6u \equiv 0$, $15+15t+9u \equiv 0$ (mòd. 12), les quals es conclou fàcilment que equivalen a les $19+3t+u \equiv 0$, $10+2t+2u \equiv 0$, $5+5t+3u \equiv 0$ (mòd. 4). Evidentment, la primera requereix que sigui $u \equiv t+1$ (mòd. 4), valor que, substituït en les restants,

es troba que també les satisfà. D'aquí es conclou que els valors 2, 5, 8, 11, de x (que resulten posant $t \equiv 0, 1, 2, 3$) s'han de combinar necessàriament amb els valors de $z \equiv 3, 6, 9, 0$, respectivament, de manera que es tenen, en total, les quatre solucions

$$\left.\begin{aligned} x &\equiv 2, 5, 8, 11, \\ y &\equiv 11, 11, 11, 11, \\ z &\equiv 3, 6, 9, 0, \end{aligned}\right\} \qquad (\text{mòd. } 12).$$

* * *

A aquestes disquisicions, per les quals ja s'ha cobert el pròposit de la secció, hi afegim encara algunes proposicions basades en principis similars, que s'usaran freqüentment en el que segueix.

38. Problema. *Trobar quants nombres positius hi ha menors que un nombre positiu donat A i simultàniament primers amb ell.*

Per abreujar, designem la quantitat de nombres positius primers amb el nombre donat i menors que ell amb el prefix φ. I així, se cerca φA.

I. Quan A és primer, és evident que tots els nombres des de 1 fins a $A-1$ són primers amb A; per tant, en aquest cas serà $\varphi A = A - 1$.

II. Quan A és potència d'un nombre primer, posem $A = p^m$, tots els nombres divisibles per p no seran primers amb A, els restants ho seran. Per la qual cosa, dels $p^m - 1$ nombres s'han de rebutjar p, $2p$, $3p$, $\ldots$, $(p^{m-1} - 1)p$; en romanen, doncs, $p^m - 1 - (p^{m-1} - 1)$, o sigui, $p^{m-1}(p-1)$. D'aquí, $\varphi p^m = p^{m-1}(p-1)$.

III. Els casos restants es redueixen fàcilment a aquests amb l'ajut de la proposició següent: *Si es descompon A en factors primers entre si M, N, P, etc., serà $\varphi A = \varphi M \cdot \varphi N \cdot \varphi P$ etc.*, la qual es demostra així. Siguin m, m', m'', etc., els nombres primers amb M i menors que M, la quantitat dels quals és $= \varphi M$. Similarment, siguin n, n', n'', etc.; p, p', p'', etc.; etc., els nombres primers amb N, P, etc., respectivament, i menors que aquests, la quantitat dels quals és φN, φP, etc. Se sap ara que tots els nombres primers amb el producte A també seran primers amb cadascun dels factors M, N, P, etc., i recíprocament (article 19); a més a més, tots els nombres que siguin congrus a algun dels m, m', m'', etc., segons el mòdul M, seran primers amb M i recíprocament, i similarment de N, P, etc. I així, la qüestió s'ha reduït a això: determinar quants nombres es donen per sota de A que siguin congrus a algun dels nombres m, m', m'', etc., segons el mòdul M, a algun dels n, n', n'', etc., segons el mòdul N, etc. Però de l'article 32 se segueix que tots els nombres que donin residus determinats segons cadascun dels mòduls M, N, P, etc., seran congrus segons el seu producte A; de manera que només n'hi haurà un per sota de A congru als residus donats segons cada un dels M, N, P, etc. Per tant, el nombre cercat serà igual al nombre de combinacions de cadascun dels nombres m, m', m'', etc., amb cadascun dels n, n', n'', dels p, p', p'', etc.; etc. Però se sap, per la teoria de combinacions, que aquest és $= \varphi M \cdot \varphi N \cdot \varphi P$ etc. *Q. E. D.*

IV. Ara, es conclou fàcilment de quina manera s'ha d'aplicar això al cas que tractem. Es descompon A en els seus factors primers, o sigui, es redueix a la forma $a^\alpha b^\beta c^\gamma$ etc., on a, b, c, etc., designen nombres

primers diferents. Llavors, serà $\varphi A = \varphi a^{\alpha}\varphi b^{\beta}\varphi c^{\gamma}$ etc. $= a^{\alpha-1}(a-1)b^{\beta-1}(b-1)c^{\gamma-1}(c-1)$ etc., o bé, més elegantment, $\varphi A = A \cdot \frac{a-1}{a} \cdot \frac{b-1}{b} \cdot \frac{c-1}{c}$ etc.

Exemple. Sigui $A = 60 = 2^2 \cdot 3 \cdot 5$, de manera que $\varphi A = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot 60 = 16$. Els nombres primers amb 60 són 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

La primera solució d'aquest problema apareix en els comentaris de l'il·lm. Euler *Theoremata arithmetica noua methodo demonstrata,* Comm. nou. Ac. Petrop. VIII, p. 74. La demostració ha estat repetida posteriorment en l'altra dissertació *Speculationes circa quasdam insignes proprietates numerorum*, Acta Petrop. VIII, p. 17.

39. Si es determina el significat del caràcter φ de manera que φA expressi la quantitat de nombres primers amb A i *no més grans* que A, es copsa que $\varphi 1$ no és $= 0$ sinó $= 1$; en tots els casos restants, no canvia res. Adoptant aquesta definició, tindrem el teorema següent:

Si a, a', a'', etc., són tots els divisors de A (no exclosos ni la unitat ni A), serà $\varphi a + \varphi a' + \varphi a'' +$ etc. $= A$.

Exemple. Sigui $A = 30$; llavors serà $\varphi 1 + \varphi 2 + \varphi 3 + \varphi 5 + \varphi 6 + \varphi 10 + \varphi 15 + \varphi 30 = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$.

Dem. Es multipliquen tots els nombres primers amb a i no més grans que a per $\frac{A}{a}$; similarment, tots

els primers amb a', per $\frac{A}{a'}$, etc., i es tindran $\varphi a + \varphi a' + \varphi a'' +$ etc. nombres, tots no més grans que A. Però,

1) Tots aquests nombres seran diferents. En efecte, és clar que tots els que siguin generats del *mateix* divisor de A seran diferents. Però si de divisors diferents M, N, i de nombres μ, ν, respectivament primers amb ells, se n'obtinguessin d'iguals, *és a dir*, si fos $\frac{A}{M}\mu = \frac{A}{N}\nu$, se seguiria $\mu N = \nu M$. Es posa $M > N$ (cosa que és lícita). Com que M és primer amb μ i divideix el nombre μN, també dividirà N, el més gran al més petit. *Q. E. A.*

2) Entre aquests nombres, es troben tots els 1, 2, 3, ..., A. Sigui t un nombre qualsevol que no supera A, δ el màxim comú divisor dels nombres A, t, i $\frac{A}{\delta}$ serà un divisor de A amb el qual $\frac{t}{\delta}$ és primer. D'aquí, evidentment, el nombre t es trobarà entre els que s'han obtingut del divisor $\frac{A}{\delta}$.

3) Es conclou d'aquí que la quantitat d'aquests nombres és A, per tant, $\varphi a + \varphi a' + \varphi a'' +$ etc. $= A$. *Q. E. D.*

40. *Si el màxim comú divisor dels nombres A, B, C, D, etc., és* $= \mu$, *es poden determinar nombres a, b, c, d, etc., de manera que sigui* $aA + bB + cC +$ *etc.* $= \mu$.

Dem. Considerem, primerament, només dos nombres A, B, i sigui $= \lambda$ el seu màxim comú divisor. Llavors, la congruència $Ax \equiv \lambda \,(\text{mòd. } B)$ serà resoluble (ar-

ticle 30). Sigui l'arrel $\equiv \alpha$ i es posa $\frac{\lambda - A\alpha}{B} = \beta$. Llavors serà $\alpha A + \beta B = \lambda$, com es desitjava.

Si s'afegeix un tercer nombre C, sigui $= \lambda'$ el màxim comú divisor dels nombres λ, C, i aquest serà simultàniament el màxim comú divisor dels nombres A, B, C.* Es determinen nombres k, γ, de manera que sigui $k\lambda + \gamma C = \lambda'$, i serà $k\alpha A + k\beta B + \gamma C = \lambda'$.

Si s'afegeix un quart nombre D, es posa λ'' el màxim comú divisor dels nombres λ', D (que es copsa fàcilment que és simultàniament el màxim comú divisor dels nombres A, B, C, D), i resulti $k'\lambda' + \delta D = \lambda''$. Llavors serà $kk'\alpha A + kk'\beta B + k'\gamma C + \delta D = \lambda''$.

Es pot procedir de manera similar per a qualssevol altres nombres que s'afegeixin.

I així, si els nombres A, B, C, D, etc., no tenen cap divisor comú, és clar que es pot fer $aA + bB + cC$ + etc. $= 1$.

41. *Si p és un nombre primer i es tenen p objectes, entre els quals qualssevol poden ser iguals, però que no tots ells ho siguin, el nombre de permutacions d'aquests objectes serà divisible per p.*

Exemple. Cinc objectes A, A, A, B, B, es poden transposar de deu maneres diferents.

---

* En efecte, és evident que λ' divideix tots els *A, B, C.* Si no fos el *màxim* comú divisor, el màxim seria més gran que λ'. Ara, com que aquest divisor màxim divideix *A, B*, també dividirà $\alpha\, A + \beta\, B$, és a dir λ', el més gran al més petit. *Q. E. A.* Això es pot deduir encara més fàcilment de l'article 18.

Sens dubte, la demostració d'aquest teorema es pot obtenir fàcilment de la coneguda teoria de permutacions. En efecte, si entre aquests objectes n'hi ha primerament a que són iguals a A, després b que són iguals a B, després c que són iguals a C, etc. (on els nombres a, b, c, etc., també poden designar la unitat), de manera que es tingui $a+b+c+\text{etc.} = p$, el nombre de permutacions serà

$$= \frac{1 \cdot 2 \cdot 3 \cdots p}{1 \cdot 2 \cdot 3 \cdots a \cdot 1 \cdot 2 \cdot 3 \cdots b \cdot 1 \cdot 2 \cdot 3 \cdots c \cdot \text{etc.}}.$$

Ara, és clar que el numerador d'aquesta fracció és divisible pel denominador ja que el nombre de permutacions ha de ser enter; però el numerador és divisible per p i el denominador, que és compost de factors menors que p, no és divisible per p (article 15). Per tant, el nombre de permutacions serà divisible per p (article 19).

No obstant això, esperem que hi haurà algú per a qui la demostració següent tampoc no li sigui ingrata.

Quan en dues permutacions l'ordre dels objectes de què estan compostes només difereix en què l'objecte que ocupa el primer lloc en una tingui una altra posició en l'altra, però els restants se succeeixen en el mateix ordre en totes dues i al que és l'últim en una el segueix en l'altra el que és primer, les anomenem *permutacions semblants*.* Així, en el nostre exemple, les permutacions $ABAAB$ i $ABABA$ seran semblants, ja que els objectes

* Si s'imaginen les permutacions semblants escrites en un cercle de manera que l'últim objecte resulti contigu al primer, no hi haurà cap discrepància en absolut, ja que cap lloc no es podrà anomenar primer o bé últim.

que en la primera ocupen els llocs primer, segon, etc., en la darrera estan col·locats en el mateix ordre en els llocs tercer, quart, etc.

Ara, com que cada permutació consta de p objectes, és clar que de cada una se'n poden trobar $p-1$ de semblants si l'objecte que era el primer es col·loca en el segon lloc, el tercer, etc. Si cap d'aquestes no pot ser idèntica [amb cap altra], és evident que el nombre de totes les permutacions surt divisible per p, ja que aquest és p vegades més gran que el nombre de totes les permutacions no semblants. Suposem, doncs, que dues permutacions $PQ\cdots TV\cdots YZ$, $V\cdots YZPQ\cdots T$, una de les quals hagi sortit de l'altra per translació dels termes, siguin idèntiques, o sigui, $P=V$, etc. Sigui P el terme que és el primer a la primera, el $(n+1)$-èsim a la darrera. Així, doncs, el terme $(n+1)$-èsim de la darrera sèrie serà igual al primer, el $(n+2)$-èsim al segon, etc., d'on el $(2n+1)$èsim, inversament, sortirà igual al primer i, per la mateixa raó, el $(3n+1)$-èsim, etc.; i en general, el terme $(kn+m)$-èsim al m-èsim (on s'ha d'imaginar que quan $kn+m$ supera p, o bé la sèrie $PQ\cdots TV\cdots YZ$ es repeteix sempre des del principi, o bé que s'ha de restar de $km+n$ el múltiple de p més pròxim). Per això, si es determina k de manera que resulti $kn\equiv 1\,(\text{mòd. }p)$, cosa que es pot fer, ja que p és primer, se segueix en general que el terme m-èsim és igual al $(m+1)$-èsim; o sigui, qualsevol terme al següent; és a dir, tots els termes són iguals, contra la hipòtesi.

42. *Si els coeficients A, B, C, …, N; a, b, c, …, n, de dues funcions de la forma*

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \cdots + N, \qquad (P)$$

$$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} + \cdots + n, \qquad (Q)$$

són tots racionals, però no tots enters, i el producte de (P) *i* $(Q) =$

$$x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \cdots + \mathfrak{Z},$$

tots els coeficients $\mathfrak{A}$, $\mathfrak{B}$, …, $\mathfrak{Z}$, *no poden ser enters.*

Dem. S'expressen totes les fraccions entre els coeficients A, B, etc., a, b, etc., en forma irreductible i s'elegeix a voluntat un primer p que divideixi un o més dels denominadors d'aquestes fraccions. Suposem, que això és lícit, que p divideix el denominador d'algun dels coeficients fraccionaris de (P), i és clar que si es divideix (Q) per p, en $\frac{(Q)}{p}$ també es dóna com a mínim un coeficient fraccionari el denominador del qual conté el factor p $\left(\text{posem el primer coeficient } \frac{1}{p}\right)$. Ara es copsa fàcilment que a (P) es donarà un terme fraccionari el denominador del qual contindrà p amb exponent *més gran* que en els denominadors de totes les precedents similars i *no menor* que en els denominadors de totes les següents; sigui aquest terme $= Gx^g$, i l'exponent d'aquest p en el denominador de G, $= t$. Un terme similar es donarà en $\frac{(Q)}{p}$; sigui aquest $= \Gamma x^\gamma$, i l'exponent de p en el denominador de Γ, $= \tau$. Aquí, evidentment, $t + \tau$ serà com a mínim $= 2$. Preparat això, el terme $x^{g+\gamma}$ en el producte de (P) i (Q) tindrà un coeficient fraccionari el denominador del qual involucrarà p amb exponent $t + \tau - 1$, la qual cosa es demostra així.

Siguin $'Gx^{g+1}$, $''Gx^{g+2}$, etc., els termes que, en (P), precedeixen el terme Gx^g, i $G'x^{g-1}$, $G''x^{g-2}$, etc., els següents; i, similarment, $'\Gamma x^{\gamma+1}$, $''\Gamma x^{\gamma+2}$, etc., els termes en $\dfrac{(Q)}{p}$ que precedeixen el terme Γx^γ, i $\Gamma' x^{\gamma-1}$, $\Gamma'' x^{\gamma-2}$, etc., els termes que el segueixen. Llavors se sap que en el producte de (P), $\dfrac{(Q)}{p}$, el coeficient del terme $x^{g+\gamma}$ serà

$$\begin{aligned} &= G\Gamma + {}'G\Gamma' + {}''G\Gamma'' + \text{etc.} \\ &\quad + {}'\Gamma G' + {}''\Gamma G'' + \text{etc.} \end{aligned}$$

La part $G\Gamma$ serà una fracció que, si s'expressa en forma irreductible, en el denominador involucra p amb exponent $t+\tau$; en canvi, les parts restants, si són fraccions, contindran en el denominador una potència més petita del nombre p, ja que totes són producte de dos factors que contenen p, l'un amb exponent no més gran que t, l'altre menor que τ, o bé l'un no més gran que τ i l'altre menor que t. D'aquí, $G\Gamma$ serà de la forma $\dfrac{e}{fp^{t+\tau}}$, però la suma dels restants, de la forma $\dfrac{e'}{f'p^{t+\tau-\delta}}$, on δ és positiu i e, f, f', són lliures del factor p; per tant, la suma de tots serà $= \dfrac{ef' + e'fp^\delta}{ff'p^{t+\tau}}$, el numerador de la qual no és divisible per p, de manera que el denominador no pot obtenir per cap reducció menys exponent que $t+\tau$. D'aquí, el coeficient del terme $x^{g+\gamma}$ en el producte de (P), (Q) serà $= \dfrac{ef' + e'fp^\delta}{ff'p^{t+\tau-1}}$; és a dir, *una fracció* el denominador de la qual conté p amb exponent $t+\tau-1$. *Q. E. D.*

43. *La congruència de m-èsim grau* $Ax^m + Bx^{m-1} + Cx^{m-2} + etc. + Mx + N \equiv 0$*, el mòdul de la qual és un nombre primer p que no divideix A, no pot ser resolta de més de m maneres diferents; o sigui, no té més de m arrels incòngrues segons p.* (Vegeu els articles 25, 26.)

Si algú ho nega, suposem que es donen congruències de diferents graus m, n, etc., que tinguin més de m, n, etc., arrels, i sigui m el mínim grau, de manera que totes les congruències similars de grau inferior hagin de satisfer el nostre teorema. Com que per al primer grau això ja s'ha demostrat més amunt (article 26), és evident que m serà $= 2$ o més gran. I així, la congruència $Ax^m + Bx^{m-1} + \text{etc.} + Mx + N \equiv 0$ admetrà almenys $m + 1$ arrels, siguin aquestes $x \equiv \alpha$, $x \equiv \beta$, $x \equiv \gamma$, etc., i suposem, cosa que és lícita, que tots els nombres α, β, γ, etc., són positius i menors que p, i α, el mínim de tots. Ara se substitueix x per $y + \alpha$ en la congruència proposada i es transforma, per això, en $A'y^m + B'y^{m-1} + C'y^{m-2} + \cdots + M'y + N' \equiv 0$. Llavors, és evident que aquesta congruència s'ha de satisfer si es posa $y \equiv 0$, o bé $\equiv \beta - \alpha$, o bé $\equiv \gamma - \alpha$, etc., arrels que seran totes diferents, i el nombre d'aquestes $= m + 1$. Però com que $y \equiv 0$ és una arrel, d'això se segueix que N' serà divisible per p. Per tant, també l'expressió $y(A'y^{m-1} + B'y^{m-2} + \text{etc.} + M')$ resultarà $\equiv 0 \,(\text{mòd. } p)$ si s'atribueix a y un dels m valors $\beta - \alpha$, $\gamma - \alpha$, etc., que tots són > 0 i $< p$; de manera que, en tots aquests casos, també $A'y^{m-1} + B'y^{m-2} + \text{etc.} + M'$ resultarà $\equiv 0$ (article 22); és a dir, la congruència $A'y^{m-1} + B'y^{m-2} + \text{etc.} + M' \equiv 0$, que és de $(m-1)$-èsim grau, té m arrels i, per tant, contradiu el nostre teorema (en efecte, es veu fàcilment que A' és $= A$, de manera que no és divisible per p, com es requereix), malgrat que havíem suposat que totes

les congruències de grau inferior al *m-èsim* satisfan el teorema. *Q. E. A.*

44. Encara que aquí hem suposat que el mòdul p no divideix el coeficient del terme principal, el teorema no es restringeix a aquest cas. En efecte, si el primer coeficient o també alguns dels següents fossin divisibles per p, tots aquests termes es podrien rebutjar i la congruència es rebaixaria, finalment, a una de grau inferior, on el primer coeficient ja no seria divisible per p si no fos que tots els coeficients es poguessin dividir per p; en aquest cas, la congruència seria idèntica i la incògnita completament indeterminada.

Aquest teorema va ser proposat i demostrat per primera vegada per l'il·lm. La Grange (*Mem. de l'Ac. de Berlin, Année* 1768*, p.* 192). Apareix també en la dissertació de l'il·lm. Le Gendre, *Recherches d'Analyse indeterminée, Hist. de l'Acad. de Paris,* 1785*, p.* 466. L'il·lm. Euler demostrà, a *Nou. Comm. Ac. Petr. XVIII, p.* 93, que la congruència $x^n - 1 \equiv 0$ no pot tenir més de n arrels diferents. I encara que aquest sigui [un cas] particular, no obstant això, el mètode que l'home més eminent va utilitzar pot adaptar-se fàcilment a totes les congruències. Un cas encara més limitat ja havia estat resolt anteriorment, Comm. Ac. Petr. V, p. 6, però aquest mètode no pot aplicar-se en general. Més avall, a la Secció VIII, encara demostrarem el teorema d'una altra manera; encara que, a primera vista, tots aquests mètodes poden semblar diferents, els experts que els vulguin comparar s'adonaran fàcilment que tots s'han edificat sobre el mateix principi. D'altra banda, com que aquest teorema s'ha de considerar aquí només com a lema, i com que una exposició completa no correspon

aquí, ens abstenim de tractar separadament dels mòduls compostos.

Secció Tercera

dels

RESIDUS DE POTÈNCIES

45. Teorema. *En tota progressió geomètrica* 1, *a*, *aa*, a^3, *etc., a part del primer,* 1, *encara es dóna un altre terme,* a^t, *congru a la unitat segons un mòdul p primer amb a, l'exponent del qual és* $t < p$.

Dem. Com que el mòdul p és primer amb a, o millor, amb qualsevol potència de a, cap terme de la progressió no serà $\equiv 0\,(\text{mòd.}\,p)$, sinó que qualsevol és congru a algun dels nombres 1, 2, ..., $p-1$. Com que la quantitat d'aquests és $p-1$, és evident que si es consideren més de $p-1$ termes de la progressió, tots no poden tenir residus mínims diferents. En conseqüència, entre els termes 1, a, aa, a^3, ..., a^{p-1}, se'n trobaran, com a mínim, dos de congrus. Així, sigui $a^m \equiv a^n$ i $m > n$, i resultarà, dividint per a^n, que $a^{m-n} \equiv 1$ (article 22), on $m - n < p$ i > 0. *Q. E. D.*

Exemple. A la progressió 1, 2, 4, 8, etc., es troba que el primer terme que és congru a la unitat segons

el mòdul 13 és $2^{12} = 4096$. I segons el mòdul 23, a la mateixa progressió resulta $2^{11} = 2048 \equiv 1$. Similarment, la sisena potència del nombre 5, 15625, és còngrua a la unitat segons el mòdul 7; la cinquena, 3125, segons 11. Doncs, en alguns casos surt còngrua a la unitat una potència d'exponent menor que $p - 1$; en altres, contràriament, és necessari ascendir fins a la potència $p - 1$.

46. Quan la progressió es continua més enllà del terme que és congru a la unitat, s'obtenen de nou els mateixos residus que es tenien al principi. Això és, si $a^t \equiv 1$, serà $a^{t+1} \equiv a$, $a^{t+2} \equiv aa$, etc., fins que s'arriba al terme a^{2t}, el residu mínim del qual serà de nou $\equiv 1$, i el *període* dels residus comença novament. I així, es té un període que comprèn t residus que, en el moment en què s'ha acabat, sempre es repeteix des de l'inici; i en tota la progressió no poden ocórrer altres residus que els que es contenen en aquest període. En general, serà $a^{mt} \equiv 1$ i $a^{mt+n} \equiv a^n$, que amb la nostra notació s'expressa així:

Si $r \equiv \rho\,(\text{mòd.}\,t)$, *serà* $a^r \equiv a^\rho\,(\text{mòd.}\,p)$.

47. Si s'han de trobar ràpidament els residus de potències afectades d'un exponent tan gran com es vulgui, s'obté un profit d'aquest teorema en el moment en què es conegui la potència còngrua a la unitat. Si, per exemple, se cerca el residu originat per la divisió de la potència 3^{1000} per 13, serà $t \equiv 3$ a causa que $3^3 \equiv 1\,(\text{mòd.}\,13)$; per tant, com que és $1000 \equiv 1\,(\text{mòd.}\,3)$, serà $3^{1000} \equiv 3\,(\text{mòd.}\,13)$.

48. Quan a^t és la potència *més petita* còngrua a la unitat (a part de $a^0 = 1$, cas que aquí no prenem en consideració), els t termes que constitueixen el període de residus seran tots diferents, com es copsa sense dificultat de la demostració de l'article 45. Llavors, però, la proposició de l'article 46 es pot invertir; això és, si $a^m \equiv a^n \,(\text{mòd.}\, p)$, serà $m \equiv n \,(\text{mòd.}\, t)$. En efecte, si m i n fossin incongrus segons el mòdul t, els seus residus mínims μ i ν serien diferents. Però $a^\mu \equiv a^m$, $a^\nu \equiv a^n$; per tant, $a^\mu \equiv a^\nu$; és a dir, no totes les potències per sota de a^t serien incòngrues, contràriament a la hipòtesi.

I així, si $a^k \equiv 1 \,(\text{mòd.}\, p)$, serà $k \equiv 0 \,(\text{mòd.}\, t)$; *és a dir*, k divisible per t.

Fins aquí hem parlat de mòduls qualssevol, a condició que siguin primers amb a. Ara, considerem separadament mòduls que són nombres absolutament primers, i després edifiquem la investigació més general sobre aquest fonament.

49. Teorema. *Si p és un nombre primer que no divideix a i a^t la potència més petita de a còngrua a la unitat segons el mòdul p, l'exponent t, o bé serà $= p-1$, o bé, una part alíquota d'aquest nombre.*

Són útils els exemples dels articles precedents.

Dem. Com que ja s'ha mostrat que t, o bé és $= p-1$, o bé, $< p-1$, només resta demostrar que, en el darrer cas, t sempre és una part alíquota de $p-1$.

I. Es reuneixen els residus mínims positius de tots els termes $1,\ a,\ aa,\ \ldots,\ a^{t-1}$, que es designen per α,

α', α'', etc., de manera que sigui $\alpha = 1$, $\alpha' \equiv a$, $\alpha'' \equiv aa$, etc. És clar que tots aquests seran diferents; en efecte, si dos termes a^m, a^n donessin el mateix, seria (suposant $m > n$) $a^{m-n} \equiv 1$ i $m - n < t$, *Q. E. A.*, ja que, *per hipòtesi*, cap potència inferior a a^t no és còngrua a la unitat. A més a més, tots els α, α', α'', etc., estan continguts en la sèrie dels nombres 1, 2, 3, ..., $p-1$, la qual, en canvi, no exhauriran, ja que $t < p-1$. Designarem per (A) el conjunt de tots els α, α', α'', etc. Així, doncs, (A) comprendrà t termes.

II. S'agafa un nombre qualsevol, β, dels 1, 2, ..., $p-1$, que falti en (A). Es multiplica β per tots els nombres α, α', α'', etc., i siguin β, β', β'', etc., els residus mínims originats per això, el nombre dels quals també serà t. Però aquests residus seran diferents tant entre si com de tots els α, α', α'', etc. En efecte, si la *primera* afirmació fos falsa, es tindria $\beta a^m \equiv \beta a^n$, de manera que, dividint per β, $a^m \equiv a^n$, contra el que hem demostrat fa un instant; si ho fos la *darrera*, es tindria $\beta a^m \equiv a^n$, d'on, quan $m < n$, $\beta \equiv a^{n-m}$; és a dir, β congru a algun dels α, α', α'', etc., contra la hipòtesi; en canvi, quan $m > n$, se seguiria, multiplicant per a^{t-m}, $\beta a^t \equiv a^{t+n-m}$, o sigui, a causa que $a^t \equiv 1$, $\beta \equiv a^{t+n-m}$, que, igualment, és una absurditat. Es designa per (B) el complex de tots els β, β', β'', etc., la quantitat dels quals és $= t$, i ja es tindran $2t$ nombres dels 1, 2, ..., $p-1$. Doncs, si (A) i (B) comprenen tots aquests nombres, resulta $\dfrac{p-1}{2} = t$, i així el teorema és demostrat.

III. Si encara en manquen alguns, sigui γ algun d'ells. Es multipliquen per aquest tots els α, α', α'', etc.,

i siguin γ, γ', γ'', etc., els residus mínims dels productes; es designa per (C) el complex de tots. Així, doncs, (C) comprendrà t nombres dels 1, 2, ..., $p-1$, que tots seran diferents tant entre si com dels nombres continguts en (A) i (B). Les primeres afirmacions es demostren de la mateixa manera que en II, la tercera, així. Si fos $\gamma a^m \equiv \beta a^n$, resultaria $\gamma \equiv \beta a^{n-m}$ o bé $\equiv \beta a^{t+n-m}$, segons que $m < n$ o bé $> n$; en tots dos casos γ [seria] congru a algun de (B), contra la hipòtesi. Es tenen, doncs, $3t$ nombres dels 1, 2, ..., $p-1$, i, si no en manca cap més, resultarà $t = \dfrac{p-1}{3}$, de manera que el teorema serà demostrat.

IV. Però si encara ara en manquen alguns, s'haurà d'avançar de la mateixa manera cap a un quart complex de nombres (D), etc. És clar que, com que la quantitat de nombres 1, 2, ..., $p-1$, és finita, finalment serà exhaurida, de manera que serà un múltiple de t; per tant, t serà una part alíquota del nombre $p-1$. *Q. E. D.*

50. Així, doncs, com que $\dfrac{p-1}{t}$ és enter, se segueix que, si cada una de les parts de la congruència $a^t \equiv 1$ s'eleva a la potència d'exponent $\dfrac{p-1}{t}$, $a^{p-1} \equiv 1$; *o sigui,* $a^{p-1} - 1$, *sempre és divisible per* p, *quan* p *és un primer que no divideix* a.

Aquest teorema, que, tant per causa de la seva elegància com per causa de la seva extraordinària utilitat, és digne de tota l'atenció, se sol anomenar *teorema de Fermat*, pel seu descobridor. Vegeu *Fermatii Opera Mathem. Tolosae* 1679 *fol. p.* 163. L'inventor no

va afegir la demostració, però va declarar que en tenia una en el seu poder. L'il·lm. Euler és el primer que en va donar a judici públic una demostració en la dissertació titulada *Theorematum quorundam ad numeros primos spectantium demostratio, Comm. Acad. Petrop.* T. *VIII.** Aquesta es basa en el desenvolupament de la potència $(a+1)^p$, d'on, de la forma dels coeficients, es dedueix facilíssimament que $(a+1)^p - a^p - 1$ sempre serà divisible per p, de manera que $(a+1)^p - (a+1)$ serà divisible per p quan $a^p - a$ sigui divisible per p. Ara, com que $1^p - 1$ sempre és divisible per p, $2^p - 2$ també ho serà sempre; d'aquí $3^p - 3$ també, etc., i, en general, $a^p - a$. I així, si p no divideix a, $a^{p-1} - 1$ també serà divisible per p. Això és suficient per a posar de manifest l'essència del mètode. L'insigne Lambert transmeté una demostració similar en *Actis Erudit.* 1769 *p.* 109. Com que el desenvolupament de la potència d'un binomi semblava bastant aliena a la teoria de nombres, l'il·lm. Euler n'investigà una altra demostració, que apareix a *Comment. nou. Petr. T. VII p.* 70, que concorda completament amb la que hem exposat en l'article precedent. En el que segueix, encara se'ns n'oferiran algunes altres. En aquest lloc encara se'n pot afegir una, que es basa en principis similars als de la primera de l'il·lm. Euler. La proposició següent, de la qual el nostre teorema només

* En el comentari anterior, *Com. Petr.* T. VI, p. 106, el gran home encara no havia superat l'escull. En la famosa controvèrsia entre Maupertuis i König, sorgida sobre el principi de la mínima acció, però que, de seguida, es va allunyar cap a coses heterogènies, König va dir que tenia a les mans un manuscrit de Leibnitz que contenia una demostració d'aquest teorema totalment concordant amb l'euleriana: *Appel au public.*, p. 106. Encara que no volem negar la fidelitat d'aquest testimoni, certament Leibnitz no va publicar mai el seu descobriment. Vegeu *Hist. de l'Ac. de Prusse, A.* 1750 *p.* 530.

és un cas particular, també s'aplicarà més avall a altres investigacions.

Suposat que p és un nombre primer, la potència p-èsima del polinomi $a+b+c+etc.$ és $\equiv a^p+b^p+c^p+etc.$ segons el mòdul p.

Dem. És sabut que la potència p-èsima del polinomi $a+b+c+etc.$ és composta de parts de la forma $\kappa a^\alpha b^\beta c^\gamma etc.$, on $\alpha+\beta+\gamma+etc.=p$ i κ designa de quantes maneres es podrien permutar p objectes dels quals α, β, γ, etc., són $=a$, b, c, etc., respectivament. Però a l'article 41, més amunt, hem mostrat que aquest nombre sempre és divisible per p llevat que tots els objectes siguin iguals, és a dir, llevat que algun dels nombres α, β, γ, etc., sigui $=p$, però els restants, $=0$. D'on se segueix que totes les parts de $(a+b+c+etc.)^p$ són divisibles per p, excepte a^p, b^p, c^p, etc.; així, doncs, quan es tracta de congruències segons el mòdul p, aquestes es podran ometre sense perill i resultarà $(a+b+c+etc.)^p\equiv a^p+b^p+c^p+etc.$ *Q. E. D.*

Ara, si es posen totes les quantitats a, b, c, etc. $=1$ i el seu nombre és $=k$, resultarà $k^p\equiv k$, com en l'article precedent.

52. Així, doncs, com que altres nombres que els que són divisors de $p-1$ no poden ser exponents de les potències més petites a què s'han d'elevar alguns nombres perquè resultin congrus a la unitat, es presenta la qüestió de si tots els divisors de $p-1$ són idonis per a això, i quan tots els nombres no divisibles per p es classifiquen segons l'exponent de la més petita de les seves potències còngrues a la unitat, quants han de correspon-

dre a cada un dels exponents. Convé observar en aquest instant que és suficient si es consideren tots els nombres positius des d'1 fins a $p-1$; en efecte, és evident que nombres congrus s'han d'elevar a la mateixa potència perquè resultin congrus a la unitat, de manera que qualsevol nombre s'ha de relacionar amb el mateix exponent que el seu residu mínim positiu. En conseqüència, ens haurem de dedicar a això: que descobrim de quina manera, respecte d'això, els nombres 1, 2, 3, …, $p-1$, s'han de distribuir entre cada un dels factors de $p-1$. Per abreujar, si d és un dels divisors del nombre $p-1$ (en els quals també cal incloure 1 i $p-1$), designarem per ψd la quantitat de nombres positius menors que p, la d-èsima potència dels quals és la més petita còngrua a la unitat.

53. Perquè aquesta disquisició es pugui entendre més fàcilment, hi afegim un exemple. Per a $p = 19$, els nombres 1, 2, 3, …, 18, es distribuiran entre els divisors del nombre 18 d'aquesta manera:

1	1
2	18
3	7, 11
6	8, 12
9	4, 5, 6, 9, 16, 17
18	2, 3, 10, 13, 14, 15.

Així, doncs, en aquest cas resulta $\psi 1 = 1$, $\psi 2 = 1$, $\psi 3 = 2$, $\psi 6 = 2$, $\psi 9 = 6$, $\psi 18 = 6$. Una petita atenció aquí ensenya que pertanyen a qualsevol exponent tants nombres com es donin no més grans que aquest i primers amb ell, o sigui, que, almenys en aquest cas, i retingut el símbol de l'article 40, és $\psi d = \varphi d$. Ara bé, que aquesta observació és certa en general, ho demostrem així.

I. Si es té algun nombre a que *pertany* a l'exponent d (*és a dir*, la d-èsima potència del qual és còngrua a la unitat, totes les inferiors incòngrues), totes les seves potències aa, a^3, a^4, ..., a^d, o sigui, els seus residus mínims, també posseiran la primera propietat (que la seva potència d-èsima sigui còngrua a la unitat) i com que això també es pot expressar així, *els residus mínims dels nombres* a, aa, a^3, ..., a^d, *(que són tots diferents) són arrels de la congruència* $x^d \equiv 1$, però aquesta no pot tenir més de d arrels diferents, és evident que, excepte els residus mínims dels nombres a, aa, a^3, ..., a^d, no es donen altres nombres entre 1 i $p-1$, inclusivament, les potències d'exponent d dels quals siguin còngrues a la unitat. D'aquí és clar que tots els nombres que pertanyen a l'exponent d es troben entre els residus mínims dels nombres a, aa, a^3, ..., a^d. Quins són, i quina [és] la seva quantitat, s'estableix així. Si k és un nombre primer amb d, totes les potències de a^k els exponents de les quals són $< d$ no seran còngrues a la unitat; en efecte, sigui $\frac{1}{k}\,(\text{mòd.}\,d) \equiv m$ (vegeu article 31) i serà $a^{km} \equiv a$; per tant, si la potència e-èsima de a^k fos còngrua a la unitat i $e < d$, també seria $a^{kme} \equiv 1$ i, d'aquí, $a^e \equiv 1$, contràriament a la hipòtesi. D'aquí és evident que el residu mínim de a^k pertany a l'exponent d. Però si k té algun divisor δ comú amb d, el residu mínim de a^k no pertany a l'exponent d; ja que, llavors, la potència $\frac{d}{\delta}$-èsima ja resulta còngrua a la unitat $\big($en efecte, $\frac{kd}{\delta}$ serà divisible per d, o sigui, $\equiv 0\,(\text{mòd.}\,d)$, de manera que $a^{\frac{kd}{\delta}} \equiv 1\big)$. D'aquí es conclou que pertanyen a l'exponent d tants nombres com nombres dels 1, 2, 3, ..., d, siguin primers amb d. Però és oportú recordar

que aquesta conclusió està lligada a la suposició que ja hi ha un nombre a que pertany a l'exponent d. Per la qual cosa, resta el dubte que pogués resultar que a algun exponent no hi pertanyés cap nombre en absolut, i la conclusió es limita al fet que ψd sigui, o bé $= 0$, o bé $= \varphi d$.

54. II. Ara, siguin d, d', d'', etc., tots els divisors del nombre $p-1$, i, com que tots els nombres 1, 2, 3, ..., $p-1$, estan distribuïts entre aquests, serà $\psi d + \psi d' + \psi d'' + etc. = p-1$. Però a l'article 40 vàrem demostrar que $\varphi d + \varphi d' + \varphi d'' + etc. = p-1$, i de l'article precedent se segueix que ψd és, o bé igual, o bé menor que φd, més gran no pot ser, i similarment per a $\psi d'$ i $\varphi d'$, etc. I així, si algun (o també més d'un) dels termes ψd, $\psi d'$, $\psi d''$, etc., fos menor que el terme corresponent de φd, $\varphi d'$, $\varphi d''$, etc., la suma d'aquells no podria ser igual a la suma d'aquests. D'on concloem, finalment, que ψd *sempre és igual a* φd, de manera que no depèn de la magnitud de $p-1$.

55. Màxima atenció, però, mereix un cas particular de la proposició precedent, això és, *sempre es donen nombres dels quals cap potència menor que la* $(p-1)$*-èsima no és còngrua a la unitat*, i certament tants entre 1 i $p-1$ com nombres per sota de $p-1$ siguin primers amb $p-1$. Com que la demostració d'aquest teorema no seria de cap manera tan òbvia com podria semblar a primera vista, i pel valor del teorema, encara se'n pot afegir una altra bastant diferent de la precedent, ja que la diversitat de mètodes sol servir per il·lustrar moltíssim les coses més obscures. Es descompon $p-1$ en els seus factors primers i resulta $p-1 = a^\alpha b^\beta c^\gamma etc.$, on a, b, c, etc., designen nombres primers diferents. Llavors,

acabarem la demostració del teorema per les [proposicions] següents:

I. Sempre es pot trobar un nombre A (o més d'un) que pertanyi a l'exponent a^α, i similarment nombres B, C, etc., que pertanyin respectivament als exponents b^β, c^γ, etc.

II. El producte de tots els nombres A, B, C, etc. (o sigui, el residu mínim d'aquest producte), pertany a l'exponent $p-1$. Demostrem això efectivament així.

I. Sigui g algun nombre dels 1, 2, 3, ..., $p-1$, que *no* satisfaci la congruència $x^{\frac{p-1}{a}} \equiv 1 \,(\text{mòd.}\, p)$; en efecte, tots aquests nombres no poden satisfer aquesta congruència, el grau de la qual és $< p-1$. Llavors, afirmo que si la potència $\dfrac{p-1}{a^\alpha}$-èsima de g es posa $\equiv h$, aquest nombre, o sigui, el seu residu mínim, pertany a l'exponent a^α.

Efectivament, és clar que la potència a^α-èsima de h serà còngrua a la potència $(p-1)$-èsima de g; *és a dir*, a la unitat, però la potència $a^{\alpha-1}$-èsima de h serà còngrua a la potència $\dfrac{p-1}{a}$-èsima de g; *és a dir*, serà incòngrua a la unitat, i molt menys poden ser còngrues a la unitat les potències $a^{\alpha-2}$, $a^{\alpha-3}$-èsimes, etc. de h. Però l'exponent de la potència més petita de h còngrua a la unitat, o sigui, l'exponent a què pertany h, ha de dividir el nombre a^α (article 48). Per tant, com que a^α no és divisible per nombres altres que ell mateix i potències més petites de a, a^α serà necessàriament l'exponent a què pertany h. *Q. E. D.* Es demostra per un mètode similar que es donen nombres que pertanyen als exponents b^β, c^γ, etc.

II. Si suposem que el producte de tots els A, B, C, etc., no pertany a l'exponent $p-1$, sinó a un menor, t, aquest t dividirà $p-1$ (article 48), o sigui, $\frac{p-1}{t}$ serà un enter més gran que la unitat. Però es copsa fàcilment que aquest quocient, o bé és un dels nombres primers a, b, c, etc., o bé és divisible, almenys, per algun d'ells (article 17), per exemple, per a, ja que per als altres la conclusió és similar. Així, t dividirà $\frac{p-1}{a}$; per tant, el producte $ABC\,etc.$ elevat a la potència $\frac{p-1}{a}$-èsima també serà congru a la unitat (article 46). Però és evident que cada un dels B, C, etc. (exceptuat A) elevats a la potència $\frac{p-1}{a}$-èsima resulten congrus a la unitat, ja que els exponents b^β, c^γ, etc., a què pertany cadascun divideixen $\frac{p-1}{a}$. D'aquí serà $A^{\frac{p-1}{a}} B^{\frac{p-1}{a}} C^{\frac{p-1}{a}}\,etc. \equiv A^{\frac{p-1}{a}} \equiv 1$. D'on se segueix que l'exponent a què pertany A ha de dividir $\frac{p-1}{a}$ (article 48); és a dir, $\frac{p-1}{a^{\alpha+1}}$ ha de ser enter; però $\frac{p-1}{a^{\alpha+1}} = \frac{b^\beta c^\gamma etc.}{a}$ no pot ser enter (article 15). D'on cal concloure, finalment, que la nostra suposició no pot ser consistent; és a dir, que el producte $ABC\,etc.$ pertany realment a l'exponent $p-1$. *Q. E. D.*

La darrera demostració sembla un xic més llarga que la primera; contràriament, la primera és menys directa que la darrera.

56. Aquest teorema procura un exemple notable de quanta cura s'ha de tenir sovint en la teoria dels nombres de no assumir com a certes coses que no ho són. El cèlebre Lambert, en la dissertació ja citada més

amunt, *Acta Erudit.* 1769, *p.* 127, fa menció d'aquesta proposició, però no ateny, certament, la necessitat de demostració. Ningú no n'havia intentat la demostració excepte el gran Euler a *Comment. nov. Ac. Petrop. T. XVIII*, l'any 1773, *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*, p. 85 i s., vegeu, principalment, l'article 37, on es parla abundantíssimament de la necessitat d'una demostració. Però la demostració que va presentar l'Home sagacíssim té dos defectes. L'un, que en l'article 31 i s. suposa tàcitament que la congruència $x^n \equiv 1$ (traduïts els raonaments mostrats allà a la nostra notació) té realment n arrels diferents, encara que anteriorment només havia demostrat que no en podia tenir *més*; l'altre, que només va induir la fórmula de l'article 34.

57. Anomenarem *arrels primitives*, com l'il·lm. Euler, els nombres que pertanyen a l'exponent $p - 1$. Així, doncs, si a és una arrel primitiva, els residus mínims de les potències a, aa, a^3, $\ldots$, a^{p-1}, seran tots diferents; d'on es dedueix fàcilment que entre ells s'han de trobar tots els nombres 1, 2, 3, $\ldots$, $p - 1$, que són tants en quantitat com aquells residus mínims; *és a dir*, qualsevol nombre no divisible per p és congru a alguna potència de a. Aquesta propietat notable és d'una utilitat molt considerable i pot ajudar no poc a les operacions aritmètiques que pertanyen a les congruències, més o menys de manera similar a com [ajuda] la introducció dels logaritmes a les operacions de l'aritmètica vulgar. Elegirem com plagui una arrel primitiva a com a *base*, a la qual referirem tots els nombres no divisibles per p, i si fos $a^e \equiv b\,(\text{mòd.}\,p)$, anomenarem e l'*índex* de b. Per exemple, si per al mòdul 19 es pren per base l'arrel primitiva 2, es correspondran

nombres	1	2	3	4	5	6	7	8	9	10
índexs	0	1	13	2	16	14	6	3	8	17

nombres	11	12	13	14	15	16	17	18
índexs	12	15	5	7	11	4	10	9.

D'altra banda, és clar que, mantenint la base, cada nombre té més d'un índex, però tots aquests seran congrus segons el mòdul $p-1$; per això, sempre que la discussió serà d'índexs, es tindran per equivalents els que són congrus segons el mòdul $p-1$, de manera similar a com es consideren equivalents els nombres quan són congrus segons el mòdul p.

58. Els teoremes que pertanyen als índexs són completament anàlegs als que atenen als logaritmes.

L'índex del producte format de qualsevol nombre de factors és congru a la suma de l'índex de cada un dels factors segons el mòdul $p-1$.

L'índex de la potència d'un nombre és congru, segons el mòdul $p-1$*, al producte de l'índex del nombre donat per l'exponent de la potència.*

Ometem les demostracions per la seva facilitat.

D'aquí es copsa que, si volem construir una taula de la qual es puguin extreure els índexs de tots els nombres per a mòduls diferents, se'n poden ometre tant tots els nombres més grans que el mòdul com tots els compostos. Un model de taula d'aquest tipus s'ha afegit al final d'aquesta obra, *Taula 1*, on, a la primera columna vertical s'han posat els nombres primers i les potències

dels nombres primers des de 3 fins a 97, que són considerats com els mòduls; junt amb aquests, cada un dels nombres presos com a base; després se segueixen els índexs dels successius nombres primers, cinc dels quals sempre són separats per un petit interval, i els nombres primers són disposats a dalt en el mateix ordre; de manera que es pugui trobar fàcilment i amb seguretat quin índex correspondrà a un nombre primer donat segons un mòdul donat.

Així, per exemple, si $p = 67$, l'índex del nombre 60, pres 12 com a base, serà $\equiv 2\,\mathrm{Ind}\,2 + \mathrm{Ind}\,3 + \mathrm{Ind}\,5\,(\mathrm{mòd.}\,66) \equiv 58 + 9 + 39 \equiv 40$.

59. *L'índex d'un valor qualsevol de l'expressió* $\frac{a}{b}$ $(\mathrm{mòd.}\,p)$ (article 31) *és congru segons el mòdul* $p-1$ *a la diferència dels índexs del numerador* a *i el denominador* b*, suposat que els nombres* a*,* b*, no són divisibles per* p*.*

En efecte, sigui c un valor qualsevol, i serà $bc \equiv a\,(\mathrm{mòd.}\,p)$; d'aquí $\mathrm{Ind}\,b + \mathrm{Ind}\,c \equiv \mathrm{Ind}\,a\,(\mathrm{mòd.}\,p-1)$, de manera que $\mathrm{Ind}\,c \equiv \mathrm{Ind}\,a - \mathrm{Ind}\,b$.

Així, si es tingués una taula en la qual es trobés l'índex de cada nombre per a qualsevol mòdul primer, i una altra de la qual es pogués derivar el nombre que pertany a un índex donat, es podrien resoldre totes les congruències de primer grau amb un treball facilíssim, ja que totes es poden reduir a unes en què el mòdul és un nombre primer (article 30). *Per exemple*, proposada la congruència $29x + 7 \equiv 0\,(\mathrm{mòd.}\,47)$, serà $x \equiv \frac{-7}{29}\,(\mathrm{mòd.}\,47)$. D'aquí, $\mathrm{Ind}\,x \equiv \mathrm{Ind}(-7) - \mathrm{Ind}\,29 \equiv \mathrm{Ind}\,40 - \mathrm{Ind}\,29 \equiv 15 - 43 \equiv 18\,(\mathrm{mòd.}\,46)$. Per al nombre l'índex del qual és 18 es troba 3. Per tant, $x \equiv$

3 (mòd. 47). Certament, no hem afegit la segona taula, però una altra alternativa a aquesta podrà complir, com mostrarem a la Secció VI.

60. De manera similar a com hem designat les arrels de les congruències de primer grau a l'article 31, en el que segueix també presentarem per un símbol les arrels de les congruències pures de grau superior. Això és, així com $\sqrt[n]{A}$ no significa res més que una arrel de l'equació $x^n = A$, una arrel qualsevol de la congruència $x^n \equiv A \,(\text{mòd.}\, p)$ es denotarà, afegit el mòdul, per $\sqrt[n]{A} \,(\text{mòd.}\, p)$. Direm que l'expressió $\sqrt[n]{A} \,(\text{mòd.}\, p)$ té tants valors com tingui incongrus segons p, ja que tots els que són congrus segons p s'han de considerar equivalents (article 26). D'altra banda, és clar que si A, B, fossin congrus segons p, les expressions $\sqrt[n]{A}$, $\sqrt[n]{B} \,(\text{mòd.}\, p)$, serien equivalents.

Ara, si es posa $\sqrt[n]{A} \equiv x \,(\text{mòd.}\, p)$, serà $n \operatorname{Ind} x \equiv \operatorname{Ind} A \,(\text{mòd.}\, p-1)$. D'aquesta congruència es dedueixen, d'acord amb els preceptes de la secció precedent, els valors de $\operatorname{Ind} x$ i, d'aquests, els valors corresponents de x. Es copsa fàcilment que x té tants valors com arrels la congruència $n \operatorname{Ind} x \equiv \operatorname{Ind} A \,(\text{mòd.}\, p-1)$. Així, doncs, $\sqrt[n]{A}$ tindrà, evidentment, només un valor quan n és primer amb $p-1$; però quan els nombres n, $p-1$, tenen un divisor comú δ, i aquest és el màxim, $\operatorname{Ind} x$ tindrà δ valors incongrus segons $p-1$, de manera que $\sqrt[n]{A}$, el mateix nombre de valors incongrus segons p, suposat que $\operatorname{Ind} A$ és divisible per δ. Si aquesta condició falla, $\sqrt[n]{A}$ no tindrà cap valor real.

Exemple. Se cerquen els valors de l'expressió $\sqrt[15]{11}$ (mòd. 19). Així, s'ha de resoldre la congruència $15 \operatorname{Ind} x$

$\equiv \operatorname{Ind} 11 \equiv 6\,(\text{mòd. } 18)$, i es troben tres valors de $\operatorname{Ind} x$ $\equiv 4,\ 10,\ 16\,(\text{mòd. } 18)$. A aquests, corresponen els valors de x, 6, 9, 4.

61. Per més ràpid que sigui aquest mètode quan hi ajuden les taules necessàries, no hem d'oblidar que és indirecte. Així, doncs, valdrà la pena esbrinar quant eficaços són els mètodes directes; aquí tractarem els que es poden extreure dels precedents; altres, que demanen consideracions més recòndites, es reserven per a la secció VIII. Comencem pel cas més simple, on $A = 1$, o sigui, on se cerquen les arrels de la congruència $x^n \equiv 1\,(\text{mòd. } p)$. Així, aquí, presa com a base una arrel primitiva qualsevol, ha de ser $n \operatorname{Ind} x \equiv 0\,(\text{mòd. } p-1)$. Quan n és primer amb $p-1$, aquesta congruència només tindrà una arrel, això és, $\operatorname{Ind} x \equiv 0\,(\text{mòd. } p-1)$; per tant, *en aquest cas*, $\sqrt[n]{1}\,(\text{mòd. } p)$ té un únic valor, això és, $\equiv 1$. Però quan els nombres n, $p-1$, tenen divisor comú (màxim) δ, la solució completa de la congruència $n \operatorname{Ind} x \equiv 0\,(\text{mòd. } p-1)$ serà $\operatorname{Ind} x \equiv 0\left(\text{mòd. } \dfrac{p-1}{\delta}\right)$ (vegeu l'article 30); *és a dir*, segons el mòdul $p-1$, $\operatorname{Ind} x$ haurà de ser congru a algun dels nombres 0, $\dfrac{p-1}{\delta}$, $\dfrac{2(p-1)}{\delta}$, $\dfrac{3(p-1)}{\delta}$, $\ldots$, $\dfrac{(\delta-1)(p-1)}{\delta}$, o sigui, tindrà δ valors incongrus segons el mòdul $p-1$; per tant, en aquest cas, x també tindrà δ valors diferents (incongrus segons el mòdul p). D'aquí es copsa que l'expressió $\sqrt[\delta]{1}$ també té δ valors diferents, els índexs dels quals coincideixen exactament amb els dits anteriorment. En conseqüència, l'expressió $\sqrt[\delta]{1}\,(\text{mòd. } p)$ equival completament a $\sqrt[n]{1}\,(\text{mòd. } p)$; és a dir, la congruència $x^\delta \equiv 1\,(\text{mòd. } p)$ té les mateixes arrels que la $x^n \equiv 1\,(\text{mòd. } p)$. La primera,

però, serà de grau inferior, suposat que δ i n siguin diferents.

Exemple. $\sqrt[15]{1}\,(\text{mòd. }19)$ té tres valors, ja que 3 és el màxim comú divisor dels nombres 15, 18, que seran simultàniament els valors de l'expressió $\sqrt[3]{1}\,(\text{mòd. }19)$. Aquests són 1, 7, 11.

62. Així, doncs, per aquesta reducció ens beneficiem que no sigui necessari resoldre altres congruències de la forma $x^n \equiv 1$ que aquelles en què n és un divisor del mòdul. Més avall mostrarem que les congruències d'aquesta forma sempre es poden rebaixar encara més, malgrat que el que precedeix no sigui suficient per a això. Aquí, però, ja podem acabar un cas, això és, aquell en què $n = 2$. En efecte, evidentment, els valors de l'expressió $\sqrt[2]{1}$ seran $+1$ i -1, ja que no n'hi pot haver més de dos, i -1 i $+1$ són sempre incongrus llevat que el mòdul sigui $= 2$, cas en què és clar que $\sqrt[2]{1}$ només pot tenir un sol valor. D'aquí se segueix que $+1$ i -1 també seran valors de l'expressió $\sqrt[2m]{1}$ quan m sigui primer amb $\dfrac{p-1}{2}$. Això succeirà sempre, quan el mòdul és de tal índole que $\dfrac{p-1}{2}$ resulti un nombre absolutament primer (llevat que per casualitat $p - 1 = 2m$, cas en què tots els nombres 1, 2, 3, $\ldots$, $p - 1$, són arrels), per exemple, quan $p = 3, 5, 7, 11, 23, 47, 59, 83, 107$, etc. Com a corol·lari, s'observa aquí que l'índex de -1 sempre és $\equiv \dfrac{p-1}{2}\,(\text{mòd. }p-1)$, qualsevol que sigui l'arrel primitiva que s'hagi pres per base. Efectivament, $2\,\text{Ind}(-1) \equiv 0\,(\text{mòd. }p-1)$. Per tant, $\text{Ind}(-1)$ serà, o bé $\equiv 0$, o bé $\equiv \dfrac{p-1}{2}\,(\text{mòd. }p-1)$; però 0 és sempre índex de $+1$, i

-1 i $+1$ sempre han de tenir els índexs diferents (excepte per al cas $p = 2$, que no val la pena considerar aquí).

63. A l'article 60 hem mostrat que l'expressió $\sqrt[n]{A}\,(\text{mòd.}\,p)$ té δ valors diferents o bé no en té cap en absolut, si δ és el màxim comú divisor dels nombres n, $p-1$. Ara, de la manera com hem ensenyat que $\sqrt[n]{A}$ i $\sqrt[\delta]{A}$ serien equivalents si fos $A \equiv 1$, provarem en general que l'expressió $\sqrt[n]{A}$ sempre es pot reduir a una altra $\sqrt[\delta]{B}$ a què equivalgui. En efecte, per a qualsevol valor d'aquella denotat per x, serà $x^n \equiv A$; ara, sigui t un valor qualsevol de l'expressió $\dfrac{\delta}{n}\,(\text{mòd.}\,p-1)$, que és evident, per l'article 31, que té valors reals, i serà $x^{tn} \equiv A^t$, però $x^{tn} \equiv x^\delta$, ja que $tn \equiv \delta\,(\text{mòd.}\,p-1)$. Per tant, $x^\delta \equiv A^t$, de manera que qualsevol valor de $\sqrt[n]{A}$ també serà un valor de $\sqrt[\delta]{A^t}$. Sempre, doncs, que $\sqrt[n]{A}$ té valors reals, serà completament equivalent a l'expressió $\sqrt[\delta]{A^t}$, ja que aquella no en té ni d'altres ni més pocs que aquesta; encara que quan $\sqrt[n]{A}$ no té cap valor real, no obstant això, podria resultar que $\sqrt[\delta]{A^t}$ tingués valors reals.

Exemple. Si se cerquen els valors de l'expressió $\sqrt[21]{2}\,(\text{mòd.}\,31)$, el màxim comú divisor dels nombres 21 i 30 serà 3, i algun valor de l'expressió $\dfrac{3}{21}\,(\text{mòd.}\,30)$, 3; per tant, si $\sqrt[21]{2}$ té valors reals, equivaldrà a l'expressió $\sqrt[3]{2^3}$, o sigui, a $\sqrt[3]{8}$, i es troba realment que els valors de la darrera expressió, que són 2, 10, 19, també satisfan la primera.

64. Perquè no ens exposem a haver d'emprendre en va aquesta operació, convé investigar la regla per la

qual es pugui discernir a l'instant si $\sqrt[n]{A}$ admetria valors reals o no. Si es té una taula d'índexs, la cosa és fàcil; efectivament, de l'article 60 és evident que es donen valors reals quan l'índex de A, presa una arrel primitiva qualsevol com a base, és divisible per δ, si no, no se'n donen. Però això també es pot trobar sense una tal taula. En efecte, posat $= k$ l'índex de A, si aquest és divisible per δ, $\dfrac{k(p-1)}{\delta}$ serà divisible per $p-1$, i recíprocament. Però l'índex del nombre $A^{\frac{p-1}{\delta}}$ serà $\dfrac{k(p-1)}{\delta}$. Per tant, si $\sqrt[n]{A}\,(\text{mòd.}\,p)$ té valors reals, $A^{\frac{p-1}{\delta}}$ serà congru a la unitat; si no, incongru. Així, a l'exemple de l'article precedent, es té que $2^{10} = 1024 \equiv 1\,(\text{mòd.}\,31)$, d'on es conclou que $\sqrt[21]{2}\,(\text{mòd.}\,31)$ té valors reals. Similarment, d'aquí ens assegurem que $\sqrt[2]{-1}\,(\text{mòd.}\,p)$ sempre tindrà dos valors reals quan p sigui de la forma $4m+1$, però cap quan p sigui de la forma $4m+3$, ja que $(-1)^{2m} = 1$ i $(-1)^{2m+1} = -1$. Aquest elegant teorema, que habitualment s'expressa així: *Si p és un nombre primer de la forma* $4m+1$*, es pot trobar un quadrat aa de manera que* $aa+1$ *resulti divisible per p; però si p és de la forma* $4m-1$*, no es dóna tal quadrat*, ha estat demostrat d'aquesta manera per l'il·lm. Euler a *Comm. nou. Acad. Petrop.* T. XVIII, p. 112, l'any 1773. Molt abans n'havia donat una altra demostració a *Comm. nou.* T. V, p. 5, que va aparèixer l'any 1760. En una dissertació prèvia, Comm. nou., T. IV, p. 25, encara no havia obtingut el fet. Més tard, també l'il·lm. La Grange transmeté una demostració del teorema a Nouveaux Mem. de l'Ac. de Berlin, A. 1775, p. 342. Encara donarem una altra demostració a la secció següent, on caldrà tractar pròpiament d'aquest tema.

65. Després que hem ensenyat a reduir totes les expressions $\sqrt[n]{A}\,(\text{mòd.}\,p)$ a altres on n és un divisor del nombre $p-1$ i que hem trobat un criteri perquè admeti valors reals o no, considerarem més acuradament tals expressions $\sqrt[n]{A}\,(\text{mòd.}\,p)$, on n és divisor de $p-1$. Primer mostrarem quina relació tindrien entre si cada un dels valors de l'expressió, després ensenyarem certs artificis amb l'auxili dels quals es podria trobar molt sovint un valor de l'expressió.

Primer, quan $A \equiv 1$ i r algun dels valors de l'expressió $\sqrt[n]{1}\,(\text{mòd.}\,p)$, o sigui, $r^n \equiv 1\,(\text{mòd.}\,p)$, totes les potències de r també seran valors de l'expressió; però, d'aquests, tants seran diferents com unitats té l'exponent a què pertany r (article 48). Així, doncs, si r és un valor que pertany a l'exponent n, les potències r, r^2, r^3, …, r^n, de r (on es pot substituir la *unitat* en lloc de l'última) contindran tots els valors de l'expressió $\sqrt[n]{1}\,(\text{mòd.}\,p)$. A la secció VIII explicarem més extensament quins recursos existeixen per a trobar els valors que pertanyin a l'exponent n.

Segon. Quan A és incongru a la unitat i de l'expressió $\sqrt[n]{A}\,(\text{mòd.}\,p)$ n'és conegut un, sigui z, els restants es dedueixen d'aquí d'aquesta manera. Siguin (tal com acabem de mostrar) $1,\ r,\ r^2,\ \ldots,\ r^{n-1}$, els valors de l'expressió $\sqrt[n]{1}$, i $z,\ zr,\ zr^2,\ \ldots,\ zr^{n-1}$, seran tots els valors de l'expressió $\sqrt[n]{A}$; com que tots aquests satisfan la congruència $x^n \equiv A$, d'això és evident que, posat qualsevol d'ells $\equiv zr^k$, la seva potència n-èsima, $z^n r^{nk}$, resulta còngrua a A, a causa que $r^n \equiv 1$ i $z^n \equiv A$; que són tots diferents, s'entén fàcilment de l'article 23; però l'expressió $\sqrt[n]{A}$ no pot tenir més valors que aquests, el nombre dels quals és n. Així, per exemple, si un valor de

l'expressió $\sqrt[2]{A}$ és z, l'altre serà $-z$. Finalment, d'aquí cal concloure que no es poden trobar tots els valors de l'expressió $\sqrt[n]{A}$, llevat que es coneguin simultàniament tots els valors de l'expressió $\sqrt[n]{1}$.

66. La segona cosa que ens havíem proposat, va ser ensenyar en quin cas es podria trobar directament un valor de l'expressió $\sqrt[n]{A}\,(\text{mòd.}\,p)$ (on se suposa que n és un divisor de $p-1$). Això esdevé quan algun valor surt congru a alguna potència de A, i com que aquest cas no ocorre rarament, no serà superflu entretenir-se una mica en aquest fet. Sigui, *si se'n dóna algun*, z un tal valor, o sigui, $z \equiv A^k$ i $A \equiv z^n\,(\text{mòd.}\,p)$. D'aquí es conclou que $A \equiv A^{kn}$; per tant, si es té un nombre k de manera que sigui $A \equiv A^{kn}$, A^k serà el valor cercat. Però a aquesta condició equival aquesta, que sigui $1 \equiv kn\,(\text{mòd.}\,t)$, on t designa l'exponent a què pertany A (articles 46, 48). Però, perquè aquesta congruència sigui possible, es requereix que n sigui primer amb t. En aquest cas serà $k \equiv \dfrac{1}{n}\,(\text{mòd.}\,t)$; però si n i t tenen un divisor comú, cap valor z no pot ser congru a una potència de A.

67. Però com que per a aquesta solució convindria conèixer t, vegem de quina manera podríem procedir si ignoréssim aquest nombre. En primer lloc, s'entén fàcilment que t ha de dividir $\dfrac{p-1}{n}$ suposat que $\sqrt[n]{A}\ (\text{mòd.}\,p)$ tingui valors reals, tal com sempre suposem aquí. En efecte, sigui y qualsevol valor i tant serà $y^{p-1} \equiv 1$ com $y^n \equiv A\ (\text{mòd.}\,p)$; per tant, elevant les parts de la darrera congruència a la potència $\dfrac{p-1}{n}$-èsima, resultarà $A^{\frac{p-1}{n}} \equiv 1$; de manera que $\dfrac{p-1}{n}$ és divisible per t (arti-

cle 48). Ara, si $\frac{p-1}{n}$ és primer amb n, la congruència de l'article precedent, $kn \equiv 1$, també es podrà resoldre segons el mòdul $\frac{p-1}{n}$ i, evidentment, un valor de k que satisfaci la congruència segons aquest mòdul també la satisfarà segons el mòdul t, que divideix $\frac{p-1}{n}$ (article 5). Llavors, doncs, s'ha trobat el que se cercava. Però si $\frac{p-1}{n}$ no és primer amb n, tots els factors primers de $\frac{p-1}{n}$ que simultàniament divideixen n es treuen de $\frac{p-1}{n}$. D'aquí trobarem el nombre $\frac{p-1}{nq}$, primer amb n, on q designa el producte de tots els factors primers que hem tret. Si ja té lloc la condició a què arribem a l'article precedent, que t sigui primer amb n, t també serà primer amb q, de manera que també dividirà $\frac{p-1}{nq}$. Per tant, si s'ha resolt la congruència $kn \equiv 1 \left(\text{mòd. } \frac{p-1}{nq}\right)$ (que es pot fer, ja que n és primer amb $\frac{p-1}{nq}$), el valor de k també satisfarà la congruència segons el mòdul t, cosa que se cercava. Tot aquest artifici consisteix a descobrir un nombre que pugui fer el paper de t, que ignorem. No obstant això, convé recordar perfectament que quan $\frac{p-1}{n}$ no és primer amb n, hem suposat que la condició de l'article precedent té lloc; si aquesta falla, totes les conclusions seran errònies; i si, seguint temeràriament les regles donades, es troba un valor per a z la n-èsima potència del qual no és còngrua a A, això és indici que la condició falla, de manera que aquest mètode no es pot aplicar en absolut.

68. Però també en aquest cas pot ser útil sovint assumir aquesta tasca; i val la pena la feina d'investigar de quina manera aquest valor fals portaria als vertaders. Així, suposem que s'han determinat nombres k, z, seguint les regles, però que z^n no és $\equiv A \,(\text{mòd.}\, p)$. Llavors, a condició que es puguin determinar els valors de l'expressió $\sqrt[n]{\frac{A}{z^n}}\,(\text{mòd.}\, p)$, obtindrem els valors de $\sqrt[n]{A}$ multiplicant cadascun d'ells per z. En efecte, si v és algun valor de $\sqrt[n]{\frac{A}{z^n}}$, serà $(vz)^n \equiv A$. Però l'expressió $\sqrt[n]{\frac{A}{z^n}}$ és més simple que $\sqrt[n]{A}$, tant que $\frac{A}{z^n}\,(\text{mòd.}\, p)$ pertany, sovint, a un exponent menor que A. Això és, si el màxim comú divisor dels nombres t, q, és d, $\frac{A}{z^n}\,(\text{mòd.}\, p)$ pertanyerà a l'exponent d, cosa que es demostra així. Substituït z pel seu valor, resulta $\frac{A}{z^n} \equiv \frac{1}{A^{kn-1}}\,(\text{mòd.}\, p)$. Però $kn-1$ és divisible per $\frac{p-1}{nq}$ (article precedent) i $\frac{p-1}{n}$ per t (igualment), o sigui, $\frac{p-1}{nd}$ per $\frac{t}{d}$. Però $\frac{t}{d}$ és primer amb $\frac{q}{d}$ (per hipòtesi); per tant, també $\frac{p-1}{nd}$ per $\frac{tq}{dd}$, o sigui $\frac{p-1}{nq}$ per $\frac{t}{d}$, de manera que $kn-1$ també serà divisible per $\frac{t}{d}$ i $(kn-1)d$ per t. D'aquí, $A^{(kn-1)d} \equiv 1\,(\text{mòd.}\, p)$. D'on es dedueix fàcilment que $\frac{A}{z^n}$ elevat a la potència d-èsima resulta congru a la unitat. Es pot demostrar, sens dubte fàcilment, que $\frac{A}{z^n}$ no podria pertànyer a un exponent menor que d, però no ens detenim en aquest fet ja que no es requereix

per al nostre fi. Així, doncs, podem estar segurs que $\frac{A}{z^n}$ (mòd. p) sempre pertany a un exponent menor que A, excepte en un únic cas, això és, quan t divideix q, de manera que $d = t$.

Però, en què ajudaria que $\frac{A}{z^n}$ pertanyés a un exponent menor que A? Es donen més nombres que poden ser A que els que poden ser $\frac{A}{z^n}$, i quan és l'ocasió d'obtenir més expressions de la forma $\sqrt[n]{A}$ segons el mateix mòdul, ens lucrem que en podem treure més de la mateixa font. Així, per exemple, sempre serà possible determinar almenys un valor de l'expressió $\sqrt[2]{A}$ (mòd. 29) si s'han donat a conèixer els valors de l'expressió $\sqrt[2]{-1}$ (mòd. 29) (que són ± 12). En efecte, es copsa fàcilment de l'article precedent que sempre es pot determinar directament un valor d'una expressió d'aquesta forma quan t és imparell, i d resultarà $= 2$ quan t és parell; però excepte -1, cap nombre no pertany a l'exponent 2.

Exemples. Se cerca $\sqrt[3]{31}$ (mòd. 37). Aquí $p - 1 = 36$, $n = 3$, $\frac{p-1}{3} = 12$, de manera que $q = 3$; així, doncs, ha de ser $3k \equiv 1$ (mòd. 4), que s'obté posant $k = 3$. D'aquí, $z \equiv 31^3$ (mòd. 37) $\equiv 6$, i es trobarà realment que $6^3 \equiv 31$ (mòd. 37). Si són coneguts els valors de l'expressió $\sqrt[3]{1}$ (mòd. 37), també es poden determinar els restants valors de l'expressió $\sqrt[3]{6}$. Aquells són 1, 10, 26; multiplicant 6 per aquests, apareixen els restants, $\equiv 23$ i 8.

Si se cerca el valor de l'expressió $\sqrt[2]{3}$ (mòd. 37), serà $n = 2$, $\frac{p-1}{n} = 18$; de manera que $q = 2$. D'aquí, ha

de ser $2k \equiv 1 \,(\text{mòd. } 9)$, d'on resulta $k \equiv 5 \,(\text{mòd. } 9)$. Per tant, $z \equiv 3^5 \equiv 21 \,(\text{mòd. } 37)$; però 21^2 no és $\equiv 3$, sinó $\equiv 34$; però $\dfrac{3}{34} \,(\text{mòd. } 37)$ és $\equiv -1$ i $\sqrt[2]{-1} \,(\text{mòd. } 37) \equiv \pm 6$; d'on s'obtenen els valors veritables $\pm 6 \cdot 21 \equiv \pm 15$.

Aquestes [proposicions] són, més o menys, les que es poden transmetre aquí de la solució de tals expressions. És palès que els mètodes directes sovint arriben a ser bastant llargs; però això tan incòmode no incumbeix a tots els mètodes directes en teoria de nombres; i per això hem jutjat que no s'ha de negligir mostrar com poden ser aquí d'útils. També convé observar aquí que no és la nostra intenció explicar amb rellevància els artificis particulars que no es mostren estranys a l'expert.

69. Retornem ara a les arrels que hem anomenat primitives. Hem mostrat que, presa una arrel primitiva qualsevol com a base, tots els nombres els índexs dels quals són primers amb $p - 1$ també seran arrels primitives, i cap més excepte aquests; d'on, simultàniament i espontàniament, s'ha donat a conèixer la quantitat d'arrels primitives (vegeu l'article 53). Però, en general, es deixa al nostre arbitri quina arrel primitiva volem adoptar per base; d'on s'entén que, també aquí, com en el càlcul logarítmic, es poden donar, en certa manera, més sistemes,* dels quals vegem amb quin vincle estan connectats. Siguin a, b, dues arrels primitives, m un altre nombre, $\equiv \beta$ l'índex del nombre b i $\equiv \mu \,(\text{mòd. } p-1)$ l'índex del nombre m quan es pren-

* Difereixen, però, en què, en logaritmes, el nombre de sistemes és infinit, però aquí n'hi ha tants com nombre d'arrels primitives. En efecte, evidentment, bases còngrues generen el mateix sistema.

gui a per base, però $\equiv \alpha$ l'índex del nombre a i $\equiv \nu\,(\text{mòd.}\,p-1)$ el del nombre m, quan es prengui b per base. Llavors serà $\alpha\beta \equiv 1\,(\text{mòd.}\,p-1)$; efectivament, $a^\beta \equiv b$, per tant, $a^{\alpha\beta} \equiv b^\alpha \equiv a\,(\text{mòd.}\,p)$ (per hipòtesi), d'aquí $\alpha\beta \equiv 1\,(\text{mòd.}\,p-1)$. Per un raonament similar es troba que $\nu \equiv \alpha\mu$ i $\mu \equiv \beta\nu\,(\text{mòd.}\,p-1)$. Així, doncs, si s'ha construït una taula d'índexs per a la base a, es pot convertir fàcilment en una altra on b és la base. En efecte, si per a la base a l'índex de b és $\equiv \beta$, per a la base b l'índex de a serà $\equiv \dfrac{1}{\beta}\,(\text{mòd.}\,p-1)$ i, multiplicant tots els índexs de la taula per aquest nombre, es tindran tots els índexs per a la base b.

70. Però encara que a un nombre donat li puguin atènyer molts índexs, agafades unes o altres arrels primitives per base, no obstant això, tots concordaran en què tots tindran el mateix màxim comú divisor amb $p-1$. En efecte, si per a la base a l'índex del nombre donat és m, i per a la base b, n, però els màxims comuns divisors μ, ν, d'aquests amb $p-1$ se suposen diferents, algun serà més gran, per exemple $\mu > \nu$, de manera que μ no dividirà n. Però, designat per α l'índex de a quan es pren b per base, serà (article precedent) $n \equiv \alpha m\,(\text{mòd.}\,p-1)$, de manera que μ també dividirà n, *Q. E. A.*

D'això també és evident que aquest màxim comú divisor dels índexs d'un nombre donat amb $p-1$ no depèn de la base, perquè és igual a $\dfrac{p-1}{t}$, on t designa l'exponent a què pertany el nombre sobre els índexs del qual es tracta. En efecte, si l'índex per a una base qualsevol és k, t serà el nombre mínim (excepte zero) que multiplicat per k esdevé un múltiple de $p-1$ (vegeu els articles 48, 58), o sigui, el valor mínim de l'expressió

$\frac{0}{k}$ (mòd. $p-1$) excepte zero; però que aquest és igual al màxim comú divisor dels nombres k i $p-1$, es deriva sense dificultat de l'article 29.

71. A més a més, es demostra fàcilment que sempre es pot agafar la base de manera que el nombre que pertany a l'exponent t obtingui un índex donat qualsevol, el màxim comú divisor del qual amb $p-1$ sigui $= \frac{p-1}{t}$. Per abreujar, designem aquest per d i sigui l'índex proposat $\equiv dm$ i l'índex del nombre proposat $\equiv dn$, quan s'agafa qualsevol arrel primitiva a per base; m, n, seran primers amb $\frac{p-1}{d}$, o sigui, amb t. Llavors, si ε és un valor de l'expressió $\frac{dn}{dm}$ (mòd. $p-1$) i, simultàniament, primer amb $p-1$, a^{ε} serà una arrel primitiva, per a la qual, presa per base, el nombre proposat obtindrà l'índex dm, com es desitjava (en efecte, serà $a^{\varepsilon dm} \equiv a^{dn} \equiv$ nombre proposat). Però que l'expressió $\frac{dn}{dm}$ (mòd. $p-1$) admet valors primers amb $p-1$, es prova així. Aquella expressió equival a la $\frac{n}{m}\left(\text{mòd. } \frac{p-1}{d}\right)$, o sigui, $\frac{n}{m}$ (mòd. t) (vegeu l'article 31, 2), i tots els seus valors seran primers amb t; en efecte, si algun valor e tingués un divisor comú amb t, aquest divisor també hauria de dividir me, de manera que també [hauria de dividir] n, que és congru a me segons t, contra la hipòtesi que n és primer amb t. Així, doncs, quan tots els divisors primers de $p-1$ també divideixen t, *tots* els valors de l'expressió $\frac{n}{m}$ (mòd. t) seran primers amb $p-1$, i la seva quantitat $= d$; però quan $p-1$ encara conté altres divisors primers f, g, h, etc.,

que no divideixen t, es posa $\equiv e$ un valor qualsevol de l'expressió $\frac{n}{m}$ (mòd. t). Llavors, però, com que tots els t, f, g, h, etc., són primers entre si, es pot trobar un nombre ε que resulti congru a e segons t, i segons f, g, h, etc., a nombres qualssevol primers amb aquests, respectivament (article 32). Així, tal nombre no és divisible per cap factor primer de $p-1$, de manera que serà primer amb $p-1$, com es desitjava. Finalment, es dedueix no difícilment de la teoria de combinacions que la quantitat de tals valors serà $= \frac{(p-1)(f-1)(g-1)(h-1)\cdot etc.}{t\,f\,g\,h\,etc.}$; però, perquè aquesta digressió no creixi en una mida excessiva, n'ometem la demostració, ja que no és especialment necessària per al nostre projecte.

72. Encara que, en general, sigui completament arbitrària quina arrel primitiva es prengui per base, no obstant això, a vegades algunes bases poden oferir cert avantatge especial sobre d'altres. A la taula I sempre hem pres per base el nombre 10 quan és arrel primitiva; en cas contrari, sempre hem determinat la base de manera que l'índex del nombre 10 hagi resultat el mínim possible; és a dir, $= \frac{p-1}{t}$, on t denota l'exponent a què pertany 10. Mostrarem què guanyem d'aquí a la secció VI, on s'aplicarà la mateixa taula encara per a altres usos. Però, com que aquí també pot restar quelcom d'arbitrari, com és evident de l'article precedent, perquè establíssim quelcom cert, d'entre totes les arrels primitives cercades que es presten, sempre hem elegit per base la *mínima*. Així, per a $p = 73$, on $t = 8$ i $d = 9$, a^{ε} té $\frac{72}{8}\cdot\frac{2}{3}$, és a dir, 6 valors, que són 5, 14, 20, 39, 40. Així, hem pres per base el mínim, 5.

73. Els mètodes per a trobar arrels primitives es basen, la major part, a temptejar. Si algú reuneix allò que hem ensenyat a l'article 55 amb el que transmetrem més avall sobre la solució de la congruència $x^n \equiv 1$, tindrà gairebé tot el que es pot obtenir per mètodes directes. L'il·lm. Euler confessa, a *Opusc. Analyt., T. I, p.* 152, que sembla extremament difícil assignar aquests nombres, i que la seva naturalesa és sotmesa als misteris més profunds dels nombres. Però temptejant de la manera següent es poden determinar bastant fàcilment. Qui hi estigui acostumat se sabrà socórrer per multitud d'artificis particulars en la prolixitat d'operacions; però això s'aprèn millor per molt hàbit que per preceptes.

1r. Es pren a voluntat un nombre primer amb p (designem el mòdul sempre així), a (sovint és molt útil per a la brevetat del càlcul si hem agafat el mínim possible, per exemple, el nombre 2), i es determina el seu període (article 46), és a dir, els residus mínims de les seves potències, fins que s'arriba a la potència a^t el residu mínim de la qual sigui 1.* Ara, si és $t = p - 1$, a és arrel primitiva.

2n. Però si $t < p - 1$, s'agafa un altre nombre b no contingut en el període de a i, de manera similar, s'investiga el seu període. Designat per u l'exponent a què pertany b, es copsa fàcilment que u no pot ser igual a t ni a una part alíquota seva; en efecte, en els dos casos resultaria $b^t \equiv 1$, que no pot ser ja que el període de a comprèn tots els nombres la potència d'exponent t

* Qualsevol copsarà espontàniament que no cal conèixer cap d'aquestes potències, ja que el residu mínim de cada una es pot obtenir fàcilment del residu mínim de la potència anterior.

dels quals és còngrua a la unitat (article 53). Si u fos $= p-1$, b serà arrel primitiva; però si u no és certament $= p-1$, sinó, en canvi, un múltiple de t, ja hem guanyat que existeix un nombre que pertany a un exponent més gran, de manera que ja som més propers al nostre objectiu, que és trobar un nombre que pertanyi a l'exponent *màxim*. Si u no és ni $= p-1$ ni un múltiple de t, podem trobar un nombre que pertanyi a un exponent més gran que t, u, naturalment, a l'exponent igual al mínim comú múltiple dels nombres t, u. Sigui aquest $= y$, i es descompon y en dos factors m, n, primers entre si de manera que un divideixi t i l'altre u.* Llavors resulti $\equiv A$ la potència $\frac{t}{m}$-èsima de a, $\equiv B\,(\text{mòd.}\,p)$ la potència $\frac{u}{n}$-èsima de b, i el producte AB serà un nombre que pertany a l'exponent y; en efecte, s'entén fàcilment que A pertany a l'exponent m, B a l'exponent n; de manera que el producte AB pertanyerà a mn, ja que m, n són primers entre si, cosa que es podrà provar directament de la mateixa manera com vàrem procedir a l'article 55, II.

3r. Ara, si $y = p-1$, AB serà arrel primitiva; si no, de manera similar a abans, es recorrerà a un altre nombre que no es presenti en el període de AB; i

* De quina manera es pot fer això es deriva sense dificultat de l'article 18. Es descompon y en factors tals que siguin, o bé nombres primers diferents, o bé potències de nombres primers diferents. Cadascun d'aquests dividirà algun dels nombres t, u (o també tots dos). S'assigna cadascun d'ells o bé al nombre t o bé al nombre u segons que divideixin aquell o aquest; quan algun divideix tots dos, és arbitrari a quin s'assigni; sigui $=m$ el producte dels que s'han assignat a t, $=n$ el producte dels restants, i es copsarà fàcilment que m divideix t, i n, u, i que és $mn=y$.

aquest, o bé serà una arrel primitiva, o bé pertanyerà a un exponent més gran que y, o bé es podrà trobar amb la seva ajuda (com abans) almenys un nombre que pertanyi a un exponent més gran que el de y. Així, doncs, com que els nombres que surten per repetició d'aquesta operació pertanyen a exponents contínuament creixents, és evident que finalment es descobrirà un nombre que pertanyi a l'exponent *màxim*; és a dir, arrel primitiva, *Q. E. F.*

74. Aquests preceptes resultaran més clars amb un exemple. Sigui $p = 73$, per al qual se cerca una arrel primitiva. Temptegem primer el nombre 2, el període del qual surt

$$\begin{array}{cccccccccccc} 1, & 2, & 4, & 8, & 16, & 32, & 64, & 55, & 37, & 1, & \textit{etc.} \\ 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & \textit{etc.} \end{array}$$

Així, doncs, com que la potència d'exponent 9 ja resulta còngrua a la unitat, 2 no és una arrel primitiva. Es tempteja un altre nombre que no ocorri en el període de 2, per exemple 3, el període del qual és

$$\begin{array}{ccccccccccc} 1, & 3, & 9, & 27, & 8, & 24, & 72, & 70, & 64, \\ 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, \end{array}$$

$$\begin{array}{cccccc} 46, & 65, & 49, & 1, & \textit{etc.} \\ 9, & 10, & 11, & 12, & \textit{etc.} \end{array}$$

Per tant, tampoc 3 no és arrel primitiva. Però el mínim comú múltiple dels exponents a què pertanyen 2, 3 (és a dir, els nombres 9, 12), és 36, que s'ha descompost en els factors 9 i 4 d'acord amb els preceptes de l'article precedent. Així, cal elevar 2 a la potència d'exponent $\frac{9}{9}$, és a dir, cal retenir el nombre 2; en canvi, 3 a la

potència d'exponent 3; el producte d'aquests és 54, que, així, pertanyerà a l'exponent 36. Finalment, si es calcula el període de 54 i es tempteja de nou un nombre no contingut en aquest, per exemple 5, s'obtindrà que aquest és una arrel primitiva.

75. Abans d'abandonar aquest argument transmetrem algunes proposicions que, malgrat la seva simplicitat, no semblen indignes d'atenció.

El producte de tots el termes del període d'un nombre qualsevol és $\equiv +1$*, quan la quantitat d'aquests, o sigui, l'exponent al qual pertany el nombre, és imparella, i* $\equiv -1$ *quan aquell exponent és parell.*

Exemple. Per al mòdul 13, el període del nombre 5 consta dels termes 1, 5, 12, 8, el producte dels quals és $480 \equiv -1 \,(\text{mòd. } 13)$.

Segons el mateix mòdul, el període del nombre 3 consta dels termes 1, 3, 9, el producte dels quals és $27 \equiv 1 \,(\text{mòd. } 13)$.

Dem. Sigui t l'exponent a què pertany el nombre i $\dfrac{p-1}{t}$ l'índex del nombre, cosa que sempre es pot fer si es determina correctament la base (article 71). Llavors, l'índex del producte de tots els termes del període serà: $\equiv (1+2+3+etc.+t-1)\dfrac{(p-1)}{t} = \dfrac{(t-1)(p-1)}{2}$; és a dir, $\equiv 0 \,(\text{mòd. } p-1)$ quan t és imparell, i $\equiv \dfrac{p-1}{2}$ quan t és parell; d'aquí, en el primer cas, aquell producte és $\equiv 1 \,(\text{mòd. } p)$; en el darrer, $\equiv -1 \,(\text{mòd. } p)$ (article 62). *Q. E. D.*

76. Si aquest nombre del teorema precedent és arrel primitiva, el seu període inclou tots els nombres 1, 2, 3, ..., $p-1$, i així, el seu producte sempre és $\equiv -1$ (perquè $p-1$ sempre és parell, exceptuat l'únic cas $p=2$ en què -1 i $+1$ equivalen). Aquest elegant teorema que se sol enunciar així: *el producte de tots els nombres menors que un nombre primer donat, augmentat en una unitat, és divisible per aquest primer*, fou presentat primer pel cèlebre Waring i atribuït al seu seguidor Wilson, *Meditt. algebr. Ed.* 3*, p.* 380. Però cap d'ells no el va poder demostrar, i el cèlebre Waring reconeix que la seva demostració sembla més difícil perquè no es podria formar cap *notació* que expressés un nombre primer. Però, al nostre judici, veritats d'aquest tipus s'han d'obtenir de nocions més que de notacions. Posteriorment, l'il·lm. La Grange en va donar una demostració a *Nouv. Mem. de l'Ac. de Berlin,* 1771. Es basa en la consideració dels coeficients originats pel desenvolupament del producte $(x+1)(x+2)(x+3)...(x+p-1)$. Això és, posat aquest producte $= x^{p-1} + Ax^{p-2} + Bx^{p-3} + etc. + Mx + N$, els coeficients A, B, etc., M, seran divisibles per p, però N serà $= 1\cdot 2\cdot 3\cdots(p-1)$. Ara, per a $x=1$, el producte és divisible per p; però llavors serà $\equiv 1+N \,(\text{mòd.}\, p)$; per tant, necessàriament $1+N$ es podrà dividir per p.

Finalment, l'il·lm. Euler, a *Opusc. analyt. T. I, p.* 329, en va donar una demostració que concorda amb la que nosaltres hem exposat aquí. Si tals homes no van jutjar aquest teorema indigne de les seves meditacions, esperem no ser reprovats si encara hi afegim una altra demostració.

77. Quan el producte de dos nombres a, b, és congru a la unitat segons el mòdul p, anomenarem *associats*

els nombres a, b, com l'il·lm. Euler. Llavors, segons la secció precedent, cada nombre positiu menor que p tindrà un associat positiu menor que p i, certament, únic. Es pot provar fàcilment que, dels nombres 1, 2, 3, ..., $p-1$, els 1 i $p-1$ són els únics que són associats a si mateixos; en efecte, els nombres associats a si mateixos seran arrels de la congruència $xx \equiv 1$, la qual, com que és de segon grau, no pot tenir més de dues arrels, és a dir, altres que 1 i $p-1$. Així, deixats de banda aquests, els nombres restants, 2, 3, ..., $p-2$, sempre seran associats a parells; per tant, el seu producte serà $\equiv 1$, de manera que el producte de tots els 1, 2, 3, ..., $p-1$ [serà] $\equiv p-1$, o sigui $\equiv -1$. *Q. E. D.*

Per exemple, per a $p = 13$, els nombres 2, 3, 4, ..., 11, s'associen així: 2 amb 7; 3 amb 9; 4 amb 10; 5 amb 8; 6 amb 11; això és, $2 \cdot 7 \equiv 1$; $3 \cdot 9 \equiv 1$; etc. D'aquí, $2 \cdot 3 \cdot 4 \cdots 11 \equiv 1$; de manera que $1 \cdot 2 \cdot 3 \cdots 12 \equiv -1$.

78. Però el teorema de Wilson es pot proposar més generalment així. *El producte de tots els nombres menors que un nombre donat* qualsevol A *i simultàniament primers amb ell, és congru segons* A *a la unitat, presa o bé positiva o bé negativa.* Cal prendre la unitat negativa quan A és de la forma p^m o bé $2p^m$, on p designa un nombre primer diferent de 2, i, a sobre, si $A = 4$; però en tots els casos restants, positiva. El teorema, tal com el va presentar el cèlebre Wilson, està contingut en el cas anterior. Per exemple, per a $A = 15$, el producte dels nombres 1, 2, 4, 7, 8, 11, 13, 14 és $\equiv 1 \,(\text{mòd. } 15)$. Per abreujar, no afegim la demostració; només observem que es pot acabar de manera similar a l'article precedent, excepte que la congruència $xx \equiv 1$ pot tenir més de dues arrels que exigeixen certes consideracions pe-

culiars. També es podria intentar una demostració de la consideració dels índexs, similarment a l'article 75, si s'aplica el que transmetrem després sobre els mòduls no primers.

79. Tornem a l'enumeració d'altres proposicions (article 75).

La suma de tots els termes del període de qualsevol nombre és $\equiv 0$, com en l'exemple de l'article 75, $1+5+12+8=26\equiv 0\,(\text{mòd. }13)$.

Dem. Sigui $=a$ el nombre del període del qual es tracta, i $=t$ l'exponent a què pertany, i la suma de tots els termes del període serà $\equiv 1+a+aa+a^3+etc.+a^{t-1}\equiv \dfrac{a^t-1}{a-1}\,(\text{mòd. }p)$. Però $a^t-1\equiv 0$; per tant, aquesta suma sempre serà $\equiv 0$ (article 22), si no és el cas que $a-1$ és divisible per p, o sigui, $a\equiv 1$; així, doncs, convé excloure aquest cas si, fins i tot, volem anomenar *període* un sol terme.

80. *El producte de totes les arrels primitives és* $\equiv 1$ excepte en l'únic cas $p=3$; en efecte, llavors es dóna només una arrel primitiva, 2.

Dem. Si es pren per base una arrel primitiva qualsevol, els índexs de totes les arrels primitives seran nombres primers amb $p-1$ i, simultàniament, menors que ell. Però la suma d'aquests nombres, és a dir, l'índex del producte de totes les arrels primitives, és $\equiv 0\,(\text{mòd. }p-1)$, de manera que el producte és $\equiv 1\,(\text{mòd. }p)$; en efecte, es copsa fàcilment que si k fos un nombre primer amb $p-1$, $p-1-k$ també seria primer amb $p-1$, de ma-

nera que parelles de nombres primers amb $p-1$ formen una suma divisible per $p-1$ (k no pot ser mai igual a $p-1-k$, excepte en el cas $p-1=2$, o sigui, $p=3$, que hem exceptuat; en efecte, evidentment, en tots els casos restants, $\frac{p-1}{2}$ no és primer amb $p-1$).

81. *La suma de totes les arrels primitives és o bé* $\equiv 0$ (quan $p-1$ és divisible per algun *quadrat*) *o bé* $\equiv \pm 1 \,(\text{mòd.}\, p)$ (quan $p-1$ és producte de nombres primers diferents; cal prendre el signe positiu si la seva quantitat és parella, però el negatiu, si és imparella).

Exemples. 1r., per a $p=13$, es tenen les arrels primitives 2, 6, 7, 11, la suma de les quals és $26 \equiv 0 \,(\text{mòd.}\, 13)$. 2n., per a $p=11$, les arrels primitives són 2, 6, 7, 8, la suma de les quals és $23 \equiv +1 \,(\text{mòd.}\, 11)$. 3r., per a $p=31$, les arrels primitives són 3, 11, 12, 13, 17, 21, 22, 24, la suma de les quals és $123 \equiv -1 \,(\text{mòd.}\, 31)$.

Dem. Hem demostrat més amunt (article 55, II) que si $p-1$ fos $= a^\alpha b^\beta c^\gamma \cdot etc.$ (on a, b, c, etc., designen nombres primers diferents) i A, B, C, nombres qualssevol que pertanyen respectivament als exponents a^α, b^β, c^γ, etc., tots els productes $ABC\,etc.$ representen arrels primitives. Però també es pot demostrar fàcilment que qualsevol arrel primitiva es pot representar per un producte d'aquest tipus i, certament, de manera única.*

* Això és, es determinen nombres $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, etc., de manera que sigui $\mathfrak{a} \equiv 1 \,(\text{mòd.}\, a^\alpha)$ i $\equiv 0 \left(\text{mòd.}\, b^\beta c^\gamma etc.\right)$, $\mathfrak{b} \equiv 1 \left(\text{mòd.}\, b^\beta\right)$ i $\equiv 0 \,(\text{mòd.}\, a^\alpha c^\gamma etc.)$ etc. (vegeu l'article 32), d'on resulta $\mathfrak{a} + \mathfrak{b} + \mathfrak{c} + etc. \equiv 1 \left(\text{mòd.}\, p-1\right)$ (article 19). Ara, si

D'on se segueix que es poden agafar aquests productes en lloc de les arrels primitives. Però, com que en aquests productes convé combinar tots els valors de A amb tots els valors de B, etc., la suma de tots els productes és igual al producte de la suma de tots els valors de A per la suma de tots els valors de B, per la suma de tots els valors de C, etc., com és sabut de la doctrina de les combinacions. Es designen tots els valors de A, B, etc., per A, A', A'', etc.; B, B', B'', etc.; etc., i la suma de totes les arrels primitives serà $\equiv (A + A' + etc.)(B + B' + etc.)$ etc. Ara, afirmo que si l'exponent α fos $= 1$, la suma $A + A' + A'' + etc.$ seria $\equiv -1 \,(\text{mòd. } p)$; en canvi, si fos $\alpha > 1$, aquesta suma seria $\equiv 0$, i, similarment, per als restants β, γ, etc. Així que aquestes [proposicions] seran demostrades, la veritat del nostre teorema serà evident. En efecte, quan $p - 1$ és divisible per algun quadrat, algun dels exponents α, β, γ, etc., superarà la unitat, de manera que algun dels factors al producte dels quals és còngrua la suma de totes les arrels primitives serà $\equiv 0$ i, per tant, també el producte; però quan $p-1$ no es pot dividir per cap quadrat, tots els exponents α, β, γ, etc., seran $= 1$, d'on la suma de totes les arrels primitives serà còngrua al producte de tants factors, cadascun dels quals és $\equiv -1$, com nombres a, b, c, etc., es tinguin, de manera que serà $\equiv \pm 1$ segons que la quantitat d'aquests nombres sigui parella o bé imparella. Però aquelles [proposicions] es proven així.

---

una arrel primitiva qualsevol, r, s'ha de representar per un producte $ABC\,etc.$, s'agafa $A \equiv r^{\mathfrak{a}}$, $B \equiv r^{\mathfrak{b}}$, $C \equiv r^{\mathfrak{c}}$, etc., i A pertanyerà a l'exponent a^{α}, B a l'exponent b^{β}, etc.; i el producte de tots els A, B, C, etc., serà $\equiv r \,\big(\text{mòd. } p\big)$; finalment, es copsa fàcilment que A, B, C, etc., no es poden determinar d'una altra manera.

1r. Quan $\alpha = 1$ i A és un nombre que pertany a l'exponent a, els restants nombres que pertanyen a aquest exponent seran A^2, A^3, ..., A^{a-1}. Però $1 + A + A^2 + A^3 + ... + A^{a-1}$ és la suma d'un període complet, de manera que és $\equiv 0$ (article 79); per tant, $A + A^2 + ... + A^{a-1} \equiv -1$.

2n. En canvi, quan $\alpha > 1$, i A és un nombre que pertany a l'exponent a^α, es tindran els nombres restants que pertanyen a aquest exponent si es rebutgen A^a, A^{2a}, A^{3a}, etc., de A^2, A^3, A^4, ..., $A^{a^\alpha - 1}$ (vegeu l'article 53); per tant, la seva suma serà $\equiv 1+A+A^2+...+A^{a^\alpha-1}-(1+A^a+A^{2a}+...+A^{a^\alpha-a})$, és a dir, còngrua a la diferència de dos períodes, de manera que $\equiv 0$. *Q. E. D.*

82. Tot el que hem exposat fins aquest punt es funda en la suposició que el mòdul és un nombre primer. Resta que considerem també el cas en què es prengui per mòdul un nombre compost. No obstant això, com que aquí no brillen propietats tan elegants com en el cas anterior, i tampoc no serien necessaris artificis subtils per a descobrir-les, sinó que gairebé totes es podrien descobrir millor per l'única aplicació dels principis precedents, aquí seria superflu i tediós exhaurir totes les minúcies. Així, exposarem breument quines d'aquest cas són comunes a l'anterior i quines pròpies.

83. Les proposicions dels articles 45–48 ja s'han demostrat generalment. Però la proposició de l'article 49 s'ha de modificar així.

Si f designa quants nombres es donen primers amb m i simultàniament menors que ell, és a dir, si $f = \varphi m$

(*article* 38), *l'exponent* t *de la potència mínima d'un nombre donat a primer amb* m *que és còngrua a la unitat segons el mòdul* m, *o bé serà* $= f$ *o bé una part alíquota d'aquest nombre.*

La demostració de la proposició de l'article 49 també pot valer en aquest cas, sempre que allà se substitueixin m en lloc de p, f en lloc de $p-1$, i, en lloc dels nombres 1, 2, 3, ..., $p-1$, els nombres primers amb m i simultàniament menors que m. Així, remetem aquesta al lector. D'altra banda, les altres demostracions de què hem parlat allà (articles 50, 51) no es poden aplicar a aquest cas sense molts subterfugis. Però, respecte de les proposicions següents, article 52 *i següents*, hi ha inherent una gran diferència entre els mòduls que són potències de nombres primers i aquells que es poden dividir per molts nombres primers. Així, contemplarem separadament els mòduls del primer tipus.

84. Si el mòdul és $m = p^n$, on p designa un nombre primer, serà $f = p^{n-1}(p-1)$ (article 38). Ara, si s'apliquen a aquest cas les disquisicions contingudes en els articles 51, 55, canviant el que cal canviar com hem prescrit a l'article precedent, es trobarà que tot el que s'ha demostrat allà també té lloc en aquest cas, sempre que abans s'hagi provat que una congruència de la forma $x^t - 1 \equiv 0 \,(\text{mòd.}\, p^n)$ no pot tenir més de t arrels diferents. Per a un mòdul primer, vàrem deduir aquesta veritat de la proposició més general de l'article 43, que en tota la seva extensió, però, només és vàlida per a mòduls primers i no s'ha d'aplicar així a aquest cas. No obstant això, demostrarem per un mètode singular que la proposició és veritat per a aquest cas particular. Més avall (secció VIII) ensenyarem a trobar-la més fàcilment.

85. Ens proposem demostrar aquest teorema: *Si el màxim comú divisor dels nombres* t *i* $p^{n-1}(p-1)$ *és* e*, la congruència* $x^t \equiv 1\,(\text{mòd.}\,p^n)$ *tindrà* e *arrels diferents.*

Sigui $e = kp^\nu$, de manera que k no contingui el factor p, i així divideixi el nombre $p-1$. Llavors, la congruència $x^t \equiv 1$ tindrà k arrels diferents segons el mòdul p; designades aquestes per A, B, C, etc., una arrel qualsevol d'aquesta congruència segons el mòdul p^n, ha de ser còngrua segons el mòdul p a algun dels nombres A, B, C, etc. Ara demostrarem que la congruència $x^t \equiv 1\,(\text{mòd.}\,p^n)$ té p^ν arrels còngrues a A segons el mòdul p, unes altres tantes a B, etc. Fet això, el nombre de totes les arrels serà kp^ν o sigui e, tal com hem afirmat. Acabarem aquella demostració de manera que, *primer*, mostrem que si α fos una arrel còngrua a A segons el mòdul p, també $\alpha + p^{n-\nu}$, $\alpha + 2p^{n-\nu}$, $\alpha + 3p^{n-\nu}$, …, $\alpha + (p^\nu - 1)p^{n-\nu}$, serien arrels; *segon*, que no poden ser arrels altres nombres congrus a A segons el mòdul p que els que estiguin compresos en la forma $\alpha + hp^{n-\nu}$ (on h denota un enter qualsevol); d'on, evidentment, es tindran p^ν arrels diferents i no més; i el mateix també tindrà lloc per a les arrels que són còngrues a cada un dels B, C, etc.; *tercer*, ensenyarem de quina manera es podria trobar sempre una arrel còngrua a A segons el mòdul p.

86. Teorema. *Si, com a l'article precedent,* t *és un nombre divisible per* p^ν *però no per* $p^{\nu+1}$*, serà* $(\alpha + hp^\mu)^t - \alpha^t \equiv 0\ (\text{mòd.}\,p^{\mu+\nu})$*, però* $\equiv \alpha^{t-1}hp^\mu t\ \big(\text{mòd.}\,p^{\mu+\nu+1}\big)$. La darrera part del teorema no té lloc quan $p = 2$ i simultàniament $\mu = 1$.

Es podria atacar la demostració d'aquest teorema pel desenvolupament de la potència d'un binomi, si es mostrés que tots els termes posteriors al segon són divisibles per $p^{\mu+\nu+1}$. Però com que la consideració dels denominadors dels coeficients condueix a algunes ambigüitats, preferim el mètode següent.

Suposem, *primer*, $\mu > 1$ i $\nu = 1$ i, a causa que $x^t - y^t = (x-y)(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + etc. + y^{t-1})$, serà $(\alpha+hp^\mu)^t - \alpha^t = hp^\mu((\alpha+hp^\mu)^{t-1} + (\alpha+hp^\mu)^{t-2}\alpha + etc. + \alpha^{t-1})$. Però és $\alpha + hp^\mu \equiv \alpha \,(\text{mòd.}\, p^2)$; per tant, cada terme $(\alpha + hp^\mu)^{t-1}$, $(\alpha + hp^\mu)^{t-2}\alpha$, etc., serà $\equiv \alpha^{t-1} \,(\text{mòd.}\, p^2)$ de manera que la suma de tots $\equiv t\alpha^{t-1} \,(\text{mòd.}\, p^2)$, o sigui, de la forma $t\alpha^{t-1} + Vp^2$, on V denota un nombre qualsevol. D'aquí, $(\alpha + hp^\nu)^t - \alpha^t$ serà de la forma $\alpha^{t-1}hp^\mu t + Vhp^{\mu+2}$, és a dir, $\equiv \alpha^{t-1}hp^\mu t \,(\text{mòd.}\, p^{\mu+2})$ i $\equiv 0 \,(\text{mòd.}\, p^{\mu+1})$. I així, el teorema s'ha demostrat per a aquest cas.

Ara, si el teorema no fos vertader per a altres valors de ν, mantenint encara $\mu > 1$, es donaria necessàriament algun límit fins al qual el teorema sempre seria vertader, i més enllà fals. Sigui $= \phi$ el valor mínim de ν per al qual és fals, d'on es copsa fàcilment que, si t fos divisible per $p^{\phi-1}$ però no per p^ϕ, el teorema encara és vertader, però fals si se substitueix tp en lloc de t. Així, tenim que

$$(\alpha + hp^\mu)^t \equiv \alpha^t + \alpha^{t-1}hp^\mu t \,(\text{mòd.}\, p^{\mu+\phi}),$$

o sigui, $= \alpha^t + \alpha^{t-1}hp^\mu t + up^{\mu+\phi}$, on u denota un nombre indeterminat. Però com que per a $\nu = 1$ el teorema ja s'ha demostrat, serà $(\alpha^t + \alpha^{t-1}hp^\mu t + up^{\mu+\phi})^p \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu+1} + \alpha^{tp-t}up^{\mu+\phi+1} \,(\text{mòd.}\, p^{\mu+\phi+1})$, de manera que $(\alpha+hp^\mu)^{tp} \equiv \alpha^{tp} + \alpha^{tp-1}hp^\mu tp \,(\text{mòd.}\, p^{\mu+\phi+1})$; és a

dir, el teorema també és vertader si se substitueix tp en lloc de t, és a dir, també per a $\nu = \phi + 1$, contràriament a la hipòtesi. D'on és evident que el teorema és vertader per a tots els valors de ν.

87. Resta el cas en què $\mu = 1$. Per un mètode completament similar al que hem usat a l'article precedent, es pot demostrar sense l'ajut del teorema del binomi que és

$$\begin{aligned}(\alpha + hp)^{t-1} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \,\big(\text{mòd.}\, p^2\big)\\ \alpha(\alpha + hp)^{t-2} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp\\ \alpha\alpha(\alpha + hp)^{t-3} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp\\ &\textit{etc.},\end{aligned}$$

d'on la suma (com que la quantitat de parts és $= t$) serà

$$\equiv t\alpha^{t-1} + \frac{(t-1)t}{2}\alpha^{t-2}hp \,\big(\text{mòd.}\, p^2\big).$$

Però com que t és divisible per p, $\dfrac{(t-1)t}{2}$ també serà divisible per p en tots els casos excepte aquell en què $p = 2$, del qual ja hem advertit en l'article precedent. Però en els casos restants serà $\dfrac{(t-1)t}{2}\alpha^{t-2}hp \equiv 0$ $\big(\text{mòd.}\, p^2\big)$, de manera que també aquella suma $\equiv t\alpha^{t-1}$ $\big(\text{mòd.}\, p^2\big)$ com a l'article precedent. Per la resta, aquesta demostració transcorre de la mateixa manera que aquella.

Així, doncs, obtenim en general, exceptuat l'únic cas $p = 2$, que és $(\alpha + hp^\mu)^t \equiv \alpha^t \,(\text{mòd.}\, p^{\mu+\nu})$, i $(\alpha +$

$hp^{\mu})^t$ no és $\equiv \alpha^t$ per a cap mòdul que sigui una potència de p més alta que $p^{\mu+\nu}$, sempre que h no és divisible per p, i p^{ν}, la potència més gran de p que divideix el nombre t.

D'aquí es deriven directament les proposicions 1 i 2 que ens havíem proposat de demostrar a l'article 85; això és,

primer, sempre que $\alpha^t \equiv 1$, també serà $(\alpha+hp^{n-\nu})^t \equiv 1 \pmod{p^n}$;

segon, si algun nombre α' és congru a A segons el mòdul p i, d'aquesta manera, també a α, però no a aquest segons el mòdul $p^{n-\nu}$, i si satisfà la congruència $x^t \equiv 1 \pmod{p^n}$, posem que α' és $= \alpha + lp^{\lambda}$, de manera que l no sigui divisible per p, i serà $\lambda < n - \nu$; però, llavors, $(\alpha + lp^{\lambda})^t$ serà congru a α^t segons el mòdul $p^{\lambda+\nu}$, però no segons el mòdul p^n, que és una potència més alta; per tant, α' no pot ser arrel de la congruència $x^t \equiv 1$.

88. *El tercer*, però, fou trobar alguna arrel de la congruència $x^t \equiv 1 \pmod{p^n}$ còngrua a A. Aquí només mostrarem de quina manera es podria fer això si ja es coneguées una arrel de la mateixa congruència segons el mòdul p^{n-1}; evidentment, això és suficient, ja que podríem avançar del mòdul p, per al qual A és arrel, al mòdul p^2, i així, successivament, a totes les potències consecutives.

Així, sigui α una arrel de la congruència $x^t \equiv 1 \left(\text{mòd.}\, p^{n-1}\right)$, i se cerca una arrel d'aquesta mateixa congruència segons el mòdul p^n; posem $= \alpha + hp^{n-\nu-1}$ aquesta, que se segueix de l'article precedent que ha de

tenir aquesta forma (posteriorment, considerarem separadament el cas en què $\nu = n-1$; ν no pot ser més gran que $n-1$). Així, ha de ser $(\alpha+hp^{n-\nu-1})^t \equiv 1\,(\text{mòd.}\,p^n)$. Però $(\alpha + hp^{n-\nu-1})^t \equiv \alpha^t + \alpha^{t-1}htp^{n-\nu-1}\,(\text{mòd.}\,p^n)$. Així, si es determina h de manera que resulti $1 \equiv \alpha^t + \alpha^{t-1}htp^{n-\nu-1}\,(\text{mòd.}\,p^n)$; o sigui (ja que per hipòtesi $1 \equiv \alpha^t\,(\text{mòd.}\,p^{n-1})$ i t és divisible per p^ν), de manera que $\dfrac{\alpha^t-1}{p^{n-1}} + \alpha^{t-1}h\dfrac{t}{p^\nu}$ resulti divisible per p, el que se cerca s'haurà executat. Que això es pot fer sempre, és evident de la secció precedent, ja que aquí suposaríem que t no es pot dividir per una potència més alta de p que p^ν, de manera que $\alpha^{t-1}\dfrac{t}{p^\nu}$ seria primer amb p.

Però si $\nu = n-1$, és a dir, si t és divisible per p^{n-1}, o sigui, també per una potència més alta de p, cada valor de A que satisfaci la congruència $x^t \equiv 1$ segons el mòdul p, també la satisfarà segons el mòdul p^n. En efecte, sigui $t = p^{n-1}\tau$, i serà $t \equiv \tau\,(\text{mòd.}\,p-1)$; per tant, com que $A^t \equiv 1\,(\text{mòd.}\,p)$, també serà $A^\tau \equiv 1\,(\text{mòd.}\,p)$. Així, es posa $A^\tau = 1+hp$ i serà $A^t = (1+hp)^{p^{n-1}} \equiv 1\,(\text{mòd.}\,p^n)$, article 87.

89. Tot el que hem descobert a l'article 57 i següents, amb l'ajut del teorema que la congruència $x^t \equiv 1$ no té més de t arrels diferents, també té lloc per a un mòdul que és una potència d'un nombre primer; i si s'anomenen *arrels primitives* els nombres que pertanyen a l'exponent $p^{n-1}(p-1)$, o sigui, en el període dels quals es troben tots els nombres no divisibles per p, també existiran aquí arrels primitives. Però també es pot aplicar a aquest cas tot allò que hem transmès més amunt sobre els índexs i el seu ús i també sobre la reso-

lució de la congruència $x^t \equiv 1$. Com que això no estaria subjecte a cap dificultat, seria superflu repetir-ho tot íntegrament. A part d'això, hem ensenyat a deduir les arrels de la congruència $x^t \equiv 1$ segons el mòdul p^n de les arrels de la mateixa congruència segons el mòdul p. Però encara s'han d'afegir algunes [proposicions] del cas on alguna potència del nombre 2 és el mòdul, ja que s'ha exceptuat més amunt.

90. *Si s'agafa per mòdul alguna potència del nombre* 2 *més alta que la segona, posem* 2^n*, la potència d'exponent* 2^{n-2} *de cada nombre imparell és còngrua a la unitat.*

Per exemple, $3^8 = 6561 \equiv 1 \,(\text{mòd. } 32)$.

En efecte, cada nombre imparell està comprès, o bé en la forma $1+4h$, o bé en la $-1+4h$; d'on la proposició se segueix directament (teorema de l'article 85).

Així, doncs, com que l'exponent a què pertany qualsevol nombre imparell segons el mòdul 2^n ha de ser un divisor de 2^{n-2}, cada un pertanyerà a algun dels nombres 1, 2, 4, 8, …, 2^{n-2}; es decideix fàcilment a quin pertanyerà, realment, així. Sigui $= 4h \pm 1$ el nombre proposat, i $= m$ l'exponent de la màxima potència del nombre 2 que divideix h (que també pot ser $= 0$, això és, quan h és imparell); llavors, l'exponent a què pertany el nombre proposat serà $= 2^{n-m-2}$ suposat que $n > m+2$; però si $n =$ o bé $< m+2$, el nombre proposat és $\equiv \pm 1$ i, d'aquesta manera, o bé pertanyerà a l'exponent 1 o bé a l'exponent 2. En efecte, es dedueix sense dificultat de l'article 86 que un nombre de la forma $\pm 1 + 2^{m+2}k$ (al qual equival $4h \pm 1$) elevat a la potència d'exponent

2^{n-m-2} resultarà congru a la unitat segons el mòdul 2^n, però incongru, [elevat] a la potència d'un exponent que és una potència inferior del nombre 2. Així, un nombre qualsevol de la forma $8k+3$ o bé $8k+5$ pertanyerà a l'exponent 2^{n-2}.

91. D'això és clar que aquí no es donen *arrels primitives* en el sentit que més amunt hem adoptat per a l'expressió, això és, cap nombre el període del qual comprengui tots els nombres menors que el mòdul i primers amb ell. No obstant això, es copsa fàcilment que aquí hi ha un anàleg. En efecte, es troba que una potència d'exponent imparell d'un nombre de la forma $8k+3$ sempre és de la forma $8k+3$, en canvi, una potència d'exponent parell, sempre de la forma $8k+1$; així, doncs, cap potència no pot ser de la forma $8k+5$ o bé $8k+7$. Per tant, com que el període d'un nombre de la forma $8k+3$ consta de 2^{n-2} termes diferents, cada un dels quals és de la forma $8k+3$ o bé de la $8k+1$, i com que no es donen més de 2^{n-2} nombres d'aquesta forma menors que el mòdul, evidentment, cada nombre de la forma $8k+1$ o bé $8k+3$ és congru segons el mòdul 2^n a alguna potència de qualsevol nombre de la forma $8k+3$. Es pot mostrar de manera similar que el període d'un nombre de la forma $8k+5$ comprèn tots els nombres de les formes $8k+1$ i $8k+5$. Així, doncs, si es pren per base un nombre de la forma $8k+5$, presos positius tots els nombres de la forma $8k+1$ i $8k+5$, i negatius tots els de la forma $8k+3$ i $8k+7$, s'obtindran índexs reals, i aquí s'han de tenir certament per equivalents els índexs congrus segons 2^{n-2}. Cal entendre d'aquesta manera la nostra taula I, on per als mòduls 16, 32 i 64 (ja que per al mòdul 8 no serà necessària cap taula) sempre hem agafat per base el nombre 5. Per exemple, al nombre 19, que és

de la forma $8n+3$, de manera que cal prendre'l *negatiu*, li correspon l'índex 7 per al mòdul 64, la qual cosa significa que és $5^7 \equiv -19\,(\text{mòd. } 64)$. Però presos negatius els nombres de les formes $8n+1$, $8n+5$, i positius els nombres de les formes $8n+3$, $8n+7$, s'haurien d'atribuir índexs en certa manera imaginaris. Introduint aquests, el càlcul dels índexs es pot reduir a l'algoritme més simple possible. Però, com que si volguéssim exposar això amb tot rigor caldria estendre's massa lluny, ens reservem aquest treball per a una altra ocasió, quan potser ens encarreguem d'examinar més abundantment la teoria de les quantitats imaginàries, que, certament, segons el nostre judici, no ha estat reduïda per ningú fins ara a nocions clares. Els experts trobaran fàcilment aquest algoritme per ells mateixos; els que estiguin menys entrenats, com aquells que ignoren els comentaris més recents sobre els *logaritmes* imaginaris, podran, no obstant això, usar igualment aquesta taula servint-se dels logaritmes, sempre que tinguin perfectament establerts els principis de més amunt.

92. Gairebé tot el que pertany als residus de potències segons un mòdul compost de molts nombres primers es pot deduir de la teoria general de les congruències; com que més avall ensenyarem més abundantment a reduir congruències qualssevol segons un mòdul compost de molts primers a congruències el mòdul de les quals és primer o potència de primer, no és això amb què ens detindrem molt aquí. Només observem que la bellíssima propietat que té lloc per als restants mòduls, això és, que sempre existeixen mòduls el període dels quals comprèn tots els nombres primers amb el mòdul, aquí falla amb l'excepció d'un únic cas, això és, quan

el mòdul és el doble d'un nombre primer o bé d'una potència d'un nombre primer. En efecte, si el mòdul m es redueix a la forma $A^aB^bC^c\,etc.$, on A, B, C, etc., designen nombres primers diferents, a part d'això, es designa $A^{a-1}(A-1)$ per α, $B^{b-1}(B-1)$ per β, etc., i si, finalment, z és un nombre primer amb m, serà $z^\alpha \equiv 1\,(\text{mòd.}\,A^a)$, $z^\beta \equiv 1\,\big(\text{mòd.}\,B^b\big)$, etc. Així, doncs, si μ és el mínim comú múltiple dels nombres α, β, γ, etc., serà $z^\mu \equiv 1$ segons tots els mòduls A^a, B^b, etc., de manera que, també, segons m, que és igual al seu producte. Però, amb l'excepció del cas en què m és el doble d'un nombre primer o bé d'una potència d'un nombre primer, el mínim comú múltiple dels nombres α, β, γ, etc., és menor que el seu producte (ja que els nombres α, β, γ, etc., no poden ser primers entre ells, sinó que tenen almenys el divisor comú 2). I així, el període de cap nombre no pot comprendre tants termes com nombres es donen primers amb el mòdul i menors que ell, ja que el nombre d'aquests és igual al producte dels α, β, γ, etc. Així, per exemple, per a $m = 1001$, la potència d'exponent 60 de qualsevol nombre primer amb m és còngrua a la unitat, ja que 60 és múltiple comú dels nombres 6, 10, 12. No obstant això, el cas en què el mòdul és el doble d'un nombre primer, o bé el doble d'una potència d'un nombre primer, és completament similar a aquell en què és primer o bé potència d'un primer.

93. Ja s'ha fet menció pertot arreu dels escrits en què altres geòmetres s'han ocupat de l'argument tractat en aquesta secció. No obstant això, enviem a aquells que desitgen explicat més abundantment allò que la brevetat ens ha permès, sobretot als comentaris següents de l'il·lm. Euler, recomanables al màxim per la perspicuï-

tat per la qual aquest gran home sempre va excel·lir per sobre de tots.

Theoremata circa residua ex diuisione potestatum relicta. Com. nou. Petr. T. VII., p. 49 i s.

Demostrationes circa residua ex diuisione potestatum per numeros primos resultantia. Ibid T. XVIII, p. 85 i s.

Es poden afegir a aquestes, *Opusculorum analyt.* T. I, *dissertt.* 5 i 8.

Secció Quarta

de les

CONGRUÈNCIES DE SEGON GRAU

94. Teorema. *Pres per mòdul un nombre qualsevol m, d'entre els nombres* 0, 1, 2, 3, ..., $m-1$, *no poden resultar congrus a un quadrat més de* $\frac{1}{2}m+1$, *quan* m *és parell, o bé més de* $\frac{1}{2}m+\frac{1}{2}$, *quan* m *és imparell.*

Dem. Com que els quadrats de nombres congrus són congrus, qualsevol nombre que pot resultar congru a un quadrat també serà congru a algun quadrat l'arrel del qual és $< m$. Així, és suficient considerar els residus mínims dels quadrats 0, 1, 4, 9, ..., $(m-1)^2$. Es copsa fàcilment que és $(m-1)^2 \equiv 1$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$, etc. D'aquí, també, quan m és parell, els residus mínims dels quadrats $\left(\frac{1}{2}m-1\right)^2$ i $\left(\frac{1}{2}m+1\right)^2$, $\left(\frac{1}{2}m-2\right)^2$ i $\left(\frac{1}{2}m+2\right)^2$, etc., seran els mateixos; però quan m és imparell, els quadrats $\left(\frac{1}{2}m-\frac{1}{2}\right)^2$ i $\left(\frac{1}{2}m+\frac{1}{2}\right)^2$,

$\left(\frac{1}{2}m - \frac{3}{2}\right)^2$ i $\left(\frac{1}{2}m + \frac{3}{2}\right)^2$, etc., seran congrus. D'on és palès que no poden resultar congrus a un quadrat altres nombres que els que siguin congrus a algun dels quadrats 0, 1, 4, 9, ..., $\left(\frac{1}{2}m\right)^2$, quan m és parell; en canvi, quan és imparell, qualsevol nombre que sigui congru a algun quadrat és congru necessàriament a algun dels 0, 1, 4, 9, ..., $\left(\frac{1}{2}m - \frac{1}{2}\right)^2$. Per tant, en el primer cas es donaran, com a molt, $\frac{1}{2}m + 1$ residus mínims diferents, en el darrer, $\frac{1}{2}m + \frac{1}{2}$. *Q. E. D.*

95. *Exemple.* Segons el mòdul 13, dels quadrats dels nombres 0, 1, 2, 3, ..., 6, es troben els residus mínims 0, 1, 4, 9, 3, 12, 10; però, després, aquests mateixos es recorren en l'ordre invers, 10, 12, 3, etc. Per tant, cada nombre no congru a cap d'aquests residus, o sigui, congru a algun dels 2, 5, 6, 7, 8, 11, no pot ser congru a cap quadrat.

Segons el mòdul 15, es troben els residus 0, 1, 4, 9, 1, 10, 6, 4, després dels quals es recorren els mateixos en l'ordre invers. Aquí, doncs, el nombre de residus que poden resultar congrus a un quadrat encara és menor que $\left(\frac{1}{2}m + \frac{1}{2}\right)$, ja que són 0, 1, 4, 6, 9, 10. Els nombres 2, 3, 5, 7, 8, 11, 12, 13, 14, i els que són congrus a algun d'aquests, no poden resultar congrus a cap quadrat segons el mòdul 15.

D'aquí es conclou que, per a qualsevol mòdul, tots els nombres es poden separar en dues classes, una de les quals contindria els nombres que puguin resultar con-

grus a un quadrat, l'altra els que no puguin. Anomenarem aquells *residus quadràtics d'aquest nombre que hem agafat per mòdul*,* aquests, *no-residus quadràtics*, o també, quan d'això no es pot originar cap ambigüitat, més simplement *residus* i *no-residus*. D'altra banda, és palès que és suficient si tots els nombres 0, 1, 2, ..., $m-1$, s'han reduït a classes; en efecte, nombres congrus s'hauran d'assignar a la mateixa classe.

També començarem aquesta disquisició amb els mòduls primers, i així, caldrà sobreentendre això encara que no es recordi expressament. Però cal excloure el nombre primer 2, o sigui, només s'han de considerar els nombres primers *imparells*.

96. *Pres per mòdul un nombre primer p, la meitat dels nombres* $1, 2, 3, \ldots, p-1$, *seran residus quadràtics, els restants, no-residus; és a dir, es donaran* $\frac{1}{2}(p-1)$ *residus, i la mateixa quantitat de no-residus.*

En efecte, es prova fàcilment que tots els quadrats $1, 4, 9, \ldots, \frac{(p-1)^2}{4}$, són incongrus. Això és, si pogués resultar $rr \equiv r'r' \,(\text{mòd.}\, p)$ i els nombres r, r', diferents i no més grans que $\frac{1}{2}(p-1)$, posat $r > r'$, cosa que és lícita, $(r-r')(r+r')$ resultaria positiu i divisible per p.

* En particular, per a aquest cas s'usa un segon sentit, diferent de com hem fet fins aquí. Això és, convindria dir que r és residu del quadrat aa segons el mòdul m quan $r \equiv aa$ (mòd. m); però en aquesta secció, per abreujar, sempre anomenem r residu quadràtic *de* m, i d'aquí no s'ha de témer cap ambigüitat. En efecte, a partir d'aquí no utilitzarem l'expressió *residu* quan significa el mateix que nombre congru, llevat que el discurs sigui de residus *mínims*, on no hi pot haver cap dubte.

Però cada un dels factors $r-r'$ i $r+r'$ és menor que p; per tant, la suposició no pot ser consistent (article 13). Així, es tenen $\frac{1}{2}(p-1)$ residus quadràtics continguts entre els nombres 1, 2, 3, ..., $p-1$; entre aquests, no n'hi poden haver més, ja que afegint-hi el residu 0 n'apareixen $\frac{1}{2}(p+1)$, nombre que no pot superar la quantitat de tots els residus. Per tant, els nombres restants seran no-residus, i la seva quantitat $= \frac{1}{2}(p-1)$.

Com que el zero sempre és un residu, excloem aquest i els nombres divisibles pel mòdul d'aquestes investigacions, ja que aquest cas és clar per ell mateix i només pertorbaria la concisió dels teoremes. També hem exclòs el mòdul 2 per la mateixa causa.

97. Com que moltes de les [proposicions] que exposarem en aquesta secció també es podrien derivar dels principis de la secció precedent, i no és inútil escrutar la mateixa veritat per mètodes diferents, mostrarem aquest nexe. S'entén fàcilment que tots els nombres congrus a un quadrat tenen índexs *parells;* al contrari, els que no poden resultar de cap manera congrus a un quadrat, imparells. Com que $p-1$ és un nombre parell, hi haurà tants índexs parells com imparells, això és, $\frac{1}{2}(p-1)$, i es donarà la mateixa quantitat tant de residus com de no-residus.

Exemple.

Per als mòduls	els residus són
3	1,
5	1, 4,
7	1, 2, 4,

11	1, 3, 4, 5, 9,
13	1, 3, 4, 9, 10, 12,
17	1, 2, 4, 8, 9, 13, 15, 16,

etc.,

els nombres restants menors que aquests mòduls són no-residus.

98. Teorema. *El producte de dos residus quadràtics d'un nombre primer p és un residu; el producte d'un residu i un no-residu és un no-residu; finalment, el producte de dos no-residus, un residu.*

Dem. I. Siguin A, B, els residus originats pels quadrats aa, bb, o sigui, $A \equiv aa$, $B \equiv bb$, i el producte AB serà congru al quadrat del nombre ab; és a dir, un residu.

II. Quan A és un residu, posem $\equiv aa$, però B un no-residu, AB serà un no-residu. En efecte, si se suposa que pot resultar $AB \equiv kk$, sigui $\equiv b$ el valor de l'expressió $\frac{k}{a}$ (mòd. p); així, serà $aaB \equiv aabb$, d'on $B \equiv bb$, és a dir, B un residu, contràriament a la hipòtesi.

Una altra. Es multipliquen per A tots els nombres entre els 1, 2, 3, $\ldots$, $p-1$, que són residus (la quantitat dels quals és $= \frac{1}{2}(p-1)$), i tots els productes seran residus quadràtics i, certament, tots seran incongrus. Ara, si un no-residu B es multiplica per A, el producte no serà congru a cap dels productes que ja es tenen; per tant, si fos un residu, es tindrien $\frac{1}{2}(p+1)$ residus incongrus entre els quals encara no hi ha el residu zero, contra l'article 96.

III. Siguin A, B, no-residus. Es multipliquen per A tots els nombres entre els 1, 2, 3, $\ldots$, $p-1$, que són residus, i es tindran $\frac{1}{2}(p-1)$ no-residus incongrus entre si (II); ara, el producte AB no pot ser congru a cap d'aquells; així, doncs, si fos un no-residu, es tindrien $\frac{1}{2}(p+1)$ no-residus incongrus entre si, contra l'article 96. Per tant, el producte etc. *Q. E. D.*

Aquests teoremes es deriven encara més fàcilment dels principis de la secció precedent. En efecte, com que els índexs dels residus sempre són parells, però els dels no-residus, imparells, l'índex del producte de dos residus o bé no-residus serà parell, de manera que el seu producte, un residu. Per contra, l'índex del producte d'un residu per un no-residu serà imparell, de manera que el seu producte, un no-residu.

Els dos mètodes de demostració també es poden aplicar a aquests teoremes: *El valor de l'expressió* $\frac{a}{b}$ (mòd. p) *serà un residu quan els nombres a, b, són simultàniament residus o bé simultàniament no-residus; però, contràriament, serà un no-residu quan un dels nombres a, b, és un residu i l'altre un no-residu.* També es poden obtenir de la traducció dels teoremes de l'article precedent.

99. En general, el producte de factors qualssevol és un residu tant quan tots són residus com quan la quantitat de no-residus que ocorren entre ells és parella; però quan la quantitat de no-residus que es troben entre els factors és imparella, el producte serà un no-residu. Així, es pot decidir fàcilment si un nombre compost és

residu o no sempre que se sàpiga què són cadascun dels seus factors. Cosa per la qual a la taula II només hem encabit nombres primers. El mètode d'aquesta taula és aquest. En el marge, s'han posat els mòduls,* a la capçalera, els successius nombres primers; quan algun d'aquests ha estat residu d'algun mòdul, a l'espai corresponent a tots dos s'ha col·locat un guió, però quan el nombre primer ha estat no-residu del mòdul, l'espai corresponent ha restat buit.

100. Abans que passem a tractar [proposicions] més difícils, se n'han d'afegir algunes dels mòduls no primers.

Si es pren per mòdul alguna potència p^n d'un nombre primer p (on suposem que p no és 2), de tots els nombres no divisibles per p i menors que el mòdul, la meitat seran residus, l'altra, no-residus; és a dir, la quantitat de cadascuna $= \frac{1}{2}(p-1)p^{n-1}$.

En efecte, si r és un residu, serà congru a algun quadrat l'arrel del qual no supera la meitat del mòdul (vegeu article 94). Ara es copsa fàcilment que es donen $= \frac{1}{2}(p-1)p^{n-1}$ nombres no divisibles per p i menors que la meitat del mòdul; així, resta que es demostri que els quadrats de tots aquests nombres són incongrus, o sigui, que produeixen residus quadràtics diferents. Si els quadrats de dos nombres a, b, no divisibles per p i menors que la meitat del mòdul fossin congrus, $aa - bb$, o sigui $(a-b)(a+b)$, seria divisible per p^n (suposat,

* També ensenyarem aviat de quina manera podríem prescindir dels mòduls compostos.

cosa que és lícita, que $a > b$). Però això no pot resultar, llevat que *o bé* un dels nombres $a - b$, $a + b$, fos divisible per p^n, cosa que no pot resultar ja que ambdós són $< p^n$, *o bé* l'un per p^m, l'altre per p^{n-m}, és a dir, ambdós per p. Però això tampoc no pot resultar. En efecte, evidentment, la suma i la diferència $2a$ i $2b$ també serien divisibles per p, de manera que també a i b, contràriament a la hipòtesi. D'aquí es conclou, però, que entre els nombres no divisibles per p i menors que el mòdul, es donen $= \frac{1}{2}(p-1)p^{n-1}$ residus; els restants, la quantitat dels quals és igualment gran, són no-residus. *Q. E. D.* Aquest teorema també es pot derivar de la consideració dels índexs, de manera similar a l'article 97.

101. *Qualsevol nombre no divisible per p que és residu de p també serà residu de p^n; però el que és no-residu de p també serà no-residu de p^n.*

La darrera part d'aquesta proposició és evident per si mateixa. Així, si la primera fos falsa, entre els nombres menors que p^n i simultàniament no divisibles per p, més serien residus de p que de p^n; *és a dir*, més de $\frac{1}{2}p^{n-1}(p-1)$. Però es podrà copsar, sense cap dificultat, que la quantitat de residus del nombre p entre aquells nombres és precisament $= \frac{1}{2}p^{n-1}(p-1)$.

És igualment fàcil, de fet, trobar un quadrat que sigui congru a un residu donat segons el mòdul p^n, si es té un quadrat congru a aquest residu segons el mòdul p.

Això és, si es té un quadrat aa que és congru a un residu donat A segons el mòdul p^μ, d'això es dedueix un

quadrat congru a A segons el mòdul p^ν (on se suposa $\nu > \mu$ i = o bé $< 2\mu$) de la manera següent. Es posa l'arrel del quadrat cercat $= \pm a + xp^\mu$, la qual es copsa fàcilment que ha de tenir aquesta forma; i ha de ser $aa \pm 2axp^\mu + xxp^{2\mu} \equiv A\,(\text{mòd.}\,p^\nu)$, o sigui, $A - aa \equiv \pm 2axp^\mu\,(\text{mòd.}\,p^\nu)$, a causa que $2\mu > \nu$. Sigui $A - aa = p^\mu d$ i x serà el valor de l'expressió $\pm\dfrac{d}{2a}\,(\text{mòd.}\,p^{\mu-\nu})$ a la qual equival $\pm\dfrac{A-aa}{2ap^\mu}\,(\text{mòd.}\,p^\nu)$.

Així, doncs, donat un quadrat congru a A segons p, se'n dedueix un quadrat congru a A segons el mòdul p^2; d'aquí es podrà pujar al mòdul p^4, d'aquí a p^8, etc.

Exemple. Proposat el residu 6, que és congru al quadrat 1 segons el mòdul 5, es troba el quadrat 9^2 al qual és congru segons 25, 16^2 al qual és congru segons 125, etc.

102. Pel que fa a nombres divisibles per p, és clar que els seus quadrats seran divisibles per pp, de manera que tots els nombres divisibles per p, però no per pp, seran no-residus de p. En general, però, si es proposa un nombre $p^k A$, on A no és divisible per p, s'hauran de distingir aquests casos:

1) Quan $k =$ o bé $> n$ serà $p^k A \equiv 0\,(\text{mòd.}\,p^n)$, és a dir, un residu.

2) Quan $k < n$ i imparell, $p^k A$ serà un no-residu.

En efecte, si és $p^k A = p^{2\kappa+1} A \equiv ss\,(\text{mòd.}\,p^n)$, ss és divisible per $p^{2\kappa+1}$, cosa que, altrament, només

podria resultar si s fos divisible per $p^{\kappa+1}$. Llavors, però, ss també és divisible per $p^{2\kappa+2}$, de manera que (com que $2\kappa+2$ no és, certament, més gran que n) també $p^k A$; és a dir, $p^{2\kappa+1}A$; o sigui, A per p, contràriament a la hipòtesi.

3) Quan $k < n$ i parell. Llavors, $p^k A$ serà residu o bé no-residu de p^n segons que A sigui residu o bé no-residu de p. En efecte, quan A és residu de p també serà residu de p^{n-k}. Però, posat $A \equiv aa \left(\text{mòd.}\, p^{n-k}\right)$, serà $Ap^k \equiv aap^k \,(\text{mòd.}\, p^n)$ i aap^k és un quadrat. Però quan A és no-residu de p, $p^k A$ no pot ser residu de p^n. En efecte, es posa $p^k A \equiv aa \,(\text{mòd.}\, p^n)$, i aa serà divisible necessàriament per p^k. El quocient serà un quadrat al qual A serà congru segons el mòdul p^{n-k}, de manera que també segons el mòdul p, és a dir, A serà un residu de p, contràriament a la hipòtesi.

103. Com que hem exclòs el cas $p = 2$, encara cal dir quelcom d'aquest. Quan el mòdul és el nombre 2, qualsevol nombre serà residu, i cap serà no-residu. En canvi, quan el mòdul és 4, tots els nombres imparells de la forma $4k + 1$ seran residus, però tots els de la forma $4k + 3$, no-residus. Finalment, quan el mòdul és 8 o bé una potència més alta del nombre 2, tots els nombres imparells de la forma $8k+1$ seran residus, però els restants, o sigui, els que són de les formes $8k+3$, $8k+5$, $8k + 7$, seran no-residus. La darrera part d'aquesta proposició és clara pel fet que el quadrat de qualsevol nombre imparell, bé sigui de la forma $4k + 1$, bé de la forma $4k - 1$, resulta de la forma $8k + 1$. Provem la primera així.

1) Si la suma o bé la diferència de dos nombres és divisible per 2^{n-1}, els quadrats dels nombres seran congrus segons el mòdul 2^n. En efecte, si l'un es posa $= a$, l'altre serà de la forma $2^{n-1}h \pm a$, el quadrat del qual es troba $\equiv aa \,(\text{mòd.}\, 2^n)$.

2) Qualsevol nombre imparell que és residu quadràtic de 2^n serà congru a algun quadrat l'arrel del qual és un nombre imparell i $< 2^{n-2}$. En efecte, sigui aa qualsevol quadrat al qual aquell nombre és congru, i el nombre $a \equiv \pm\alpha \left(\text{mòd.}\, 2^{n-1}\right)$, de manera que α no superi la meitat del mòdul (article 4), i serà $aa \equiv \alpha\alpha$. Per tant, el nombre proposat també serà $\equiv \alpha\alpha$. Evidentment, però, tant a com α seran imparells i $\alpha < 2^{n-2}$.

3) Els quadrats de tots els nombres imparells menors que 2^{n-2} seran incongrus segons el mòdul 2^n. En efecte, siguin r i s dos tals nombres; si els quadrats d'aquests fossin congrus segons 2^n, $(r-s)(r+s)$ seria divisible per 2^n (posat $r > s$). Però es copsa fàcilment que els nombres $r-s$, $r+s$, no poden ser simultàniament divisibles per 4; per tant, si un només és divisible per 2, per tal que el producte resultés divisible per 2^n, l'altre hauria de ser divisible per 2^{n-1}, *Q. E. A.*, ja que tots dos són $< 2^{n-2}$.

4) Finalment, si aquests quadrats es redueixen als seus *residus mínims positius*, es tindran 2^{n-3} residus quadràtics diferents menors que el mòdul,* cadascun dels quals serà de la forma $8k+1$. Però com que existeixen precisament 2^{n-3} nombres de la forma $8k+1$ menors

* Ja que la quantitat de nombres imparells menors que 2^{n-2} és 2^{n-3}.

que el mòdul, necessàriament tots aquests es trobaran entre aquells residus. *Q. E. D.*

Per a trobar un quadrat congru segons el mòdul 2^n a un nombre donat de la forma $8k+1$ es pot aplicar un mètode similar al de l'article 101; vegeu també l'article 88. Finalment, per als nombres parells valen els mateixos que hem exposat en general a l'article 102.

104. Sobre la quantitat de valors diferents (és a dir, incongrus segons el mòdul) que admet una expressió tal com $V = \sqrt{A}\,(\text{mòd.}\,p^n)$, suposat que A és residu de p^n, de les [proposicions] precedents, es conclouen fàcilment aquestes (suposem, com abans, que el nombre p és primer i, per raó de brevetat, incloem constantment el cas $n = 1$) I. Si A no és divisible per p, V té *un sol* valor per a $p = 2$, $n = 1$, posem $V \equiv 1$; *dos*, quan p és imparell i també per a $p = 2$, $n = 2$; posant l'un $\equiv v$, l'altre serà $\equiv -v$; *quatre*, per a $p = 2$, $n > 2$, això és, posant un $\equiv v$, els restants seran $\equiv -v$, $2^{n-1} + v$, $2^{n-1} - v$. II. Si A és divisible per p però no per p^n, sigui $p^{2\mu}$ la potència més alta de p que divideix A (en efecte, evidentment, el seu exponent haurà de ser parell) i $A = ap^{2\mu}$. Llavors, és clar que tots els valors de V són divisibles per p^μ i que els quocients sorgits de la divisió resulten valors de l'expressió $V' = \sqrt{a}\,\big(\text{mòd.}\,p^{n-2\mu}\big)$; d'aquí sortiran tots els valors diferents de V multiplicant per p^μ tots els valors de l'expressió V' situats entre 0 i $p^{n-\mu}$; per tant, aquells s'expressaran per vp^μ, $vp^\mu + p^{n-\mu}$, $vp^\mu + 2p^{n-\mu}$, $\ldots$, $vp^\mu + (p^\mu - 1)p^{n-\mu}$, si v representa indefinidament tots els valors *diferents* de l'expressió V', de manera que la quantitat d'aquells resulta p^μ, $2p^\mu$, o bé $4p^\mu$, segons que la quantitat d'aquests (pel cas I) sigui 1, 2, o bé 4.

III. Si A és divisible per p^n, es copsarà fàcilment, establint $n = 2m$ o bé $n = 2m - 1$ segons que sigui parell o imparell, que tots els nombres divisibles per p^m, però no cap altre, són valors de V; per tant, tots els valors diferents seran els 0, p^m, $2p^m$, $\ldots$, $(p^{n-m} - 1)p^m$, la quantitat dels quals és p^{n-m}.

105. Resta el cas en què el mòdul m és compost de molts nombres primers. Sigui $m = abc\ldots$, on a, b, c, etc., designen nombres primers diferents o bé potències de primers diferents, i és clar instantàniament que si n és residu de m, n també serà residu de cada un dels a, b, c, etc., de manera que, certament, n és no-residu de m, si és no-residu d'algun dels nombres a, b, c, etc. També recíprocament, si n és residu de cada un dels a, b, c, etc., també serà residu del producte m. En efecte, suposant que $n \equiv A^2$, B^2, C^2, etc., segons els mòduls a, b, c, etc., respectivament, és clar que si es trobés un nombre N congru a A, B, C, etc., segons els mòduls a, b, c, etc., respectivament (article 32), seria $n \equiv NN$ segons tots aquests mòduls, de manera que també segons el producte m. Com que es copsa fàcilment que de la combinació, d'aquesta manera, de *qualsevol* valor de A, o sigui, de l'expressió $\sqrt{n}\,(\text{mòd.}\,a)$, amb *qualsevol* valor de B, amb *qualsevol* valor de C, etc., surt un valor de N, o sigui, de l'expressió $\sqrt{n}\,(\text{mòd.}\,m)$; que, també, de combinacions diferents es produeixen diferents N; i que tots [els valors de N] de totes [les combinacions], la quantitat de tots els valors diferents de N serà igual al producte de les quantitats de valors de A, B, C, etc., que hem ensenyat a determinar a l'article precedent. A més a més, és evident que si fos conegut un valor de l'expressió $\sqrt{n}\,(\text{mòd.}\,m)$, o sigui, de N, aquest seria, simultània-

ment, un valor de tots els A, B, C, etc.; i com que, per l'article precedent, d'aquí es poden deduir tots els valors restants d'aquestes quantitats, se segueix fàcilment que d'un valor de N es poden obtenir tots els altres.

Exemple. Sigui 315 el mòdul, del qual se cerca si 46 és residu o no-residu. Els divisors primers del nombre 315 són 3, 5, 7, i el nombre 46 és un residu de qualsevol d'ells; per tant, també serà residu de 315. A més a més, com que $46 \equiv 1$ i $\equiv 64 \,(\text{mòd. } 9)$; $\equiv 1$ i $\equiv 16 \,(\text{mòd. } 5)$; $\equiv 4$ i $\equiv 25 \,(\text{mòd. } 7)$; es troben les arrels dels quadrats per als quals 46 és congru segons el mòdul 315: 19, 26, 44, 89, 226, 271, 289, 296.

106. De les [proposicions] precedents es conclou que, només que es pugui distingir sempre si un *nombre primer* donat és residu o no-residu d'un nombre *primer donat*, tots els casos restants es poden reduir a aquest. Així, ens caldrà indagar amb tot l'afany criteris segurs per a aquell cas. Però, abans que emprenguem aquesta recerca, mostrarem un cert criteri, exigit per la secció, que, encara que a la pràctica no tingui gairebé cap utilitat, no obstant això, és digne de menció per la seva simplicitat i generalitat.

Qualsevol nombre A no divisible pel nombre primer $2m+1$ és residu o bé no-residu d'aquest primer segons que $A^m \equiv +1$ o bé $\equiv -1 \,(\text{mòd. } 2m+1)$.

En efecte, sigui a l'índex del nombre A per al mòdul $2m+1$ en un sistema qualsevol, i a serà parell quan A és un residu de $2m+1$, però imparell quan A és no-residu. I l'índex del nombre A^m serà ma, és a dir, $\equiv 0$ o

bé $\equiv m\,(\text{mòd. } 2m)$, segons que a sigui parell o imparell. D'aquí, finalment, A^m serà $\equiv +1$ en el primer cas, però $\equiv -1\,(\text{mòd. } 2m+1)$ en el darrer (vegeu articles 57, 62).

Exemple. Com que $3^6 \equiv 1\,(\text{mòd. } 13)$, 3 és residu de 13, però 2 és no-residu de 13, perquè $2^6 \equiv -1\,(\text{mòd. } 13)$.

Però sempre que els nombres que cal examinar són moderadament grans, aquest criteri serà completament inútil per la immensitat del càlcul.

107. Certament, proposat un mòdul, és facilíssim assignar-li tots els nombres que en són residus o bé no-residus. Això és, si aquell nombre es posa $= m$, s'han de determinar els quadrats les arrels dels quals no superen la meitat de m, o bé nombres congrus a aquests quadrats segons m (a la pràctica es donen mètodes encara més ràpids), i, llavors, tots els nombres congrus a algun d'aquests segons m seran residus de m, però tots els nombres no congrus a cap d'aquests seran no-residus. Però la qüestió inversa, *proposat algun nombre, assignar-li tots els nombres dels quals ell sigui residu o no-residu*, és de recerca molt més alta. Així, investigarem a continuació aquest problema, de la solució del qual depèn el que ens hem proposat a l'article precedent, començant pels casos més simples.

108. Teorema. -1 *és residu quadràtic de tots els nombres primers de la forma* $4n+1$*, però no-residu de tots els nombres de la forma* $4n+3$.

Exemple. -1 és residu dels nombres 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc., originat pels quadrats dels nombres 2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22, etc.,

respectivament; per contra, és no-residu dels nombres 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, etc.

Ja hem fet menció d'aquest teorema a l'article 64. La demostració, però, s'obté fàcilment de l'article 106. Efectivament, per a un nombre primer de la forma $4n+1$ és $(-1)^{2n} \equiv 1$, però per a un nombre de la forma $4n+3$ es té $(-1)^{2n+1} \equiv -1$. Aquesta demostració concorda amb la que hem transmès en el *lloc citat*. Però a causa de l'elegància i de la utilitat del teorema, no serà superflu mostrar-la encara d'una altra manera.

109. Designarem per la lletra C el complex de tots els residus d'un nombre primer p que són menors que p, exclòs el residu 0; i, com que la quantitat d'aquests residus sempre és $= \frac{p-1}{2}$, és evident que aquesta serà parella sempre que p sigui de la forma $4n+1$, però imparella sempre que p sigui de la forma $4n+3$. A la manera de l'article 77, on es tractava de nombres en general, s'anomenaran *residus associats* aquells el producte dels quals és $\equiv 1 \,(\text{mòd.}\, p)$; en efecte, evidentment, si r és residu, $\frac{1}{r} \,(\text{mòd.}\, p)$ també serà residu. I com que un mateix residu no pot tenir més associats entre els residus de C, és clar que tots els residus de C es poden distribuir en classes, cadascuna de les quals contingui un parell de residus associats. Ara, es copsa que, si no es donés cap residu que fos associat a si mateix, és a dir, si qualsevol classe contingués un parell de residus *diferents*, el nombre de tots els residus seria el doble que el nombre de totes les classes; però si es donen alguns residus associats a si mateixos, és a dir, algunes classes que només contenen un únic residu, o bé, si algú ho prefereix, el mateix residu dues vegades, posada $= a$

la quantitat d'aquestes classes i $= b$ la quantitat de les restants, el nombre de tots els residus de C serà $= a+2b$. Per tant, quan p és de la forma $4n+1$, a serà un nombre parell; però quan p és de la forma $4n+3$, a serà imparell. Els nombres menors que p altres que 1 i $p-1$ no poden ser associats a si mateixos (vegeu article 77); primer, 1 ocorre certament entre els residus; d'on, en el primer cas, $p-1$ (o sigui, -1, que aquí val el mateix) ha de ser residu, però, en el darrer, no-residu; en efecte, altrament, en aquell cas seria $a = 1$ però en aquest $a = 2$, cosa que no pot ser.

110. Aquesta demostració també es deu a l'il·lm. Euler que, nogensmenys, trobà el primer la primera (vegeu *Opusc. Anal.* T. I, *p.* 135). Qualsevol veurà fàcilment que aquesta és basada en principis similars als de la nostra segona demostració del teorema de Wilson de l'article 77. Però si volem suposar aquest teorema, es podrà presentar la demostració encara més fàcilment. Això és, $\frac{p-1}{2}$ d'entre els nombres 1, 2, 3, ..., $p-1$, seran residus quadràtics de p, i la mateixa quantitat, no-residus; per tant, la quantitat de no-residus serà parella quan p és de la forma $4n+1$ i imparella quan és de la forma $4n+3$. D'aquí, el producte de tots els nombres 1, 2, 3, ..., $p-1$, serà residu en el primer cas, no-residu en el darrer (article 91). Però aquest producte sempre és $\equiv -1 \,(\text{mòd.}\, p)$; de manera que -1 també serà residu en el primer cas, no-residu en el darrer.

111. Així, si r és residu d'algun nombre primer de la forma $4n+1$, $-r$ també serà residu d'aquest primer; en canvi, tots els no-residus de tal nombre també es mantin-

dran no-residus en prendre el signe contrari.* Succeeix el contrari per als nombres primers de la forma $4n+3$, els residus dels quals resulten no-residus i recíprocament, quan es canvia el signe (vegeu l'article 98).

D'altra banda, es deriva fàcilment del que precedeix la regla general: -1 és un residu de tots els nombres que no es poden dividir ni per 4 ni per cap nombre primer de la forma $4n+3$, no-residu de tots els restants (vegeu els articles 103 i 105).

112. Passem a tractar els residus $+2$ i -2.

Si de la taula II recollim tots els nombres primers dels quals $+2$ és residu, tindrem els 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Però s'adverteix fàcilment que entre aquests nombres no se'n troba cap de les formes $8n+3$ i $8n+5$.

Així, vegem si aquest indici es podria elevar a certesa.

Primer, observem que qualsevol nombre compost de la forma $8n+3$ o bé $8n+5$ conté necessàriament un factor primer d'alguna de les formes $8n+3$ o bé $8n+5$; en efecte, evidentment, només de nombres primers de les formes $8n+1$ o bé $8n+7$, no es poden compondre altres nombres que els que són de les formes $8n+1$ o bé $8n+7$. Així, si el nostre indici és cert en general, no es donarà cap nombre en absolut de la forma $8n+3$,

* Així, doncs, quan es parli de fins a quin punt un nombre qualsevol és residu o bé no-residu d'un nombre de la forma $4n+1$, podrem negligir completament el seu signe, o bé atribuir-li el signe dubtós $\pm$.

$8n + 5$, del qual $+2$ sigui residu; i així, certament, no existeix cap nombre d'aquesta forma per sota de 100 del qual $+2$ sigui residu. Però, si més enllà d'aquest límit es trobessin tals nombres, posem $= t$ el mínim de tots. Així, t serà de la forma $8n + 3$ o bé $8n + 5$, i $+2$ en serà residu, però no-residu de tots els nombres menors similars. Es posa $2 \equiv aa\,(\text{mòd.}\,t)$; i sempre es podrà agafar a de manera que sigui imparell i, simultàniament, $< t$ (en efecte, a tindrà com a mínim dos valors positius menors que t, la suma dels quals $= t$, i de manera que un dels quals és parell i l'altre imparell, vegeu articles 104, 105). Fet això, sigui $aa = 2 + tu$, o sigui, $tu = aa - 2$, i aa serà de la forma $8n + 1$; així, doncs, tu de la forma $8n - 1$, de manera que u de la forma $8n + 3$ o bé $8n + 5$, segons que t sigui de la darrera forma o bé de la primera. Però de l'equació $aa = 2 + tu$ se segueix que també $2 \equiv aa\,(\text{mòd.}\,u)$, *és a dir*, 2 també serà residu de u. Però es copsa fàcilment que és $u < t$; per tant, t no és el nombre mínim contrari al nostre indici, contra la hipòtesi. D'on, evidentment, se segueix que el que havíem trobat per indici és cert en general.

Combinant això amb les proposicions de l'article 111, s'obtenen els teoremes següents.

I. $+2$ *serà no-residu de tots els nombres primers de la forma* $8n + 3$*; però* -2*, residu.*

II. *Tant* $+2$ *com* -2 *seran no-residus de tots els nombres primers de la forma* $8n + 5$*.*

113. Per un indici similar, de la taula II es troben els nombres primers dels quals -2 és residu: 3, 11, 17,

19, 41, 43, 59, 67, 73, 83, 89, 97.* Com que entre aquests no se'n troba cap de les formes $8n + 5$, $8n + 7$, investigarem si aquest indici també podria assolir la força d'un teorema general. Es mostra, de manera similar a l'article precedent, que qualsevol nombre compost de la forma $8n + 5$ o bé $8n + 7$ conté un factor primer de la forma $8n + 5$ o bé de la forma $8n + 7$, de manera que si el nostre indici és vertader en general, -2 no podria ser residu de cap nombre en absolut de la forma $8n + 5$ o bé $8n + 7$. Però si es donessin tals nombres, es posa $= t$ el mínim de tots i resulti $-2 = aa - tu$. On si, com més amunt, s'agafa a imparell i menor que t, u serà de la forma $8n+5$ o bé $8n+7$ segons que t sigui de la forma $8n + 7$ o bé $8n + 5$. Però de $aa + 2 = tu$ i $a < t$, qualsevol podrà derivar fàcilment que u també seria menor que t. Finalment, -2 també serà un residu de u; és a dir, t no serà el nombre mínim que s'oposa al nostre indici, contra la hipòtesi. Per tant, necessàriament, -2 és no-residu de tots els nombres de les formes $8n + 5$, $8n + 7$.

Combinant això amb les proposicions de l'article 111, surten aquests teoremes:

I. *Tant* -2 *com* $+2$ *són no-residus de tots els nombres primers de la forma* $8n + 5$, com ja hem trobat a l'article precedent.

II. -2 *és no-residu, però* $+2$*, residu, de tots els nombres primers de la forma* $8n + 7$.

* Això és, considerant -2 com a producte de $+2$ i -1, vegeu l'article 111.

D'altra banda, a totes dues demostracions també hauríem pogut agafar per a a un valor parell; però, llavors, hauria calgut distingir el cas en què a fos de la forma $4n+2$ d'aquell en què a fos de la forma $4n$. El desenvolupament, però, procedeix igual com més amunt i no està sotmès a cap dificultat.

114. Encara resta un cas, això és, on el nombre primer és de la forma $8n+1$. Però aquest eludeix el mètode precedent i demana artificis completament peculiars.

Sigui a una arrel primitiva qualsevol per al mòdul primer $8n+1$, i serà $a^{4n} \equiv -1 \,(\text{mòd.}\, 8n+1)$ (article 62), congruència que també es pot presentar així, $(a^{2n}+1)^2 \equiv 2a^{2n} \,(\text{mòd.}\, 8n+1)$, o també així, $(a^{2n}-1)^2 \equiv -2a^{2n} \,(\text{mòd.}\, 8n+1)$. D'on se segueix que tant $2a^{2n}$ com $-2a^{2n}$ són residus de $8n+1$; però, com que a^{2n} és un quadrat no divisible pel mòdul, també, evidentment, tant $+2$ com -2 seran residus (article 98).

115. No serà inútil afegir encara una altra demostració d'aquest teorema, que té una relació similar amb la precedent com la segona demostració del teorema de l'article 108 (article 109) amb la primera (article 108). Llavors, els experts copsaran més fàcilment que les dues demostracions, tant aquelles com aquestes, no són heterogènies en tal grau com potser semblaria a primera vista.

I. Per a qualsevol mòdul primer de la forma $4m+1$, entre els nombres menors que ell, 1, 2, 3, ..., $4m$, se'n troben m que poden ser congrus a un biquadrat, però els $3m$ restants, no podran.

Certament, això es deriva fàcilment dels principis de la secció precedent, però, sense ells, la demostració tampoc no és difícil. En efecte, hem demostrat que -1 sempre és residu quadràtic per a un tal mòdul. Així, sigui $ff \equiv -1$, i és clar que, si z fos un nombre qualsevol no divisible pel mòdul, els biquadrats dels quatre nombres $+z$, $-z$, $+fz$, $-fz$ (que es copsa fàcilment que són incongrus) serien congrus entre si; a més a més, és evident que el biquadrat de qualsevol nombre que no és congru a cap d'aquests quatre no pot resultar congru als biquadrats d'aquells (en efecte, altrament, la congruència $x^4 \equiv z^4$, que és de quart grau, tindria més de 4 arrels, contra l'article 43). D'aquí es conclou fàcilment que tots els nombres 1, 2, 3, ..., $4m$, només originen m biquadrats incongrus, per als quals es troben m congrus entre aquests nombres, però els restants no podran ser congrus a cap biquadrat.

II. Segons un mòdul primer de la forma $8n+1$, -1 podrà resultar congru a un biquadrat (-1 serà *residu biquadràtic* d'aquest nombre primer).

En efecte, la quantitat de tots els residus biquadràtics menors que $8n+1$ (excloent-ne el zero) serà $= 2n$, és a dir, parella. A més a més, es prova fàcilment que, si r fos un residu biquadràtic de $8n+1$, el valor de l'expressió $\frac{1}{r}$ (mòd. $8n+1$) també seria un tal residu. D'aquí, tots els residus biquadràtics es podran distribuir en classes de manera similar a com hem distribuït els residus quadràtics en l'article 109; i també la part restant de la demostració procedeix totalment de la mateixa manera que allà.

III. Ara sigui $g^4 \equiv -1$ i h el valor de l'expressió $\frac{1}{g}$ (mòd. $8n+1$). Llavors serà $(g \pm h)^2 = g^2 + h^2 \pm 2gh \equiv g^2 + h^2 \pm 2$ (a causa que $gh \equiv 1$). Però $g^4 \equiv -1$, de manera que $-h^2 \equiv g^4 h^2 \equiv g^2$, d'on, finalment, $g^2 + h^2 \equiv 0$ i $(g \pm h)^2 \equiv \pm 2$; *és a dir*, tant $+2$ com -2 són residus quadràtics de $8n+1$. *Q. E. D.*

116. D'altra banda, del que precedeix, es dedueix fàcilment la regla general següent: $+2$ *és residu de qualsevol nombre que no es pugui dividir ni per* 4 *ni per cap primer de la forma* $8n+3$ *o bé* $8n+5$*, però dels restants* (per exemple, de tots els nombres de les formes $8n+3$, $8n+5$, bé siguin primers, bé compostos), *no-residu.*

-2 *és residu de qualsevol nombre que no es pugui dividir ni per* 4 *ni per cap primer de la forma* $8n+5$ *o bé* $8n+7$*, però no-residu de tots els restants.*

Aquests teoremes elegants ja foren coneguts pel sagaç Fermat, *Op. Mathem. p.* 168. Però no va comunicar mai la demostració que va declarar que tenia. Posteriorment, va ser investigada, sempre en va, per l'il·lm. Euler; l'il·lm. La Grange va trobar el primer una demostració rigorosa, *Nouv. Mém. de l'Ac. de Berlin* 1775, p. 349, 351. Sembla que això encara ho ignorà l'il·lm. Euler quan va escriure la dissertació conservada en *Opusc. Analyt.* T. I, p. 259.

117. Prosseguim amb els residus $+3$ i -3. Comencem pel darrer.

A la taula II es descobreixen aquests nombres primers per als quals -3 és residu: 3, 7, 13, 19, 31, 37, 43,

61, 67, 73, 79, 97, entre els quals no se'n troba cap de la forma $6n+5$. Però que tampoc més enllà dels límits de la taula no es dóna cap primer d'aquesta forma per al qual -3 és residu, ho demostrem així. Primerament, és clar que qualsevol nombre compost de la forma $6n+5$ conté necessàriament algun factor primer de la mateixa forma. Així, doncs, fins on no es doni cap nombre primer de la forma $6n+5$ per al qual -3 sigui residu, de tals tampoc no se'n donarà cap que sigui compost. Però si, més enllà dels límits de la nostra taula, es donessin tals nombres, sigui $= t$ el mínim de tots, i es posa $-3 = aa - tu$. Llavors, si s'agafés a parell i menor que t, serà $u < t$, i -3 residu de u. Però quan a és de la forma $6n \pm 2$, tu serà de la forma $6n+1$, de manera que u, de la forma $6n+5$, *Q. E. A.* ja que hem suposat que t és el nombre mínim que s'oposa al nostre indici. Però quan a és de la forma $6n$, tu serà de la forma $36n+3$, de manera que $\frac{1}{3}tu$, de la forma $12n+1$; per tant, $\frac{1}{3}u$ serà de la forma $6n+5$; en canvi, és clar que -3 també serà un residu de $\frac{1}{3}u$ i és $\frac{1}{3}u < t$, *Q. E. A.* Així, és evident que -3 no pot ser residu de cap nombre de la forma $6n+5$.

Com que qualsevol nombre de la forma $6n+5$ està inclòs necessàriament o bé en la forma $12n+5$ o bé en la $12n+11$, però la primera forma en la $4n+1$ i la darrera en la $4n+3$, es tenen aquests teoremes:

I. *Tant* $+3$ *com* -3 *són no-residus de qualsevol nombre primer de la forma* $12n+5$.

II. -3 *és no-residu de qualsevol nombre primer de la forma* $12n+11$*; però* $+3$*, residu.*

118. A la taula II, es troben aquests nombres per als quals +3 és residu: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, entre els quals cap no és de la forma $12n+5$ o bé $12n+7$. Però es pot comprovar, completament de la mateixa manera que en els articles 112, 113, 117, que no es donen en absolut nombres de la forma $12n+5$, $12n+7$, per als quals +3 sigui residu; per tant, ens estalviem aquesta feina. Així, unit [això] amb l'article 111, tenim els teoremes:

I. *Tant* +3 *com* −3 *són no-residus de qualsevol nombre primer de la forma* $12n+5$ (tal com ja hem trobat a l'article precedent).

II. +3 *és no-residu de qualsevol nombre primer de la forma* $12n+7$*;* −3*, residu.*

119. Però, per aquest mètode, no es pot trobar res per als nombres de la forma $12n+1$, que, en conseqüència, requereixen artificis singulars. Certament, es conclou fàcilment per indici que +3 i −3 són residus de tots els nombres primers d'aquesta forma. Però, evidentment, només s'ha de demostrar que −3 és residu de tals nombres, ja que llavors +3 també n'ha de ser necessàriament residu (article 111). Però, més generalment, demostrarem que −3 és residu de qualsevol nombre primer de la forma $3n+1$.

Sigui p un nombre primer d'aquesta forma i a un nombre que pertany a l'exponent 3 per al mòdul p (és evident que aquests es donen per l'article 54, ja que 3 és un submúltiple de $p-1$). Així, serà $a^3 \equiv 1 \,(\text{mòd.}\, p)$; és a dir, a^3-1, o sigui, $(a^2+a+1)(a-1)$, divisible per p. Però és clar que a no pot ser $\equiv 1 \,(\text{mòd.}\, p)$, ja que 1 pertany a

l'exponent 1; per tant, $a-1$ no serà divisible per p, sinó que ho serà a^2+a+1 i, d'aquí, també $4aa+4a+4$; és a dir, serà $(2a+1)^2 \equiv -3 \,(\text{mòd.}\, p)$, o sigui, -3 residu de p. *Q. E. D.*

D'altra banda, és clar que aquesta demostració (que és independent de les precedents) també aplega els nombres primers de la forma $12n+7$, que ja hem acabat a l'article precedent.

Encara convé observar que aquesta anàlisi es pot presentar a la manera dels mètodes usats en els articles 109, 115, però, per abreujar, no ens detindrem en aquest fet.

120. Del que precedeix, es conclouen fàcilment aquests teoremes (vegeu articles 102, 103, 105).

I. -3 *és residu de tots els nombres que no es poden dividir ni per* 8*, ni per* 9*, ni per cap nombre primer de la forma* $6n+5$*, però no-residu de tots els restants.*

II. $+3$ *és residu de tots els nombres que no es poden dividir ni per* 4*, ni per* 9*, ni per cap primer de la forma* $12n+5$ *o bé* $12n+7$*; no-residu de tots els restants.*

En primer lloc, es té aquest cas particular:

-3 és *residu* de tots els nombres primers de la forma $3n+1$, o sigui, el que és el mateix, *de tots els que són residus de* 3; però *no-residu* de tots els nombres primers de la forma $6n+5$, o sigui, exclòs el nombre 2, de tots els de la forma $3n+2$; és a dir, *de tots els que són no-residus de* 3. Es copsa fàcilment, però, que tots els casos restants se segueixen d'aquests espontàniament.

Les proposicions que pertanyen als residus $+3$ i -3 ja foren conegudes per Fermat, *Opera Wallisii* T. II, p. 857. Però l'il·lm. Euler va transmetre el primer les demostracions, *Comm. nov. Petr.* T. VIII, p. 105 i s. Per això és més sorprenent que les demostracions de les proposicions que pertanyen als residus $+2$ i -2, basades en artificis completament similars, sempre haguessin fugit de la seva sagacitat. Vegeu també els comentaris de l'il·lm. La Grange a *Nouv. Mem. de l'Ac. de Berlin* 1775, p. 352.

121. Per indici, es desprèn que $+5$ no és residu de cap nombre imparell de la forma $5n + 2$ o bé $5n + 3$, és a dir, de cap nombre imparell que sigui no-residu d'ell. Però, que aquesta regla no pateix cap excepció es demostra així. Sigui $= t$ el nombre mínim, si se'n dóna cap, que cal exceptuar d'aquesta regla; així, aquest nombre és no-residu de 5, però 5 és residu de t. Sigui $aa = 5 + tu$ de manera que a sigui parell i menor que t. Així, doncs, u serà imparell i menor que t, però $+5$ serà residu de u. Ara, si a no és divisible per 5, tampoc no ho serà u; però, evidentment, tu és residu de 5; per tant, com que t és no-residu de 5, u també en serà no-residu; és a dir, es dóna un no-residu del nombre 5 menor que t del qual $+5$ és residu, contràriament a la hipòtesi. Però, si a és divisible per 5, es posa $a = 5b$ i $u = 5v$, d'on $tv \equiv -1 \equiv 4 \,(\text{mòd. } 5)$, *és a dir,* tv serà residu del nombre 5. En la resta, la demostració procedeix igualment que en el cas anterior.

122. Així, doncs, tant $+5$ com -5 seran no-residus de tots els nombres primers que són no-residus de 5 i, simultàniament, de la forma $4n + 1$, és a dir, de tots els nombres primers de la forma $20n + 13$ o bé $20n + 17$;

però $+5$ serà no-residu, i -5, residu, de tots els nombres primers de la forma $20n + 3$ o bé $20n + 7$.

Es pot demostrar de manera completament similar que -5 és no-residu de tots els nombres primers de les formes $20n+11$, $20n+13$, $20n+17$, $20n+19$, i es copsa fàcilment que d'aquí se segueix que $+5$ és residu de tots els nombres primers de la forma $20n+11$ o bé $20n+19$, però no-residu de tots els de la forma $20n + 13$ o bé $20n+17$. I com que qualsevol nombre primer, excepte 2 i 5 (dels quals ± 5 és residu), està contingut en alguna de les formes $20n + 1$, 3, 7, 9, 11, 13, 17, 19, és clar que ja es pot manifestar una decisió de tots, exceptuant-ne els que siguin de la forma $20n+1$, o bé de la forma $20n+9$.

123. Es desprèn fàcilment per indici que $+5$ i -5 són residus de tots els nombres primers de la forma $20n+1$, o bé $20n+9$. Si això és veritat en general, es tindrà la llei elegant que $+5$ *és residu de tots els nombres primers que són residus de* 5 (en efecte, aquests estan continguts en alguna de les formes $5n + 1$ o bé $5n + 4$, o sigui, en alguna de les $20n + 1$, 9, 11, 19, per a la tercera i la quarta de les quals allò ja s'ha mostrat); *però no-residu de tots els nombres que siguin no-residus de* 5 com ja hem demostrat més amunt. Però és clar que aquest teorema és suficient per a decidir si $+5$ (i -5 si es considerés com a producte de $+5$ i -1) és residu o no-residu d'un nombre donat qualsevol. Finalment, s'observa l'analogia d'aquest teorema amb aquell que hem exposat a l'article 120 del residu -3.

Però la verificació d'aquell indici no és especialment fàcil. Quan es proposa un nombre primer de la forma $20n+1$, o més generalment de la forma $5n+1$, la

cosa es pot resoldre de manera similar als articles 114, 119. Això és, sigui a un nombre qualsevol que pertany a l'exponent 5 per al mòdul $5n+1$, que és evident per la secció precedent que d'aquests se'n donen, i serà $a^5 \equiv 1$, o sigui, $(a-1)(a^4+a^3+a^2+a+1) \equiv 0 \,(\text{mòd.}\, 5n+1)$. Però com que no pot ser $a \equiv 1$ i, així, no és $a-1 \equiv 0$, serà necessàriament $a^4+a^3+a^2+a+1 \equiv 0$. Per tant, també $4(a^4+a^3+a^2+a+1) = (2aa+a+2)^2 - 5a^2$ serà $\equiv 0$, és a dir, $5a^2$ serà residu de $5n+1$, de manera que també 5, ja que a^2 és residu no divisible per $5n+1$ (en efecte, a no és divisible per $5n+1$ a causa que $a^5 \equiv 1$). *Q. E. D.*

El cas en què es proposa un nombre primer de la forma $5n+4$ demana artificis més subtils. Però, com que les proposicions que cal resoldre es tractaran més generalment en les [seccions] següents, aquí només les ataquem breument.

I. Si p és un nombre primer i b un no-residu quadràtic donat de p, el valor de l'expressió

$$\frac{(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}}{\sqrt{b}} \qquad \text{(A)}$$

(de la qual, desenvolupada, es copsa fàcilment que desapareix la irracionalitat) sempre serà divisible per p, qualsevol nombre que es prengui per x. En efecte, de la inspecció dels coeficients que s'obtenen del desenvolupament de A, és clar que tots els termes des del segon fins al penúltim (inclosos) són divisibles per p, de manera que és $A \equiv 2(p+1)(x^p + xb^{\frac{p-1}{2}}) \,(\text{mòd.}\, p)$. Però, com que b és no-residu de p, serà $b^{\frac{p-1}{2}} \equiv -1 \,(\text{mòd.}\, p)$ (article 106); però x^p sempre és $\equiv x$ (secció precedent), d'on resulta $A \equiv 0$. *Q. E. D.*

II. En la congruència $A \equiv 0\,(\text{mòd.}\,p)$, la indeterminada x té p dimensions i tots els nombres 0, 1, 2, $\ldots$, $p-1$, seran arrels d'aquella. Ara, se suposa que e és un divisor de $p+1$, i, si es desenvolupa, l'expressió $\dfrac{(x+\sqrt{b})^e-(x-\sqrt{b})^e}{\sqrt{b}}$ (que designem per B) serà lliure d'irracionalitat, la indeterminada x tindrà en ella $e-1$ dimensions, i se sap, dels primers elements de l'anàlisi, que A és divisible per B (formalment). Ara, dic que es donen $e-1$ valors de x per als quals, substituïts en B, B sortiria divisible per p. Es efecte, es posa $A = BC$ i x tindrà $p-e+1$ dimensions en C, de manera que la congruència $C \equiv 0\,(\text{mòd.}\,p)$, no més de $p-e+1$ arrels. D'on és clar, fàcilment, que tots els nombres restants dels 0, 1, 2, 3, $\ldots$, $p-1$, la quantitat dels quals és $= e-1$, seran arrels de la congruència $B \equiv 0$.

III. Ara, se suposa que p és de la forma $5n+4$; $e = 5$; b, no-residu de p; i el nombre a, determinat de manera que $\dfrac{(a+\sqrt{b})^5-(a-\sqrt{b})^5}{\sqrt{b}}$ sigui divisible per p. Però aquella expressió resulta $= 10a^4 + 20aab + 2bb = 2((b+5aa)^2 - 20a^4)$. Així, doncs, $(b+5aa)^2 - 20a^4$ també serà divisible per p, és a dir, $20a^4$, residu de p; i com que $4a^4$ és residu no divisible per p (en efecte, s'entén fàcilment que a no es pot dividir per p), 5 també serà residu de p. *Q. E. D.*

D'aquí és clar que el teorema presentat a l'inici d'aquest article és veritat en general.

Encara observem que demostracions de tots dos casos es deuen a l'il·lm. La Grange, *Mem. de l'Ac. de Berlin* 1775, p. 352 i s.

124. Per un mètode similar es demostra que

-7 és no-residu de qualsevol nombre primer que sigui no-residu de 7.

Per indici, es pot concloure que

-7 és residu de qualsevol nombre que sigui residu de 7.

Però això no ha estat demostrat rigorosament per ningú fins aquest punt. Certament, la demostració és fàcil per als residus de 7 que són de la forma $4n - 1$; efectivament, pel mètode suficientment conegut del que precedeix, es pot mostrar que $+7$ sempre és no-residu de tals nombres primers, de manera que -7, residu. Però d'aquí guanyem poc; en efecte, els casos restants no es poden tractar per aquest mètode. Certament, encara podríem acabar un cas de manera similar als articles 119, 123. Això és, si p és un nombre primer de la forma $7n+1$ i a pertany a l'exponent 7 per al mòdul p, es copsa fàcilment que $\frac{4(a^7-1)}{a-1} = (2a^3+a^2-a-2)^2+7(a^2+a)^2$ és divisible per p, de manera que $-7(a^2+a)^2$ és residu de p. Però $(a^2+a)^2$, en tant que quadrat, és residu de p i, a sobre, no divisible per p; en efecte, com que s'ha suposat que a pertany a l'exponent 7, no pot ser ni $\equiv 0$, ni $\equiv -1$ (mòd. p), és a dir, ni a ni $a+1$ no seran divisibles per p, de manera que el quadrat $(a+1)^2a^2$, tampoc. D'on, evidentment, 7 també serà residu de p. *Q. E. D.* Però els nombres primers de la forma $7n+2$ o bé $7n+4$ eludeixen tots els mètodes tractats fins aquí. D'altra banda, també aquesta demostració ha estat detectada primer per l'il·lm. La Grange *en el lloc citat.* Més avall,

secció VII, ensenyarem més generalment que l'expressió $\frac{4(x^p-1)}{x-1}$ sempre es pot reduir a la forma $X^2 \mp pY^2$ (on cal agafar el signe superior quan p és un nombre primer de la forma $4n+1$, l'inferior quan és de la forma $4n+3$), on X, Y, denoten funcions racionals de x, lliures de fraccions. L'il·lm. La Grange no va dur a terme aquesta dissecció més enllà del cas $p = 7$ (vegeu *el lloc citat*, p. 352).

125. Així, doncs, com que els mètodes precedents no són suficients per a establir demostracions generals, ja és hora d'exposar-ne un altre, lliure d'aquest defecte. Comencem per un teorema la demostració del qual ha eludit bastant de temps el nostre esforç, encara que a primera vista sembli tan obvi que, certament, alguns no han entès la necessitat de demostració. És aquest: *Qualsevol nombre, excepte els quadrats presos positivament, és no-residu d'alguns nombres primers.* Però com que només hem d'utilitzar aquest teorema com a auxiliar per a altres demostracions, aquí no expliquem altres casos que els que necessitem per a aquest fi. El mateix se sabrà espontàniament més endavant dels casos restants. Així, mostrarem que *qualsevol nombre primer de la forma* $4n+1$ *agafat bé positivament, bé negativament,** *és no-residu d'alguns nombres primers* i, encara més, de tals que siguin menors que ell.

Primer, quan es proposa un nombre primer p de la forma $4n+1$ pres *negativament*, sigui $2a$ el nombre parell més pròxim més gran que $\sqrt{p}$; llavors es copsa fàcilment que $4aa$ sempre serà $< 2p$, o sigui, $4aa - p < p$. Però $4aa - p$ és de la forma $4n+3$, i $+p$ és residu quadràtic

* Però és evident en si que convé exceptuar $+1$.

de $4aa - p$ (ja que $p \equiv 4aa \,(\text{mòd.}\, 4aa - p)$); així, doncs, si $4aa - p$ és un nombre primer, $-p$ en serà no-residu; si no, algun factor de $4aa - p$ serà necessàriament de la forma $4n + 3$; i com que $+p$ també ha de ser residu d'aquest, $-p$ en serà no-residu. *Q. E. D.*

Per als nombres primers presos *positivament* distingim dos casos. *Primer*, sigui p un nombre primer de la forma $8n + 5$. Sigui a un nombre positiu qualsevol $< \sqrt{\frac{1}{2}p}$. Llavors, $8n + 5 - 2aa$ serà un nombre positiu de la forma $8n+5$ o bé $8n+3$ (segons que a sigui parell o bé imparell), de manera que, necessàriament, divisible per algun nombre primer de la forma $8n+3$ o bé $8n+5$; en efecte, el producte de nombres qualssevol de la forma $8n+1$ i $8n+7$ no pot tenir ni la forma $8n+3$ ni la $8n+5$. Sigui aquest q, i serà $8n + 5 \equiv 2a^2 \,(\text{mòd.}\, q)$. Però 2 serà no-residu de q (article 112), de manera que també $2a^2$* i $8n + 5$. *Q. E. D.*

126. Però no es pot demostrar per artificis tan obvis que un nombre primer qualsevol de la forma $8n + 1$ pres positivament sempre és no-residu d'algun nombre primer menor. Però com que aquesta veritat és d'importància màxima, no podem passar per alt una demostració rigorosa per molt que sigui una mica extensa. Passem primer al següent

LEMA. *Si es tenen dues sèries de nombres A, B, C, etc. . . .*, (I), *A′, B′, C′, etc. . . .*, (II) (que la quantitat de termes en cada una d'elles sigui la mateixa o

* Article 98. En efecte, és clar que a^2 és residu de q no divisible per q, ja que altrament també el nombre primer p seria divisible per q, *Q. E. A.*

no, no importa) *disposades de manera que, si p denota qualsevol nombre primer o bé potència d'un primer que divideix algun terme (o també més d'un) de la segona sèrie, siguin divisibles per p com a mínim tants termes a la primera sèrie com ho són a la segona, llavors dic que el producte de tots els nombres* (I) *serà divisible pel producte de tots els nombres* (II).

Exemple. Consti (I) dels nombres 12, 18, 45; (II), de 3, 4, 5, 6, 9. Llavors, seran divisibles per 2, 4, 3, 9, 5: en (I), 2, 1, 3, 2, 1, termes, i, en (II), 2, 1, 3, 1, 1, termes, respectivament; però el producte de tots els termes (I) = 9720 és divisible pel producte de tots els termes (II) = 3240.

Dem. Sigui = Q el producte de tots els termes (I), = Q' el producte de tots els termes de la sèrie (II). És clar que qualsevol nombre primer que sigui divisor de Q' també serà divisor de Q. Ara mostrarem que qualsevol factor primer de Q' té, com a mínim, tantes dimensions en Q com tingui en Q'. Sigui p un tal divisor, i se suposa que a la sèrie (I) a termes són divisibles per p, però no per p^2; b termes divisibles per p^2, però no per p^3; c termes per p^3, però no per p^4, etc.; denotin similarment les lletres a', b', c', etc., per a la sèrie (II), i es copsarà fàcilment que p té $a+b+c+etc.$ dimensions en Q, i $a'+b'+c'+etc.$ en Q'. Però, certament, a' no és més gran que a, b' no més gran que b, etc. (per hipòtesi); per tant, $a'+b'+c'+etc.$ no serà, certament, $> a+b+c+etc.$ I així, com que cap nombre primer no podria tenir més dimensions en Q' que en Q, Q serà divisible per Q' (article 17). *Q. E. D.*

127. Lema. *A la progressió* 1, 2, 3, 4, $\cdots$, n, *no poden ser divisibles per un nombre qualsevol* h *més termes que en la* a, $a+1$, $a+2$, $\cdots$, $a+n-1$, *que consta del mateix nombre de termes.*

En efecte, es copsa sense dificultat que, si n fos múltiple de h, a cada una de les progressions serien divisibles per h $\dfrac{n}{h}$ termes; si no, es posa $n = eh + f$, de manera que f sigui $< h$, i a la primera sèrie e termes seran divisibles per h, però a la darrera, o bé la mateixa quantitat, o bé $e+1$.

D'aquí se segueix com a corol·lari la proposició de la coneguda teoria de nombres figuratius, però, fins ara, no demostrada directament per ningú, si no ens enganyem, que $\dfrac{a(a+1)(a+2)\ldots(a+n-1)}{1\cdot 2\cdot 3\cdots n}$ sempre és un nombre enter.

Finalment, aquest lema s'hauria pogut proposar més generalment així:

A la progressió a, $a+1$, $a+2$, $\ldots$, $a+n-1$, es donen com a mínim tants termes congrus segons el mòdul h a un nombre donat qualsevol, r, com termes divisibles per h en la 1, 2, 3, $\ldots$, n.

128. Teorema. *Sigui* a *un nombre qualsevol de la forma* $8n+1$, p *un nombre qualsevol primer amb* a, *del qual* $+a$ *és residu, però* m, *un nombre arbitrari; llavors, dic que a la progressió* a, $\dfrac{1}{2}(a-1)$, $2(a-4)$, $\dfrac{1}{2}(a-9)$, $2(a-16)$, $\ldots$, $2(a-m^2)$, *o bé* $\dfrac{1}{2}(a-m^2)$,

segons que m sigui parell o bé imparell, es donen com a mínim tants termes divisibles per p com es donin en la $1, 2, 3, \ldots, 2m+1$. Designem la primera progressió per (I); la darrera, per (II).

Dem. I. Quan $p = 2$, tots els termes en (I), excepte el primer, és a dir, m termes, seran divisibles; però el mateix nombre ho seran en (II).

II. Sigui p un nombre imparell, o bé el doble o el quàdruple d'un nombre imparell, i $a \equiv rr \,(\text{mòd.}\, p)$. Llavors, a la progressió $-m$, $-(m-1)$, $-(m-2)$, $\ldots$, $+m$ (que concorda en quantitat de termes amb (I) i (II) i es designarà per (III)), seran congrus a r segons el mòdul p com a mínim tants termes com a la sèrie (II) [siguin] divisibles per p (article precedent). Però entre aquells no poden ocórrer parelles que discrepin només en el signe, no en magnitud.* Finalment, cadascun d'ells tindrà un corresponent a la sèrie (I) que serà divisible per p. Això és, si $\pm b$ fos algun terme de la sèrie (III) congru a r segons p, $a - bb$ serà divisible per p. Així, doncs, si b és parell, el terme $2(a-bb)$ de la sèrie (I) serà divisible per p. Però si b és imparell, el terme $\frac{1}{2}(a-bb)$ serà divisible per p; ja que, evidentment, $\dfrac{a-bb}{p}$ serà un enter *parell* perquè $a - bb$ és divisible per 8; però p, com a molt per 4 (en efecte, a és de la forma $8n+1$, per hipòtesi; en

* En efecte, si fos $r \equiv -f \equiv +f \,\big(\text{mòd.}\, p\big)$, $2f$ resultaria divisible per p, de manera que també $2a$ (a causa que $ff \equiv a \,\big(\text{mòd.}\, p\big)$). Però això altre només podria resultar quan $p = 2$, ja que, per hipòtesi, a és primer amb p. Però, d'aquest cas, ja n'hem parlat separadament.

canvi bb, que és el quadrat d'un nombre imparell, serà de la mateixa forma; per tant, la diferència serà de la forma $8n$). D'aquí es conclou, finalment, que, a la sèrie (I), són divisibles per p tants termes com en (III) siguin congrus a r segons p, *és a dir*, tants com en (II) siguin divisibles per p, o bé més. *Q. E. D.*

III. Sigui p de la forma $8n$, i $a \equiv rr\,(\text{mòd.}\,2p)$. En efecte, es copsa fàcilment que a, ja que per hipòtesi és residu de p, també serà residu de $2p$. Llavors, seran congrus a r segons p, com a mínim, tants termes a la sèrie (III) com, a (II), són divisibles per p, i les magnituds d'aquells seran totes desiguals. Però a cada un d'ells li'n correspondrà algun en (I) divisible per p. En efecte, si $+b$ o bé $-b$ és $\equiv r\,(\text{mòd.}\,p)$, serà $bb \equiv rr\,(\text{mòd.}\,2p)$* de manera que el terme $\frac{1}{2}(b - rr)$ és divisible per p, i molt més $2(b - rr)$. Per tant, en (I) seran divisibles per p com a mínim tants termes com en (II). *Q. E. D.*

129. Teorema. *Si a és un nombre primer de la forma $8n + 1$, es donarà necessàriament algun nombre primer per sota de $2\sqrt{a} + 1$ del qual a sigui no-residu.*

Dem. Sigui a, si pot ser, residu de tots els primers menors que $2\sqrt{a} + 1$. Llavors, es copsarà fàcilment que a també serà residu de tots els nombres compostos menors que $2\sqrt{a}$ (compareu els preceptes pels quals hem ensenyat a decidir si un nombre proposat és residu

* Això és, $bb - rr = (b - r)(b + r)$ serà compost de dos factors, un dels quals és divisible per p (per hipòtesi), l'altre per 2 (ja que tant b com r són imparells); de manera que $bb - rr$ és divisible per $2p$.

o no d'un nombre compost; article 105). Sigui $= m$ el nombre més pròxim menor que $\sqrt{a}$. Llavors, a la sèrie (I) $\ldots$ a, $\frac{1}{2}(a-1)$, $2(a-4)$, $\frac{1}{2}(a-9)$, $\ldots$, $2(a-mm)$, o bé $\frac{1}{2}(a-mm)$, seran divisibles per un nombre qualsevol menor que $2\sqrt{a}$ tants termes o més que en la (II) $\ldots$ 1, 2, 3, 4, $\ldots$, $2m+1$ (article precedent). Però, d'aquí, se segueix que el producte de tots els termes (I) és divisible pel producte de tots els termes (II) (article 126). Però allò és o bé $= a(a-1)(a-4)\cdots(a-mm)$ o bé la meitat d'aquest producte (segons que m [sigui] parell o bé imparell). Per tant, el producte $a(a-1)(a-4)\cdots(a-mm)$ es podrà dividir, certament, pel producte de tots els termes (II), i, com que tots aquests termes són primers amb a, també aquell producte, omès el factor a. Però el producte de tots els termes (II) també es pot expressar així $(m+1)((m+1)^2-1)((m+1)^2-4)\cdots((m+1)^2-m^2)$. Així, doncs,

$$\frac{1}{m+1}\cdot\frac{a-1}{(m+1)^2-1}\cdot\frac{a-4}{(m+1)^2-4}\cdots\frac{a-m^2}{(m+1)^2-m^2}$$

resultarà un nombre enter, encara que sigui un producte de fraccions menors que la unitat; en efecte, ja que $\sqrt{a}$ ha de ser necessàriament irracional, serà $m+1>\sqrt{a}$, de manera que $(m+1)^2>a$. Finalment, d'aquí es conclou que la nostra suposició no pot tenir lloc. *Q. E. D.*

Ara, com que a és, certament, >4, serà $2\sqrt{a}<a$, de manera que es donarà algun primer $<a$ del qual a és no-residu.

130. Després que hem demostrat rigorosament que qualsevol nombre primer de la forma $4n+1$, tant agafat positivament com negativament, és no-residu d'algun

nombre primer menor, passem immediatament a una comparació més exacta i més general sobre en quina mesura, dels nombres primers, un és residu o bé no-residu de l'altre.

Més amunt hem demostrat amb tot rigor que -3 i $+5$ són residus o bé no-residus de tots els nombres primers que són residus o bé no-residus de 3, 5, respectivament.

Però, per indici bastit amb els nombres següents, es troba que

-7, -11, $+13$, $+17$, -19, -23, $+29$, -31, $+37$, $+41$, -43, -47, $+53$, -59, etc., són residus o bé no-residus de tots els nombres primers que, presos positivament, són residus o bé no-residus d'aquells primers, respectivament. Aquest indici es pot confegir molt fàcilment amb l'ajut de la taula II.

Però, posada una lleugera atenció, qualsevol observarà que, d'aquests nombres primers, són afectats de signe positiu els que són de la forma $4n+1$, però negatiu els que són de la forma $4n+3$.

131. Demostrarem aviat que això que hem detectat aquí per indici té lloc en general. Però, abans que emprenguem aquesta tasca, serà necessari extreure tot el que se segueix del teorema si se suposa vertader. Enunciem així el teorema.

Si p és un nombre primer de la forma $4n+1$, $+p$ serà residu o bé no-residu de qualsevol nombre primer que, pres positivament, és residu o bé no-residu de p; però si p és de la forma $4n+3$, ho serà $-p$.

Com que gairebé tot el que es pot dir dels residus quadràtics es basa en aquest teorema, no serà dissonant la denominació *teorema fonamental*, que usarem en el que segueix.

Perquè els nostres raonaments es puguin expressar tan breument com sigui possible, denotarem els nombres primers de la forma $4n+1$ per a, a', a'', etc., els nombres primers de la forma $4n+3$ per b, b', b'', etc.; nombres qualssevol de la forma $4n+1$ per A, A', A'', etc., però nombres qualssevol de la forma $4n+3$ per B, B', B'', etc.; finalment, la lletra R, interposada entre dues quantitats, indicarà que la primera és residu de la següent; així com la lletra N tindrà la significació contrària. Per exemple, $+5R11$, $\pm 2N5$ indicarà que $+5$ és residu de 11, $+2$ o bé -2 són no-residus de 5. Ara, reunit el teorema fonamental amb els teoremes de l'article 111, es dedueixen fàcilment les proposicions següents.

	Si		serà
1.	$\pm aRa'$	$\cdots$	$\pm a'Ra$
2.	$\pm aNa'$	$\cdots$	$\pm a'Na$
3.	$\left\{\begin{matrix}+aRb\\-aNb\end{matrix}\right\}$	$\cdots$	$\pm bRa$
4.	$\left\{\begin{matrix}+aNb\\-aRb\end{matrix}\right\}$	$\cdots$	$\pm bNa$
5.	$\pm bRa$	$\cdots$	$\left\{\begin{matrix}+aRb\\-aNb\end{matrix}\right.$
6.	$\pm bNa$	$\cdots$	$\left\{\begin{matrix}+aNb\\-aRb\end{matrix}\right.$

	Si		será
7.	$\left\{\begin{array}{l}+bRb'\\-bNb'\end{array}\right\}$	$\cdots$	$\left\{\begin{array}{l}+b'Nb\\-b'Rb\end{array}\right\}$
8.	$\left\{\begin{array}{l}+bNb'\\-bRb'\end{array}\right\}$	$\cdots$	$\left\{\begin{array}{l}+b'Rb\\-b'Nb\end{array}\right\}$

132. En aquestes es contenen tots els casos que poden ocórrer comparant dos nombres primers; les que segueixen pertanyen a nombres qualssevol, però les seves demostracions són menys òbvies.

	Si		será
9.	$\pm aRA$	$\cdots$	$\pm ARa$
10.	$\pm bRA$	$\cdots$	$\left\{\begin{array}{l}+ARb\\-ANb\end{array}\right\}$
11.	$+aRB$	$\cdots$	$\pm BRa$
12.	$-aRB$	$\cdots$	$\pm BNa$
13.	$+bRB$	$\cdots$	$\left\{\begin{array}{l}-BRb\\+BNb\end{array}\right\}$
14.	$-bRB$	$\cdots$	$\left\{\begin{array}{l}+BRb\\-BNb\end{array}\right\}$

Com que les demostracions de totes aquestes proposicions són dependents dels mateixos principis, no serà necessari desenvolupar-les totes; la demostració de la proposició 9, que afegim, pot servir com a exemple. Però abans que tot, s'observa que qualsevol nombre de

la forma $4n+1$, o bé no té cap factor de la forma $4n+3$, o bé en té dos, o bé quatre, etc.; és a dir, la quantitat de tals factors (entre els quals també poden haver-n'hi d'iguals) sempre serà parella; en canvi, qualsevol de la forma $4n+3$ implica una quantitat imparella de factors de la forma $4n+3$ (és a dir, o bé un, o bé tres, o bé cinc, etc.). La quantitat de factors de la forma $4n+1$ es manté indeterminada.

La proposició 9 es demostra així. Sigui A el producte de factors primers a', a'', a''', etc., b, b', b'', etc., i la quantitat de factors b, b', b'', etc., serà parella (també pot no presentar-se'n cap, cosa que rendeix el mateix). Ara, si a és residu de A, també serà residu de tots els factors a', a'', a''', etc.; b, b', b'', etc.; per tant, per les proposicions 1, 3 de l'article precedent, cadascun d'aquests factors serà residu de a, de manera que, també, el producte A. Per a $-A$, ha de ser el mateix. Però si $-a$ és residu de A, [resulta] això mateix de tots els factors a', a'', etc., b, b', etc.; cada un dels a', a'', etc., seran residus de a, però cada un dels b, b', etc., no-residus. Però com que la quantitat dels darrers és parella, el producte de tots, *és a dir*, A, serà residu de a, i, d'aquí, també $-A$.

133. Emprenguem una investigació encara més general. Examinem dos nombres imparells qualssevol primers entre si, P, Q, afectats de signes qualssevol. S'imagina P descompost en els seus factors primers sense tenir en consideració el seu signe, i es designarà per p quants n'apareixen entre aquests dels quals Q és no-residu. Però si algun nombre primer del qual Q és no-residu ocorre més entre els factors de P, també caldrà comptar-lo més. Similarment, sigui q la quantitat de

factors primers de Q dels quals P és no-residu. Llavors, els nombres p, q, tindran una relació mútua certa que depèn de la naturalesa dels nombres P, Q. Això és, si un dels nombres p, q, és parell o bé imparell, la forma dels nombres P, Q, ensenyarà si l'altre és parell o bé imparell. Aquesta relació es mostra a la taula següent.

p, q, seran simultàniament parells o bé simultàniament imparells quan els nombres P, Q, tinguin les formes:

1.	$+A$	$+A'$
2.	$+A$	$-A'$
3.	$+A$	$+B$
4.	$+A$	$-B$
5.	$-A$	$-A'$
6.	$+B$	$-B'$

Contràriament, un dels nombres p, q, serà parell i l'altre imparell quan els nombres P, Q, tinguin les formes:

7.	$-A$	$+B$
8.	$-A$	$-B$
9.	$+B$	$+B'$
10.	$-B$	$-B'$

Exemple. Siguin proposats els nombres $+1197$ i -55, que s'hauran de referir al cas quart. D'una banda, 1197 és no-residu d'un factor primer de 55, això és, el nombre 5, de l'altra, -55 és no-residu dels tres factors primers de 1197, això és, dels nombres 3, 7, 19.

Si P i Q designen nombres primers, aquestes proposicions es converteixen en les que hem transmès a l'article 131. Això és, aquí p i q no poden resultar més

grans que 1; per tant, quan se suposa que p és parell, serà necessàriament $= 0$; és a dir, Q serà residu de P; però quan p és imparell, Q serà no-residu de P. I recíprocament. Així, escrits a, b, en lloc de A, B, de 8 se segueix que si $-a$ fos residu o bé no-residu de b, $-b$ seria no-residu o bé residu de a, cosa que concorda amb 3 i 4 de l'article 131.

És clar, en general, que Q no pot ser residu de P, llevat que fos $p = 0$; així, doncs, si p és imparell, Q serà, certament, no-residu de P.

D'aquí també es poden derivar sense dificultat les proposicions de l'article precedent.

D'altra banda, aviat serà clar que aquesta representació general és més que una especulació estèril, ja que, sense ella, una demostració completa del teorema fonamental amb prou feines es podria portar a terme.

134. Ataquem ara la deducció d'aquestes proposicions.

I. Imaginem, com abans, P descompost en els seus factors primers, negligits els signes, i, a sobre, també Q es descompon en factors de qualsevol manera, però de forma que es tingui en compte el signe de Q. Es combinen cada un d'aquells amb cada un d'aquests. Llavors, si s designa la quantitat de totes les combinacions en què un factor de Q és no-residu d'un factor de P, p i s seran o bé simultàniament parells, o bé simultàniament imparells. En efecte, siguin f, f', f'', etc., els factors primers de P i, entre els factors en què s'ha descompost Q, siguin m els que són no-residus de f, m' no-residus

de f', m'' no-residus de f'', etc. Llavors, qualsevol copsarà fàcilment que serà $s = m + m' + m'' + etc.$, però p expressa quants nombres d'entre els m, m', m'', etc., són imparells. D'on és clar espontàniament que s serà parell quan p sigui parell, imparell quan p sigui imparell.

II. Això val en general, de qualsevol manera en què Q sigui descompost en factors. Baixem a casos particulars. Contemplem, primer, el cas en què un dels nombres, P, és positiu, i l'altre, Q, o bé de la forma $+A$, o bé de la forma $-B$. Es descomponen P, Q, en els seus factors primers, s'atribueix a cada un dels factors de P el signe positiu, però a cada un dels factors de Q signe positiu o bé negatiu segons si són de la forma a o bé b; però llavors, evidentment, Q resultarà de la forma $+A$ o bé $-B$, tal com es requereix. Es combina cada un dels factors de P amb cada un dels factors de Q i, com abans, designi s la quantitat de combinacions en què el factor de Q és no-residu del factor de P i, similarment, t, la quantitat de combinacions en què el factor de P és no-residu del factor de Q. Però del teorema fonamental se segueix que aquelles combinacions seran idèntiques a aquestes, de manera que $s = t$. Finalment, d'això que acabem de demostrar, se segueix que és $p \equiv s \,(\text{mòd. } 2)$, $q \equiv t \,(\text{mòd. } 2)$, d'on resulta $p \equiv q \,(\text{mòd. } 2)$.

Així, es tenen les proposicions 1, 3, 4 i 6 de l'article 133.

Les proposicions restants es poden trobar directament per un mètode similar, però necessiten una consideració nova; en canvi, es deriven més fàcilment de les precedents de la manera següent.

III. Denotin novament P, Q, nombres imparells qualssevol primers entre si, p, q, les quantitats respectives de factors primers de P, Q, dels quals Q, P, són no-residus. Finalment, sigui p' la quantitat de factors primers de P dels quals $-Q$ és no-residu (quan Q és negatiu per ell mateix, evidentment, $-Q$ indicarà un nombre positiu). Ara, es distribueixen tots els factors primers de P en quatre classes.

1) En factors de la forma a, dels quals Q és residu.

2) Factors de la forma b, dels quals Q és residu. Sigui χ la seva quantitat.

3) Factors de la forma a, dels quals Q és no-residu. Sigui ψ la seva quantitat.

4) Factors de la forma b, dels quals Q és no-residu. La quantitat dels quals, $= \omega$.

Llavors, es copsa fàcilment que serà $p = \psi + \omega$, $p' = \chi + \psi$.

Ara, quan P és de la forma $\pm A$, $\chi + \omega$, serà un nombre parell, de manera que també $\chi - \omega$; per tant, resultarà $p' = p + \chi - \omega \equiv p \,(\text{mòd. } 2)$; però quan P és de la forma $\pm B$, per un raonament similar es troba que els nombres p, p', són incongrus segons el mòdul 2.

IV. Apliquem això a cadascun dels casos. Primerament, siguin, tant P com Q, de la forma $+A$, i, de la proposició 1, serà $p \equiv q \,(\text{mòd. } 2)$; però serà $p' \equiv p \,(\text{mòd. } 2)$; per tant, també $p' \equiv q \,(\text{mòd. } 2)$. Això concorda amb la proposició 2. De manera similar, si P és

de la forma $+A$, Q de la forma $-A$, serà $p \equiv q \,(\text{mòd. } 2)$, de la proposició 2, que hem demostrat fa un instant; d'aquí, com que $p' \equiv p$, serà $p' \equiv q$. Així també s'ha demostrat la proposició 5.

De la mateixa manera, es deriven la proposició 7 de la 3; la proposició 8, bé de la 4, bé de la 7; la proposició 9 de la 6; la proposició 10, d'aquesta mateixa.

135. Certament, les proposicions de l'article 133 no s'han demostrat per l'article precedent, sinó que, en canvi, s'ha mostrat que la seva veritat depèn de la veritat del teorema fonamental que hem suposat per algun temps. Però és evident, per aquest mètode de deducció, que aquelles valen per als nombres P, Q, només que el teorema fonamental tingui lloc per a tots els factors primers d'aquests nombres comparats entre si, encara que no sigui veritat en general. Així, doncs, ara atacarem la demostració del teorema fonamental. Comencem aquesta amb l'explicació següent.

Direm que el teorema fonamental és veritat fins a algun nombre M, si val per a dos nombres primers qualssevol cap dels quals no supera M.

S'ha d'entendre de manera similar si diem que els teoremes dels articles 131, 132, 133, són veritat fins a algun terme. Però es copsa fàcilment que, si se sap fins a algun terme la veritat del teorema fonamental, aquestes proposicions hauran de tenir lloc fins al mateix terme.

136. Es confirma fàcilment per indici que el teorema fonamental és veritat per a nombres petits, i es pot determinar el límit fins al qual, certament, té lloc.

Demanem que aquest indici s'hagi instituït, encara que és completament indiferent fins on l'haguem aconseguit; en especial, seria suficient si només l'haguéssim confirmat fins al nombre 5, però això s'ha assolit per la sola observació que és $+5N3$, $\pm 3N5$.

Ara, si el teorema fonamental no és veritat en general, es donarà algun límit, T, fins al qual valdrà, però de manera que no valdrà fins al nombre més gran més pròxim, $T+1$. Però això és el mateix que si diem que es donen dos nombres primers, el més gran dels quals és $T+1$, que, comparats entre si, contradiuen el teorema fonamental, però dos altres nombres primers qualssevol estan d'acord amb aquest teorema sempre que tots dos siguin menors que $T+1$. D'on se segueix que les proposicions dels articles 131, 132, 133, també hauran de tenir lloc fins a T. Ara mostrarem, en canvi, que aquesta suposició no pot ser consistent. Però, segons les formes diferents que poden tenir tant $T+1$ com el nombre primer menor que $T+1$ que hem suposat que, comparat amb $T+1$, contradiu el teorema, caldrà distingir els casos següents. Designem per p aquest nombre primer.

Quan tant $T+1$ com p són de la forma $4n+1$, el teorema fonamental pot ser fals de dues maneres, això és, si fos, *o bé* $\pm pR(T+1)$ i $\pm(T+1)Np$ simultàniament, *o bé* $\pm pN(T+1)$ i $\pm(T+1)Tp$ simultàniament.

Quan tant $T+1$ com p són de la forma $4n+3$, el teorema fonamental serà fals si fos, *o bé* $+pR(T+1)$ i $-(T+1)Np$ simultàniament (o bé, cosa que rendeix el mateix, $-pN(T+1)$ i $+(T+1)Rp$), *o bé* $+pN(T+1)$ i $-(T+1)Rp$ (o sigui, $-pR(T+1)$ i $+(T+1)Np$).

Quan $T+1$ és de la forma $4n+1$ però p de la forma $4n+3$, el teorema fonamental serà fals si fos, *o bé* $\pm pR(T+1)$ i $+(T+1)Np$ (o sigui, $-(T+1)Rp$), *o bé* $\pm pN(T+1)$, i $-(T+1)Np$ (o sigui, $+(T+1)Rp$).

Quan $T+1$ és de la forma $4n+3$, però p de la forma $4n+1$, el teorema fonamental serà fals si fos, *o bé* $+pR(T+1)$ (o sigui, $-pN(T+1)$) i $\pm(T+1)Np$, *o bé* $+pN(T+1)$ (o sigui, $-pR(T+1)$) i $\pm(T+1)Rp$.

Si es pogués demostrar que cap d'aquests vuit casos no pot tenir lloc, simultàniament serà cert que la veritat del teorema fonamental no està circumscrita a cap límit. Així, ataquem ara aquesta feina; però, com que alguns d'aquests casos depenen d'altres, no es podrà conservar el mateix ordre amb què els hem enumerat aquí.

137. *Primer cas. Quan* $T+1$ *és de la forma* $4n+1$, $(=a)$, *i* p *de la mateixa forma; si,* a *sobre,* $\pm pRa$, *no pot ser* $\pm aNp$. Aquest cas fou el primer més amunt.

Sigui $+p \equiv e^2 \,(\text{mòd. } a)$, i e parell i $< a$ (cosa que es pot obtenir sempre). Ara, s'han de distingir dos casos.

I. Quan e no és divisible per p. Es posa $e^2 = p + af$, i f serà positiu, de la forma $4n+3$ (o sigui, de la forma B), $< a$, i no divisible per p. A més a més, serà $e^2 \equiv p \,(\text{mòd. } f)$, és a dir, pRf, de manera que, de la proposició 11 de l'article 132, $\pm fRp$ (en efecte, com que p, $f < a$, aquestes proposicions valdran per a aquests). Però també és $afRp$; per tant, també resultarà $\pm aRp$.

II. Quan e és divisible per p, es posa $e = gp$ i $e^2 = p + aph$, o sigui, $pg^2 = 1 + ah$. Llavors, h serà de la forma $4n+3$, (B), i primer amb p i g^2. A més a més, serà pg^2Rh, de manera que, també, pRh; d'aquí (proposició 11 de l'article 132), $\pm hRp$. Però també és $-ahRp$, ja que $-ah \equiv 1 \,(\text{mòd.}\, p)$; per tant, també resultarà $\mp aRp$.

138. *Segon cas. Quan* $T+1$ *és de la forma* $4n+1$, $(= a)$, p *de la forma* $4n+3$, *i* $\pm pR(T+1)$, *no pot ser* $+(T+1)Np$, *o sigui,* $-(T+1)Rp$. Aquest cas fou el cinquè més amunt.

Sigui, com més amunt, $e^2 = p + fa$, i e parell i $< a$.

I. Quan e no és divisible per p, f tampoc no serà divisible per p. Però, a part d'això, f serà positiu, de la forma $4n + 1$ (o sigui A) i $< a$, i $+pRf$, de manera que (proposició 10 de l'article 132) $+fRp$. Però també és $+faRp$; per tant, resultarà $+aRp$, o sigui, $-aNp$.

II. Quan e és divisible per p, sigui $e = pg$ i $f = ph$. Així, serà $g^2p = 1 + ha$. Llavors, h serà positiu, de la forma $4n + 3$, (B), i primer amb p i g^2. A més a més, $+g^2pRh$, de manera que $+pRh$; d'aquí resulta (proposició 13 de l'article 132) $-hRp$. Però és $-haRp$, d'on resulta $+aRp$ i $-aNp$.

139. *Tercer cas. Quan* $T+1$ *és de la forma* $4n+1$, $(= a)$, p *de la mateixa forma, i* $\pm pNa$, *no pot ser* $\pm aRp$. (Segon cas de més amunt.)

S'agafa algun nombre primer menor que a del qual $+a$ sigui no-residu, els quals hem demostrat més amunt

que es donen (articles 125, 129). Aquí, però, convindria considerar dos casos separadament, segons que aquest nombre primer fos de la forma $4n + 1$ o bé $4n + 3$; en efecte, no es va demostrar que es donin tals nombres primers *d'ambdues* formes.

I. Sigui aquest nombre primer de la forma $4n+1$ i $= a'$. Llavors, serà $\pm a'Na$ (article 137), de manera que $\pm a'pRa$. Així, doncs, sigui $e^2 \equiv a'p\,(\text{mòd. } a)$, i e parell, $< a$. Llavors, s'hauran de distingir de nou quatre casos.

1) Quan e no és divisible ni per p ni per a'. Es posa $e^2 = a'p \pm af$, agafat el signe de manera que f resulti positiu. Llavors, serà $f < a$, primer amb a' i p, de la forma $4n + 3$ per al signe superior, de la forma $4n + 1$ per a l'inferior. Per abreujar, designem per $[x, y]$ la quantitat de factors primers del nombre y dels quals x és no-residu. Llavors, serà $a'pRf$, de manera que $[a'p, f] = 0$. D'aquí, $[f, a'p]$ serà un nombre parell (proposicions 1, 3, de l'article 133), és a dir, o bé $= 0$, o bé $= 2$. Per tant, f serà o bé residu de cada un dels nombres a', p, o bé de cap dels dos. Però allò és impossible, ja que $\pm af$ seria residu de a' i $\pm aNa'$ (per hipòtesi); d'on resulta $\pm fNa'$. D'aquí, f ha de ser no-residu de cada un dels nombres a', p. Però, a causa que $\pm afRp$, serà $\pm aNp$. *Q. E. D.*

2) Quan e és divisible per p, però no per a', sigui $e = gp$ i $g^2p = a' \pm ah$, amb el signe determinat de manera que h resulti positiu. Llavors, serà $h < a$, primer amb a', g i p, i de la forma $4n + 3$ per al signe superior, però de la forma $4n + 1$ per a l'inferior. De l'equació $g^2p = a' \pm ah$, si es multiplica per p i a', es pot deduir sense dificultat que $pa'Rh \cdots (\alpha)$, $\pm ahpRa' \ldots (\beta)$,

$aa'hRp \ldots (\gamma)$. De (α), se segueix que $[pa', h] = 0$, de manera que (proposicions 1, 3, de l'article 133) $[h, pa']$ és parell; és a dir, h serà, o bé no-residu de cada un dels p, a', o bé de cap dels dos. *En el primer cas*, de (β) se segueix $\pm apNa'$, i, com que, per hipòtesi, seria $\pm aNa'$, serà pRa'. D'aquí, pel teorema fonamental, que val per als nombres p, a', menors que $T + 1$, és $\pm a'Rp$. D'aquí, i del fet que hNp, resulta, per (γ), $\pm aNp$. *Q. E. D. En el darrer cas*, de (β) se segueix $\pm apRa'$; d'aquí, $\pm pNa'$, $\pm a'Np$, i, finalment, d'aquí i de hRp, resulta $\pm aNp$, per (γ). *Q. E. D.*

3) Quan e és divisible per a', però no per p. Per a aquest cas, la demostració procedeix gairebé de la mateixa manera com en el precedent, i no podrà entretenir ningú que l'hagi penetrada.

4) Quan e és divisible tant per a' com per p, de manera que, també, pel producte $a'p$ (en efecte, suposem que els nombres a' i p són *diferents*, ja que, altrament, allò que ens proposem demostrar, que és aNp', ja estaria contingut a la hipòtesi aNa'), sigui $e = ga'p$ i $g^2a'p = 1 \pm ah$. Llavors, serà $h < a$, primer amb a' i p, i de la forma $4n + 3$ per al signe superior, de la forma $4n + 1$ per a l'inferior. Però es copsa fàcilment que d'aquesta equació es poden deduir les $a'pRh$, $\pm ahpRa'$, $\pm aha'Rp$, que coincideixen amb les que hem trobat a (2). Pel que resta, però, la demostració és la mateixa.

II. Quan aquest nombre primer és de la forma $4n + 3$, la demostració és tan similar a la precedent que ens semblaria superflu afegir-la. Només observem, en favor dels que desitgin vivament desenvolupar-la per ells mateixos (cosa que recomanem molt), que, després que

s'hagi arribat a l'equació $e^2 = bp \pm af$ (on b designa aquell nombre primer), serà útil per a la claredat si es considera separadament cada signe.

140. *Quart cas. Quan* $T+1$ *és de la forma* $4n+1$, $(= a)$, *p de la forma* $4n+3$, *i* $\pm pNa$, *no podrà ser* $+aRp$, *o sigui,* $-aNp$. (Sisè cas de més amunt.)

Com que la demostració d'aquest cas també seria completament similar a la demostració del tercer cas, l'ometem per abreujar.

141. *Cinquè cas. Quan* $T+1$ *és de la forma* $4n+3$, $(= b)$, *p de la mateixa forma, i* $+pRb$ *(o sigui,* $-pNb$*), no pot ser* $+bRp$, *o sigui,* $-bNp$. (Tercer cas de més amunt.)

Sigui $p \equiv e^2 \,(\text{mòd.}\, b)$, i e parell i $< b$.

I. Quan e no és divisible per p. Es posa $e^2 = p+bf$, i f serà positiu, de la forma $4n+3$, $< b$, i primer amb p. A més a més, serà pRf, de manera que, per la proposició 13 de l'article 132, $-fRp$. D'aquí i de $+bfRp$, resulta $-bRp$, de manera que $+bNp$. *Q. E. D.*

II. Quan e és divisible per p, sigui $e = pg$ i $ggp = 1+bh$. Llavors, h serà de la forma $4n+1$ i primer amb p, $p \equiv g^2p^2 \,(\text{mòd.}\, h)$, de manera que pRh; d'aquí, resulta $+hRp$ (proposició 10 de l'article 132), d'on, i de $-bhRp$, se segueix $-bRp$, o sigui, $+bNp$. *Q. E. D.*

142. *Sisè cas. Quan* $T+1$ *és de la forma* $4n+3$, $(= b)$, *p de la forma* $4n+1$, *i* pRb, *no podrà ser* $\pm bNp$. (Setè cas de més amunt.)

N'ometem la demostració, totalment similar a la precedent.

143. *Setè cas. Quan* $T+1$ *és de la forma* $4n+3$, $(=b)$, *p de la mateixa forma, i* $+pNb$, *o sigui,* $-pRb$, *no podrà ser* $+bNp$, *o sigui,* $-bRp$. (Quart cas de més amunt.)

Sigui $-p \equiv e^2 \,(\text{mòd.}\, b)$, i e parell i $< b$.

I. Quan e no és divisible per p. Sigui $-p = e^2 - bf$, i f serà positiu, de la forma $4n+1$, primer amb p, i menor que b (efectivament, e no és, certament, més gran que $b-1$, $p < b-1$; per tant, serà $bf = e^2 + p < b^2 - b$, és a dir, $f < b-1$). A més a més, serà $-pRf$; d'aquí (proposició 10 de l'article 132), $+fRp$, d'on, i de $+bfRp$, resulta $+bRp$, o sigui, $-bNp$.

II. Quan e és divisible per p, sigui $e = pg$ i $g^2 p = -1 + bh$. Llavors, h serà positiu, de la forma $4n+3$, primer amb p, i $< b$. A més a més, serà $-pRh$, d'on resulta (proposició 14 de l'article 132) $+hRp$. D'aquí i de $bhRp$, se segueix $+bRp$, o sigui, $-bNp$. *Q. E. D.*

144. *Vuitè cas. Quan* $T+1$ *és de la forma* $4n+3$, $(=b)$, *p de la forma* $4n+1$, *i* $+pNb$, *o sigui,* $-pRb$, *no podrà ser* $\pm bRp$. (Últim cas de més amunt.)

La demostració procedeix igual com en el cas precedent.

145. En les demostracions precedents sempre hem agafat per a e un valor parell (articles 137-144); convé observar que també s'hauria pogut admetre un valor im-

parell, però, llavors, s'haurien hagut d'introduir encara més distincions. Aquells que es delecten en aquestes disquisicions, no faran res inútil si exerciten les seves forces en el desenvolupament d'aquests casos. Llavors, s'haurien d'haver suposat, a part d'això, els teoremes que pertanyen als residus $+2$ i -2; però, com que la nostra demostració s'ha acabat sense aquests teoremes, d'aquí obtenim un mètode nou per a demostrar aquella. Aquest no s'ha de menysprear de cap manera, ja que els mètodes que hem usat més amunt per a la demostració del teorema que ± 2 és residu de qualsevol nombre primer de la forma $8n + 1$ podrien semblar menys directes. Suposarem demostrats els casos restants (que atenyen nombres primers de les formes $8n + 3$, $8n + 5$, $8n + 7$) pels mètodes transmesos més amunt, i que aquell teorema s'ha trobat només per indici; però elevarem aquest indici al grau de certesa per les reflexions següents.

Si ± 2 no fos residu de tots els nombres primers de la forma $8n + 1$, es posa $= a$ el mínim primer d'aquesta forma per al qual ± 2 és no-residu, de manera que el teorema valgui per a tots els primers menors que a. Llavors, s'agafa algun nombre primer $< \frac{1}{2}a$ del qual a és no-residu (es dedueix fàcilment de l'article 129 que, d'aquests, se'n donen). Sigui aquest $= p$, i, pel teorema fonamental, serà pNa. D'aquí resulta $\pm 2pRa$. Així, sigui $e^2 \equiv 2p \,(\text{mòd. } a)$, de manera que e sigui imparell i $< a$. Llavors, caldrà distingir dos casos.

I. Quan e no és divisible per p. Sigui $e^2 = 2p + aq$ i q serà positiu, de la forma $8n + 7$ o bé de la forma $8n + 3$ (segons si p és de la forma $4n + 1$, o bé $4n + 3$), $< a$, i no divisible per p. Ara, es distribueixen tots els factors

primers de q en quatre classes; això és, siguin e de la forma $8n+1$, f de la forma $8n+3$, g de la forma $8n+5$, h de la forma $8n+7$; sigui E el producte dels factors de la primera classe, F, G, H, els productes dels factors de la segona, tercera i quarta classes, respectivament.* Fet això així, considerem, *primer*, el cas en què p és de la forma $4n+1$, o sigui, q de la forma $8n+7$. Llavors, es copsa fàcilment que serà $2RE$, $2RH$, d'on pRE, pRH, i, d'aquí, finalment, ERp, HRp. A més a més, 2 serà no-residu de qualsevol factor de la forma $8n+3$ o bé $8n+5$, de manera que, també, p; d'aquí, qualsevol tal factor és no-residu de p; d'on es conclou fàcilment que FG seria residu de p, si $f+g$ fos parell, no-residu, si $f+g$ fos imparell. Però $f+g$ no pot ser imparell; en efecte, es copsarà fàcilment, enumerant tots els casos, que $EFGH$, o sigui, q, resultaria o bé de la forma $8n+3$, o bé $8n+5$, si $f+g$ fos imparell, no importa quins siguin cada un dels e, f, g, h, contra la hipòtesi. Així, doncs, serà $FGRp$, $EFGHRp$, o sigui, qRp, i, d'aquí, finalment, per causa que $aqRp$, aRp, *contra la hipòtesi*. *Segon*, quan p és de la forma $4n+3$, es pot mostrar de manera similar que serà pRE, de manera que ERp, $-pRF$, i, així, FRp; finalment, $g+h$ és parell, i, d'aquí, $GHRp$, d'on se segueix, finalment, que qRp, aRp, *contra la hipòtesi*.

II. Quan e és divisible per p, la demostració es podrà acabar de manera similar i ser desenvolupada sense dificultat pels experts (només per als quals s'ha escrit aquest article). Nosaltres l'ometem per abreujar.

---

*Si en alguna classe no hi hagués cap factor, en lloc del producte d'aquests caldria escriure 1.

146. Pel teorema fonamental i les proposicions que pertanyen als residus -1 i ± 2, sempre es pot determinar si qualsevol nombre donat és residu o no-residu d'un nombre primer donat. Però no serà inútil fer visibles aquí, de nou, també les restants [proposicions], que hem transmès més amunt, perquè es tinguin reunides totes les que són necessàries per a la solució del

PROBLEMA. *Proposats dos nombres qualssevol P, Q, trobar si l'un, Q, és residu o no-residu de l'altre, P.*

Solució. I. Sigui $P = a^\alpha b^\beta c^\gamma etc.$, on a, b, c, etc., designen nombres primers diferents agafats positivament (ja que, evidentment, P s'ha de prendre absolut). Per abreujar, en aquest article, anomenarem, simplement, *relació* de dos nombres x, y, aquella en què el primer, x, és residu o bé no-residu del darrer, y. Així, doncs, la relació de Q, P, depèn de les relacions de Q, a^α; Q, b^β; etc. (article 105).

II. Per distingir la relació de Q, a^α (de fet, per a les restants Q, b^β, etc., val el mateix), cal distingir dos casos.

1. Quan Q és divisible per a. Es posa $Q = Q' a^e$, de manera que Q' no sigui divisible per a. Llavors, si $e = \alpha$, o bé $e > \alpha$, serà QRa^α; però, si $e < \alpha$ i imparell, serà QNa^α; finalment, si $e < \alpha$ i parell, Q tindrà la mateixa relació amb a^α que Q' té amb $a^{\alpha - e}$. Així, aquest cas s'ha reduït a

2. Quan Q no és divisible per a. Aquí distingim de nou dos casos.

(A) Quan $a = 2$. Llavors, quan $\alpha = 1$, sempre serà QRa^α; però quan $\alpha = 2$, es requereix que Q sigui de la forma $4n + 1$; finalment, quan $\alpha = 3$, o bé > 3, Q ha de ser de la forma $8n + 1$. Si aquesta condició té lloc, serà QRa^α.

(B) Quan a és algun nombre primer. Llavors, Q tindrà la mateixa relació amb a^α que té amb a (vegeu l'article 101).

III. La relació d'un nombre qualsevol Q amb un nombre primer a (imparell) s'investiga així. Quan $Q > a$, se substitueix en lloc de Q el seu residu mínim positiu segons el mòdul a.* Aquest tindrà la mateixa relació amb a que té Q.

A més a més, es descompon Q, o sigui, el nombre pres en el seu lloc, en els seus factors primers p, p', p'', etc., als quals cal afegir el factor -1 quan Q és negatiu. Llavors, se sap que la relació de Q amb a depèn de les relacions de cada un dels p, p', p'', etc., amb a. Això és, si entre aquells factors, $2m$ són no-residus de a, serà QRa; en canvi, si $2m + 1$, serà QNa. Però es copsa fàcilment que, si entre els factors p, p', p'', etc., n'ocorren dos, o bé quatre, o bé sis, o bé, en general, $2k$ d'iguals, tots aquests es poden rebutjar.

IV. Si -1 i 2 es troben entre els factors p, p', p'', etc., la seva relació amb a es pot trobar pels articles 108, 112, 113, 114. Però la relació dels restants amb a depèn de la relació de a amb ells (*teorema fonamental* i

* *Residu* amb el significat de l'article 4. Sovint és preferible agafar el residu mínim *absolut*.

proposicions de l'article 131). Sigui p un d'ells, i es trobarà (tractant els nombres a, p, de la mateixa manera que, abans, Q i a, respectivament més grans que ells) que la relació de a amb p o bé es pot determinar pels articles 108-114 (això és, si el residu mínim de a (mòd. p) no té cap factor imparell), o bé depèn, a sobre, de la relació de p amb certs nombres primers menors que p. El mateix val per als factors restants p', p'', etc. Ara es copsa fàcilment que, per continuació d'aquestes operacions, s'arribarà finalment a nombres les relacions dels quals es puguin determinar per les proposicions dels articles 108–114. Aquestes [proposicions] resultaran més clares amb un exemple.

Exemple. Se cerca la relació del nombre +453 amb 1236. És $1236 = 4 \cdot 3 \cdot 103$; $+453 R 4$, per II, 2 (A); $+453 R 3$, per II, 1. Així, doncs, resta que s'explori la relació de +453 amb 103. Serà, però, la mateixa que té +41 ($\equiv 453$ (mòd. 103)) amb 103; la mateixa de +103 amb 41 (*teorema fonamental*); o sigui, la de −20 amb 41. Però és $-20 R 41$, ja que $-20 = -1 \cdot 2 \cdot 2 \cdot 5$; $-1 R 41$ (article 108); i $+5 R 41$, perquè $41 \equiv 1$, de manera que és residu de 5 (teorema fonamental). D'aquí, se segueix que $+453 R 103$, i, d'aquí, finalment, $+453 R 1236$. En canvi, realment és $453 \equiv 297^2$ (mòd. 1236).

147. Proposat un nombre qualsevol A, es poden mostrar certes *fórmules* en les quals es contenen tots els nombres primers amb A dels quals A és residu, o sigui, tots els que poden ser *divisors* de nombres de la forma $xx - A$ (on xx designa un quadrat indeterminat).*

* Anomenarem, més simplement, *divisors de* $xx - A$, els nombres d'aquesta forma; d'on és clar espontàniament què són *no-divisors*.

Però, per abreujar, només considerarem els divisors que són imparells i primers amb A, ja que els casos restants es poden reduir fàcilment a aquests.

En primer lloc, sigui A o bé un nombre primer positiu de la forma $4n + 1$, o bé negatiu de la forma $4n - 1$. Llavors, segons el teorema fonamental, tots els nombres primers que, presos positivament, són residus de A seran divisors de $xx - A$; però tots els nombres primers (exceptuant-ne el nombre 2, que sempre és divisor) que són no-residus de A seran no-divisors de $xx - A$. Siguin r, r', r'', etc., tots els residus de A menors que A (excloent-ne el zero), però n, n', n'', etc., tots els no-residus. Llavors, qualsevol nombre primer contingut en alguna de les formes $Ak + r$, $Ak + r'$, $Ak + r''$, etc., serà divisor de $xx - A$; en canvi, qualsevol primer contingut en alguna de les formes $Ak + n$, $Ak + n'$, $Ak + n''$, etc., serà no-divisor, on k designa un nombre enter indeterminat. Anomenem aquelles formes *formes de divisors de* $xx - A$; aquestes, en canvi, *formes de no-divisors*. La quantitat de cadascuna serà $\frac{1}{2}(A-1)$. A més a més, si B és un nombre imparell compost, i és ARB, tots els factors primers de B es contenen en alguna de les formes dels primers, de manera que B també. Per tant, *qualsevol* nombre imparell contingut en la forma de no-divisors serà no-divisor de la forma $xx - A$. Però no és lícit invertir aquest teorema; efectivament, si B és un no-divisor compost imparell de la forma $xx - A$, entre els factors primers de B, alguns seran no-divisors, i, si la quantitat d'aquests és *parella*, B es trobarà, no obstant això, en alguna forma de divisors; vegeu l'article 99.

Exemple. D'aquesta manera, per a $A = -11$, es troben com a formes de divisors de $xx+11$ les $11k+1$, 3,

4, 5, 9; en canvi, les formes de no-divisors seran $11k+2$, 6, 7, 8, 10. Així, -11 serà no-residu de tots els nombres imparells que es contenen en alguna de les darreres formes, però residu de tots els primers que pertanyen a alguna de les primeres.

Es donen formes similars per als divisors i els no-divisors de $xx - A$, qualsevol que sigui el nombre que A designi. Però es copsa fàcilment que només convé considerar els valors de A que no siguin divisibles per cap quadrat; en efecte, és clar que si fos $A = a^2A'$, tots els divisors* de $xx-A$ també serien divisors de $xx-A'$, i, similarment, no-divisors. Distingirem, però, tres casos: 1) quan A és de la forma $+(4n+1)$, o bé $-(4n-1)$; 2) quan A és de la forma $-(4n+1)$, o bé $+(4n-1)$; 3) quan A és parell, o sigui, de la forma $\pm(4n+2)$.

148. *Primer cas*, quan A és de la forma $+(4n+1)$, o bé $-(4n-1)$. Es descompon A en els seus factors primers i s'atribueix el signe positiu als que són de la forma $4n+1$, però el signe negatiu als que són de la forma $4n-1$ (d'on el producte d'aquests resultarà $= A$). Siguin a, b, c, d, etc., aquests factors. Es distribueixen tots els nombres menors que A i primers amb A en dues classes i, certament, a la primera classe, tots els nombres que són no-residus de cap dels nombres a, b, c, d, etc., o bé de dos, o bé de quatre, o bé, en general, d'una quantitat parella; però a la segona, els que són no-residus d'un dels nombres a, b, c, etc., o bé de tres, o bé, en general, d'una quantitat imparella. Es designen els primers per r, r', r'', etc., els darrers per n, n', n'', etc. Llavors, les formes $Ak+r$, $Ak+r'$, $Ak+r''$, etc., seran formes

* Naturalment, els que siguin primers amb A.

de divisors de $xx - A$; però les formes $Ak + n$, $Ak + n'$, $Ak + n''$, etc., seran formes de no-divisors de $xx - A$ (*és a dir, un nombre primer qualsevol, excepte* 2*, serà divisor o bé no-divisor de* $xx - A$ *segons que estigui contingut en alguna de les primeres formes o bé de les darreres*). En efecte, si p és un nombre primer positiu, i residu o bé no-residu d'algun dels nombres a, b, c, etc., aquest mateix nombre serà residu o bé no-residu de p (teorema fonamental). Per tant, si entre els nombres a, b, c, etc., n'hi ha m, dels quals p és no-residu, la mateixa quantitat seran no-residus de p, de manera que si p està contingut en alguna de les primeres formes, m serà parell i ARp; si, però, en alguna de les darreres, m serà imparell i ANp.

Exemple. Sigui $A = +105 = -3 \times +5 \times -7$. Llavors, els nombres r, r', r'', etc., seran els 1, 4, 16, 46, 64, 79 (que són no-residus de cap del nombres 3, 5, 7); 2, 8, 23, 32, 53, 92 (que són no-residus dels nombres 3, 5); 26, 41, 59, 89, 101, 104 (que són no-residus dels nombres 3, 7); 13, 52, 73, 82, 97, 103 (que són no-residus dels nombres 5, 7). Però, els nombres n, n', n'', etc., seran els 11, 29, 44, 71, 74, 86; 22, 37, 43, 58, 67, 88; 19, 31, 34, 61, 76, 94; 17, 38, 47, 62, 68, 83. Els sis primers són no-residus de 3, els sis posteriors no-residus de 5, després se segueixen els no-residus de 7, finalment els que són no-residus de tots tres simultàniament.

De la teoria de les combinacions, i dels articles 32, 96, es dedueix fàcilment que la quantitat de nombres r, r', r'', etc., serà

$$= t\left(1 + \frac{l(l-1)}{1 \cdot 2} + \frac{l(l-1)(l-2)(l-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \cdots\right),$$

la quantitat de nombres n, n', n'', etc.,

$$= t\left(l + \frac{l(l-1)(l-2)}{1\cdot 2\cdot 3} + \frac{l(l-1)\cdots(l-4)}{1\cdot 2\cdots 5} + \cdots\right),$$

on l designa la quantitat de nombres a, b, c, etc.; $t = 2^{-l}(a-1)(b-1)(c-1)etc.$, i cal continuar cada una de les sèries fins que es trenca (Això és, es donaran t nombres que són residus de tots els a, b, c, etc., $\frac{tl(l-1)}{1\cdot 2}$ que són no-residus de dos, etc., però la brevetat no permet explicar més extensament aquesta demostració). Però la suma* de cada una de les sèries és $= 2^{l-1}$. Això és, la posterior prové de la $1 + (l-1) + \frac{(l-1)(l-2)}{1\cdot 2} +$ *etc.*, unint els termes segon i tercer, quart i cinquè, etc.; la darrera, en canvi, de la mateixa, unint els termes primer i segon, tercer i quart, etc. Així, es donaran tantes formes de divisors de $xx - A$ com formes es donen de no-divisors; això és, $\frac{1}{2}(a-1)(b-1)(c-1)\,etc.$

149. Aquí podem considerar simultàniament *els casos segon i tercer*. Això és, aquí A sempre es podrà posar $= (-1)Q$, o bé $= (+2)Q$, o bé $= (-2)Q$, on Q designa nombres de la forma $+(4n+1)$, o bé $-(4n-1)$, els quals hem considerat a l'article precedent. Sigui, en general, $A = \alpha Q$, de manera que α sigui o bé -1, o bé $= \pm 2$. Llavors, A serà residu de tots els nombres dels quals o bé cada un dels α i Q és residu, o bé cap dels dos; però no-residu de tots aquells dels quals només algun dels nombres α, Q és no-residu. D'aquí es deriven fàcilment les formes de divisors i de no-divisors de $xx - A$. Si

* Negligit el factor t.

$\alpha = -1$, es distribueixen tots els nombres menors que $4A$ i primers amb ell en dues classes; en la primera, els que estan en alguna forma de divisors de $xx - Q$ i, simultàniament, en la forma $4n + 1$, i els que estan en alguna forma de no-divisors de $xx - Q$ i, simultàniament, en la forma $4n + 3$; en la darrera, els restants. Siguin r, r', r'', etc., els primers; i n, n', n'', etc., els darrers; i A serà residu de tots els nombres primers continguts en alguna de les formes $4Ak + r$, $4Ak + r'$, $4Ak + r''$, etc., però no-residu de tots els primers continguts en alguna de les formes $4Ak + n$, $4Ak + n'$, etc. Si $\alpha = \pm 2$, es distribueixen tots els nombres menors que $8Q$ i primers amb ell en dues classes; en la primera, els que estan continguts en alguna forma de divisors de $xx - Q$ i, simultàniament, en alguna de les formes $8n + 1$, $8n + 7$, per al signe superior, o bé de les formes $8n+1$, $8n+3$, per a l'inferior, i els que estan continguts en alguna forma de no-divisors de $xx - Q$ i, simultàniament, en alguna de les $8n + 3$, $8n + 5$, per al signe superior, o bé de les $8n + 5$, $8n + 7$, per a l'inferior; en la segona [classe], els restants. Llavors, designats per r, r', r'', etc., els nombres de la primera classe, i per n, n', n'', etc., els nombres de la darrera classe, $\pm 2Q$ serà residu de tots els nombres primers continguts en alguna de les formes $8Qk + r$, $8Qk + r'$, $8Qk + r''$, etc., però no-residu de tots els primers [continguts] en alguna de les formes $8Qk + n$, $8Qk + n'$, $8Qk + n''$, etc. D'altra banda, es pot demostrar fàcilment que, també aquí, s'han donat tantes formes de divisors de $xx - A$ com de no-divisors.

Exemple. D'aquesta manera, es troba que $+10$ és residu de tots els nombres primers continguts en alguna de les formes $40k + 1$, 3, 9, 13, 27, 31, 37, 39, però no-

residu de tots els primers que es contenen en alguna de les formes $40k + 7$, 11, 17, 19, 21, 23, 29, 33.

150. Aquestes formes tenen més propietats bastant notables, de les quals, però, només n'afegim una. Si B és un nombre compost primer amb A, entre els factors primers del qual n'ocorren $2m$ que es contenen en alguna forma de no-divisors de $xx - A$, B estarà contingut en alguna forma de divisors de $xx - A$; però, si la quantitat de factors primers de B continguts en alguna forma de no-divisors de $xx - A$ és imparella, B també estarà contingut en una forma de no-divisors de $xx - A$. N'ometem la demostració, que no és difícil. D'aquí se segueix, però, que no només qualsevol nombre primer, sinó també qualsevol imparell compost primer amb A que es contingui en alguna forma de no-divisors, serà no-divisor; en efecte, algun factor primer d'un tal nombre ha de ser necessàriament no-divisor.

151. El teorema fonamental, que s'ha de considerar realment entre els més elegants d'aquest tipus, no ha estat presentat per ningú, fins ara, en la forma senzilla en què s'ha proposat més amunt. Això és més sorprenent perquè certes proposicions que s'han hagut de construir, a partir de les quals s'hauria pogut arribar a ell fàcilment, ja eren conegudes per l'il·lm. Euler. Va conèixer que es donen certes formes en les quals es contenen tots els divisors primers dels nombres de la forma $xx - A$, i altres en les quals estan compresos tots els no-divisors primers dels nombres de la mateixa forma, de manera que aquestes exclouen aquelles, i va descobrir el mètode per a trobar aquelles formes; però tots els seus intents d'arribar a la demostració sempre foren debades

i només proporcionaren una més gran versemblança a aquella veritat descoberta per indici. Certament, en algun tractat, *Novae demonstrationes circa divisores numerorum formae* $xx + nyy$, que va ser llegit en públic a Acad. Petrop. 1775, Nou. 20 i que es va conservar després de la mort d'aquest home eminent en *T.* 1 *Nou. Act.* d'aquesta Ac., p. 47 i s., sembla que es creia agraciat en els seus desitjos; però s'hi infiltrà aquest error, això és, a la p. 65, va suposar *tàcitament* que existeixen tals formes de divisors i de no-divisors,* d'on no era difícil derivar *quines* haurien de ser; però el mètode que va utilitzar per a la comprovació d'aquella suposició no sembla idoni. En una altra publicació, *De criteriis aequationis* $fxx + gyy = hzz$ *utrumque resolutionem admittat necne, Opusc. Anal. T.* 1, (on f, g, h, són dades; x, y, z, indeterminades), trobà, per indici, que sempre que l'equació sigui resoluble per a algun valor de $h = s$, aquesta serà resoluble per a qualsevol altre valor congru a s segons el mòdul $4fg$, suposat que sigui un nombre primer, proposició de la qual es pot demostrar no difícilment la suposició de què hem parlat. Però també la demostració d'aquest teorema va eludir tots els seus esforços,** la qual cosa no és sorprenent, ja que, al nostre

---

* Certament, es donen nombres r, r', r'', etc., n, n', n'', etc., tots diferents i $< 4A$, tals que tots els divisors primers de $xx - A$ es continguin en alguna de les formes $4Ak + r$, $4Ak + r'$, etc., i tots els no-divisors primers, en alguna de les $4Ak + n$, $4Ak + n'$, etc. (on k designa un nombre indeterminat).

** Com ell mateix reconeix, lloc citat, p. 216, "Encara es desitja la demostració d'aquest teorema elegantíssim, després que s'ha investigat debades per molts des de fa temps [. . .]. Per això haurà de ser distingit molt excel·lentment aquell qui reïxi a trobar la demostració d'aquest teorema". Amb quin anhel aquest home immortal desitjava la demostració d'aquest teorema, i d'altres que només són casos particulars del teorema fonamental, es pot veure

judici, calia fer servir el teorema fonamental. D'altra banda, la veritat d'aquesta proposició sorgirà espontàniament de les que ensenyarem a la secció següent.

Després d'Euler, el mateix argument prestà servei al preclar Le Gendre en el seu excel·lent tractat *Recherches d'analyse indéterminée, Hist. de l'Ac. des Sc.* 1785, p. 465 *s.*, on arribà a un teorema que, si te'l mires bé, és igual que el teorema fonamental, això és, si p, q, designen dos nombres primers positius, els residus mínims absoluts de les potències $p^{\frac{q-1}{2}}$, $q^{\frac{p-1}{2}}$, segons els mòduls q, p, respectivament, o bé seran tots dos $+1$, o bé tots dos -1, quan p, o bé q, sigui de la forma $4n+1$; però, quan tant p com q siguin de la forma $4n+3$, un residu mínim serà $+1$, l'altre -1, p. 516; cosa de la qual es deriva, segons l'article 106, que la *relació* (en el significat adoptat a l'article 146) de p amb q i la de q amb p són la *mateixa*, quan p, o bé q, sigui de la forma $4n+1$; *oposada*, quan tant p com q siguin de la forma $4n+3$. Aquesta proposició, [que] està continguda entre les proposicions de l'article 131, també se segueix de 1, 3, 9, de l'article 133; però, en canvi, el teorema fonamental es pot derivar d'aquesta. El preclar Le Gendre també va intentar la demostració, de la qual, com que és extremament enginyosa, en parlarem més extensament a la secció següent. Però, com que en ella va suposar molt sense demostració (com ell mateix reconeix a la pàgina 520, *Nous avons supposé seulement* etc.), i com que, en part, no ha estat demostrat fins ara per ningú i, en part, no es pot demostrar, certament, segons el nostre judici, sense

---

en molts altres llocs, Opusc. Analt. Conf. *Additamentum ad diss. VIII, T.* 1*, i diss. XIII, T. II*, i en més dissertacions a Comment. Petrop., ja mencionades arreu.

el teorema fonamental, sembla que la via que va emprendre no pot conduir a l'objectiu, i la nostra demostració s'haurà de tenir per la primera. D'altra banda, més avall transmetrem *dues altres demostracions* d'aquest teorema profundíssim, diferents del tot de l'anterior i entre elles.

152. Fins ara, hem tractat la congruència pura $xx \equiv A \,(\text{mòd.}\, m)$ i hem ensenyat a discernir la seva resolubilitat. La recerca *de les seves arrels* s'ha reduït, per l'article 105, al cas en què m és, o bé primer, o bé potència d'un primer; però, després, per l'article 101, a aquell en què m és primer. Però per a aquest cas, el que vàrem transmetre a l'article 61 *i s.*, junt amb el que ensenyarem a les seccions V i VIII, comprèn gairebé tot el que es pot trobar per mètodes directes. Però, on aquests són aplicables, sovint són infinitament més extensos que els indirectes que ensenyarem a la secció VI, de manera que són remarcables no tant per la seva utilitat a la pràctica, com per la seva bellesa. *Les congruències de segon grau no pures* es poden reduir fàcilment a pures. Proposada la congruència $axx + bx + c \equiv 0$, que cal solucionar segons el mòdul m, la congruència $4aaxx + 4abx + 4ac \equiv 0 \,(\text{mòd.}\, 4am)$ equivaldrà a aquesta; és a dir, qualsevol nombre que satisfaci l'una, també satisfarà l'altra. Aquesta, però, es pot expressar així, $(2ax+b)^2 \equiv bb - 4ac \,(\text{mòd.}\, 4am)$, d'on es poden trobar tots els valors de $2ax + b$ menors que $4am$, si se'n donen. Designats aquests per r, r', r'', etc., totes les solucions de la congruència proposada es deduiran de les solucions de les congruències $2ax \equiv r - b$, $2ax \equiv r' - b$, etc. $(\text{mòd.}\, 4am)$ que vàrem ensenyar a trobar a la secció II. D'altra banda, observem que, sovint, la solució es

pot contreure per artificis diversos; per exemple, en lloc de la congruència proposada se'n pot trobar una altra, $a'xx + 2b'x + c' \equiv 0$, equivalent a ella, i en la qual a' divideixi m; però la brevetat no permet explicar aquí això, que pot ser convenient a l'última Secció.

Secció Cinquena

de les

FORMES I EQUACIONS INDETERMINADES

de segon grau

153. En aquesta secció tractarem principalment de les funcions de dues indeterminades x, y, de la forma $axx + 2bxy + cyy$, on a, b, c, són enters donats, les quals anomenarem *formes de segon grau*, o bé, més simplement, *formes*. En aquesta disquisició es construirà la solució del famós problema de trobar totes les solucions d'una equació indeterminada qualsevol de segon grau que impliqui dues incògnites, bé aquestes incògnites hagin d'obtenir només valors enters, bé racionals. Certament, aquest problema ja ha estat resolt amb tota generalitat per l'il·lm. La Grange, i, a més a més, moltes coses que pertanyen a la naturalesa de les *formes* han estat proveïdes de demostracions tant per aquest mateix gran geòmetra, com per l'il·lm. Euler, per qui en part han estat trobades primer, en part, en altre temps, trobades per Fermat. Però a nosaltres, en insistir aferrissadament en la recerca de les formes, se'ns han ofert tantes

coses noves, que hem valorat que valia la pena reprendre per complet tot l'argument, tant més perquè estem segurs que els descobriments d'aquells Homes, dispersos en molts llocs, han estat coneguts per pocs; a més a més, perquè el mètode pel qual nosaltres les tractarem és propi nostre en la seva major part; finalment, perquè, certament, les nostres no podrien ser enteses sense una nova exposició de les seves. Però no se'ns presenta cap dubte que encara resten ocultes moltes coses notables d'aquest tipus, en les quals altres puguin exercitar les seves forces. D'altra banda, sempre ensenyarem en el seu lloc les que pertanyen a la història de les veritats insignes.

Designarem per (a, b, c) la forma $axx + 2bxy + cyy$ quan no es tracti de les indeterminades x, y. Així, aquesta expressió denotarà indefinidament la suma de tres parts: el producte d'un nombre donat a pel quadrat d'una indeterminada qualsevol; el producte del doble del nombre b per aquesta indeterminada per una altra indeterminada; el producte del nombre c pel quadrat d'aquesta segona indeterminada. Per exemple, $(1, 0, 2)$ expressarà la suma d'un quadrat i del doble d'un quadrat. D'altra banda, qualsevol de les formes (a, b, c) i (c, b, a) designen el mateix, si només considerem *les parts en si*, però difereixen si, a més a més, tenim en compte *l'ordre* de les parts; per tant, d'ara endavant les distingirem curosament; què en traurem, d'aquí, es veurà suficientment en el que segueix.

154. Direm que algun nombre donat es *representa* per una forma donada si s'atribueixen valors enters a la forma indeterminada tals que el valor d'aquesta resulti igual al nombre donat. Aquí tindrem el següent

TEOREMA. *Si el nombre M es pot representar per la forma $(a,\ b,\ c)$ de manera que els valors de les indeterminades per als quals això s'efectua siguin primers entre ells, $bb-ac$ serà un residu quadràtic del nombre M.*

Dem. Siguin m, n, els valors de les indeterminades; això és, $amm+2bmn+cnn=M$, i agafem nombres μ, ν, de manera que sigui $\mu m+\nu n=1$ (article 40). Llavors, es prova fàcilment per desenvolupament que és $(amm+2bmn+cnn)(a\nu\nu-2b\mu\nu+c\mu\mu)=(\mu(mb+nc)-\nu(ma+nb))^2-(bb-ac)(m\mu+n\nu)^2$, o sigui, $M(a\nu\nu-2b\mu\nu+c\mu\mu)=(\mu(mb+nc)-\nu(ma+nb))^2-(bb-ac)$. Per tant, serà $bb-ac\equiv(\mu(mb+nc)-\nu(ma+nb))^2$ (mòd. M), *és a dir*, $bb-ac$, un residu quadràtic de M.

Anomenarem *determinant* de la forma el nombre $bb-ac$, de la naturalesa del qual depenen principalment les propietats de la forma $(a,\ b,\ c)$, com ensenyarem en el que segueix.

155. Així, $\mu(mb+nc)-\nu(ma+nb)$ serà un valor de l'expressió $\sqrt{bb-ac}$ (mòd. M). Però se sap que es poden determinar d'infinites maneres nombres μ, ν, de manera que sigui $\mu m+\nu n=1$, d'on sortiran uns i altres valors d'aquella expressió, dels quals veurem quina connexió tenen entre si. No només sigui $\mu m+\nu n=1$, sinó, també, $\mu' m+\nu' n=1$, i es posa $\mu(mb+nc)-\nu(ma+nb)=v$, $\mu'(mb+nc)-\nu'(ma+nb)=v'$. Multiplicant l'equació $\mu m+\nu n=1$ per μ', l'altra, $\mu' m+\nu' n=1$, per μ, i restant, resulta $\mu'-\mu=n(\mu'\nu-\mu\nu')$; i, similarment, multiplicant aquella per ν', aquesta per ν, resulta, restant, $\nu'-\nu=m(\mu\nu'-\mu'\nu)$. D'aquí surt immediatament $v-v'=(\mu'\nu-\mu\nu')(amm+2bmn+cnn)=(\mu'\nu-$

$\mu\nu')M$, o sigui, $v' \equiv v\,(\text{mòd. } M)$. Així, doncs, de qualsevol manera que s'hagin determinat μ, ν, la fórmula $\mu(mb+nc)-\nu(ma+nb)$ no pot donar valors *diferents* (és a dir, incongrus) de l'expressió $\sqrt{bb-ac}\,(\text{mòd. } M)$. Així, si v és un valor qualsevol d'aquella fórmula, direm que la representació del nombre M per la forma $axx+2bxy+cyy$ en què $x=m$, $y=n$, *pertany al valor* v *de l'expressió* $\sqrt{bb-ac}\,(\text{mòd. } M)$. D'altra banda, es pot mostrar fàcilment que, si v fos algun valor d'aquella fórmula, i $v' \equiv v\,(\text{mòd. } M)$, en lloc dels nombres μ, ν, que donen v, se'n poden agafar uns altres, μ', ν', que donin v'. Això és, fent $\mu' = \mu + \dfrac{n(v'-v)}{M}$, $\nu' = \nu - \dfrac{m(v'-v)}{M}$, resultarà $\mu' m + \nu' n = \mu m + \nu n = 1$; però el valor de la fórmula obtinguda de μ', ν', superarà el valor de l'obtinguda de μ, ν, en la quantitat $(\mu'\nu - \mu\nu')M$, que resulta $= (\mu m+\nu n)(v'-v) = v'-v$, o sigui, aquell valor serà $= v'$.

156. Si es tenen dues representacions del mateix nombre M per la mateixa forma $(a,\ b,\ c)$ en les quals les indeterminades tenen valors primers entre si, aquestes poden pertànyer, o bé al mateix valor de l'expressió $\sqrt{bb-ac}\,(\text{mòd. } M)$, o bé a diferents. Sigui $M = amm + 2bmn + cnn = am'm' + 2bm'n' + cn'n'$, i $\mu m + \nu n = 1$, $\mu' m' + \nu' n' = 1$, i és clar que, si fos $\mu(mb+nc)-\nu(ma+nb) \equiv \mu'(m'b+n'c) - \nu'(m'a+n'b)\,(\text{mòd. } M)$, la congruència es manté sempre, qualssevol altres valors idonis que s'agafin per a μ, ν; μ', ν', cas en què direm que les dues representacions pertanyen al *mateix* valor de l'expressió $\sqrt{bb-ac}\,(\text{mòd. } M)$; però si la congruència no té lloc per a alguns valors de μ, ν; μ', ν', no tindrà lloc per a cap, i les representacions pertanyeran a valors *diferents*. Però si $\mu(mb+nc)-\nu(ma+nb) \equiv$

$-(\mu'(m'b + n'c) - \nu'(m'a + n'b))$, es dirà que les representacions pertanyen a valors *oposats* de l'expressió $\sqrt{bb - ac}$. També s'utilitzaran totes aquestes denominacions quan es tracti de més representacions del mateix nombre per formes *diferents*, però que tenen el mateix determinant.

Exemple. Sigui (3, 7, −8) la forma proposada, el determinant de la qual és = 73. Per a aquesta forma es tenen representacions del nombre 57: $3 \cdot 13^2 + 14 \cdot 13 \cdot 25 - 8 \cdot 25^2$; $3 \cdot 5^2 + 14 \cdot 5 \cdot 9 - 8 \cdot 9^2$. Per a la primera, es pot posar $\mu = 2$, $\nu = -1$, d'on el valor de l'expressió $\sqrt{73}$ (mòd. 57) a què pertany la representació surt $= 2(13 \cdot 7 - 25 \cdot 8) + (13 \cdot 3 + 25 \cdot 7) = -4$. De manera similar, fent $\mu = 2$, $\nu = 1$, es troba que la segona representació pertany al valor +4. Per tant, les dues representacions pertanyen a valors oposats.

Abans que es progressi més enllà, observem que són excloses completament de les investigacions següents les formes el determinant de les quals és = 0, ja que només pertorbarien l'elegància dels teoremes, de manera que demanen un tractament peculiar.

157. Si una forma F, les indeterminades de la qual són x, y, es pot transformar en una altra F', les indeterminades de la qual són x', y', per tals substitucions $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, de manera que α, β, γ, δ, siguin enters, direm que la primera *implica* la darrera, o bé que la darrera *està continguda en la primera*. Sigui F la forma $axx + 2bxy + cyy$, i F' la forma $a'x'x' + 2b'x'y' + c'y'y'$, i es tindran les tres equacions següents:

$$a' = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma,$$
$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta,$$
$$c' = a\beta\beta + 2b\beta\delta + c\delta\delta.$$

Multiplicant la segona equació per ella mateixa, la primera per la tercera, i restant, esborrades les parts que es destrueixen, resulta $b'b' - a'c' = (bb - ac)(\alpha\delta - \beta\gamma)^2$. D'on se segueix que el determinant de la forma F' és divisible pel determinant de la forma F i que el quocient és un quadrat; així, doncs, evidentment, aquests determinants tindran *el mateix signe*. Així, si, a més a més, la forma F' es pot transformar en la forma F per una substitució similar, *és a dir*, si tant F' està contiguda en F com F en F', els determinants de les formes seran iguals* i $(\alpha\delta - \beta\gamma)^2 = 1$. En aquest cas, anomenarem les formes *equivalents*. Per tant, la igualtat de determinants és una condició necessària per a l'equivalència de formes, encara que aquesta no se segueixi en absolut només d'aquella. Anomenarem *transformació pròpia* la substitució $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, si $\alpha\delta - \beta\gamma$ és un nombre positiu, *impròpia*, si $\alpha\delta - \beta\gamma$ és negatiu; direm que la forma F' està continguda *pròpiament o bé impròpiament* en la forma F, si F es pot transformar en la forma F' per una transformació pròpia o bé impròpia. Així, si les formes F, F', són equivalents, serà $(\alpha\delta - \beta\gamma)^2 = 1$, de manera que, si la transformació és pròpia, és $\alpha\delta - \beta\gamma = +1$; si és impròpia, $= -1$. Si més transformacions són pròpies simultàniament, o bé

* De l'anàlisi precedent, és evident que aquesta proposició també s'estén a les formes el determinant de les quals és = 0. Però l'equació $(\alpha\delta - \beta\gamma)^2 = 1$ no s'ha d'estendre a aquest cas.

impròpies simultàniament, les anomenarem *semblants*; contràriament, una pròpia i una impròpia, *dissemblants*.

158. *Si els determinants de les formes F, F', són iguals i F' està continguda en F, també F estarà continguda en F' i, certament, pròpiament o bé impròpiament, segons que F' es contingui en F pròpiament o bé impròpiament.* Es transforma F en F' posant $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, i F' es transformarà en F posant $x' = \delta x - \beta y$, $y' = -\gamma x + \alpha y$. En efecte, és clar que, per aquesta substitució, de F' resulta el mateix que resultaria de F posant $x = \alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y)$, $y = \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y)$, o sigui, $x = (\alpha\delta - \beta\gamma)x$, $y = (\alpha\delta - \beta\gamma)y$. Però, d'aquí, és evident que de F resulta $(\alpha\delta - \beta\gamma)^2 F$, *és a dir*, la mateixa F (article precedent). Però es copsa que la darrera transformació és pròpia o bé impròpia segons que la primera sigui pròpia o bé impròpia.

Si, d'una banda, F' es conté *pròpiament* en F i, de l'altra, F, en F', anomenarem les formes *pròpiament equivalents*; si aquelles [es contenen] mútuament impròpiament, *impròpiament equivalents*. D'altra banda, la utilitat d'aquestes distincions es donarà a conèixer de seguida.

Exemple. La forma $2xx - 8xy + 3yy$, per les substitucions $x = 2x' + y'$, $y = 3x' + 2y'$, es transforma en la forma $-13x'x' - 12x'y' - 2y'y'$, però aquesta en aquella fet $x' = 2x - y$, $y' = -3x + 2y$. Per tant, les formes (2, -4, 3), (-13, -6, -2) seran *pròpiament equivalents*.

Els problemes que ens disposem a tractar ara són aquests: I. Proposades dues formes qualssevol que tenen

el mateix determinant, investigar si són equivalents o no, i si pròpiament, o bé impròpiament, o bé de les dues maneres, ja que això també pot ser. En canvi, quan tenen determinants diferents, si almenys una implica l'altra pròpiament, o bé impròpiament, o bé de les dues maneres. Finalment, trobar totes les transformacions de l'una en l'altra, tant les pròpies com les impròpies. II. Proposada una forma qualsevol, trobar si un nombre donat es podria representar per ella, i assignar totes les representacions. Però, com que, aquí, les formes de determinant negatiu requereixen un altre mètode que les formes de determinant positiu, primer tractarem allò que és comú a totes dues, i després considerarem separadament les formes de cada un dels tipus.

159. *Si la forma F implica la forma F', i aquesta, la forma F'', també la forma F implicarà la forma F''.*

Siguin x, y; x', y'; x'', y'', les indeterminades de les formes F, F', F'', respectivament, i es transforma F en F' posant $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$; F' en F'', posant $x' = \alpha' x'' + \beta' y''$, $y' = \gamma' x'' + \delta' y''$; és clar que F es transformarà en F'' posant $x = \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y'')$, $y = \gamma(\alpha' x'' + \beta' y'') + \delta(\gamma' x'' + \delta' y'')$, o sigui, $x = (\alpha\alpha' + \beta\gamma')x'' + (\alpha\beta' + \beta\delta')y''$, $y = (\gamma\alpha' + \delta\gamma')x'' + (\gamma\beta' + \delta\delta')y''$. Per tant, F implicarà F''.

Com que $(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma') = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma')$, de manera que és positiu si tant $\alpha\delta - \beta\gamma$ com $\alpha'\delta' - \beta'\gamma'$ són positius, o bé tots dos negatius, però és negatiu si un d'aquests nombres és positiu i l'altre negatiu, la forma F implicarà *pròpiament* la forma F'', si F implica F' i F', F'', de

la mateixa manera, i *impròpiament*, si [s'impliquen] de manera diferent.

D'aquí se segueix que si es tenen formes qualssevol F, F', F'', F''', etc., cadascuna de les quals implica la següent, la primera implicarà l'última, i, certament, *pròpiament*, si la quantitat de formes que impliquen impròpiament la seva següent fos parella, i *impròpiament* si aquesta quantitat [fos] imparella.

Si la forma F és equivalent a la forma F' i la forma F' a la forma F'', la forma F serà equivalent a la forma F'', i, certament, pròpiament, si la forma F equival a la forma F' de la mateixa manera que la forma F' a la forma F'', i impròpiament, si diferentment.

En efecte, com que les formes F, F', són equivalents, respectivament, a les F', F'', tant aquelles implicaran respectivament aquestes, de manera que F, F'', com aquestes, aquelles. Per tant, F, F'', seran equivalents. Però, del que precedeix, se segueix que F implica F'' pròpiament, o bé impròpiament, segons que F sigui equivalent a F' i F' a F'' de la mateixa manera, o bé diferentment; i el mateix per a F'' i F; per tant, en el primer cas, F, F'', seran pròpiament equivalents, en el darrer, impròpiament.

Les formes $(a, -b, c)$, (c, b, a), $(c, -b, a)$ equivalen a la forma (a, b, c), i, certament, les dues primeres impròpiament, l'última, pròpiament.

Efectivament, $axx + 2bxy + cyy$ es transforma en $ax'x' - 2bx'y' + cy'y'$ posant $x = x' + 0 \cdot y'$, $y = 0 \cdot x' - y'$, transformació que és impròpia, ja que $1 \cdot -1 - 0 \cdot 0 = -1$;

però a la forma $cx'x'+2bx'y'+cy'y'$, per la transformació impròpia $x = 0 \cdot x' + y'$, $y = x' + 0 \cdot y'$; i a la forma $cx'x' - 2bx'y' + ay'y'$, per la pròpia $x = 0 \cdot x' - y'$, $y = x' + 0 \cdot y'$.

D'aquí, és evident que qualsevol forma equivalent a la forma (a, b, c) equival *pròpiament*, bé a la mateixa, bé a la forma $(a, -b, c)$; i, similarment, si aquella forma implica la forma (a, b, c), o bé està continguda en ella, aquesta implicarà pròpiament, bé la forma (a, b, c), bé la forma $(a, -b, c)$, o bé estarà pròpiament continguda en una d'elles. Anomenarem les formes (a, b, c), $(a, -b, c)$, *oposades*.

160. Si les formes (a, b, c), (a', b', c'), tenen el mateix determinant i, a més a més, és $c = a'$ i $b \equiv -b' \,(\text{mòd.}\, c)$, o sigui, $b + b' \equiv 0 \,(\text{mòd.}\, c)$, direm que aquestes formes són *contigües*, i, certament, quan sigui necessària una determinació més acurada, direm que la primera és contigua a la darrera per *la primera part*, la darrera a la primera per *l'última part*.

Així, per exemple, la forma $(7, 3, 2)$ és contigua a la forma $(3, 4, 7)$ per l'última part; la forma $(3, 1, 3)$, a la seva oposada, $(3, -1, 3)$, per totes dues parts.

Formes contigües sempre són pròpiament equivalents. Efectivament, la forma $axx + 2bxy + cyy$ es transforma en la forma contigua $cx'x' + 2b'x'y' + c'y'y'$ per la substitució $x = -y'$, $y = x' + \dfrac{b + b'}{c} y'$ (que és pròpia perquè $0 \cdot \dfrac{b + b'}{c} - 1 \cdot -1 = 1$), com es prova fàcilment per desenvolupament, amb l'ajuda de l'equació

$bb - ac = b'b' - cc'$; per hipòtesi, però, $\dfrac{b+b'}{c}$ és un enter. D'altra banda, aquestes definicions i conclusions no tenen lloc si $c = a' = 0$. Però aquest cas no pot ocórrer si no és en formes el determinant de les quals és un nombre quadrat.

Les formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, són pròpiament equivalents si $a = a'$, $b \equiv b'\ (\text{mòd.}\ a)$. En efecte, la forma $(a,\ b,\ c)$ equival pròpiament a la forma $(c,\ -b,\ a)$ (article precedent), però aquesta serà contigua per la primera part a la forma $(a',\ b',\ c')$.

161. *Si la forma* $(a,\ b,\ c)$ *implica la forma* $(a',\ b',\ c')$*, qualsevol divisor comú dels nombres* $a,\ b,\ c$*, també dividirà els nombres* $a',\ b',\ c'$*, i qualsevol divisor comú dels nombres* $a,\ 2b,\ c$*, els* $a',\ 2b',\ c'$*.*

En efecte, si la forma $axx + 2bxy + cyy$ es transforma en la forma $a'x'x' + 2b'x'y' + c'y'y'$ per les substitucions $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, es tindran les equacions

$$a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a',$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b',$$
$$a\beta\beta + 2b\beta\delta + c\delta\delta = c',$$

d'on se segueix immediatament la proposició (per a la segona part de la proposició, utilitzant $2a\alpha\beta + 2b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = 2b'$ en lloc de la segona equació).

D'aquí se segueix que el màxim comú divisor dels nombres a, b $(2b)$, c, divideix simultàniament el màxim comú divisor dels nombres a', b' $(2b')$, c'. Així, doncs, si, a més a més, la forma $(a',\ b',\ c')$ implica la forma $(a,\ b,$

c), és a dir, les formes són equivalents, el màxim comú divisor dels nombres a, b $(2b)$, c, serà igual al màxim comú divisor dels nombres a', b' $(2b')$, c', ja que tant aquell ha de dividir aquest, com aquest, aquell. Així, si, en aquest cas, a, b $(2b)$, c, no tenen divisor comú, és a dir, si el màxim és $= 1$, tampoc a', b' $(2b')$, c', no tindran divisors comuns.

162. Problema. *Si la forma* $AXX + 2BXY + CYY \ldots F$ *implica la forma* $axx + 2bxy + cyy \ldots f$, *i si s'ha donat alguna transformació d'aquella en aquesta, deduir d'aquesta totes les transformacions restants similars a aquesta.*

Solució. Sigui donada la transformació $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$, i suposem, primer, que és donada una altra similar a aquesta, $X = \alpha' x + \beta' y$, $Y = \gamma' x + \delta' y$; i investiguem què se segueix d'aquí. Llavors, posats $= D$, d, els determinants de les formes F, f, i $\alpha\delta - \beta\gamma = e$, $\alpha'\delta' - \beta'\gamma' = e'$, serà $d = Dee = De'e'$ (article 157); i, com que, per hipòtesi, e, e', tenen el mateix signe, $e = e'$. Es tindran, però, les sis equacions següents:

$$A\alpha\alpha + 2B\alpha\gamma + C\gamma\gamma = a, \quad [1]$$
$$A\alpha'\alpha' + 2B\alpha'\gamma' + C\gamma'\gamma' = a, \quad [2]$$
$$A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta = b, \quad [3]$$
$$A\alpha'\beta' + B(\alpha'\delta' + \beta'\gamma') + C\gamma'\delta' = b, \quad [4]$$
$$A\beta\beta + 2B\beta\delta + C\delta\delta = c, \quad [5]$$
$$A\beta'\beta' + 2B\beta'\delta' + C\delta'\delta' = c. \quad [6]$$

Si, per abreujar, designem per a', $2b'$, c' els nombres $A\alpha\alpha' + B(\alpha\gamma' + \gamma\alpha') + C\gamma\gamma'$, $A(\alpha\beta' + \beta\alpha') + B(\alpha\delta' + \beta\gamma' + \gamma\beta' + \delta\alpha') + C(\gamma\delta' + \delta\gamma')$, $A\beta\beta' + B(\beta\delta' + \delta\beta') +$

$C\delta\delta'$, de les equacions precedents en deduirem les noves següents:*

$$a'a' - D(\alpha\gamma' - \gamma\alpha')^2 = aa, \quad [7]$$
$$2a'b' - D(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') = 2ab, \quad [8]$$
$$4b'b' - D((\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 + 2ee') = 2bb + 2ac,$$

d'on resulta, sumant $2Dee' = 2d = 2bb - 2ac$,

$$4b'b' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 = 4bb, \quad [9]$$
$$a'c' - D(\alpha\delta' - \gamma\beta')(\beta\gamma' - \delta\alpha') = bb,$$

d'on, restant $D(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = bb - ac$, resulta

$$a'c' - D(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta') = ac, \quad [10]$$
$$2b'c' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta') = 2bc, \quad [11]$$
$$c'c' - D(\beta\delta' - \delta\beta')^2 = cc. \quad [12]$$

Ara, suposem que m és el màxim comú divisor dels nombres a, $2b$, c, i que s'han determinat nombres $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ de manera que resulti $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$ (article 40); es multipliquen les equacions 7, 8, 9, 10, 11, 12, respectivament, per $\mathfrak{AA}$, $2\mathfrak{AB}$, $\mathfrak{BB}$, $2\mathfrak{AC}$, $2\mathfrak{BC}$, $\mathfrak{CC}$, i se sumen els productes. Si, per abreujar, ara posem

$$\mathfrak{A}a' + 2\mathfrak{B}b' + \mathfrak{C}c' = T, \quad [13]$$
$$\mathfrak{A}(\alpha\gamma' - \gamma\alpha') + \mathfrak{B}(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')$$
$$+\mathfrak{C}(\beta\delta' - \delta\beta') = U, \quad [14]$$

* L'origen d'aquestes equacions és aquest: 7 resulta de $1 \cdot 2$ (és a dir, si l'equació (1) es multiplica per l'equació (2), o millor, si la primera part d'aquella es multiplica per la primera part d'aquesta i la darrera part d'aquella per la darrera d'aquesta i es posen iguals els productes); 8, de $1 \cdot 4 + 2 \cdot 3$; la següent, que no està numerada, de $1 \cdot 6 + 2 \cdot 5 + 3 \cdot 4 + 3 \cdot 4$; la següent, no numerada, de $3 \cdot 4$; 11, de $3 \cdot 6 + 4 \cdot 5$; 12, de $5 \cdot 6$. També en el que segueix utilitzarem sempre una notació similar. Però hem de deixar el desenvolupament per als lectors.

on T, U, evidentment, seran enters, sortirà

$$TT - DUU = mm.$$

Així, hem estat conduïts a l'elegant conclusió que *de dues transformacions similars qualssevol de la forma F en la f se segueix una solució en enters de l'equació indeterminada $tt - Duu = mm$, això és, $t = T$, $u = U$.* D'altra banda, com que en els nostres raonaments no hem suposat que les transformacions són *diferents*, *una* transformació considerada dues vegades ha de produir la solució. Però, llavors, com que $\alpha' = \alpha$, $\beta' = \beta$, etc., resulta $a' = a$, $b' = b$, $c' = c$, de manera que $T = m$, $U = 0$, solució que és òbvia per si mateixa.

Ara, considerem conegudes la primera transformació i la solució de l'equació indeterminada, i investiguem de quina manera l'altra transformació es pot deduir d'aquí, o sigui, de quina manera α', β', γ', δ', depenen de α, β, γ, δ, T, U. Per a aquest fi, multipliquem primer l'equació [1] per $\delta\alpha' - \beta\gamma'$, [2] per $\alpha\delta' - \gamma\beta'$, [3] per $\alpha\gamma' - \gamma\alpha'$, [4] per $\gamma\alpha' - \alpha\gamma'$ i sumem-ne els productes, d'on sortirà

$$(e + e')a' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')a. \qquad [15]$$

De manera similar, de $(\delta\beta' - \beta\delta')([1] - [2]) + (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')([3] + [4]) + (\alpha\gamma' - \gamma\alpha')([5] - [6])$ resulta

$$2(e + e')b' = 2(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')b. \qquad [16]$$

Finalment, de $(\delta\beta' - \beta\delta')([3] - [4]) + (\alpha\delta' - \gamma\beta')[5] + (\delta\alpha' - \beta\gamma')[6]$, surt

$$(e + e')c' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')c. \qquad [17]$$

Substituint aquests valors (15, 16, 17) en 13, resulta

$$(e+e')T = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c),$$

o sigui, $2eT = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')m,$ [18]

d'on es pot deduir T molt més fàcilment que de [13]. Combinant aquesta equació amb 15, 16, 17, s'obtindrà $ma' = Ta$, $2mb' = 2Tb$, $mc' = Tc$. Substituint aquests valors de a', $2b'$, c', en les equacions 7-12, i escrivint $mm + DUU$ en lloc de TT, aquelles es transformen, després de les manipulacions convenients, en les

$$(\alpha\gamma' - \gamma\alpha')^2 mm = aaUU,$$
$$(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')mm = 2abUU,$$
$$(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 mm = 4bbUU,$$
$$(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta')mm = acUU,$$
$$(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta')mm = 2bcUU,$$
$$(\beta\delta' - \delta\beta')^2 mm = ccUU.$$

D'aquí, amb l'ajut de l'equació [14] i de $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, es dedueix fàcilment (multiplicant primera, segona, quarta; segona, tercera, cinquena; quarta, cinquena, sisena, respectivament, per $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, i sumant els productes) que $(\alpha\gamma' - \gamma\alpha')Umm = maUU$, $(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')Umm = 2mbUU$, $(\beta\delta' - \delta\beta')Umm = mcUU$ i, d'aquí, dividint per mU,*

$$aU = (\alpha\gamma' - \gamma\alpha')m, \quad [19]$$
$$2bU = (\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')m, \quad [20]$$
$$cU = (\beta\delta' - \delta\beta')m, \quad [21]$$

* Això no seria lícit si fos $U = 0$; però, llavors, la veritat de les equacions 19, 20, 21, se seguiria immediatament de la primera, tercera i sisena precedents.

equacions de les quals es pot deduir alguna U molt més fàcilment que de [14]. Simultàniament, d'aquí es conclou que de qualsevol manera que es determinin $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ (que es pot fer d'infinites maneres diferents), tant T com U obtenen el mateix valor.

Ara, si l'equació 18 es multiplica per α, la 19, per 2β, la 20, per $-\alpha$, resulta, per addició, que $2\alpha eT + 2(\beta a + \alpha b)U = 2(\alpha\delta - \beta\gamma)\alpha' m = 2e\alpha' m$.

De manera similar, de $\beta[18]+\beta[20]-2\alpha[21]$ resulta $2\beta eT + 2(\beta b - \alpha c)U = 2(\alpha\delta - \beta\gamma)\beta' m = 2e\beta' m$.

A més a més, de $\gamma[18] + 2\delta[19] - \gamma[20]$ resulta $2\gamma eT + 2(\delta a + \gamma b)U = 2(\alpha\delta - \beta\gamma)\gamma' m = 2e\gamma' m$.

Finalment, de $\delta[18] + \delta[20] - 2\gamma[21]$ surt $2\delta eT + 2(\delta b - \gamma c)U = 2(\alpha\delta - \beta\gamma)\delta' m = 2e\delta' m$.

Si se substitueixen els valors de 1, 3, 5, per a, b, c, en aquestes fórmules, resulta

$\alpha' m = \alpha T - (\alpha B - \gamma C)U,$
$\beta' m = \beta T - (\beta B + \delta C)U,$
$\gamma' m = \gamma T + (\alpha A + \gamma B)U,$
$\delta' m = \delta T + (\beta A + \delta B)U.$

De l'anàlisi precedent se segueix que no es dóna cap transformació de la forma F en f similar a la proposada que no estigui continguda en la fórmula (I)

$$X = \frac{1}{m}(\alpha t - (\alpha B + \gamma C)u)x + \frac{1}{m}(\beta t - (\beta B + \delta C)u)y,$$
$$Y = \frac{1}{m}(\gamma t + (\alpha A + \gamma B)u)x + \frac{1}{m}(\delta t + (\beta A + \delta B)u)y,$$

on t, u designen formalment tots els nombres enters que satisfan l'equació $tt - Duu = mm$. D'aquí, però, encara no podem concloure que tots els valors de t, u, que satisfan aquella equació, substituïts en la fórmula (I), donin transformacions idònies. Però

1. Es pot confirmar fàcilment per desenvolupament, amb ajut de les equacions 1, 3, 5, i de la $tt-Duu = mm$, que la forma F sempre es transforma en la forma f per una substitució originada per valors qualssevol de t, u. Per abreujar, suprimim el càlcul, més llarg que difícil.

2. Qualsevol transformació deduïda de la fórmula serà similar a la proposada. Efectivament, $\frac{1}{m}(\alpha t-(\alpha B+\gamma C)u)\cdot\frac{1}{m}(\delta t+(\beta A+\delta B)u)-\frac{1}{m}(\beta t-(\beta B+\delta C)u)\cdot\frac{1}{m}(\gamma t+(\alpha A+\gamma B)u) = \frac{1}{mm}(\alpha\delta-\beta\gamma)(tt-Duu) = \alpha\delta-\beta\gamma$.

3. Si les formes F, f, tenen determinants diferents, pot resultar que la fórmula (I), per a alguns valors de t, u, doni lloc a substitucions que impliquin *fraccions*, de manera que s'hagin de rebutjar. Però totes les restants seran transformacions idònies, i no se'n donaran d'altres excepte aquestes.

4. Però si les formes F, f, tenen el mateix determinant, de manera que són *equivalents*, la fórmula (I) no produirà transformacions que impliquin fraccions, de manera que, en aquest cas, exhibirà la solució completa del problema. Demostrem-ho així.

Del teorema de l'article precedent se segueix, en aquest cas, que, simultàniament, m serà un divisor comú

dels nombres A, $2B$, C. Com que $tt - Duu = mm$, resulta $tt - BBuu = mm - ACuu$; per tant, $tt - BBuu$ serà divisible per mm; també d'aquí, *a posteriori*, $4tt - 4BBuu$, de manera que (ja que $2B$ és divisible per m) també $4tt$, per mm; i, en conseqüència, $2t$ [serà divisible] per m. D'aquí, $\frac{2}{m}(t + Bu)$, $\frac{2}{m}(t - Bu)$, seran enters i, certament (com que la seva diferència, $\frac{4}{m}Bu$, és parella), o bé tots dos [seran] parells, o bé tots dos, imparells. Si cada un d'ells fos imparell, el producte també seria un imparell que, com a quàdruple del nombre $\frac{1}{mm}(tt - BBuu)$, que hem mostrat fa un moment que és enter, és necessàriament parell; per tant, aquest cas és impossible, de manera que $\frac{2}{m}(t+Bu)$, $\frac{2}{m}(t-Bu)$, són sempre parells, d'on $\frac{1}{m}(t + Bu)$, $\frac{1}{m}(t - Bu)$, seran enters. D'aquí, però, es dedueix sense cap dificultat que tots els quatre coeficients de (I) són sempre enters. *Q. E. D.*

Del que precedeix, es conclou que si es tenen totes les solucions de l'equació $tt - Duu = mm$, d'aquí es deriven totes les transformacions de la forma (A, B, C) en la forma (a, b, c) similars a la transformació donada. En el que segueix, ensenyarem a trobar-les. Aquí, només observem que la quantitat de solucions és sempre finita quan D és negatiu, o bé positiu i, simultàniament, un quadrat; però, quan D és positiu no quadrat, infinita. Quan aquest cas té lloc i, simultàniament, D no és $= d$ (3r més amunt), s'haurà d'investigar, a més a més, de quina manera es poden distingir *a priori* els valors de t, u, que donen substitucions lliures de fraccions d'aquells que proporcionen fraccions. Però, per a

aquest cas, exposarem més avall un altre mètode lliure d'aquesta incomoditat (article 214).

Exemple. La forma $xx + 2yy$ es transforma en la forma (6, 24, 99) per la substitució pròpia $x = 2x' + 7y'$, $y = x' + 5y'$; es desitgen *totes* les transformacions pròpies d'aquella forma en aquesta. Aquí, $D = -2$, $m = 3$, de manera que cal resoldre l'equació $tt + 2uu = 9$. Aquesta, se satisfà de sis maneres diferents, això és, posant $t = 3$, -3, 1, -1, 1, -1; $u = 0$, 0, 2, 2, -2, -2, respectivament. La solució tercera i la sisena donen substitucions amb fraccions, de manera que s'han de rebutjar; de les restants, se segueixen les quatre substitucions

$$x = \begin{cases} 2x' + 7y' \\ -2x' - 7y' \\ -2x' - 9y' \\ 2x' + 9y' \end{cases} \qquad y = \begin{cases} x' + 5y' \\ -x' - 5y' \\ x' + 3y' \\ -x' - 3y' \end{cases}$$

(la primera de les quals és la proposada).

163. Més amunt, ja hem dit de passada que pot resultar que alguna forma F n'impliqui una altra, F', tant pròpiament com impròpiament. Es copsa que això s'esdevé si entre les formes F, F', se'n pot interposar una altra, G, de manera que F impliqui G, G [impliqui] F', i la forma G sigui preparada de manera que sigui impròpiament equivalent a si mateixa. En efecte, si se suposa que F implica pròpiament o bé impròpiament G, com que G implica impròpiament G, F implicarà impròpiament o bé pròpiament G (respectivament), de manera que, en tots dos casos, tant pròpiament com impròpiament (article 159). De la mateixa manera, d'aquí es dedueix que de qualsevol manera que se suposi que G

implica F', F sempre ha d'implicar F' tant pròpiament com impròpiament. Però, que es donen formes tals que siguin impròpiament equivalents a si mateixes, es veu en el cas més obvi, en què el terme central de la forma és $= 0$. En efecte, una tal forma serà oposada (article 159), de manera que impròpiament equivalent, a si mateixa. Més generalment, qualsevol forma $(a,\ b,\ c)$ en què $2b$ és divisible per a està dotada d'aquesta propietat. En efecte, la forma $(c,\ b,\ a)$ serà contigua a aquesta per la primera part (article 160), de manera que pròpiament equivalent; però $(c,\ b,\ a)$, per l'article 159, equival impròpiament a la forma $(a,\ b,\ c)$; per tant, $(a,\ b,\ c)$ equivaldrà impròpiament a si mateixa. Anomenarem *ambigües* les tals formes $(a,\ b,\ c)$, en les quals $2b$ és divisible per a. Així, tindrem aquest teorema:

Una forma F implicarà una altra forma F' tant pròpiament com impròpiament, si es pot trobar una forma ambigua continguda en F que impliqui F'. Aquesta proposició, però, també es pot invertir; això és,

164. Teorema. *Si la forma $Axx+2Bxy+Cyy\ \ldots\ (F)$ implica la forma $A'x'x'+2B'x'y'+C'y'y'\ \ldots\ (F')$ tant pròpiament com impròpiament, es pot trobar una forma ambigua continguda en F i que impliqui la forma F'.*

Suposem que la forma F es transforma en la forma F' tant per la substitució $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, com per la $x = \alpha' x' + \beta' y'$, $y = \gamma' x' + \delta' y'$, diferent d'aquella. Llavors, designats per e, e', els nombres $\alpha\delta - \beta\gamma$, $\alpha'\delta' - \beta'\gamma'$, serà $B'B' - A'C' = ee(BB - AC) = e'e'(BB-AC)$; d'aquí, $ee = e'e'$ i, com que, per hipòtesi, e, e', tenen signes oposats, $e = -e'$, o sigui, $e + e' = 0$.

Ara, és clar que si en F' se substitueix x' per $\delta' x'' - \beta' y''$ i y' per $-\gamma' x'' + \alpha' y''$, es produeix la mateixa forma que si en F s'escriu *o bé* 1) $\alpha(\delta' x'' - \beta' y'') + \beta(-\gamma' x'' + \alpha' y'')$, és a dir, $(\alpha\delta' - \beta\gamma')x'' + (\beta\alpha' - \alpha\beta')y''$, per x, i $\gamma(\delta' x'' - \beta' y'') + \delta(-\gamma' x'' + \alpha' y'')$, és a dir, $(\gamma\delta' - \delta\gamma')x'' + (\delta\alpha' - \gamma\beta')y''$, per y; *o bé* 2) $\alpha'(\delta' x'' - \beta' y'') + \beta'(-\gamma' x'' + \alpha' y'')$, és a dir, $e'x''$, per x, i $\gamma'(\delta' x'' - \beta' y'') + \delta'(-\gamma' x'' + \alpha' y'')$, és a dir, $e'y''$, per y. Així, designats per a, b, c, d, els nombres $\alpha\delta' - \beta\gamma'$, $\beta\alpha' - \alpha\beta'$, $\gamma\delta' - \delta\gamma'$, $\delta\alpha' - \gamma\beta'$, la forma F es transformarà, per les dues substitucions $x = ax'' + by''$, $y = cx'' + dy''$; $x = e'x''$, $y = e'y''$, en la mateixa forma, d'on obtenim les tres equacions següents:

$$Aaa + 2Bac + Ccc = Ae'e', \qquad [1]$$
$$Aab + B(ad + bc) + Ccd = Be'e', \qquad [2]$$
$$Abb + 2Bbd + Cdd = Ce'e'. \qquad [3]$$

Dels valors de a, b, c, d, però, es troba

$$ad - bc = ee' = -ee = -e'e'. \qquad [4]$$

D'aquí resulta, de $d[1] - c[2]$, $(Aa + Bc)(ad - bc) = (Ad - Bc)e'e'$, de manera que $A(a + d) = 0$. A més a més, de $(a + d)[2] - b[1] - c[3]$, resulta $(Ab + B(a + d) + Cc)(ad - bc) = (-Ab + B(a + d) - Cc)e'e'$, de manera que $B(a + d) = 0$. Finalment, de $a[3] - b[2]$, resulta $(Bb + Cd)(ad - bc) = (-Bb + Ca)e'e'$, de manera que $C(a + d) = 0$. Per tant, com que tots els A, B, C, no poden ser $= 0$, serà, necessàriament, $a + d = 0$, o sigui, $a = -d$.

De $a[2] - b[1]$, resulta $(Ba + Cc)(ad - bc) = (Ba - Ab)e'e'$, d'on

$$Ab - 2Ba - Cc = 0. \qquad [5]$$

De les equacions $e + e' = 0$, $a + d = 0$, o sigui, $\alpha\delta - \beta\gamma + \alpha'\delta' - \beta'\gamma' = 0$, $\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha' = 0$, se segueix que $(\alpha + \alpha')(\delta + \delta') = (\beta + \beta')(\gamma + \gamma')$, o sigui, $(\alpha + \alpha') : (\gamma + \gamma') = (\beta + \beta') : (\delta + \delta')$. Sigui aquesta raó,* en nombres mínims, igual a la raó $m : n$, de manera que m, n, siguin primers entre si, i s'agafen μ, ν, de manera que resulti $\mu m + \nu n = 1$. A més a més, sigui r el màxim comú divisor dels nombres a, b, c; per això, el seu quadrat dividirà $aa + bc$, o sigui, $bc - ad$, o sigui, ee; per tant, r també dividirà e. Fet això així, si se suposa que la forma F es transforma en la forma $Mtt + 2Ntu + Puu$ ... (G) per la substitució $x = mt + \frac{\nu e}{r}u$, $y = nt - \frac{\mu e}{r}u$, aquesta serà ambigua i implicarà la forma F'.

Dem. I. Perquè sigui clar que la forma G és ambigua, mostrarem que és $M(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2Nr$, d'on, com que r divideix a, b, c, $\frac{1}{r}(b\mu\mu - 2a\mu\nu - c\nu\nu)$ serà enter, de manera que $2N$, múltiple de M. Però serà $M = Amm + 2Bmn + Cnn$, $Nr = (Am\nu - B(m\mu - n\nu) - Cn\mu)e$. A més a més, es confirma fàcilment per desenvolupament que és $2e + 2a = e - e' + a - d = (\alpha - \alpha')(\delta + \delta') - (\beta - \beta')(\gamma + \gamma')$, $2b = (\alpha + \alpha')(\beta - \beta') - (\alpha - \alpha')(\beta + \beta')$. D'aquí, com que $m(\gamma + \gamma') = n(\alpha + \alpha')$, $m(\delta + \delta') = n(\beta + \beta')$, serà $m(2e + 2a) = -2nb$, o sigui,

$$me + ma + nb = 0. \qquad [7]$$

* Si tots els $\alpha + \alpha'$, $\gamma + \gamma'$, $\beta + \beta'$, $\delta + \delta'$, fossin $= 0$, la raó seria indeterminada, de manera que el mètode no seria aplicable. Però un xic d'atenció ensenya que això no pot ser consistent amb les nostres suposicions. En efecte, seria $\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma'$, és a dir, $e = e'$, de manera que, com que $e = -e'$, $e = e' = 0$. Però, d'aquí, també $B'B' - A'C'$, és a dir, el determinant de la forma F', resultaria $= 0$, formes que hem exclòs completament.

De la mateixa manera, serà $2e - 2a = e - e' - a + d = (\alpha+\alpha')(\delta-\delta') - (\beta+\beta')(\gamma-\gamma')$, $2c = (\gamma-\gamma')(\delta+\delta') - (\gamma+\gamma')(\delta-\delta')$, i, d'aquí, $n(2e-2a) = -2mc$, o sigui,

$$ne - na + mc = 0. \qquad [8]$$

Ara, si a $mm(b\mu\mu - 2a\mu\nu - c\nu\nu)$ s'afegeix $(1-m\mu-n\nu)(m\nu(e-a) + (m\mu+1)b) + (me+ma+nb)(m\mu\nu+\nu) + (ne-na+mc)m\nu\nu$, que, evidentment, és $= 0$, a causa que $1-\mu m-\nu n = 0$, $me+ma+nb = 0$, $ne-na+mc = 0$, surt, desenvolupats degudament els productes i esborrades les parts que es destrueixen, $2m\nu e + b$. Per tant, serà

$$mm(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2m\nu e + b. \qquad [9]$$

De la mateixa manera, sumant a $mn(b\mu\mu - 2a\mu\nu - c\nu\nu)$, $(1 - m\mu - n\nu)((n\nu - m\mu)e - (1 + m\mu + n\nu)a) - (me + ma + nb)m\mu\mu + (ne - na + mc)n\nu\nu$, es troba

$$mn(b\mu\mu - 2a\mu\nu - c\nu\nu) = (n\nu - m\mu)e - a. \qquad [10]$$

Finalment, sumant a $nn(b\mu\mu - 2a\mu\nu - c\nu\nu)$, $(m\mu + n\nu - 1)(n\mu(e+a) + (n\nu+1)c) - (me+ma+nb)n\mu\mu - (ne - na + mc)(n\mu\nu + \mu)$, resulta

$$nn(b\mu\mu - 2a\mu\nu - c\nu\nu) = -2n\mu e - c. \qquad [11]$$

Ara, de 9, 10, 11, es dedueix $(Amm + 2Bmn + Cnn)(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2e(Am\nu + B(n\nu - m\mu) - Cn\mu) + Ab - 2Ba - Cc$, o sigui, a causa de [6], $M(b\mu\mu - 2a\mu\nu - c\nu\nu) = 2Nr$. *Q. E. D.*

II. Per a provar que la forma G implica la forma F', demostrarem, *primer*, que G es transforma en F'

posant $t = (\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y'$, $u = \dfrac{r}{e}(n\alpha - m\gamma)x' + \dfrac{r}{e}(n\beta - m\delta)y' \ldots$ (S); *segon*, que $\dfrac{r}{e}(n\alpha - m\gamma)$, $\dfrac{r}{e}(n\beta - m\delta)$ són enters.

1. Com que F es transforma en G posant $x = mt + \dfrac{\nu e}{r}u$, $y = nt - \dfrac{\mu e}{r}u$, la forma G es transformarà, per la substitució (S), en la mateixa forma en què es transforma F posant $x = m((\mu\alpha+\nu\gamma)x'+(\mu\beta+\nu\delta)y')+\nu((n\alpha-m\gamma)x'+(n\beta-m\delta)y')$, és a dir, $= \alpha(m\mu+n\nu)x'+\beta(m\mu+n\nu)y'$, o sigui, $= \alpha x'+\beta y'$; i $y = n((\mu\alpha+\nu\gamma)x'+(\mu\beta+\nu\delta)y') - \mu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$, és a dir, $= \gamma(n\nu + m\mu)x' + \delta(n\nu + m\mu)y'$, o sigui, $= \gamma x' + \delta y'$. Però, per aquesta substitució, F es transforma en F'; per tant, per la substitució (S), G també es transformarà en F'.

2. Dels valors de e, b, d, es troba que $\alpha' e + \gamma b - \alpha d = 0$, o sigui, a causa que $d = -a$, $n\alpha' e + n\alpha a + n\gamma b = 0$; d'aquí, de [8], $n\alpha' e + n\alpha a = m\gamma e + m\gamma a$, o sigui,

$$(n\alpha - m\gamma)a = (m\gamma - n\alpha')e. \qquad [12]$$

A més a més, resulta $\alpha n b = -\alpha m(e + a)$, $\gamma m b = -m(\alpha' e + \alpha a)$, de manera que

$$(n\alpha - m\gamma)b = (\alpha' - \alpha)me. \qquad [13]$$

Finalment, resulta $\gamma' e - \gamma a + \alpha c = 0$; d'aquí, multiplicant per n i substituint per na el valor de [8], resulta

$$(n\alpha - m\gamma)c = (\gamma - \gamma')ne. \qquad [14]$$

De manera similar, es troba $\beta' e + \delta b - \beta d = 0$, o sigui, $n\beta' e + n\delta b + n\beta a = 0$, de manera que, per [7], $n\beta' e + n\beta a = m\delta e + m\delta a$, o sigui,

$$(n\beta - m\delta)a = (m\delta - n\beta')e. \qquad [15]$$

A més a més, resulta $\beta nb = -\beta m(e+a)$, $\delta mb = -m(\beta' e + \beta a)$, de manera que

$$(n\beta - m\delta)b = (\beta' - \beta)me. \qquad [16]$$

Finalment, $\delta' e - \delta a + \beta c = 0$; d'aquí, multiplicant per n i substituint per na el valor de [8], resulta

$$(n\beta - m\delta)c = (\delta - \delta')ne. \qquad [17]$$

Ara, com que el màxim comú divisor dels nombres a, b, c, és r, es poden agafar enters $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, de manera que resulti $\mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c = r$. Fet això, de 12, 13, 14; 15, 16, 17, serà

$$\mathfrak{A}(m\gamma - n\alpha') + \mathfrak{B}(\alpha' - \alpha)m + \mathfrak{C}(\gamma - \gamma')n = \tfrac{r}{e}(n\alpha - m\gamma),$$
$$\mathfrak{A}(m\delta - n\beta') + \mathfrak{B}(\beta' - \beta)m + \mathfrak{C}(\delta - \delta')n = \frac{r}{e}(n\beta - m\delta),$$

de manera que $\dfrac{r}{e}(n\alpha - m\gamma)$, $\dfrac{r}{e}(n\beta - m\delta)$, enters. *Q. E. D.*

165. *Exemple.* La forma $3xx + 14xy - 4yy$ es transforma en la forma $-12x'x' - 18x'y' + 39y'y'$, tant pròpiament, posant $x = 4x' + 11y'$, $y = -x' - 2y'$, com impròpiament, posant $x = -74x' + 89y'$, $y = 15x' - 18y'$. Aquí, doncs, $\alpha + \alpha'$, $\beta + \beta'$, $\gamma + \gamma'$, $\delta + \delta'$ són -70, 100, 14, -20; però és $-70 : 14 = 100 : -20 = 5 : -1$. Així, fem $m = 5$, $n = -1$, $\mu = 0$, $\nu = -1$. En canvi, els nombres a, b, c, es troben -237, -1170, 48, el màxim comú divisor dels quals és $= 3 = r$; finalment, resulta $e = 3$. D'aquí, la transformació (S) serà la $x = 5t - u$, $y = -t$. Per aquesta, la forma (3, 7, -4) es transforma en la forma ambigua $tt - 16tu + 3uu$.

Si les formes F, F', són equivalents, la forma G, continguda en F, també estarà continguda en F'. Però, com que també implica aquesta forma, li serà equivalent i, conseqüentment, també a la forma F. Així, doncs, en aquest cas, el teorema s'enunciarà així:

Si F, F', són equivalents, tant pròpiament com impròpiament, es podrà trobar una forma ambigua equivalent a totes dues. D'altra banda, en aquest cas, $e = \pm 1$, de manera que també r, que divideix e, serà $= 1$.

Sigui això suficient pel que fa a transformació de formes en general; i, així, passem a la consideració de les *representacions*.

166. *Si la forma F implica la forma F', qualsevol nombre que es pot representar per F' també ho podrà ser per F.*

Siguin x, y; x', y', respectivament, les indeterminades de les formes F, F', i suposem que el nombre M es representa per F' fent $x' = m$, $y' = n$, i que la forma F es transforma en F' per la substitució $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. Llavors, és evident que, si es posa $x = \alpha m + \beta n$, $y = \gamma m + \delta n$, F es transformarà en M.

Si M es pot representar per la forma F' de més maneres, per exemple, fent també $x' = m'$, $y' = n'$, d'aquí se seguiran més representacions de M per F. En efecte, si tant fos $\alpha m + \beta n = \alpha m' + \beta n'$ com $\gamma m + \delta n = \gamma m' + \delta n'$, seria, o bé $\alpha\delta - \beta\gamma = 0$, de manera que també el determinant de la forma $F = 0$, contrari a la hipòtesi, o bé $m = m'$, $n = n'$. D'aquí se segueix que M es

pot representar per F com a mínim de tantes maneres diferents com per F'.

Així, doncs, si tant F implica F' com F', F; és a dir, si F, F', són equivalents; i si un nombre M es pot representar per alguna d'elles, també es podrà representar per l'altra i, certament, de tantes maneres diferents per l'una com per l'altra.

Finalment, observem que, en aquest cas, el màxim comú divisor dels nombres m, n, és igual al màxim comú divisor dels nombres $\alpha m + \beta n$, $\gamma m + \delta n$. Sigui aquell Δ, i els nombres μ, ν, agafats de manera que resulti $\mu m + \nu n = \Delta$. Llavors, serà $(\delta\mu - \gamma\nu)(\alpha m + \beta n) - (\beta\mu - \alpha\nu)(\gamma m + \delta n) = (\alpha\delta - \beta\gamma)(\mu m + \nu n) = \pm\Delta$. D'aquí, el màxim comú divisor dels nombres $\alpha m + \beta n$, $\gamma m + \delta n$ dividirà Δ, però també Δ dividirà aquell, ja que, evidentment, divideix $\alpha m + \beta n$, $\gamma m + \delta n$. Per tant, aquell serà, necessàriament, $= \Delta$. Així, doncs, quan m, n, són primers entre si, $\alpha m + \beta n$, $\gamma m + \delta n$, també seran primers entre si.

167. Teorema. *Si les formes* $axx + 2bxy + cyy \ldots (F)$, $a'x'x' + 2b'x'y' + c'y'y' \ldots (F')$, *són equivalents, el seu determinant* $= D$, *i la darrera es transforma en la primera posant* $x' = \alpha x + \beta y$, $y' = \gamma x + \delta y$; *si, a més a més, el nombre* M *es representa per* F, *fent* $x = m$, $y = n$, *de manera que per* F', *fent* $x' = \alpha m + \beta n = m'$, $y' = \gamma m + \delta n = n'$, *i, certament, de manera que* m *sigui primer amb* n, *i també* m' *amb* n', *ambdues representacions pertanyeran al mateix valor de* $\sqrt{D}\,(\text{mòd. } M)$ *o bé a oposats, segons si la transformació de la forma* F' *en* F *és pròpia, o bé impròpia.*

Dem. Es determinen nombres μ, ν, de manera que resulti $\mu m + \nu n = 1$, i es posa $\dfrac{\delta\mu - \gamma\nu}{\alpha\delta - \beta\gamma} = \mu'$, $\dfrac{-\beta\mu + \alpha\nu}{\alpha\delta - \beta\gamma} = \nu'$ (que seran enters a causa que $\alpha\delta - \beta\gamma = \pm 1$). Llavors, serà $\mu' m' + \nu' n' = 1$ (confronteu el final de l'article precedent). A més a més, sigui $\mu(bm + cn) - \nu(am + bn) = V$, $\mu'(b'm' + c'n') - \nu'(a'm' + b'n') = V'$, i V, V', seran els valors de l'expressió $\sqrt{D}\,(\text{mòd. } M)$ a què pertanyen la primera i la segona representació. Si, en V', se substitueixen μ', ν', m', n', pels seus valors, però en V, $a'\alpha\alpha + 2b'\alpha\gamma + c'\gamma\gamma$, per a, $a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta$, per b, $a'\beta\beta + 2b'\beta\delta + c'\delta\delta$, per c, es trobarà, fet el desenvolupament, $V = V'(\alpha\delta - \beta\gamma)$. Per tant, serà $V = V'$ o bé $V = -V'$, segons que $\alpha\delta - \beta\gamma = +1$ o bé $= -1$, és a dir, les representacions pertanyeran al mateix valor de l'expressió $\sqrt{D}\,(\text{mòd. } M)$ o bé a oposats, segons que la transformació de la forma F' en F sigui pròpia o bé impròpia. *Q. E. D.*

Així, si es tenen més representacions del nombre M per la forma (a, b, c) per valors primers entre si de les indeterminades x, y, que pertanyen a valors *diferents* de l'expressió $\sqrt{D}\,(\text{mòd. } M)$, les representacions corresponents a la forma (a', b', c') pertanyeran, respectivament, als mateixos valors, i si no es dóna cap representació del nombre M per alguna forma que pertanyi a un valor determinat, per a una forma equivalent a aquella tampoc no se'n donarà cap que pertanyi a aquest valor.

168. Teorema. *Si el nombre M es representa per la forma $axx + 2bxy + cyy$ atribuint a x, y, valors m, n, primers entre si, i el valor de l'expressió $\sqrt{D}\,(\text{mòd. } M)$*

a què pertany aquesta representació és N, les formes $(a,\ b,\ c)$, $(M,\ N,\ \frac{NN-D}{M})$, *seran pròpiament equivalents.*

Dem. De l'article 155, és clar que es poden trobar nombres enters μ, ν, de manera que sigui $m\mu + n\nu = 1$, $\mu(bm + cn) - \nu(am + bn) = N$. Fet això, la forma $(a,\ b,\ c)$, per la substitució $x = mx' - \nu y'$, $y = nx' + \mu y'$, que, evidentment, és pròpia, es transforma en una forma el determinant de la qual és $= D(m\mu + n\nu)^2$, és a dir, $= D$, o sigui, en una forma equivalent; forma que, si es posa $= (M',\ N',\ \frac{N'N'-D}{M})$, serà $M' = amm + 2bmn + cnn = M$, $N' = -m\nu a + (m\mu - n\nu)b + n\mu c = N$. Per tant, la forma en què $(a,\ b,\ c)$ es canvia per aquella transformació serà $(M,\ N,\ \frac{NN-D}{M})$. *Q. E. D.*

D'altra banda, de les equacions $m\mu + n\nu = 1$, $\mu(mb + nc) - \nu(ma + nb) = N$, es dedueix

$$\mu = \frac{nN + ma + nb}{amm + 2bmn + cnn} = \frac{nN + ma + nb}{M},$$

$$\nu = \frac{mb + nc - mN}{M},$$

i, així, aquests nombres seran enters.

A més a més, cal observar que aquesta proposició no té lloc si $M = 0$; en efecte, llavors, el terme $\frac{NN-D}{M}$ resulta *indeterminat.**

* En efecte, si volem estendre la terminologia a aquest cas, [dir] que N és valor de l'expressió $\sqrt{D}$ (mòd. M), o sigui, $NN \equiv D$ (mòd. M), significarà que $NN - D$ és múltiple de M, de manera que $= 0$.

169. Si es tenen moltes representacions del nombre M per $(a,\ b,\ c)$ que pertanyen al mateix valor, N, de l'expresssió $\sqrt{D}\,(\text{mòd.}\,M)$ (on sempre suposem els valors de x, y, primers entre si), d'aquí també es dedueixen moltes transformacions pròpies de la forma $(a,\ b,\ c)$, (F), en $(M,\ N,\ \frac{NN-D}{M})$, (G). Això és, si una tal representació també prové dels valors $x = m'$, $y = n'$, (F) també es transforma en (G) per la substitució $x = m'x' + \frac{m'N - m'b - n'c}{M}y'$, $y = n'x' + \frac{n'N + m'a + n'b}{M}y'$. Recíprocament, de qualsevol transformació pròpia de la forma (F) en (G) se seguirà una representació del nombre M per la forma (F) pertanyent al valor N. Això és, si (F) es transforma en (G) posats $x = mx' - \nu y'$, $y = nx' + \mu y'$, M es representa per (F) posant $x = m$, $y = n$, i, com que, aquí, $m\mu + n\nu = 1$, el valor de l'expressió $\sqrt{D}\,(\text{mòd.}\,M)$ a què la representació pertany serà $\mu(bm + cn) - \nu(am + bn)$, és a dir N. Però de moltes representacions pròpies diferents se segueixen la mateixa quantitat de representacions diferents pertanyents a N.* D'aquí es conclou fàcilment que, si es tenen totes les transformacions pròpies de la forma (F) en (G), d'aquestes se segueixen totes les representacions de M per (F) que pertanyen al valor N. D'on la qüestió d'haver d'investigar les representacions d'un nombre donat per una forma donada (en les quals les in-

*Si se suposa que la mateixa representació prové de dues transformacions pròpies diferents, aquelles s'hauran d'obtenir així: 1) $x = mx' - \nu y'$, $y = nx' + \mu y'$; 2) $x = mx' - \nu' y'$, $y = nx' + \mu' y'$. Però de les dues equacions $m\mu + n\nu = m\mu' + n\nu'$, $\mu(mb + nc) - \nu(ma + nb) = \mu'(mb + nc) - \nu'(ma + nb)$ es dedueix fàcilment que és o bé $M = 0$, o bé $\mu = \mu'$, $\nu = \nu'$. Però ja hem exclòs $M = 0$.

determinades prenen valors primers entre si) s'ha reduït a la qüestió de trobar totes les transformacions pròpies d'aquella forma en una donada equivalent.

Ara, havent d'aplicar a això el que hem ensenyat a l'article 162, es conclou fàcilment: Si $x = \alpha$, $y = \gamma$ fos alguna representació del nombre M per la forma (F) pertanyent al valor N, la fórmula general que comprèn totes les representacions d'aquest nombre per la forma (F) pertanyents al valor N seria $x = \dfrac{\alpha t - (\alpha b + \gamma c)u}{m}$, $y = \dfrac{\gamma t + (\alpha a + \gamma b)u}{m}$, on m és el màxim comú divisor dels nombres a, $2b$, c; i t, u, formalment, tots els nombres que satisfan l'equació $tt - Duu = mm$.

170. Si una forma (a, b, c) equival a alguna d'ambigua, de manera que tant pròpiament com impròpiament a la forma $(M, N, \dfrac{NN - D}{M})$, o sigui, tant pròpiament a la forma $(M, N, \dfrac{NN - D}{M})$, com a $(M, -N, \dfrac{NN - D}{M})$, es tindran representacions del nombre M per la forma (F) que pertanyen tant al valor N com al valor $-N$. I recíprocament, si es tenen moltes representacions del nombre M per la mateixa forma (F) que pertanyen a valors *oposats*, N, $-N$, de l'expressió $\sqrt{D}\,(\text{mòd. } M)$, la forma (F) serà equivalent a la forma (G) tant pròpiament com impròpiament, i es podrà trobar una forma ambigua a la qual (F) equivalgui.

Siguin suficients aquí aquestes generalitats de representacions; més avall parlarem de les representacions en les quals les indeterminades tenen valors no primers entre si. Respecte d'altres propietats, les formes el de-

terminant de les quals és negatiu s'han de tractar de manera totalment diferent que les formes de determinant positiu; per tant, ara considerarem ambdues separadament. Comencem per aquelles, ja que són més senzilles.

171. Problema. *Proposada una forma qualsevol* $(a,\ b,\ a')$ *el determinant de la qual és negatiu* $= -D$, *on* D *designa un nombre positiu, trobar una forma pròpiament equivalent a aquesta,* $(A,\ B,\ C)$, *en la qual* A *no és* $> \sqrt{\frac{4}{3}D}$, B *no és* $> \frac{1}{2}A$, C *no és* $< A$.

Solució. Suposem que en la forma proposada no tenen lloc simultàniament totes tres condicions; en efecte, altrament, no seria necessari cercar cap altra forma. Sigui b' el residu mínim absolut del nombre $-b$ segons el mòdul a'* i $a'' = \dfrac{b'b' + D}{a'}$, que serà enter ja que $b'b' \equiv bb$, $b'b' + D \equiv bb + D \equiv aa' \equiv 0\,(\text{mòd.}\,a')$. Ara, si $a'' < a'$, resulti novament b'' el residu mínim absolut de $-b'$ segons el mòdul a'', i $a''' = \dfrac{b''b'' + D}{a''}$. Si, aquí, de nou, és $a''' < a''$, sigui novament b''' el residu mínim absolut de $-b''$ segons el mòdul a''', i $a^{IV} = \dfrac{b'''b''' + D}{a'''}$. Es continua aquesta operació fins que a la progressió a, a', a'', a''', a^{IV}, etc., s'arribi a un terme a^{m+1} que no sigui menor que el seu precedent a^m, cosa que, final-

* Convé observar que si el primer terme o bé l'últim, a o bé a', d'alguna forma $(a,\ b,\ a')$ és $= 0$, el seu determinant és un quadrat positiu; per tant, en el cas present, allò no pot succeir. Per una raó similar, els termes extrems a, a' d'una forma de determinant negatiu no poden tenir signes oposats.

ment, ha de succeir, ja que, altrament, es tindria una progressió infinita de nombres enters contínuament decreixents. Llavors, la forma $(a^m,\ b^m,\ a^{m+1})$ satisfarà totes les condicions.

Dem. I. A la progressió de les formes $(a,\ b,\ a')$, $(a',\ b',\ a'')$, $(a'',\ b'',\ a''')$, etc., qualsevol és contigua a la precedent; per tant, l'última serà pròpiament equivalent a la primera (articles 159, 160).

II. Com que b^m és el residu mínim absolut de $-b^{m-1}$ segons el mòdul a^m, no serà més gran que $\frac{1}{2}a^m$ (article 4).

III. Com que $a^m a^{m+1} = D + b^m b^m$ i a^{m+1} no és $< a^m$, $a^m a^m$ no serà $> D + b^m b^m$; i, com que b^m no és $> \frac{1}{2}a^m$, $a^m a^m$ no serà $> D + \frac{1}{4}a^m a^m$, i $\frac{3}{4}a^m a^m$ no $> D$; i, finalment, a^m no $> \sqrt{\frac{4}{3}D}$.

Exemple. Sigui (304, 217, 155) la forma proposada, el determinant de la qual és $= -31$. Aquí es troba la progressió de formes (304, 217, 155), (155, −62, 25), (25, 12, 7), (7, 2, 5), (5, −2, 7). L'última és la buscada. De la mateixa manera, equivalents a la forma (121, 49, 20), el determinant de la qual és $= -19$, es troben les (20, −9, 5), (5, −1, 4), (4, 1, 5); per tant, (4, 1, 5) serà la forma buscada.

Anomenarem *formes reduïdes* les tals formes $(A,\ B,\ C)$, el determinant de les quals és negatiu, i en les

quals A no és $> \sqrt{\frac{4}{3}D}$, B no és $> \frac{1}{2}A$, i A no és $> C$. Per tant, es podrà trobar una forma reduïda pròpiament equivalent a qualsevol forma de determinant negatiu.

172. Problema. *Trobar condicions sota les quals dues formes reduïdes no idèntiques del mateix determinant $-D$, $(a,\ b,\ c)$, $(a',\ b',\ c')$, puguin ser pròpiament equivalents.*

Solució. Suposem, cosa que és lícita, que a' no és $> a$ i que la forma $axx + 2bxy + cyy$ es transforma en $a'x'x' + 2b'x'y' + cy'y'$ per la substitució pròpia $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. Llavors, es tindran les equacions

$$a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a', \quad [1]$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b', \quad [2]$$
$$\alpha\delta - \beta\gamma = 1. \quad [3]$$

De [1] se segueix que $aa' = (a\alpha + b\gamma)^2 + D\gamma\gamma$; per tant, aa' serà positiu; i, com que $ac = D + bb$, $a'c' = D + b'b'$, també ac, $a'c'$, seran positius; per tant, a, a', c, c', tots tindran el mateix signe. Però tant a com a' no són $> \sqrt{\frac{4}{3}D}$, de manera que aa' no és $> \frac{4}{3}D$; per tant, encara menys $D\gamma\gamma (= aa' - (a\alpha + b\gamma)^2)$ no podrà ser més gran que $\frac{4}{3}D$. D'aquí, γ serà, o bé $= 0$, o bé $= \pm 1$.

I. Si $\gamma = 0$, de [3] se segueix que és, o bé $\alpha = 1$, $\delta = 1$, o bé $\alpha = -1$, $\delta = -1$. En tots dos casos, de [1] resulta $a' = a$ i, de [2], $b' - b = \pm\beta a$. Però b no és $> \frac{1}{2}a$,

i b' no és $> \frac{1}{2}a'$ i, en conseqüència, tampoc no és $> \frac{1}{2}a$. Per tant, l'equació $b' - b = \pm\beta a$ no pot ser consistent si no fos que,

o bé $b = b'$, d'on se seguiria $c' = \frac{b'b' + D}{a'} = \frac{bb + D}{a} = c$; per tant, les formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, serien idèntiques, contrariament a la hipòtesi,

o bé $b = -b' = \pm\frac{1}{2}a$. En aquest cas, també serà $c' = c$ i la forma $(a',\ b',\ c')$ serà $(a,\ -b,\ c)$, és a dir, oposada a la forma $(a,\ b,\ c)$. Simultàniament, a causa que $2b = \pm a$, és clar que aquestes formes són ambigües.

II. Si $\gamma = \pm 1$, de [1] resulta $a\alpha\alpha + c - a' = \pm 2b\alpha$. Però c no és menor que a, de manera que no és menor que a'; d'aquí, $a\alpha\alpha + c - a'$, o sigui, $2b\alpha$, no és menor, certament, que $a\alpha\alpha$. Per tant, com que $2b$ no és més gran que a, α serà no menor que $\alpha\alpha$; d'on, necessàriament, $\alpha = 0$, o bé $\alpha = \pm 1$.

1) Si $\alpha = 0$, de [1] resulta $a' = c$, i, com que a no és ni més gran que c ni menor que a', serà, necessàriament, $a' = a = c$. A més a més, de [3] resulta $\beta\gamma = -1$, d'on, de [2], $b + b' = \pm\delta c = \pm\delta a$. D'aquí, de manera similar com en (I), se segueix que és:

o bé $b = b'$, cas en què les formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, serien idèntiques, contràriament a la hipòtesi;

o bé $b = -b'$, cas en què les formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, seran oposades.

2) Si $\alpha = \pm 1$, de [1] se segueix que $\mp 2b = a + c - a'$. Per tant, com que ni a ni c no són $< a'$, $2b$ serà no $< a$ i no $< c$. Però $2b$ tampoc no és ni $> a$ ni $> c$, d'on, necessàriament, $\pm 2b = a = c$, i, d'aquí, de l'equació $\mp 2b = a + c - a'$, també $= a'$. Així, doncs, de [2] resulta $b' = a(\alpha\beta + \gamma\delta) + b(\alpha\delta + \beta\gamma)$, o sigui, a causa que $\alpha\delta - \gamma\beta = 1$, $b' - b = a(\alpha\beta + \gamma\delta) + 2b\beta\gamma = a(\alpha\beta + \gamma\delta \pm \beta\gamma)$; per tant, necessàriament, com abans,

o bé $b = b'$, d'on les formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, són idèntiques, contràriament a la hipòtesi,

o bé $b = -b'$, de manera que aquelles formes són oposades. Simultàniament, en aquest cas, per causa que $a = \pm 2b$, les formes seran ambigües.

De totes aquestes [proposicions] es conclou que les formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, no poden ser pròpiament equivalents, llevat que fossin oposades i, simultàniament, *o bé* ambigües *o bé* $a = c = a' = c'$. En aquests casos, s'ha pogut preveure fàcilment *a priori* que les formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, equivalen pròpiament; en efecte, si les formes són oposades, han de ser impròpiament equivalents, i si, a sobre, són ambigües, també pròpiament; però si $a = c$, la forma $(\dfrac{D + (a-b)^2}{2},\ a - b,\ a)$ serà contigua, i en conseqüència equivalent, a la forma $(a,\ b,\ c)$; però, per causa que $D + bb = ac = aa$, resulta $\dfrac{D + (a-b)^2}{a} = 2a - 2b$, i la forma $(2a - 2b,\ a - b,\ a)$ és ambigua; per tant, $(a,\ b,\ c)$ també equivaldrà pròpiament a la seva oposada.

Ara es pot discernir de manera igualment fàcil quan dues formes reduïdes no oposades $(a,\ b,\ c)$, $(a',\ b',$

c'), podrien ser impròpiament equivalents. En efecte, seran impròpiament equivalents si (a, b, c), $(a', -b', c')$, que no seran idèntiques, són pròpiament equivalents; i recíprocament. D'aquí, és clar que la condició sota la qual *aquelles* són impròpiament equivalents és que siguin idèntiques i, a sobre, o bé ambigües o bé $a = c$. Però les formes reduïdes que no són ni idèntiques ni oposades no poden ser equivalents ni pròpiament ni impròpiament.

173. PROBLEMA. *Proposades dues formes, F i F', del mateix determinant negatiu, investigar si són equivalents.*

Solució. Se cerquen dues formes reduïdes f, f', pròpiament equivalents a les formes F, F', respectivament; si les formes f, f', són equivalents pròpiament, o bé impròpiament, o bé de les dues maneres, també ho seran F, F'; però si f, f', no són equivalents de cap manera, tampoc no ho seran F, F'.

Per l'article precedent, es poden donar quatre casos:

1) Si f, f', no són ni idèntiques ni oposades, F, F', no seran equivalents de cap manera.

2) Si f, f', són, *primer*, o bé idèntiques o bé oposades, i *segon*, o bé ambigües o bé tenen els seus termes extrems iguals, F, F', seran equivalents tant pròpiament com impròpiament.

3) Si f, f', són idèntiques, però ni són ambigües ni tenen els termes extrems iguals, F, F', només equivaldran pròpiament.

4) Si f, f', són oposades, però ni són ambigües ni tenen els termes extrems iguals, F, F', només seran equivalents impròpiament.

Exemple. Per a les formes (45, 35, 30), (7, 18, 47), el determinant de les quals és $= -5$, es troben les reduïdes equivalents (1, 0, 5), (2, 1, 3); per tant, aquelles no seran equivalents de cap manera. Però, a les formes (23, 38, 63), (15, 20, 27), equival la mateixa reduïda (2, 1, 3), a la qual, com que, simultàniament, és ambigua, les formes (23, 38, 63), (15, 20, 27), equivaldran tant pròpiament com impròpiament. A les formes (37, 53, 78), (53, 73, 102), equivalen les reduïdes (9, 2, 9), (9, -2, 9), que, com que són oposades i els seus termes extrems són iguals, les formes proposades seran equivalents tant pròpiament com impròpiament.

174. La quantitat de totes les formes reduïdes que tenen determinant donat $-D$ sempre és finita i bastant mòdica respecte del nombre D; aquestes formes es poden trobar de dues maneres. Designem formalment per (a, b, c) les formes reduïdes de determinant $-D$, on, així, s'han de determinar tots els valors de a, b, c.

Primer mètode. S'agafen per a a tots els nombres, tant positius com negatius, no més grans que $\sqrt{\frac{4}{3}D}$ dels quals $-D$ és residu quadràtic i, per a cada a, resulti b successivament igual a tots els valors de l'expressió $\sqrt{-D}\,(\text{mòd.}\, a)$ no més grans que $\frac{1}{2}a$, agafats tant positivament com negativament; per a cadascun dels valors determinats de a, b, es posa $c = \frac{D + bb}{a}$. Si, d'aquesta

manera, s'originen formes en què $c < a$, aquestes hauran de ser rebutjades, però les restants seran, evidentment, reduïdes.

Segon mètode. S'agafen per a b tots els nombres, tant positius com negatius, no més grans que $\frac{1}{2}\sqrt{\frac{4}{3}D}$, o sigui, $\sqrt{\frac{1}{3}D}$; per a cada b, es descompon $bb + D$ en dos factors de totes les maneres en què es pot fer (tenint en compte també la diferència dels signes), ambdós no menors que $2b$, i es posa un dels factors, certament el menor quan els factors són diferents, $= a$, l'altre $= c$. Si s'han rebutjat les formes produïdes d'aquesta manera en què $a > \sqrt{\frac{4}{3}D}$, totes les restants seran, evidentment, reduïdes. Finalment, és clar que no es pot donar cap forma reduïda que no es trobi per tots dos mètodes.

Exemple. Sigui $D = 85$. Aquí, el límit dels valors de a és $\sqrt{\frac{340}{3}}$, que és entre 10 i 11. Però els nombres entre 1 i 10 (inclusivament) dels quals -85 és residu són 1, 2, 5, 10. D'on es tenen les dotze formes (1, 0, 85), (2, 1, 43), (2, -1, 43), (5, 0, 17), (10, 5, 11), (10, -5, 11); (-1, 0, -85), (-2, 1, -43), (-2, -1, -43), (-5, 0, -17), (-10, 5, -11), (-10, -5, -11).

Per l'altre mètode, el límit dels valors de b és $\sqrt{\frac{85}{3}}$, que està situat entre 5 i 6. Per a $b = 0$, es produeixen les formes (1, 0, 85), (-1, 0, -85), (5, 0, 17), (-5, 0, -17); per a $b = \pm 1$, les (2, ± 1, 43), (-2, ± 1, -43). Per a $b = \pm 2$, no se'n té cap, ja que 89 no es pot descompon-

dre en dos factors que tots dos siguin no > 4. El mateix val per a ± 3, ± 4. Finalment, per a $b = \pm 5$, apareixen $(10, \pm 5, 11)$, $(-10, \pm 5, -11)$.

175. Si de totes les formes reduïdes d'un determinant donat, de cada dues formes que, encara que no idèntiques, no obstant això són pròpiament equivalents, se'n rebutja l'una o l'altra, les formes que queden estaran proveïdes de la propietat remarcable que qualsevol forma del mateix determinant és pròpiament equivalent a una d'elles i, certament, només a una (en efecte, altrament, entre aquestes n'hi hauria algunes de pròpiament equivalents). D'on és clar que *totes les formes del mateix determinant es poden distribuir en tantes classes com formes hagin quedat*, això és, assignant a la mateixa classe les formes pròpiament equivalents a una mateixa reduïda. Així, per a $D = 85$, queden les formes $(1, 0, 85)$, $(2, 1, 43)$, $(5, 0, 17)$, $(10, 5, 11)$, $(-1, 0, -85)$, $(-2, 1, -43)$, $(-5, 0, -17)$, $(-10, 5, -11)$; per tant, totes les formes de determinant -85 es podran distribuir en vuit classes, segons que equivalguin pròpiament a la primera forma, o bé a la segona, etc. Però es copsa que formes col·locades en una mateixa classe són pròpiament equivalents, formes de classes diferents no poden ser pròpiament equivalents. Però, més avall, exposarem molt més abundantment aquest argument de classificació de formes. Aquí afegim una única observació. Ja hem mostrat més amunt que si el determinant de la forma (a, b, c) és negatiu $= -D$, a i c tenen el mateix signe (ja que $ac = bb + D$, de manera que és positiu); per la mateixa raó es copsa fàcilment que si les formes (a, b, c), (a', b', c'), són equivalents, tots els a, c, a', c', hauran de tenir els mateixos signes. En efecte, si la primera es transforma en la darrera per la substitució

$x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, serà $a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma = a'$, d'aquí, $aa' = (a\alpha + b\gamma)^2 + D\gamma\gamma$, de manera que, certament, és no negatiu; però, com que ni a ni a' no poden ser $= 0$, aa' serà positiu i, en conseqüència, els signes de a, a', els mateixos. D'aquí, és evident que les formes els termes exteriors de les quals siguin positius s'han separat completament d'aquelles els termes exteriors de les quals siguin negatius, i és suficient considerar de les formes reduïdes només les que tenen els seus termes exteriors positius, ja que la quantitat de les restants és la mateixa i s'originen d'aquelles atribuint signes oposats als termes exteriors; i val el mateix per a les formes que s'han de rebutjar de les reduïdes i per a les que queden.

176. Així, aquí adjuntem, per a alguns determinants negatius, una taula de formes segons les quals es poden separar en classes totes les restants del mateix determinant; però, d'acord amb les observacions de l'article precedent, només la meitat, això és, aquelles els termes exteriors de les quals són positius.

D				
1	$(1,0,1)$			
2	$(1,0,2)$			
3	$(1,0,3)$,	$(2,1,2)$		
4	$(1,0,4)$,	$(2,0,2)$		
5	$(1,0,5)$,	$(2,1,3)$		
6	$(1,0,6)$,	$(2,0,3)$		
7	$(1,0,7)$,	$(2,1,4)$		
8	$(1,0,8)$,	$(2,0,4)$,	$(3,1,3)$	
9	$(1,0,9)$,	$(2,1,5)$,	$(3,0,3)$	
10	$(1,0,10)$,	$(2,0,5)$		
11	$(1,0,11)$,	$(2,1,6)$,	$(3,1,4)$,	$(3,-1,4)$
12	$(1,0,12)$,	$(2,0,6)$,	$(3,0,4)$,	$(4,2,4)$

Fóra superflu continuar aquí aquesta taula més enllà, ja que, més avall, ensenyarem a disposar-la molt més apropiadament.

Així, és clar que qualsevol forma de determinant -1 equival pròpiament a la forma $xx + yy$, si els seus termes exteriors són positius, o bé a la $-xx - yy$, si són negatius; qualsevol forma de determinant -2, els termes exteriors de la qual són positius, a la forma $xx + 2yy$, etc.; qualsevol forma de determinant -11, els termes exteriors de la qual són positius, a alguna de les $xx - 11yy$, $2xx+2xy+6yy$, $3xx+2xy+4yy$, $3xx-2xy+4yy$, etc.

177. Problema. *Es té una sèrie de formes de les quals qualsevol és contigua a la precedent per la part posterior; es desitja alguna transformació pròpia de la primera en una forma qualsevol de la sèrie.*

Solució. Siguin $(a,\ b,\ a') = F$, $(a',\ b',\ a'') = F'$, $(a'',\ b'',\ a''') = F''$, $(a''',\ b''',\ a^{IV}) = F'''$, etc., les formes. Es designen $\dfrac{b+b'}{a'}$, $\dfrac{b'+b''}{a''}$, $\dfrac{b''+b'''}{a'''}$, etc., respectivament per h', h'', h''', etc. Siguin $x,\ y;\ x',\ y';\ x'',\ y''$; etc., les indeterminades de les formes F, F', F'', etc. Se suposa que F es transforma en

$$\begin{aligned}
&F', \text{ posats } x = \alpha' x' + \beta' y', \qquad y = \gamma' x' + \delta' y';\\
&F'', \text{ posats } x = \alpha'' x'' + \beta'' y'', \quad y = \gamma'' x'' + \delta'' y'';\\
&F''', \text{ posats } x = \alpha''' x''' + \beta''' y''', y = \gamma''' x''' + \delta''' y''';\\
&\textit{etc.}
\end{aligned}$$

Llavors, com que F es transforma en F' posats $x = -y'$, $y = x' + h'y'$; F' en F'', posats $x' = -y''$,

$y' = x'' + h''y''$; F'' en F''', posats $x'' = -y'''$, $y'' = x''' + h'''y'''$; etc. (article 160), es descobrirà fàcilment l'algoritme següent (article 159):

$$\begin{array}{llll} \alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h'; \\ \alpha'' = \beta' & \beta'' = h''\beta' - \alpha' & \gamma'' = \delta' & \delta'' = h''\delta' - \gamma'; \\ \alpha''' = \beta'' & \beta''' = h'''\beta'' - \alpha'' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \gamma''; \end{array}$$

etc.,

o sigui,

$$\begin{array}{llll} \alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h'; \\ \alpha'' = \beta' & \beta'' = h''\beta' & \gamma'' = \delta' & \delta'' = h''\delta' - 1; \\ \alpha''' = \beta'' & \beta''' = h'''\beta'' - \beta' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \delta'; \end{array}$$

etc.

Que totes aquestes transformacions són pròpies, es pot deduir sense cap dificultat tant de la seva formació com de l'article 159.

Aquest algoritme extremament simple i prest per al càlcul és anàleg a l'algoritme exposat a l'article 27, al qual també es pot reduir.* D'altra banda, aquesta solució no està restringida a les formes de determinant

* Això és, amb la notació de l'article 27, serà $\beta^n = \pm[-h'', h''', -h^{IV}, \ldots, \pm h^n]$, on els signes posats ambiguament han de ser −, −; −, +; +, −; +, +, segons que n sigui de la forma $4k$+0, 1, 2, 3, i $\delta^n = \pm[h', -h'', h''', \ldots, \pm h^n]$, on els signes ambigus han de ser +, −; +, +; −, −; −, +, segons que n sigui de la forma $4k$+0, 1, 2, 3. Però la brevetat no ens permet exposar més extensament això, que qualsevol podrà confirmar fàcilment per si mateix.

negatiu, sinó que s'estén a tots els casos, sempre que cap dels nombres a', a'', a''', etc., no sigui $= 0$.

178. Problema. *Proposades dues formes F, f, pròpiament equivalents, del mateix determinant negatiu, trobar alguna transformació pròpia de l'una en l'altra.*

Solució. Suposem que la forma F és (A, B, A'), i que pel mètode de l'article 171 s'ha trobat una progressió de formes (A', B', A''), (A'', B'', A'''), etc., fins a (A^m, B^m, A^{m+1}), la qual sigui reduïda; i, similarment, que f és (a, b, a'), i pel mateix mètode s'ha trobat una sèrie (a', b', a''), (a'', b'', a'''), etc., fins a (a^n, b^n, a^{n+1}) que sigui reduïda. Llavors, poden tenir lloc dos casos.

I. Si les formes (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) són, o bé idèntiques, o bé oposades i simultàniament ambigües. Llavors, les formes (A^{m-1}, B^{m-1}, A^m), $(a^n, -b^{n-1}, a^{n-1})$, seran contigües (on A^{m-1} designa el penúltim terme de la progressió A, A', A'', $\ldots$, A^m, i, similarment, B^{m-1}, a^{n-1}, b^{n-1}). En efecte, $A^m = a^n$, $B^{m-1} \equiv -B^m$ (mòd. A^m), $b^{n-1} \equiv -b^n$ (mod a^n, o sigui, A^m), d'on $B^{m-1} - b^{n-1} \equiv b^n - B^m$, de manera que $\equiv 0$, si les formes (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}), són idèntiques, i $\equiv 2b^n$, de manera que $\equiv 0$, si són oposades i ambigües. Per tant, en la progressió de formes (A, B, A'), (A', B', A''), $\ldots$, (A^{m-1}, B^{m-1}, A^m), $(a^n, -b^{n-1}, a^{n-1})$, $(a^{n-1}, -b^{n-2}, a^{n-2})$, $\ldots$, $(a', -b, a)$, (a, b, a'), qualsevol forma serà contigua a la precedent, de manera que, per l'article precedent, es podrà trobar una transformació pròpia de la primera, F, en l'última, f.

II. Si les formes (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}), no són idèntiques sinó oposades i simultàniament $A^m =$

$A^{m+1} = a^n = a^{n+1}$. Llavors, la progressió de formes $(A,\ B,\ A')$, $(A',\ B',\ A'')$, $\ldots$, $(A^m,\ B^m,\ A^{m+1})$, $(a^n,\ -b^{n-1},\ a^{n-1})$, $(a^{n-1},\ -b^{n-2},\ a^{n-2})$, $\ldots$, $(a',\ -b,\ a)$, $(a,\ b,\ a')$, tindrà la mateixa propietat predita. En efecte, $A^{m+1} = a^n$, i $B^m - b^{n-1} = -(b^n + b^{n-1})$ és divisible per a^n. D'on, per l'article precedent, es trobarà una transformació pròpia de la primera forma, F, en l'última, f.

Exemple. Així, per a les formes (23, 38, 63), (15, 20, 27), es té la progressió (23, 38, 63), (63, 25, 10), (10, 5, 3), (3, 1, 2), (2, −7, 27), (27, −20, 15), (15, 20, 27); per tant, $h' = 1$, $h'' = 3$, $h''' = 2$, $h^{IV} = -3$, $h^V = -1$, $h^{VI} = 0$. D'aquí, es dedueix que la transformació de la forma $23xx + 76xy + 63yy$ en $15tt + 40tu + 27uu$ és la $x = -13t - 18u$, $y = 8t + 11u$.

D'aquesta solució se segueix sense cap dificultat la solució del problema: *Si les formes F, f, són impròpiament equivalents, trobar una transformació impròpia de la forma F en f.* En efecte, sigui $f = att + 2btu + a'uu$, i la forma oposada $app - 2bpq + a'qq$ serà pròpiament equivalent a la forma F. Se cerca una transformació pròpia de la forma F en aquella, $x = \alpha p + \beta q$, $y = \gamma p + \delta q$, i és clar que F es transforma en f, posat $x = \alpha t - \beta u$, $y = \gamma t - \delta u$, i que aquesta transformació és impròpia.

Així, doncs, si les formes F, f, són equivalents tant pròpiament com impròpiament, es podrà trobar tant alguna transformació pròpia com alguna d'impròpia.

179. Problema. *Si les formes F, f, són equivalents, trobar totes les transformacions de la forma F en f.*

Solució. Si les formes F, f, són equivalents només d'una manera, és a dir, o bé només pròpiament, o bé només impròpiament, se cerca, per l'article precedent, una transformació de la forma F en f, i és clar que no se'n poden donar d'altres que les que són similars a aquesta. Però si les formes F, f, equivalen tant pròpiament com impròpiament, se cerquen dues transformacions, l'una pròpia i l'altra impròpia. Ara, sigui la forma $F = (A, B, C)$, $BB - AC = -D$, i el màxim comú divisor dels nombres A, $2B$, C, $= m$. Llavors, de l'article 162, és clar que, en el primer cas, totes les transformacions de la forma F en f es poden deduir d'una transformació; en el darrer, totes les pròpies d'una pròpia i totes les impròpies d'una impròpia, sempre que es tinguin totes les solucions de l'equació $tt + Duu = mm$. Així, doncs, trobades aquestes, el problema estarà resolt.

Es té, però, $D = AC - BB$, $4D = 4AC - 4BB$; per tant, $\dfrac{4D}{mm} = 4\dfrac{A}{m}\dfrac{C}{m} - \left(\dfrac{2B}{m}\right)^2$ serà enter. Ara,

1) si $\dfrac{4D}{mm} > 4$, serà $D > mm$; per tant, en $tt + Duu = mm$, u haurà de ser necessàriament $= 0$, de manera que t no pot tenir altres valors que $+m$ i $-m$. D'aquí, si F, f, són equivalents només d'una manera i [es té] alguna transformació $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, no poden tenir-ne lloc d'altres excepte aquesta mateixa, que surt de $t = m$ (article 162), i la $x = -\alpha x' - \beta y'$, $y = -\gamma x' - \delta y'$. Però si F, f, equivalen tant pròpiament com impròpiament i es té alguna transformació pròpia $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, i una d'impròpia $x = \alpha' x' + \beta' y'$, $y = \gamma' x' + \delta' y'$, excepte aquella (de $t = m$) i la $x = -\alpha x' - \beta y'$, $y = -\gamma x' - \delta y'$ (de $t = -m$),

no se'n donarà cap altra de pròpia; i, similarment, cap d'impròpia excepte $x = \alpha' x' + \beta' y'$, $y = \gamma' x' + \delta' y'$; i $x = -\alpha' x' - \beta' y'$, $y = -\gamma' x' - \delta' y'$.

2) Si $\frac{4D}{mm} = 4$, o sigui, $D = mm$, l'equació $tt + Duu = mm$ admet les quatre solucions t, $u = m$, 0; $-m$, 0; 0, 1; 0, -1. D'aquí, si F, f, són equivalents només d'una manera, i [es té] alguna transformació $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, es donaran en total *quatre* transformacions, $x = \pm\alpha x' \pm \beta y'$, $y = \pm\gamma x' \pm \delta y'$, $x = \mp\frac{\alpha B + \gamma C}{m} x' \mp \frac{\beta B + \delta C}{m} y'$, $y = \pm\frac{\alpha A + \gamma B}{m} x' \pm \frac{\beta A + \delta B}{m} y'$. Però si F, f, equivalen de dues maneres, o sigui, juntament amb aquella transformació donada se'n té una altra de diferent, aquesta també en proporcionarà quatre diferents d'aquelles, de manera que es tindran *vuit* transformacions. D'altra banda, en aquest cas, es pot demostrar fàcilment que F, f, sempre equivalen realment de dues maneres. Efectivament, com que $D = mm = AC - BB$, m també dividirà B. El determinant de la forma $\left(\frac{A}{m}, \frac{B}{m}, \frac{C}{m}\right)$ serà $= -1$; per tant, serà equivalent a la forma (1, 0, 1), o bé a la (-1, 0, -1). Però es copsa fàcilment que, per la mateixa transformació per la qual $\left(\frac{A}{m}, \frac{B}{m}, \frac{C}{m}\right)$ es transforma en (± 1, 0, ± 1), la forma (A, B, C) es transforma en ($\pm m$, 0, $\pm m$), ambigua. Per tant, la forma (A, B, C), equivalent a una ambigua, equivaldrà tant pròpiament com impròpiament a qualsevol forma a què equivalgui.

3) Si $\frac{4D}{mm} = 3$, o sigui, $4D = 3mm$. Llavors, m serà parell i totes les solucions de l'equació $tt + Duu =$

mm seran les sis t, $u = m$, 0; $-m$, 0; $\frac{1}{2}m$, 1; $-\frac{1}{2}m$, -1; $\frac{1}{2}m$, -1; $-\frac{1}{2}m$, 1. Així, si es tenen dues transformacions diferents de la forma F en f, $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$; $x = \alpha' x' + \beta' y'$, $y = \gamma' x' + \delta' y'$, es tindran dotze transformacions, això és, sis similars a la primera, $x = \pm\alpha x' \pm \beta y'$, $y = \pm\gamma x' \pm \delta y'$;

$$x = \pm\left(\frac{1}{2}\alpha - \frac{\alpha B + \gamma C}{m}\right)x' \pm \left(\frac{1}{2}\beta - \frac{\beta B + \delta C}{m}\right)y',$$
$$y = \pm\left(\frac{1}{2}\gamma + \frac{\alpha A + \gamma B}{m}\right)x' \pm \left(\frac{1}{2}\delta + \frac{\beta A + \delta B}{m}\right)y';$$
$$x = \pm\left(\frac{1}{2}\alpha + \frac{\alpha B + \gamma C}{m}\right)x' \pm \left(\frac{1}{2}\beta + \frac{\beta B + \delta C}{m}\right)y',$$
$$y = \pm\left(\frac{1}{2}\gamma - \frac{\alpha A + \gamma B}{m}\right)x' \pm \left(\frac{1}{2}\delta - \frac{\beta A + \delta B}{m}\right)y';$$

i sis similars a la segona, que provenen d'aquestes, posant α', β', γ', δ', per α, β, γ, δ.

Però, que, en aquest cas, F, f, sempre equivalen de totes dues maneres, ho demostrem així. El determinant de la forma $\left(\frac{2A}{m}, \frac{2B}{m}, \frac{2C}{m}\right)$ serà $= -\frac{4D}{mm} = -3$, de manera que (article 176) és equivalent, o bé a la forma $(\pm 1, 0, \pm 3)$, o bé a la $(\pm 2, \pm 1, \pm 2)$. D'on es copsa fàcilment que la forma (A, B, C) equival, o bé a la forma $\left(\pm\frac{1}{2}m, 0, \pm\frac{3}{2}m\right)$, o bé a la $\left(\pm m, \frac{1}{2}m, \pm m\right)$,* que totes dues són ambigües, de manera que [equival] de les dues maneres a qualsevol equivalent.

* Es pot demostrar que la forma (A, B, C) equival necessàriament a la darrera, però això no és necessari aquí.

4) Si se suposa que $\frac{4D}{mm} = 1$, resulta que $\left(\frac{2B}{m}\right)^2 = 4\frac{AC}{mm} - 2$, de manera que $\equiv 2\,(\text{mòd. }4)$. Però, com que cap quadrat no pot ser $\equiv 2\,(\text{mòd. }4)$, aquest cas no pot tenir lloc.

5) Suposant que $\frac{4D}{mm} = 1$, resulta que $\left(\frac{2B}{m}\right)^2 = 4\frac{AC}{mm} - 1 \equiv -1\,(\text{mòd. }4)$. Que, com que és impossible, aquest cas tampoc no pot tenir lloc.

D'altra banda, com que D no és ni $= 0$ ni negatiu, no es poden donar altres casos excepte els enumerats.

180. Problema. *Trobar totes les representacions d'un nombre donat M per la forma $axx+2bxy+cyy\ldots F$, de determinant negatiu $-D$, en les quals es trobin primers entre si els valors de x, y.*

Solució. De l'article 154 és clar que F no pot representar de cap manera el que se cerca, llevat que $-D$ sigui un residu quadràtic de M. Així, s'investiguen primer tots els valors diferents (és a dir, incongrus) de l'expressió $\sqrt{-D}\,(\text{mòd. }M)$, i que siguin N, $-N$, N', $-N'$, N'', $-N''$, etc.; perquè el càlcul surti més simple, es poden determinar tots els N, N', etc., de manera que no siguin $> \frac{1}{2}M$. Ara, com que qualsevol representació ha de pertànyer a algun d'aquests valors, es consideren separadament cadascun d'ells.

Si les formes F, $\left(M,\ N,\ \frac{D+NN}{M}\right)$ no són pròpiament equivalents, no es pot donar cap representació

de M que pertanyi al valor N (article 168). Però si ho són, s'investiga una transformació pròpia de la forma F en $Mx'x' + 2Nx'y' + \frac{D+NN}{m}y'y'$; sigui aquesta $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, i $x = \alpha$, $y = \gamma$, serà una representació del nombre M per F pertanyent a N. Sigui $= m$ el màxim comú divisor dels nombres A, $2B$, C, i es distingiran tres casos (article precedent):

1) Si $\frac{4D}{mm} > 4$, no es donaran altres representacions pertanyents a N que les *dues* $x = \alpha 4$, $y = \gamma$; $x = -\alpha$, $y = -\gamma$ (articles 169, 180).

2) Si $\frac{4D}{mm} = 4$, es tindran les *quatre* representacions $x = \pm\alpha$, $y = \pm\gamma$; $x = \mp\frac{1}{m}(\alpha B + \gamma C)$, $y = \pm\frac{1}{m}(\alpha A + \gamma B)$.

3) Si $\frac{4D}{mm} = 3$, es tindran les *sis* representacions $x = \pm\alpha$, $y = \pm\gamma$; $x = \pm\left(\frac{1}{2}\alpha - \frac{1}{m}(\alpha B + \gamma C)\right)$, $y = \pm\left(\frac{1}{2}\gamma + \frac{1}{m}(\alpha A + \gamma B)\right)$; $x = \pm\left(\frac{1}{2}\alpha + \frac{1}{m}(\alpha B + \gamma C)\right)$, $y = \pm\left(\frac{1}{2}\gamma - \frac{1}{m}(\alpha A + \gamma B)\right)$.

Les representacions que pertanyen als valors $-N$, N', $-N'$, etc., s'han de cercar de la mateixa manera.

181. La investigació de les representacions del nombre M per la forma F en què x, y, tenen valors

no primers entre si es pot reduir fàcilment al cas ja considerat. Una tal representació resulta posant $x = \mu e$, $y = \mu f$, de manera que μ és el màxim comú divisor dels μe, μf, o sigui, e, f, primers entre si. Llavors, serà $M = \mu\mu(Aee + 2Bef + Cff)$, de manera que divisible per $\mu\mu$; però la substitució $x = e$, $y = f$, serà una representació del nombre $\frac{M}{\mu\mu}$ per la forma F en què x, y, tenen valors primers entre si. Així, si M no és divisible per cap quadrat (excepte 1), *per exemple*, si és un nombre primer, no es donaran tals representacions de M. Però si A implica divisors quadràtics, siguin aquests $\mu\mu$, $\nu\nu$, $\pi\pi$, etc. Primer, se cerquen totes les representacions del nombre $\frac{M}{\mu\mu}$ per una forma (A, B, C) en què x, y, tenen valors primers entre si; valors que, si es multipliquen per μ, proporcionaran totes les representacions de M en què el màxim comú divisor dels nombres x, y, és μ. De manera similar, totes les representacions de $\frac{M}{\nu\nu}$ en què els valors de x, y, són primers entre si proporcionaran totes les representacions de M en què el màxim comú divisor dels valors de x, y, és ν, etc.

Així, doncs, és palès que, pels preceptes precedents, es poden trobar totes les representacions d'un nombre donat per una forma donada de determinant negatiu.

182. Baixem a alguns casos particulars, tant per la seva notable elegància com pel constant esforç esmerçat en ells per l'il·lm. Euler, d'on han obtingut una consideració gairebé clàssica.

I. No es pot representar cap nombre per la forma $xx + yy$ de manera que x sigui primer amb y (o sigui, descompondre'l en dos quadrats primers entre si), llevat que -1 en sigui un residu quadràtic; però els tals nombres, agafats positivament, s'hi podran [representar] tots. Sigui M un tal nombre, i N, $-N$, N', $-N'$, N'', $-N''$, etc., tots els valors de l'expressió $\sqrt{-1}\,(\text{mòd. } M)$. Llavors, per l'article 176, la forma $\left(M,\ N,\ \dfrac{NN+1}{M}\right)$ serà pròpiament equivalent a la forma (1, 0, 1). Sigui $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, alguna transformació pròpia d'aquesta en aquella, i les representacions del nombre M per la forma $xx + yy$ que pertanyen a N seran aquestes quatre:* $x = \pm\alpha$, $y = \pm\gamma$; $x = \mp\gamma$, $y = \pm\alpha$.

Com que la forma (1, 0, 1) és ambigua, és clar que la forma $\left(M,\ -N,\ \dfrac{NN+1}{M}\right)$ també li és pròpiament equivalent, i aquella es transforma pròpiament en aquesta posats $x = \alpha x' - \beta y'$, $y = -\gamma x' + \delta y'$. D'aquí es deriven quatre representacions de M pertanyents a $-N$, $x = \pm\alpha$, $y = \mp\gamma$; $x = \pm\gamma$, $y = \mp\alpha$. Així, és evident que es donen vuit representacions de M, la meitat de les quals pertanyerà a N, i l'altra, a $-N$; però totes aquestes només mostren *una única* descomposició del nombre M en dos quadrats, $M = \alpha\alpha + \gamma\gamma$, suposat que només considerem els quadrats, però no l'ordre ni els signes de les arrels.

Així, si no es donen altres valors de l'expressió $\sqrt{-1}\,(\text{mòd. } M)$ excepte N i $-N$, cosa que succeeix, *per exemple*, quan M és un nombre primer, M es podrà

* En efecte, és clar que aquest cas és contingut en (2) de l'article 180.

descompondre en dos quadrats primers entre si només d'una manera. Ara, com que -1 és un residu quadràtic de qualsevol nombre primer de la forma $4n + 1$ (article 108), i, evidentment, un nombre primer no es pot descompondre en dos quadrats no primers entre si, tenim el teorema:

Qualsevol nombre primer de la forma $4n + 1$ *es pot descompondre en dos quadrats i, certament, només d'una manera.* $1 = 0 + 1$, $5 = 1 + 4$, $13 = 4 + 9$, $17 = 1 + 16$, $29 = 4 + 25$, $37 = 1 + 36$, $41 = 16 + 25$, $53 = 4 + 49$, $61 = 25 + 36$, $73 = 9 + 64$, $89 = 25 + 64$, $97 = 16 + 81$, etc.

Aquest elegantíssim teorema ja fou conegut per Fermat, però va ser demostrat primer per l'il·lm. Euler, *Comm. nov. Petr. T. V. anys* 1754, 1755, *p.* 3 *i s.* En el *T. IV* hi ha una dissertació que pertany a aquest mateix argument, p. 3 i següents, però, llavors, encara no havia resolt el fet completament, vegeu principalment l'article 27.

Així, doncs, si algun nombre de la forma $4n + 1$ es pot descompondre en dos quadrats o bé de moltes maneres, o bé de cap manera, certament no serà primer.

Però recíprocament, si l'expressió $\sqrt{-1}\,(\text{mòd. } M)$, a part de N i $-N$, encara té altres valors, encara es donaran altres representacions de M que pertanyen a aquests. Així, en aquest cas, M es podrà descompondre en dos quadrats de moltes maneres, per exemple, $65 = 1 + 64 = 16 + 49$, $221 = 25 + 196 = 100 + 121$.

Les representacions restants, en les quals x, y, obtenen valors no primers entre si, es poden trobar fàcil-

ment pel nostre mètode general. Observem, només, que si un nombre que inclou alguns factors de la forma $4n+3$ no es pot alliberar d'ells per cap divisió per quadrats (cosa que resultarà si algun o bé molts de tals factors té *dimensió imparella*), aquest no es pot descompondre en dos quadrats de cap manera.*

II. Cap nombre del qual -2 és no-residu no es pot representar per la forma $xx + 2yy$ de manera que x sigui primer amb y; tots els altres s'hi podran [representar]. Sigui -2 residu del nombre M, i N algun valor de l'expresssió $\sqrt{-2}$ (mòd. M). Llavors, per l'article 176, les formes $(1,\ 0,\ 2)$, $\left(M,\ N,\ \dfrac{NN+2}{M}\right)$, seran pròpiament equivalents. Si aquella es transforma pròpiament en aquesta posant $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, la representació del nombre M pertanyent a N serà $x = \alpha$, $y = \gamma$. Excepte aquesta i la $x = -\alpha$, $y = -\gamma$, cap altra no pertanyerà a N (article 180).

---

* Si el nombre M és $= 2^{\mu} S a^{\alpha} b^{\beta} c^{\gamma} \cdots$, de manera que a, b, c, etc. siguin nombres primers diferents de la forma $4n + 1$, i S és el producte de tots els factors primers de M de la forma $4n + 3$ (forma a la qual es pot reduir qualsevol nombre positiu fent $\mu = 0$ quan M és imparell i $S = 1$ quan M no implica cap factor de la forma $4n + 3$), M no es podrà descompondre en dos quadrats *de cap manera* si S és no quadrat; però si S és un quadrat, es donaran $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)etc.$ descomposicions de M, quan algun del nombres α, β, γ, etc. sigui imparell, o bé $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)etc. + \frac{1}{2}$, quan tots els α, β, γ, etc. són parells (suposat que només es considerin els quadrats mateixos). Aquells que estiguin prou versats en el càlcul de combinacions podran deduir sense dificultat la demostració d'aquest teorema de la nostra teoria general (en la qual, igual que en altres *particularitats* no ens és permès de detenir-nos). Vegeu l'article 105.

De manera similar a més amunt, es copsa que les representacions $x = \pm\alpha$, $y = \mp\gamma$, pertanyen al valor $-N$. Però totes aquestes quatre representacions només exhibeixen una única partició de M en un quadrat i el doble d'un quadrat, i si, excepte N i $-N$, no es donen altres valors de l'expressió $\sqrt{-2}\,(\text{mòd.}\,M)$, no es donaran altres descomposicions. D'aquí, amb l'ajut de la proposició de l'article 116, es dedueix fàcilment el teorema:

Qualsevol nombre primer de la forma $8n+1$ *o bé* $8n+3$ *es pot descompondre en un quadrat i el doble d'un quadrat, i això només d'una manera.* $1 = 1+0$, $3 = 1+2$, $11 = 9+2$, $17 = 9+8$, $19 = 1+18$, $41 = 9+32$, $43 = 25+18$, $59 = 9+50$, $67 = 49+18$, $73 = 1+72$, $83 = 81+2$, $89 = 81+8$, $97 = 25+72$, etc.

Aquest teorema, com molts de similars, també era conegut per Fermat, però l'il·lm. La Grange en donà el primer una demostració, *Suite des recherches d'Arithmetique, Nouv. Mem. de l'Ac. de Berlin* 1775*, p.* 323 *s.* Moltes [proposicions] pertanyents al mateix argument ja les havia acabades l'il·lm. Euler, *Specimen de usu obseruationum in mathesi pura, Comm. nou. Petr. T. IV p.* 185 *i s.* Però una demostració completa del teorema sempre va eludir la seva diligència, p. 220. Compareu també la dissertació en el T. VIII (anys 1760, 1761), *Supplementum quorundam theorematum arithmeticorum*, al final.

III. Per un mètode similar es demostra que qualsevol nombre per al qual -3 sigui un residu quadràtic es pot representar, o bé per la forma $xx+3yy$, o bé per la $2xx+2xy+2yy$, de manera que el valor de x sigui primer

al valor de y. Per tant, com que -3 és un residu de tots els nombres primers de la forma $3n + 1$ (article 119) i, evidentment, per la forma $2xx + 2xy + 2yy$ només es poden representar nombres parells, de la mateixa manera que més amunt es té el teorema:

Qualsevol nombre primer de la forma $3n+1$ *es pot descompondre en un quadrat i el triple d'un quadrat, i, certament, només d'una manera.* $1 = 1 + 0$, $7 = 4 + 3$, $13 = 1 + 12$, $19 = 16 + 3$, $31 = 4 + 27$, $37 = 25 + 12$, $43 = 16 + 27$, $61 = 49 + 12$, $67 = 64 + 3$, $73 = 25 + 48$, etc.

L'il·lm. Euler transmeté el primer una demostració d'aquest teorema en el comentari elogiat fa un moment, *Comm. nou. Petr. T. VIII, p.* 105 *s.*

De manera similar, podríem progressar més enllà i mostrar, per exemple, que qualsevol nombre primer de la forma $20n+1$, o bé $20n+3$, o bé $20n+7$, o bé $20n+9$ (ja que -5 és residu d'aquests), es pot representar per una o altra de les formes $xx + 5yy$, $2xx + 2xy + 3yy$, i, certament, els nombres primers de la forma $20n + 1$ i $20n + 9$ per la primera, els primers de la forma $20n + 3$, $20n+7$, per la darrera, i també els dobles dels primers de la forma $20n+1$, $20n+9$, per la forma $2xx+2xy+3yy$, els dobles dels primers de la forma $20n + 3$, $20n + 7$, per la forma $xx + 5yy$; però qualsevol podrà derivar aquesta proposició, i una infinitat d'altres particulars, pels seus propis mitjans, del que precedeix i del que s'ha de transmetre més avall. Així, passem a les *formes de determinant positiu* i com que la naturalesa d'aquestes és completament una quan el determinant és quadrat, una altra quan és no quadrat, aquí excloem primer les

formes de determinant quadrat i més tard les considerarem separadament.

183. Problema. *Proposada una forma qualsevol* $(a,\ b,\ a')$ *el determinant de la qual és no quadrat positiu* $= D$, *trobar una forma* $(A,\ B,\ C)$ *pròpiament equivalent a aquesta, en la qual* B *sigui positiu i* $< \sqrt{D}$, *i* A, *si és positiu, o bé* $-A$, *si* A *és negatiu, estigui situat entre* $\sqrt{D}$ *i* $\sqrt{D} - B$.

Solució. Suposem que a la forma proposada encara no té lloc alguna de les condicions; en efecte, altrament, no seria necessari cercar cap altra forma. Observem, a més a més, que en una forma de determinant *no quadrat*, ni el primer terme ni l'últim no poden ser $= 0$ (article 171, nota). Sigui $b' \equiv -b\,(\text{mòd.}\,a')$ i situat entre els límits $\sqrt{D}$ i $\sqrt{D} \mp a'$ (agafat el signe superior quan a' és positiu, l'inferior, quan és negatiu), que es demostra fàcilment que es pot fer per una raó similar a l'article 3, i es posa $\dfrac{b'b' - D}{a'} = a''$, que serà un enter, ja que $b'b' - D \equiv bb - D \equiv aa' \equiv 0\,(\text{mòd.}\,a')$. Ara, si $a'' < a'$, resulti novament $b'' \equiv -b'\,(\text{mòd.}\,a'')$ i situat entre $\sqrt{D}$ i $\sqrt{D} \mp a''$ (segons que a'' sigui positiu o bé negatiu) i $\dfrac{b''b'' - D}{a''} = a'''$. Si, aquí, de nou, és $a''' < a''$, sigui $b''' \equiv -b''\,(\text{mòd.}\,a''')$ i situat entre $\sqrt{D}$ i $\sqrt{D} \mp a'''$, i $\dfrac{b'''b''' - D}{a'''} = a^{IV}$. Es continua aquesta operació fins que en la progressió a', a'', a''', a^{IV}, etc., s'arribi a un terme a^{m+1} no menor que el terme precedent a^m, cosa que, finalment, ha d'ocórrer, ja que, altrament, es tindria una progressió infinita de nombres enters contínuament decreixents. Llavors, posats $a^m = A$, $b^m = B$,

$a^{m+1} = C$, la forma $(A,\ B,\ C)$ satisfarà totes les condicions.

Dem. I. Com que a la progressió de formes $(a,\ b,\ a')$, $(a',\ b',\ a'')$, $(a'',\ b'',\ a''')$, etc., qualsevol és contigua a la precedent, l'última, $(A,\ B,\ C)$, serà pròpiament equivalent a la primera, $(a,\ b,\ a')$.

II. Com que B està situat entre $\sqrt{D}$ i $\sqrt{D} \mp A$ (agafant sempre el signe superior quan A és positiu, l'inferior quan A és negatiu), és clar que, si es posa $\sqrt{D} - B = p$, $B - (\sqrt{D} \mp A) = q$, els p, q, seran positius. Ara, es confirma fàcilment que serà $qq + 2pq + 2p\sqrt{D} = D + AA - BB$; per tant, $D + AA - BB$ serà un nombre positiu, que posarem $= r$. D'aquí, a causa que $D = BB - AC$, resulta $r = AA - AC$, de manera que $AA - AC$ és un nombre positiu; però, com que, per hipòtesi, A no és més gran que C, evidentment allò només pot resultar de manera diferent si AC és negatiu, de manera que els signes de A, C, oposats. D'aquí, $BB = D + AC < D$, de manera que $B < \sqrt{D}$.

III. A més a més, com que $-AC = D - BB$, serà $AC < D$, i, d'aquí (ja que A no és $< C$), $A < \sqrt{D}$. Per tant, $\sqrt{D} \mp A$ serà positiu, de manera que, també, B, que està situat entre els límits $\sqrt{D}$ i $\sqrt{D} \mp A$.

IV. D'aquí, amb més raó, $\sqrt{D} + B \mp A$ és positiu i, com que $\sqrt{D} - B \mp A = -q$ és negatiu, $\pm A$ estarà situat entre $\sqrt{D} + B$ i $\sqrt{D} - B$. *Q. E. D.*

Exemple. Sigui proposada la forma (67, 97, 140), el determinant de la qual és = 29. Aquí es troba la progressió de formes (67, 97, 140), (140, −97, 67), (67,

$-37,\ 20)$, $(20,\ -3,\ -1)$, $(-1,\ 5,\ 4)$. L'última serà la buscada.

Anomenaren *formes reduïdes* les tals formes $(A,\ B,\ C)$, de determinant positiu no quadrat D, en què A, agafat positivament, està situat entre $\sqrt{D}+B$ i $\sqrt{D}-B$, però B és positiu i $< \sqrt{D}$. Així, les formes reduïdes de determinant positiu no quadrat difereixen un xic de les formes reduïdes de determinant negatiu; però, a causa de la gran analogia entre aquestes i aquelles, no hem volgut introduir denominacions diferents.

184. Si l'equivalència de dues formes *reduïdes* de determinant positiu es pogués discernir de manera igualment fàcil que per a les formes de determinant negatiu (article 172), podríem decidir sense cap dificultat l'equivalència de dues formes *qualssevol* del mateix determinant positiu. Però aquí això es té de manera molt diferent, i pot resultar que moltes formes reduïdes siguin equivalents entre si. Així, abans que ataquem aquest problema, serà necessari inquirir més profundament en la natura de les formes reduïdes (de determinant positiu no quadrat, cosa que aquí cal entendre sempre).

1) Si $(a,\ b,\ c)$ és una forma reduïda, a i c tindran signes oposats. Efectivament, posat el determinant de la forma $= D$, serà $ac = bb - D$, de manera que negatiu, a causa que $b < \sqrt{D}$.

2) El nombre c, i igualment a agafat positivament, estarà situat entre $\sqrt{D} + b$ i $\sqrt{D} - b$. Efectivament, $-c = \dfrac{D - bb}{a}$; per tant, feta abstracció del signe, c estarà entre $\dfrac{D - bb}{\sqrt{D} + b}$ i $\dfrac{D - bb}{\sqrt{D} - b}$; és a dir, entre $\sqrt{D} - b$ i $\sqrt{D} + b$.

3) D'aquí és clar que $(c,\ b,\ a)$ també serà una forma reduïda.

4) Tant a com c seran $< 2\sqrt{D}$. En efecte, cadascun d'ells és $< \sqrt{D}+b$, de manera que, amb més raó, $< 2\sqrt{D}$.

5) El nombre b estarà situat entre $\sqrt{D}$ i $\sqrt{D} \mp a$ (agafat el signe superior quan a és positiu, l'inferior, si és negatiu). En efecte, com que $\pm a$ està entre $\sqrt{D}+b$ i $\sqrt{D}-b$, $\pm a-(\sqrt{D}-b)$, o sigui, $b-(\sqrt{D}\mp a)$, serà positiu; però $b-\sqrt{D}$ és negatiu; per la qual cosa, b estarà situat entre $\sqrt{D}$ i $\sqrt{D} \mp a$. Es demostra completament de la mateixa manera que b està entre $\sqrt{D}$ i $\sqrt{D} \mp c$ (segons que c sigui positiu o bé negatiu).

6) *Per a qualsevol forma reduïda* $(a,\ b,\ c)$ *n'hi ha una de reduïda contigua a ella per les dues parts, i no més.*

Si resulta $a' = c$, $b' \equiv -b\,(\text{mòd. } a')$ i situat entre $\sqrt{D}$ i $\sqrt{D} \mp a'$,* i $c' = \dfrac{b'b' - D}{a'}$, la forma $(a',\ b',\ c')$ serà contigua per l'última part a la forma $(a,\ b,\ c)$, i és evident, simultàniament, que si es donés alguna forma reduïda contigua per l'última part a la forma $(a,\ b,\ c)$, aquella no pot ser diferent de la $(a',\ b',\ c')$. Però que aquesta és vertaderament reduïda ho demostrem així.

A) Si es posa $\sqrt{D}+b\mp a' = p$, $\pm a'-(\sqrt{D}-b) = q$, $\sqrt{D}-b = r$, de 2), més amunt, i de la definició de forma reduïda, els p, q, r, seran positius. A més a més, es posa $b'-(\sqrt{D}\mp a') = q'$, $\sqrt{D}-b' = r'$, i q', r', seran positius,

* On hi ha signes ambigus, sempre valen els superiors quan a' és positiu, els inferiors, quan a' és negatiu.

ja que b' està situat entre $\sqrt{D}$ i $\sqrt{D} \mp a'$. Finalment, sigui $b + b' = \pm ma'$, i m serà un enter. Ara, és clar que és $p + q' = b + b'$, de manera que $b + b'$, o sigui, $\pm ma'$, és positiu i, en conseqüència, també m; d'on se segueix que $m - 1$ no és, certament, negatiu. A més a més, resulta $r + q' \pm ma' = 2b' \pm a'$, o sigui, $2b' = r + q' \pm (m-1)a'$, d'on $2b'$ i b' seran necessàriament positius. I, com que $b' + r' = \sqrt{D}$, serà $b' < \sqrt{D}$.

B) A més a més, resulta que $r \pm ma' = \sqrt{D} + b'$, o sigui, $r \pm (m-1)a' = \sqrt{D} + b' \mp a'$; per tant, $\sqrt{D} + b' \mp a'$ serà positiu. D'aquí, i com que $\pm a' - (\sqrt{D} - b') = q'$, de manera que positiu, $\pm a'$ estarà situat entre $\sqrt{D} + b'$ i $\sqrt{D} - b'$. En conseqüència, $(a',\ b',\ c')$ serà una forma reduïda.

Es demostra de la mateixa manera que, si resulta $'c = a$, $'b \equiv -b\,(\text{mòd.}\,'c)$ i situat entre $\sqrt{D}$ i $\sqrt{D} \pm' c$, i $'a = \dfrac{'b'b - D}{'c}$, la forma $('a,\ 'b,\ 'c)$ serà reduïda. Però, evidentment, aquesta forma és contigua per la primera part a la forma $(a,\ b,\ c)$, i cap altra reduïda excepte $('a,\ 'b,\ 'c)$ no podrà estar dotada d'aquesta propietat.

Exemple. La forma reduïda $(5,\ 11,\ -14)$, el determinant de la qual és $= 191$, és contigua per l'última part a la reduïda $(-14,\ 3,\ 13)$, però per la primera part a la $(-22,\ 9,\ 5)$.

7) Si a la forma reduïda $(a,\ b,\ c)$, la reduïda $(a',\ b',\ c')$ li és contigua per l'última part, la forma $(c',\ b',\ a')$ serà contigua per la primera part a la reduïda $(c,\ b,\ a)$; i si la forma $('a,\ 'b,\ 'c)$ és contigua per la primera part a la reduïda $(a,\ b,\ c)$, la reduïda $('c,\ 'b,\ 'a)$ serà contigua

per l'última part a la reduïda (c, b, a). A més a més, les formes $(-'a, 'b, -'c)$, $(-a, b, -c)$, $(-a', b', -c')$, també seran reduïdes i la segona serà contigua a la primera, i la tercera a la segona per l'última part; o sigui, la primera a la segona, i la segona a la tercera, per la primera part; i, similarment, per a les tres formes $(-c', b', -a')$, $(-c, b, -a)$, $(-'c, 'b, -'a)$. Aquestes [proposicions] són tan òbvies que no necessiten explicació.

185. La quantitat de totes les formes reduïdes de determinant donat D sempre és finita, i aquestes es poden trobar de dues maneres. Designem formalment totes les formes reduïdes de determinant D per (a, b, c) de manera que convé determinar tots els valors de a, b, c.

Primer mètode. S'agafen per a a tots els nombres (tant positius com negatius) menors que $2\sqrt{D}$ dels quals D és residu quadràtic; per a cada a, es posa b igual a tots els valors positius de l'expressió $\sqrt{D}\,(\text{mòd.}\,a)$ que estan situats entre $\sqrt{D}$ i $\sqrt{D}\mp a$; però c, per a cadascun dels valors determinats de a, b, es posa $= \dfrac{bb-D}{a}$. Si d'aquesta manera s'originen formes en les quals $\pm a$ està situat fora de $\sqrt{D}+b$, $\sqrt{D}-b$, s'han de rebutjar.

Segon mètode. S'agafen per a b tots els nombres positius menors que $\sqrt{D}$; per a cada b, es descompon $bb-D$ de totes les maneres en què es pugui fer en parells de factors que, negligit el signe, estiguin situats entre $\sqrt{D}+b$ i $\sqrt{D}-b$, i es posa l'un $= a$, l'altre $= c$. És evident que cada una de les descomposicions en factors ocasiona dues formes, ja que cada factor s'ha de posar tant $= a$ com $= c$.

Exemple. Sigui $D = 79$, i els valors de a seran vint-i-dos, ± 1, 2, 3, 5, 6, 7, 9, 10, 13, 14, 15. D'on es troben dinou formes: (1, 8, −15), (2, 7, −15), (3, 8, −5), (3, 7, −10), (5, 8, −3), (5, 7, −6), (6, 7, −5), (6, 5, −9), (7, 4, −9), (7, 3, −10), (9, 5, −6), (9, 4, −7), (10, 7, −3), (10, 3, −7), (13, 1, −6), (14, 3, −5), (15, 8, −1), (15, 7, −2), (15, 2, −5), i unes altres tantes que resulten d'aquestes si es canvien els signes dels termes exteriors, posem (−1, 8, 15), (−2, 7, 15), etc., de manera que totes són trenta-vuit. Però, d'aquestes, s'han de rebutjar les sis ($\pm$13, 1, $\mp$6), ($\pm$14, 3, $\mp$5), ($\pm$15, 2, $\mp$5); les restants trenta-dues comprenen totes les reduïdes. Pel segon mètode apareixen les mateixes formes en l'ordre següent:* ($\pm$7, 3, $\mp$10), ($\pm$10, 3, $\mp$7), ($\pm$7, 4, $\mp$9), ($\pm$9, 4, $\mp$7), ($\pm$6, 5, $\mp$9), ($\pm$9, 5, $\mp$6), ($\pm$2, 7, $\mp$15), ($\pm$3, 7, $\mp$10), ($\pm$5, 7, $\mp$6), ($\pm$6, 7, $\mp$5), ($\pm$10, 7, $\mp$3), ($\pm$15, 7, $\mp$2), ($\pm$1, 8, $\mp$15), ($\pm$3, 8, $\mp$5), ($\pm$5, 8, $\mp$3), ($\pm$15, 8, $\mp$1).

186. Sigui F una forma reduïda de determinant D, i F' una forma reduïda contigua per l'última part a ella; de nou, F'' una reduïda contigua per l'última part a aquesta, F''' una reduïda contigua per l'última part a F'', etc. Llavors, és clar que totes les formes F', F'', F''', etc., estan completament determinades i són pròpiament equivalents tant entre si com a la forma F. Però com que la quantitat de totes les formes reduïdes de determinant donat és finita, és evident que totes les formes en la progressió infinita F, F', F'', etc., no poden ser diferents. Suposem que F^m i F^{m+n} són idèntiques, i F^{m-1}, F^{m+n-1}, seran reduïdes, contigües per la primera part

* Per a $b = 1$, -78 no es pot trencar en dos factors que, negligit el signe, estiguin situats entre $\sqrt{79}+1$, $\sqrt{79}-1$; per tant, cal passar per alt aquest valor; i, per la mateixa raó, els valors 2 i 6.

a la mateixa forma reduïda, de manera que idèntiques; d'aquí, de la mateixa manera, F^{m-2} i F^{m+n-2}, etc., i, finalment, F i F^n seran idèntiques. Per tant, si en la progressió F, F', F'', etc., es continua suficientment enllà, finalment es retrobarà necessàriament la primera forma F; i si suposem que F^n és la primera idèntica a F, o sigui, que totes les F', F'', $\ldots$, F^{n-1}, són diferents de F, es copsa fàcilment que totes les formes F, F', F'', $\ldots$, F^{n-1}, són diferents. Anomenarem *període de la forma* F el complex d'aquestes formes. Així, doncs, si es prolonga la progressió més enllà de l'última forma del període, apareixeran de nou les mateixes formes F, F', F'', etc., i tota la progressió infinita F', F'', etc., estarà constituïda d'aquest període de la forma F repetit infinitament.

La progressió F, F', F'', etc., també es pot continuar retrocedint anteposant a la forma F una reduïda ${}'F$ que li sigui contigua per la primera part; a aquesta, de nou, una reduïda ${}''F$ que li sigui contigua per la primera part, etc. D'aquesta manera, es tindrà una progressió de formes infinita *en els dos sentits*

$$\ldots, {}'''F, {}''F, {}'F, F, F', F'', F''', \ldots$$

i es copsa fàcilment que ${}'F$ serà idèntica a F^{n-1}, ${}''F$ a F^{n-2}, etc., de manera que la progressió de la part esquerra també està constituïda pel període de la forma F repetit infinitament.

Si s'atribueixen a les formes F, F', F'', etc., ${}'F$, ${}''F$, etc., els índexs 0, 1, 2, etc., -1, -2, etc., i, en general, l'índex m a la forma F^m i l'índex $-m$ a la forma ${}^mF$, és clar que *formes qualssevol de la sèrie seran idèntiques*

o bé diferents segons que els seus índexs siguin congrus o bé incongrus segons el mòdul n.

Exemple. El període de la forma (3, 8, −5), el determinant de la qual és = 79, es troba que és (3, 8, −5), (−5, 7, 6), (6, 5, −9), (−9, 4, 7), (7, 3, −10), (−10, 7, 3). Després de l'última, apareix de nou (3, 8, −5). Així, aquí és $n = 6$.

187. Aquí, algunes observacions generals sobre aquests períodes.

1) Si les formes F, F', F'', etc.; $'F$, $''F$, $'''F$, etc., es representen per $(a,\ b,\ -a')$, $(-a',\ b',\ a'')$, $(a'',\ b'',\ -a''')$, etc.; $(-'a,\ 'b,\ a)$, $(''a,\ ''b,\ -'a)$, $(-'''a,\ '''b,\ ''a)$, etc., tots els a, a', a'', a''', etc.; $'a$, $''a$, $'''a$, etc., tindran el *mateix signe* (article 184, 1) i tots els b, b', b'', etc., $'b$, $''b$, etc., seran positius.

2) D'aquí és evident que el nombre n (la quantitat de formes de què consta el període de la forma F) sempre és *parell*. En efecte, el primer terme d'una forma qualsevol, F^m, d'aquest període tindrà, evidentment, el mateix signe que el primer terme, a, de la forma F, si m és parell, oposat si m és imparell. Per tant, com que F^n i F són idèntiques, n serà necessàriament parell.

3) De l'article 184, 6, l'algoritme pel qual es troben els nombres b', b'', b''', etc.; a'', a''', etc., és aquest:

	entre els límits $\sqrt{D}$ i	
$b' \equiv -b\,(\text{mòd. } a')$	$\sqrt{D} \mp a'$	$a'' = \dfrac{D - b'b'}{a'}$
$b'' \equiv -b'\,(\text{mòd. } a'')$	$\sqrt{D} \mp a''$	$a''' = \dfrac{D - b''b''}{a''}$

$$b''' \equiv -b'' \,(\text{mòd. } a''') \qquad \sqrt{D} \mp a''' \qquad a^{IV} = \frac{D - b'''b'''}{a'''}$$

etc.,

on, a la segona columna, s'ha d'agafar el signe superior o bé l'inferior, segons que a, a', a'' etc., siguin positius o bé negatius. En lloc de les fórmules de la tercera columna, també es poden utilitzar les següents, que són més còmodes quan D és un nombre gran:

$$a'' = \frac{b + b'}{a'}(b - b') + a,$$
$$a''' = \frac{b' + b''}{a''}(b' - b'') + a',$$
$$a^{IV} = \frac{b'' + b'''}{a'''}(b'' - b''') + a'', \text{ etc.}$$

4) Qualsevol forma F^m continguda en el període de la forma F té pròpiament el mateix període que F. Això és, el període d'aquella serà F^m, F^{m+1}, ... , F^{n-1}, F, F', ..., F^{m-1}, en què es recorren les mateixes i en el mateix ordre que en el període de la forma F, i que només discrepa d'aquest respecte de l'inici i el final.

5) D'aquí, és clar que totes les formes reduïdes del mateix determinant D es poden *distribuir* en períodes. S'agafa alguna d'aquestes formes, F, a voluntat, i s'investiga el seu període F, F', F'', ..., F^{n-1}, que designarem per P. Si aquest encara no contingués totes les formes reduïdes de determinant D, sigui G alguna no continguda en ell, i Q el seu període. Llavors, és clar que P i Q no poden tenir cap forma comuna; en efecte, altrament G també hauria d'estar continguda en P i els períodes coincidirien completament. Si P i Q encara no exhaureixen totes les formes reduïdes, alguna de les que manquen, H, donarà lloc a un tercer període R que no

tindrà cap forma comuna ni amb P ni amb Q. Podrem continuar d'aquesta manera fins que totes les formes reduïdes siguin exhaurides. Així, *per exemple*, totes les formes reduïdes de determinant 79 es distribueixen en sis períodes:

I. (1, 8, −15), (−15, 7, 2), (2, 7, −15), (−15, 8, 1).

II. (−1, 8, 15), (15, 7, −2), (−2, 7, 15), (15, 8, −1).

III. (3, 8, −5), (−5, 7, 6), (6, 5, −9), (−9, 4, 7), (7, 3, −10), (−10, 7, 3).

IV. (−3, 8, 5), (5, 7, −6), (−6, 5, 9), (9, 4, −7), (−7, 3, 10), (10, 7, −3).

V. (5, 8, −3), (−3, 7, 10), (10, 3, −7), (−7, 4, 9), (9, 5, −6), (−6, 7, 5).

VI. (−5, 8, 3), (3, 7, −10) (−10, 3, 7), (7, 4, −9), (−9, 5, 6), (6, 7, −5).

6) Anomenarem *formes associades* les que consten dels mateixos termes, però posats en ordre invers, com $(a,\ b,\ -a')$, $(-a',\ b,\ a)$. Llavors, es copsa fàcilment de l'article 184, 7, que, si el període de la forma reduïda F és F, F', F'', …, F^{n-1}; si f és associada a la forma F; i si les formes f', f'', …, f^{n-1}, són associades, respectivament, a les formes F^{n-1}, F^{n-2}, …, F'', F', el període de la forma f és f, f', f'', …, f^{n-2}, f^{n-1}, de manera que consta de tantes formes com el període de la forma F. Anomenarem *períodes associats* els períodes de formes associades. Així, en el nostre exemple, els períodes III i VI, IV i V, són associats.

7) Però també pot resultar que la forma f ocorri en el període de la seva associada F, com en els períodes

I i II del nostre exemple, de manera que el període de la forma F coincideix amb el període de la forma f, o sigui, que *el període de la forma F és associat a si mateix*. Sempre que succeeixi això, es trobaran dues formes ambigües en aquest període. En efecte, suposem que el període de la forma F consta de $2n$ formes, o sigui, que F i F^{2n} són idèntiques; a més a més, sigui $2m+1$ l'índex de la forma f en el període de la forma F,* o sigui, F^{2m+1} i F associades. Llavors, és clar també que F' i F^{2m} seran associades, també F'' i F^{2m-1}, etc., de manera que també F^m i F^{m+1}. Sigui $F^m = (a^m, b^m, -a^{m+1})$, $F^{m+1} = (-a^{m+1}, b^{m+1}, a^{m+2})$. Llavors, serà $b^m + b^{m+1} \equiv 0 \,(\text{mòd.}\, a^{m+1})$; però, de la definició de formes associades, serà $b^m = b^{m+1}$ i, d'aquí, $2b^{m+1} \equiv 0 \,(\text{mòd.}\, a^{m+1})$; o sigui, la forma F^{m+1} és ambigua. De la mateixa manera, F^{2m+1} i F^{2n} seran associades; d'aquí, F^{2m+2} i F^{2n-1}; F^{2m+3} i F^{2n-2}; etc.; i, finalment, F^{m+n} i F^{m+n+1}, la darrera de les quals serà ambigua, com es prova fàcilment per un raonament similar. Però com que $m+1$ i $m+n+1$ són incongrus segons el mòdul $2n$, les formes F^{m+1} i F^{m+n+1} no seran idèntiques (article 186, on n denota el mateix que aquí $2n$). Així, en I, les formes ambigües són (1, 8, −15), (2, 7, −15); però, en II, (−1, 8, 15), (−2, 7, 15).

8) Recíprocament, *qualsevol període en què ocorri una forma ambigua és associat a si mateix*. En efecte, es copsa fàcilment que si F^m és una forma reduïda ambigua, una forma associada a ella (que també és reduïda) li és simultàniament contigua per la primera part; és a dir, F^{m-1} i F^m són associades. Però, llavors, tot

* Aquí l'índex serà necessàriament imparell, ja que, evidentment, els primers termes de les formes F, f tenen signes oposats (vegeu 2, més amunt).

el període serà associat a si mateix. D'aquí és clar que *no pot resultar que en algun període hi hagi continguda només una única forma ambigua.*

9) Però tampoc *no n'hi pot haver, en un mateix període, més de dues.* En efecte, suposem que en el període de la forma F, que consta de $2n$ formes, es donen tres formes ambigües F^λ, F^μ, F^ν, que pertanyen, respectivament, als índexs λ, μ, ν, de manera que λ, μ, ν, siguin nombres diferents situats entre els límits 0 i $2n-1$ (inclusivament). Llavors, les formes $F^{\lambda-1}$ i F^λ seran associades; i, similarment, $F^{\lambda-2}$ i $F^{\lambda+1}$, etc.; i, finalment, F i $F^{2\lambda-1}$. Per la mateixa raó, F i $F^{2\mu-1}$ seran associades, i també F i $F^{2\nu-1}$; per tant, $F^{2\lambda-1}$, $F^{2\mu-1}$, $F^{2\nu-1}$, [seran] idèntiques, i els índexs $2\lambda-1$, $2\mu-1$, $2\nu-1$, seran congrus segons el mòdul $2n$, i, en conseqüència, també $\lambda \equiv \mu \equiv \nu \,(\text{mòd.}\, n)$, *Q. E. A.*, ja que, evidentment, entre els límits 0 i $2n-1$ no poden estar situats tres nombres diferents congrus segons el mòdul n.

188. Com que totes les formes del mateix període són pròpiament equivalents, neix la qüestió de si també formes de períodes diferents poden ser pròpiament equivalents. Però abans que mostrem que *això és impossible*, cal exposar quelcom de la transformació de formes reduïdes.

Com que a continuació s'haurà de tractar molt sovint de les transformacions de formes, perquè evitem tant com es pugui una excessiva extensió, usarem sempre, a partir d'aquí, l'escriptura abreujada següent. Si alguna forma $LXX+2MXY+NYY$ es transforma en la forma $lxx+2mxy+nyy$ per la substitució $X = \alpha x+\beta y$,

$Y = \gamma x + \delta y$, direm, més simplement, que $(L,\ M,\ N)$ es transforma en $(l,\ m,\ n)$ per la susbtitució $\alpha,\ \beta,\ \gamma,\ \delta$. D'aquesta manera no serà necessari denotar amb símbols propis les indeterminades de cadascuna de les formes de què es tracta. Però és palès que en qualsevol forma s'haurà de distingir perfectament *la primera* indeterminada de *la segona*.

Sigui proposada la forma reduïda $(a,\ b,\ -a')\ \ldots\ f$, de determinant D. Es forma, de manera similar com en l'article 186, la progressió de formes reduïdes i infinita en els dos sentits, $\ldots,\ {}''f,\ {}'f,\ f,\ f',\ f'',\ \ldots$, i sigui, certament, $f' = (-a',\ b',\ a'')$, $f'' = (a'',\ b'',\ -a''')$, etc.; ${}'f = (-{}'a,\ {}'b,\ a)$, ${}''f = ({}''a,\ {}''b,\ -{}'a)$, etc. Es posa $\dfrac{b+b'}{-a'} = h'$, $\dfrac{b'+b''}{a''} = h''$, $\dfrac{b''+b'''}{-a'''} = h'''$, etc.; $\dfrac{{}'b+b}{a} = h$, $\dfrac{{}''b+{}'b}{-{}'a} = {}'h$, $\dfrac{{}'''b+{}''b}{{}''a} = {}''h$, etc. Llavors, és clar que si (com a l'article 177) els nombres α', α'', α''', etc.; β', β'', β''', etc.; etc., es formen segons l'algoritme següent:

$\alpha' = 0$, $\beta' = -1$, $\gamma' = 1$, $\delta' = h'$;
$\alpha'' = \beta'$, $\beta'' = h''\beta'$, $\gamma'' = \delta'$, $\delta'' = h''\delta' - 1$;
$\alpha''' = \beta''$, $\beta''' = h'''\beta'' - \beta'$, $\gamma''' = \delta''$, $\delta''' = h'''\delta'' - \delta'$;
$\alpha^{IV} = \beta'''$, $\beta^{IV} = h^{IV}\beta''' - \beta''$, $\gamma^{IV} = \delta'''$, $\delta^{IV} = h^{IV}\delta''' - \delta''$;
etc.,

f es transformarà

en	per la substitució
f',	$\alpha',\ \beta',\ \gamma',\ \delta'$;
f'',	$\alpha'',\ \beta'',\ \gamma'',\ \delta''$;
f''',	$\alpha''',\ \beta''',\ \gamma''',\ \delta'''$; etc.,

i totes aquestes transformacions seran pròpies.

Com que $'f$ es transforma en f per la substitució pròpia 0, -1, 1, h (article 161), f es transformarà en $'f$ per la substitució pròpia h, 1, -1, 0. Per una raó similar, $'f$ es transformarà en $''f$ per la substitució pròpia $'h$, 1, -1, 0; $''f$ en $'''f$ per la substitució pròpia $''h$, 1, -1, 0, etc. D'aquí, per l'article 159, es conclou de la mateixa manera que en l'article 177 que, si els nombres $'\alpha$, $''\alpha$, $'''\alpha$, etc.; $'\beta$, $''\beta$, $'''\beta$, etc.; etc., es formen segons l'algoritme següent:

$'\alpha = h$, $'\beta = 1$, $'\gamma = -1$, $'\delta = 0$;
$''\alpha = 'h'\alpha - 1$, $''\beta = '\alpha$, $''\gamma = 'h'\gamma$, $''\delta = '\gamma$;
$'''\alpha = ''h''\alpha - '\alpha$, $'''\beta = ''\alpha$, $'''\gamma = ''h''\gamma - '\gamma$, $'''\delta = ''\gamma$;
$^{IV}\alpha = '''h'''\alpha - ''\alpha$, $^{IV}\beta = '''\alpha$, $^{IV}\gamma = '''h'''\gamma - ''\gamma$, $^{IV}\delta = '''\gamma$;
etc.,

f es transformarà

en	per la substitució
$'f$,	$'\alpha$, $'\beta$, $'\gamma$, $'\delta$;
$''f$,	$''\alpha$, $''\beta$, $''\gamma$, $''\delta$;
$'''f$,	$'''\alpha$, $'''\beta$, $'''\gamma$, $'''\delta$; etc.,

i totes aquestes transformacions seran pròpies.

Si es posa $\alpha = 1$, $\beta = 0$, $\gamma = 0$, $\delta = 1$, aquests nombres tindran la mateixa relació amb la forma f que α', β', γ', δ', tenen amb f'; α'', β'', γ'', δ'', amb f''; etc., $'\alpha$, $'\beta$, $'\gamma$, $'\delta$, amb $'f$, etc. Això és, per la substitució α, β, γ, δ, la forma f es transformarà en f. Però, llavors, les progressions infinites α', α'', α''', etc.; $'\alpha$, $''\alpha$, $'''\alpha$, etc., s'uneixen apropiadament, intercalant el terme α, de manera que es pot concebre que en constitueixen una sola contínua, infinita per les dues bandes, segons la mateixa llei, i que progressa $\ldots$, $'''\alpha$, $''\alpha$, $'\alpha$, α, α', α'',

α''', ... La llei de progressió és aquesta: $'''\alpha + ''\alpha = ''h''\alpha$, $''\alpha + \alpha = 'h'\alpha$, $'\alpha + \alpha' = h\alpha$, $\alpha + \alpha'' = h'\alpha'$, $\alpha' + \alpha''' = h''\alpha''$, etc., o sigui, generalment (si suposem que un índex negatiu escrit a la dreta indica el mateix que un positiu a l'esquerra), $\alpha^{m-1} + \alpha^{m+1} = h^m\alpha^m$. De manera similar, la progressió ..., $''\beta$, $'\beta$, β, β', β'', ..., serà contínua, la seva llei, $\beta^{m-1} + \beta^{m+1} = h^{m+1}\beta^m$, i pròpiament idèntica amb la precedent, avançats tots els termes un lloc, $''\beta = '\alpha$, $'\beta = \alpha$, $\beta = \alpha'$, etc. La llei de la progressió contínua ..., $''\gamma$, $'\gamma$, γ, γ', γ'', ... serà $\gamma^{m-1} + \gamma^{m+1} = h^m\gamma^m$, i la llei de ..., $''\delta$, $'\delta$, δ, δ', δ'', ... serà $\delta^{m-1} + \delta^{m+1} = h^{m+1}\delta^m$, i, a sobre, en general, $\delta^m = \gamma^{m+1}$.

Exemple. Sigui f, la forma proposada, (3, 8, −5), que es transformarà

	en la forma	per la substitució			
^{VII}f	$(-10, 7, 3)$	-805,	-152,	$+143$,	$+27$
^{VI}f	$(3, 8, -5)$	-152,	$+45$,	$+27$,	-8
^{V}f	$(-5, 7, 6)$	$+45$,	$+17$,	-8,	-3
^{IV}f	$(6, 5, -9)$	$+17$,	-11,	-3,	$+2$
$'''f$	$(-9, 4, 7)$	-11,	-6,	$+2$,	$+1$
$''f$	$(7, 3, -10)$	-6,	$+5$,	$+1$,	-1
$'f$	$(-10, 7, 3)$	$+5$,	$+1$,	-1,	0
f	$(3, 8, -5)$	$+1$,	0,	0,	$+1$
f'	$(-5, 7, 6)$	0,	-1,	$+1$,	-3
f''	$(6, 5, -9)$	-1,	-2,	-3,	-7
f'''	$(-9, 4, 7)$	-2,	$+3$,	-7,	$+10$
f^{IV}	$(7, 3, -10)$	$+3$,	$+5$,	$+10$,	$+17$
f^{V}	$(-10, 7, 3)$	$+5$,	-8,	$+17$,	-27
f^{VI}	$(3, 8, -5)$	-8,	-45,	-27,	-152
f^{VII}	$(-5, 7, 6)$	-45,	$+143$,	-152,	$+483$

etc.

189. Amb relació a aquest algoritme, cal observar les [proposicions] següents.

1) Tots els a, a', a'', etc.; $'a$, $''a$, etc., tindran el mateix signe; tots els b, b', b'', etc.; $'b$, $''b$, etc., seran positius; a la progressió $\ldots$, $''h$, $'h$, h, h', h'', $\ldots$, els signes s'alternaran, això és, si tots els a, a', etc., són positius, h^m o bé ${}^m h$ serà positiu quan m és parell, negatiu quan m és imparell; però si a, a', etc., són negatius, h^m o bé ${}^m h$ serà negatiu per a m parell, positiu per a m imparell.

2) Si a és positiu, de manera que h' negatiu, h'' positiu, etc., serà $\alpha'' = -1$, negatiu, $\alpha''' = h''\alpha''$, negatiu i $> \alpha''$ (o bé $= \alpha''$ si $h'' = 1$); $\alpha^{IV} = h'''\alpha''' - \alpha''$, positiu i $> \alpha'''$ (ja que $h'''\alpha'''$ és positiu, α'' negatiu); $\alpha^{V} = h^{IV}\alpha^{IV} - \alpha'''$, positiu i $> \alpha^{IV}$ (ja que $h^{IV}\alpha^{IV}$ és positiu), etc. D'aquí es conclou fàcilment que la progressió α', α'', α''', etc., creix a l'infinit i que sempre s'alternen dos signes positius i dos negatius, de manera que α^m tingui signes $+$, $+$, $-$, $-$, segons que $m \equiv 0$, 1, 2, 3 (mòd. 4). Si a és negatiu, per un raonament similar es troba α'' negatiu, α''' positiu i, o bé $>$, o bé $= \alpha''$; α^{IV} positiu $> \alpha'''$; α^{V} negatiu $> \alpha^{IV}$, etc., de manera que la progressió α', α'', α''', etc., creixi contínuament, i el signe del terme α^m sigui $+$, $-$, $-$, $+$, segons que $m \equiv 0$, 1, 2, 3 (mòd. 4).

3) D'aquesta manera, es troba que totes quatre progressions infinites α', α'', α''', etc.; γ, γ', γ'', etc.; α', α, $'\alpha$, $''\alpha$, etc.; γ, $'\gamma$, $''\gamma$, etc., creixen contínuament, de manera que també les següents, idèntiques a elles, β, β', β'', etc.; $'\delta$, δ, δ', δ'', etc.; β, $'\beta$, $''\beta$, etc.; $'\delta$, $''\delta$, etc.; i, segons que $m \equiv 0$, 1, 2, 3 (mòd. 4), el signe de α^m és

$+$, $\pm$, $-$, $\mp$; el de β^m, $\pm$, $-$, $\mp$, $+$; el de γ^m, $\pm$, $+$, $\mp$, $-$; el de δ^m, $+$, $\mp$, $-$, $\pm$; el de ${}^m\alpha$, $+$, $\pm$, $-$, $\mp$; el de ${}^m\beta$, $\mp$, $+$, $\pm$, $-$; el de ${}^m\gamma$, $\mp$, $-$, $\pm$, $+$; el de ${}^m\delta$, $+$, $\mp$, $-$, $\pm$, on valen els superiors quan a és positiu, els inferiors quan a és negatiu. En primer lloc, es té aquesta propietat: Si m designa un índex positiu qualsevol, α^m i γ^m tindran el mateix signe quan a és positiu, oposat quan a és negatiu, i, similarment, β^m, i, contràriament, δ^m; ${}^m\alpha$ i ${}^m\gamma$, o bé ${}^m\beta$ i ${}^m\delta$, tindran el mateix signe quan a és negatiu, oposat quan a és positiu.

4) Amb les notacions de l'article 32, la magnitud dels α^m, etc., es pot mostrar elegantment així: posant $\mp h' = k'$, $\pm h'' = k''$, $\mp h''' = k'''$, etc., $\pm h = k$, $\mp' h = {}'k$, $\pm'' h = {}''k$, etc., de manera que tots els k', k'', etc.; k, ${}'k$, etc., siguin nombres positius, $\alpha^m = \pm[k'', k''', k^{IV}, \ldots, k^{m-1}]$; $\beta^m = \pm[k'', k''', k^{IV}, \ldots, k^m]$; $\gamma^m = \pm[k', k'', k''', \ldots, k^{m-1}]$; $\delta^m = \pm[k', k'', k''', \ldots, k^m]$; ${}^m\alpha = \pm[k, {}'k, {}''k, \ldots, {}^{m-1}k]$; ${}^m\beta = \pm[k, {}'k, {}''k, \ldots, {}^{m-2}k]$; ${}^m\gamma = \pm[{}'k, {}''k, {}'''k, \ldots, {}^{m-1}k]$; ${}^m\delta = \pm[{}'k, {}''k, {}'''k, \ldots, {}^{m-2}k]$; però els *signes* s'han de determinar segons els preceptes transmesos fa un moment. Segons aquestes fórmules, de les quals ometem la demostració per la seva facilitat, sempre es podrà acabar el càlcul rapidíssimament.

190. Lema. *Si es designen per m, μ, m', n, ν, n', nombres enters qualssevol, però de manera que cap dels tres darrers no sigui $= 0$, afirmo que si $\frac{\mu}{\nu}$ està situat entre els límits $\frac{m}{n}$ i $\frac{m'}{n'}$, exclusivament, i és $mn' - nm' = \mp 1$, el denominador ν serà més gran que n i n'.*

Dem. Evidentment, $\mu nn'$ estarà situat entre $\nu mn'$ i $\nu nm'$, de manera que difereix menys de cadascun d'aquests límits que un límit de l'altre; és a dir, serà $\nu mn' - \nu nm' > \mu nn' - \nu mn'$ i $> \mu nn' - \nu nm'$, o sigui, $\nu > n'(\mu n - \nu m)$ i $> n(\mu n' - \nu m')$. D'aquí se segueix que, com que, certament, $\mu m - \nu n$ no és $= 0$ (en efecte, altrament seria $\frac{\mu}{\nu} = \frac{m}{n}$, contràriament a la hipòtesi), ni $\mu n' - \nu m' = 0$ (per una raó similar), sinó que cadascuna és, com a mínim, $= 1$, serà $\nu > n'$ i $> n$. *Q. E. D.*

Així, es copsa que ν no pot ser $= 1$; és a dir, si fos $mn' - nm' = \pm 1$, entre les fraccions $\frac{m}{n}$ i $\frac{m'}{n'}$ no podria estar-hi situat cap nombre enter. Per tant, tampoc el zero no pot estar situat entre elles, és a dir, aquestes fraccions no poden tenir signes oposats.

191. Teorema. *Si la forma reduïda* $(a,\ b,\ -a')$ *de determinant* D *es transforma en la reduïda* $(A,\ B,\ -A')$ *del mateix determinant per la substitució* $\alpha,\ \beta,\ \gamma,\ \delta$, primer, $\frac{\pm\sqrt{D} - b}{a}$ *estarà situat entre* $\frac{\alpha}{\gamma}$ *i* $\frac{\beta}{\delta}$ *(suposat que ni* γ *ni* $\delta = 0$*, és a dir, si cada un dels límits és finit), agafat el signe superior quan cap d'aquests límits no té signe oposat al signe de* a *(o sigui, més clarament, quan o bé tots dos tenen el mateix, o bé l'un el mateix i l'altre és* $= 0$*), l'inferior quan cap no té el mateix que* a; segon, $\frac{\pm\sqrt{D} + b}{a'}$, *entre* $\frac{\gamma}{\alpha}$ *i* $\frac{\delta}{\beta}$ *(suposat que ni* α *ni* $\beta = 0$*), agafat el signe superior quan cap dels límits no té signe oposat al signe de* a' *(o bé* a*), l'inferior quan cap no té el mateix que* a'.*

* És evident que no poden tenir lloc altres casos, ja que, de

Dem. Es tenen les equacions $a\alpha\alpha + 2b\alpha\gamma - a'\gamma\gamma = A$ ...[1]; $a\beta\beta + 2b\beta\delta - a'\delta\delta = -A'$ ...[2]. D'on es dedueix

$$\frac{\alpha}{\gamma} = \frac{\pm\sqrt{D + \frac{aA}{\gamma\gamma}} - b}{a}, \qquad [3]$$

$$\frac{\beta}{\delta} = \frac{\pm\sqrt{D - \frac{aA'}{\delta\delta}} - b}{a}, \qquad [4]$$

$$\frac{\gamma}{\alpha} = \frac{\pm\sqrt{D - \frac{a'A}{\alpha\alpha}} + b}{a'}, \qquad [5]$$

$$\frac{\delta}{\beta} = \frac{\pm\sqrt{D + \frac{a'A'}{\beta\beta}} + b}{a'}. \qquad [6]$$

L'equació 3, 4, 5, 6 s'haurà de rebutjar si γ, δ, α, β, són, respectivament, $= 0$. Però aquí resta un dubte: quins *signes* s'han d'atribuir a les quantitats radicals?; decidirem això de la manera següent.

És clar immediatament que en [3] i [4] s'han d'agafar necessàriament els signes superiors quan ni $\frac{\alpha}{\gamma}$ ni $\frac{\beta}{\delta}$ no tingui signe oposat al signe de a, ja que, agafat el signe inferior, $\frac{a\alpha}{\gamma}$, $\frac{a\beta}{\delta}$, resultarien quantitats negatives. Però, com que A i A' tenen els mateixos signes, $\sqrt{D}$ cau

---

l'article precedent, a causa que $\alpha\delta - \beta\gamma = \pm 1$, tots dos límits no poden tenir signes oposats ni poden ser simultàniament $= 0$.

entre $\sqrt{D + \frac{aA}{\gamma\gamma}}$ i $\sqrt{D - \frac{aA'}{\delta\delta}}$, de manera que, en aquest cas, $\frac{\sqrt{D} - b}{a}$, entre $\frac{\alpha}{\gamma}$ i $\frac{\beta}{\delta}$. Per tant, la primera part del teorema està demostrada per al primer cas.

De la mateixa manera, es copsa que en [5] i [6] s'han d'agafar necessàriament els signes inferiors quan ni $\frac{\gamma}{\alpha}$ ni $\frac{\delta}{\beta}$ no tinguin el mateix signe que a', o sigui, a, ja que, agafat el superior, $\frac{a'\gamma}{\alpha}$, $\frac{a'\delta}{\beta}$, resultarien necessàriament quantitats positives. D'on se segueix directament que, per a aquest cas, $\frac{-\sqrt{D} + b}{a'}$ està situat entre $\frac{\gamma}{\alpha}$ i $\frac{\delta}{\beta}$. Així, la segona part del teorema també està demostrada per al darrer cas. Si es pogués mostrar de manera igualment fàcil que en [3] i [4] s'han d'agafar els signes inferiors quan cap de les quantitats $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$, no tingui el mateix signe que a, i en [5] i [6] els superiors, quan $\frac{\gamma}{\alpha}$ i $\frac{\delta}{\beta}$ no tinguin signes oposats, d'aquí, de manera similar, se seguiria, per a aquell cas, que $\frac{-\sqrt{D} - b}{a}$ està situat entre $\frac{\alpha}{\gamma}$ i $\frac{\beta}{\delta}$, per a aquest, que $\frac{\sqrt{D} + b}{a'}$ entre $\frac{\gamma}{\alpha}$ i $\frac{\delta}{\beta}$; o sigui, també estarien demostrades la primera part del teorema per al darrer cas, i la segona per al primer cas. Però com que allò, que no és certament difícil, no es podria fer no obstant això sense certs circumloquis, preferim el mètode següent.

Quan cap dels nombres α, β, γ, δ, no és $= 0$, $\frac{\alpha}{\gamma}$ i $\frac{\beta}{\delta}$ tindran el mateix signe que $\frac{\gamma}{\alpha}$, $\frac{\delta}{\beta}$. Així, quan cap d'aquestes quantitats no té el mateix signe que a', o sigui, a, de manera que $\frac{-\sqrt{D}+b}{a'}$ cau entre $\frac{\gamma}{\alpha}$ i $\frac{\delta}{\beta}$, cap de les quantitats $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$, no tindrà el mateix signe que a, i $\frac{a'}{-\sqrt{D}+b} = \frac{-\sqrt{D}-b}{a}$ (a causa que $aa' = D - bb$) caurà entre $\frac{\alpha}{\gamma}$ i $\frac{\beta}{\delta}$. Per tant, per al cas en què ni α ni β no és $= 0$, la primera part del teorema també està demostrada per al segon cas (efectivament, la condició que ni γ ni $\delta = 0$ ja està afegida en el mateix teorema). De manera similar, quan cap dels nombres α, β, γ, δ, no és $= 0$, i ni $\frac{\alpha}{\gamma}$ ni $\frac{\beta}{\delta}$ no té signe oposat al signe de a o bé a', de manera que $\frac{\sqrt{D}-b}{a}$ està situat entre $\frac{\alpha}{\gamma}$ i $\frac{\beta}{\delta}$, ni $\frac{\gamma}{\alpha}$ ni $\frac{\delta}{\beta}$ tampoc no tindrà signe oposat al signe de a' i $\frac{a}{\sqrt{D}-b} = \frac{\sqrt{D}+b}{a'}$ caurà entre $\frac{\gamma}{\alpha}$ i $\frac{\delta}{\beta}$. Així, doncs, en el cas en què ni γ ni δ no és $= 0$, la segona part del teorema també està demostrada per al segon cas.

Així, només restaria per demostrar que la primera part del teorema també té lloc per al segon cas quan algun dels nombres α, β sigui $= 0$, i la segona part per al primer cas si o bé γ o bé $\delta = 0$. Però *tots aquests casos són impossibles*. En efecte, per a la *primera* part del

teorema, suposem que ni γ ni δ no és $= 0$, que $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$, no tenen el mateix signe que a, i que és 1) $\alpha = 0$. Llavors, de l'equació $\alpha\delta - \beta\gamma = \pm 1$ resulta $\beta = \pm 1$, $\gamma = \pm 1$. D'aquí, per [1], $A = -a'$; per tant, A i a', de manera que també a i A', tenen signes oposats, d'on resulta $\sqrt{D - \frac{aA'}{\delta\delta}} > \sqrt{D} > b$. D'aquí, és clar que en [4] s'ha d'agafar necessàriament el signe inferior, ja que, agafat el superior, $\frac{\beta}{\delta}$ obtindria, evidentment, el mateix signe que a. Així, resulta $\frac{\beta}{\delta} > \frac{-\sqrt{D} - b}{a} > 1$ (a causa que $a < \sqrt{D} + b$, per la definició de forma reduïda), *Q. E. A.*, ja que $\beta = \pm 1$ i δ no $= 0$. 2) Sigui $\beta = 0$. Llavors, de l'equació $\alpha\delta - \beta\gamma = \pm 1$, resulta $\alpha = \pm 1$, $\delta = \pm 1$. D'aquí, per [2], $-A' = -a'$; per tant, a', a i A tindran els mateixos signes, d'on resulta $\sqrt{D + \frac{aA}{\alpha\alpha}} > \sqrt{D} > b$. D'aquí és clar que en [3] s'ha d'agafar el signe inferior, ja que, agafat el superior, $\frac{\alpha}{\gamma}$ obtindria el mateix signe que a. Així, resulta $\frac{\alpha}{\gamma} > \frac{-\sqrt{D} - b}{a} > 1$, *Q. E. A.* per la mateixa raó que abans. Per a la *segona* part, si suposem que ni α ni β no és $= 0$, que $\frac{\gamma}{\alpha}$, $\frac{\delta}{\beta}$, no tenen signes oposats al signe de a', i que 1) $\gamma = 0$, de l'equació $\alpha\delta - \beta\gamma = \pm 1$ resulta $\alpha = \pm 1$, $\delta = \pm 1$. D'aquí, per [1], $A = a$, per tant, a' i A' tindran els mateixos signes, d'on resulta que $\sqrt{\frac{D + a'A'}{\beta\beta}} > \sqrt{D} > b$. En conseqüència, en [6] s'haurà d'agafar el signe superior, ja que, agafat l'inferior, $\frac{\delta}{\beta}$ obtindria el signe oposat al

signe de a'. Així, doncs, resulta $\frac{\delta}{\beta} > \frac{\sqrt{D}+b}{a'} > 1$, *Q. E. A.*, ja que $\delta = \pm 1$ i β no és $= 0$. Finalment 2), si fos $\delta = 0$, de $\alpha\delta - \beta\gamma = \pm 1$ resulta $\beta = \pm 1$, $\gamma = \pm 1$, de manera que, per [2], $-A' = a$. D'aquí, $\sqrt{D - \frac{a'A}{\alpha\alpha}} > \sqrt{D} > b$; per tant, en [5] s'ha d'agafar el signe superior. D'aquí, $\frac{\gamma}{\alpha} > \frac{\sqrt{D}+b}{a'} > 1$, *Q. E. A.* Per tant, el teorema està demostrat en tota la seva extensió.

Com que la diferència entre $\frac{\alpha}{\gamma}$ i $\frac{\beta}{\delta}$ és $= \frac{1}{\gamma\delta}$, la diferència entre $\frac{\pm\sqrt{D}-b}{a}$ i $\frac{\alpha}{\gamma}$, o bé $\frac{\beta}{\delta}$, serà $< \frac{1}{\gamma\delta}$; però entre $\frac{\pm\sqrt{D}-b}{a}$ i $\frac{\alpha}{\gamma}$, o bé entre aquella quantitat i $\frac{\beta}{\delta}$, no podrà estar situada cap fracció el denominador de la qual no sigui més gran que γ o bé δ (*lema precedent*). De la mateixa manera, la diferència entre la quantitat $\frac{\pm\sqrt{D}+b}{a}$ i la fracció $\frac{\gamma}{\alpha}$, o bé $\frac{\delta}{\beta}$, serà menor que $\frac{1}{\alpha\beta}$, i entre aquella quantitat i cap d'aquestes fraccions no pot estar situada cap fracció el denominador de la qual no sigui més gran que α i β.

192. De l'aplicació del teorema precedent a l'algoritme de l'article 188, se segueix que la quantitat, que designarem per L, $\frac{\sqrt{D}-b}{a}$ està situada entre $\frac{\alpha'}{\gamma'}$ i $\frac{\beta'}{\delta'}$; entre $\frac{\alpha''}{\gamma''}$ i $\frac{\beta''}{\delta''}$; entre $\frac{\alpha'''}{\gamma'''}$ i $\frac{\beta'''}{\delta'''}$, etc. (en efecte, es dedueix fàcilment de l'article 189, 3, final, que cap d'aquests

límits no té signe oposat al signe de a; per tant, s'ha d'atribuir el signe positiu a la quantitat radical $\sqrt{D}$), o sigui, entre $\frac{\alpha'}{\gamma'}$ i $\frac{\alpha''}{\gamma''}$; entre $\frac{\alpha''}{\gamma''}$ i $\frac{\alpha'''}{\gamma'''}$, etc. Així, totes les fraccions $\frac{\alpha'}{\gamma'}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha^V}{\gamma^V}$, etc., estaran situades a la mateixa banda de L i totes les $\frac{\alpha''}{\gamma''}$, $\frac{\alpha^{IV}}{\gamma^{IV}}$, $\frac{\alpha^{VI}}{\gamma^{VI}}$, a l'altra banda. Però com que $\gamma' < \gamma'''$, $\frac{\alpha'}{\gamma'}$ estarà situat *fora* de $\frac{\alpha'''}{\gamma'''}$ i L; i, per una raó similar, $\frac{\alpha''}{\gamma''}$, fora de L i $\frac{\alpha^{IV}}{\gamma^{IV}}$; $\frac{\alpha'''}{\gamma'''}$, fora de L i $\frac{\alpha^V}{\gamma^V}$, etc. D'on és evident que aquestes quantitats estan situades en l'ordre següent: $\frac{\alpha'}{\gamma'}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha^V}{\gamma^V}$, …, L, …, $\frac{\alpha^{VI}}{\gamma^{VI}}$, $\frac{\alpha^{IV}}{\gamma^{IV}}$, $\frac{\alpha''}{\gamma''}$. Però la diferència entre $\frac{\alpha'}{\gamma'}$ i L serà menor que la diferència entre $\frac{\alpha'}{\gamma'}$ i $\frac{\alpha''}{\gamma''}$; *és a dir*, $< \frac{1}{\gamma'\gamma''}$; i, per una raó similar, la diferència entre $\frac{\alpha''}{\gamma''}$ i L serà $< \frac{1}{\gamma''\gamma'''}$, etc. Per la qual cosa, les fraccions $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, etc., s'aproximen contínuament al límit L, i, com que γ', γ'', γ''', creixen contínuament a l'infinit, la diferència entre les fraccions i el límit pot resultar menor que qualsevol quantitat donada.

Per l'article 189, cap de les quantitats $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$, $\frac{''\gamma}{''\alpha}$, etc. no tindrà el mateix signe que a; d'aquí, per raonaments completament similars als precedents, se segueix

que aquelles i la $\dfrac{-\sqrt{D}+b}{a'}$, que designarem per L', estan situades en l'ordre següent: $\dfrac{\gamma}{\alpha}$, $\dfrac{''\gamma}{''\alpha}$, $\dfrac{^{IV}\gamma}{^{IV}\alpha}$, ..., L', ..., $\dfrac{^{V}\gamma}{^{V}\alpha}$, $\dfrac{'''\gamma}{'''\alpha}$, $\dfrac{'\gamma}{'\alpha}$. Però la diferència entre $\dfrac{\gamma}{\alpha}$ i L' serà menor que $\dfrac{1}{'\alpha\alpha}$, la diferència entre $\dfrac{'\gamma}{'\alpha}$ i L' menor que $\dfrac{1}{''\alpha'\alpha}$, etc. Per tant, les fraccions $\dfrac{\gamma}{\alpha}$, $\dfrac{'\gamma}{'\alpha}$, etc., s'aproximaran contínuament a L' i la diferència podrà resultar menor que qualsevol quantitat donada.

En l'exemple de *l'article* 188 resulta $L = \dfrac{\sqrt{79}-8}{3} = 0,2960648$, i les fraccions aproximadores, $\dfrac{0}{1}$, $\dfrac{1}{3}$, $\dfrac{2}{7}$, $\dfrac{3}{10}$, $\dfrac{5}{17}$, $\dfrac{8}{27}$, $\dfrac{45}{152}$, $\dfrac{143}{483}$, etc. Però és $\dfrac{143}{483} = 0,2960662$. En el mateix lloc, resulta $L' = \dfrac{-\sqrt{79}+8}{5} = -0,1776388$, i les fraccions aproximadores, $\dfrac{0}{1}$, $-\dfrac{1}{5}$, $-\dfrac{1}{6}$, $-\dfrac{2}{11}$, $-\dfrac{3}{17}$, $-\dfrac{8}{45}$, $-\dfrac{27}{152}$, $-\dfrac{143}{805}$, etc. Però és $\dfrac{143}{805} = 0,1776397$.

193. Teorema. *Si les formes reduïdes f, F, són pròpiament equivalents, cadascuna estarà continguda en el període de l'altra.*

Sigui $f = (a,\ b,\ -a')$, $F = (A,\ B,\ -A')$, D el determinant d'aquestes formes, i es transforma aquella en aquesta per la substitució pròpia $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$. Llavors, afirmo que si se cerca el període de la forma f i es troba la progressió infinita per les dues bandes de les formes

reduïdes i la de les transformacions de la forma f en aquestes de la mateixa manera que en l'article 188, *o bé* $+\mathfrak{A}$ serà igual a algun terme de la progressió $\ldots$, $''\alpha$, $'\alpha$, α, α', α'', $\ldots$, posat aquest $= \alpha^m$, $+\mathfrak{B}$ serà $= \beta^m$, $+\mathfrak{C} = \gamma^m$, $+\mathfrak{D} = \delta^m$; *o bé* $-\mathfrak{A}$ serà igual a algun terme α^m, i $-\mathfrak{B}$, $-\mathfrak{C}$, $-\mathfrak{D}$, respectivament, $= \beta^m$, γ^m, δ^m (on m també pot designar un índex negatiu). Evidentment, en ambdós casos, F serà idèntica a f^m.

Dem. I. Es tenen les quatre equacions $a\mathfrak{A}\mathfrak{A} + 2b\mathfrak{A}\mathfrak{C} - a'\mathfrak{C}\mathfrak{C} = A \ldots [1]$, $a\mathfrak{A}\mathfrak{B} + b(\mathfrak{A}\mathfrak{D} + \mathfrak{B}\mathfrak{C}) - a'\mathfrak{C}\mathfrak{D} = B \ldots [2]$, $a\mathfrak{B}\mathfrak{B} + 2b\mathfrak{B}\mathfrak{D} + a'\mathfrak{D}\mathfrak{D} = -A' \ldots [3]$; $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1 \ldots [4]$. Considerem, però, *primer*, el cas en què algun dels nombres $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ és $= 0$.

1r) Si $\mathfrak{A} = 0$, de [4] resulta $\mathfrak{B}\mathfrak{C} = -1$, de manera que $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$. D'aquí, de [1], $-a' = A$; de [2], $-b \pm a'\mathfrak{D} = B$, o sigui, $B \equiv -b \,(\text{mòd. } a'$ o bé $A)$; d'on se segueix que la forma $(A,\ B,\ -A')$ és contigua per l'última part a la forma $(a,\ b,\ -a')$. Però, com que aquella és reduïda, serà necessàriament idèntica a f'. Així, doncs, $B = b'$, de manera que, de [2], $b + b' = -a'\mathfrak{C}\mathfrak{D} = \pm a'\mathfrak{D}$; d'aquí, a causa que $\dfrac{b+b'}{-a'} = h'$, resulta $\mathfrak{D} = \mp h'$. D'on es conclou que $\mp\mathfrak{A}$, $\mp\mathfrak{B}$, $\mp\mathfrak{C}$, $\mp\mathfrak{D}$ són, respectivament, $= 0$, -1, $+1$, h', o sigui, $= \alpha'$, β', γ', δ'.

2n) Si $\mathfrak{B} = 0$, de [4] resulta $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; de [3], $a' = A'$; de [2], $b \mp a'\mathfrak{C} = B$, o sigui, $b \equiv B \,(\text{mòd. } a')$. Però com que, tant f com F són formes reduïdes, tant b com B estaran situats entre $\sqrt{D}$ i $\sqrt{D} \mp a'$ (segons que a' sigui positiu o bé negatiu, article 185, 5). Per tant, serà necessàriament $b = B$ i $\mathfrak{C} = 0$. D'aquí, les formes

f, F, són idèntiques i $\pm\mathfrak{A}$, $\pm\mathfrak{B}$, $\pm\mathfrak{C}$, $\pm\mathfrak{D}$, són $= 1$, 0, 0, 1, $= \alpha$, β, γ, δ (respectivament).

3r) Si $\mathfrak{C} = 0$, de [4] resulta $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; de [1], $a = A$; de [2], $\pm a\mathfrak{B} + b = B$, o sigui, $b \equiv B\,(\text{mòd.}\, a)$. Però, com que tant b com B estan situats entre $\sqrt{D}$ i $\sqrt{D} \mp a$, serà, necessàriament, $B = b$ i $\mathfrak{B} = 0$. Per tant, aquest cas no difereix del precedent.

4t) Si $\mathfrak{D} = 0$, de [4] resulta $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$; de [3], $a = -A'$; de [2], $\pm a\mathfrak{A} - b = B$, o sigui, $B \equiv -b\,(\text{mòd.}\, a)$. D'aquí, la forma F serà contigua per la primera part a la forma f i, en conseqüència, idèntica a la forma $'f$. Per tant, a causa que $\dfrac{'b + b}{a} = h$ i $B = 'b$, serà $\pm\mathfrak{A} = h$. D'on es conclou que $\pm\mathfrak{A}$, $\pm\mathfrak{B}$, $\pm\mathfrak{C}$, $\pm\mathfrak{D}$ són, respectivament, $= h$, 1, -1, 0, $= '\alpha$, $'\beta$, $'\gamma$, $'\delta$.

Així, resta el cas en què cap dels nombres $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, no és $= 0$. Aquí, pel Lema de l'article 190, les quantitats $\dfrac{\mathfrak{A}}{\mathfrak{C}}$, $\dfrac{\mathfrak{B}}{\mathfrak{D}}$, $\dfrac{\mathfrak{C}}{\mathfrak{A}}$, $\dfrac{\mathfrak{D}}{\mathfrak{B}}$, tindran el mateix signe, i d'aquí s'originen dos casos, ja que aquest signe, o bé podria concordar amb el signe de a, a', o bé ser oposat a ell.

II. Si $\dfrac{\mathfrak{A}}{\mathfrak{C}}$, $\dfrac{\mathfrak{B}}{\mathfrak{D}}$, tenen el mateix signe que a, la quantitat $\dfrac{\sqrt{D} - b}{a}$ (que designarem per L) estarà situada entre aquestes fraccions (article 191). Ara, demostrarem que $\dfrac{\mathfrak{A}}{\mathfrak{C}}$ serà igual a alguna de les fraccions $\dfrac{\alpha''}{\gamma''}$, $\dfrac{\alpha'''}{\gamma'''}$, $\dfrac{\alpha^{IV}}{\gamma^{IV}}$, etc., i $\dfrac{\mathfrak{B}}{\mathfrak{D}}$ a la immediata següent; això és, si $\dfrac{\mathfrak{A}}{\mathfrak{C}}$ fos

$= \frac{\alpha^m}{\gamma^m}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ seria $= \frac{\alpha^{m+1}}{\gamma^{m+1}}$. A l'article precedent, hem mostrat que les quantitats $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, etc. (que, per abreujar, denotarem per (1), (2), (3), etc.) i L segueixen aquest ordre (I): (1), (3), (5), ..., L, ..., (6), (4), (2); la primera d'aquestes quantitats és $= 0$ (a causa que $\alpha' = 0$), i totes les restants tenen el mateix signe que L, o sigui, a. Però, com que, per hipòtesi, $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ (per a les quals escriurem $\mathfrak{M}$, $\mathfrak{N}$), tenen el mateix signe, és clar que aquestes quantitats estaran situades a la dreta de (1) (o bé, si es prefereix, en el mateix costat que L), i, certament, com que L està situat entre elles, una a la dreta de L, l'altra a l'esquerra. Però es pot mostrar fàcilment que $\mathfrak{M}$ no pot estar situat a la dreta de (2), en efecte, altrament, $\mathfrak{N}$ estaria situat entre (1) i L, d'on se seguiria, *primer*, que (2) està situat entre $\mathfrak{M}$ i $\mathfrak{N}$, de manera que el denominador de la fracció (2) és més gran que el denominador de la fracció $\mathfrak{N}$ (article 190); *segon*, que $\mathfrak{N}$ està situat entre (1) i (2), de manera que el denominador de la fracció $\mathfrak{N}$ és més gran que el denominador de la fracció (2), *Q. E. A.*

Suposem que $\mathfrak{M}$ no és igual a cap de les fraccions (2), (3), (4), etc., i veiem què se seguiria d'això. Llavors, és evident que si la fracció $\mathfrak{M}$ està situada a l'esquerra de L, necessàriament està situada, o bé entre (1) i (3), o bé entre (3) i (5), o bé entre (5) i (7), etc. (ja que L és irracional, de manera que, certament, diferent de $\mathfrak{M}$, i les fraccions (1), (3), (5), etc. es poden aproximar a L per qualsevol quantitat donada, diferent de L). Però si $\mathfrak{M}$ està situat a la dreta de L, estarà situat necessàriament, o bé entre (2) i (4), o bé entre (4) i (6), o bé entre

(6) i (8), etc. Així, suposem que $\mathfrak{M}$ està situat entre (m) i $(m+2)$, i és clar que les quantitats $\mathfrak{M}$, (m), $(m+1)$, $(m+2)$, L estan situades en l'ordre següent (II):* (m), $\mathfrak{M}$, $(m+2)$, L, $(m+1)$. Llavors, serà necessàriament $\mathfrak{N} = (m+1)$. En efecte, $\mathfrak{N}$ estarà situat a la dreta de L; però si també estigués situat a la dreta de $(m+1)$, $(m+1)$ estaria situat entre $\mathfrak{M}$ i $\mathfrak{N}$, d'on $\gamma^{m+1} > \mathfrak{C}$, però $\mathfrak{M}$ entre (m) i $(m+1)$; d'on $\mathfrak{C} > \gamma^{m+1}$ (article 190), *Q. E. A.*; però si $\mathfrak{N}$ estigués situat a l'esquerra de $(m+1)$, o sigui, entre $(m+2)$ i $(m+1)$, seria $\mathfrak{D} > \gamma^{m+2}$, i, com que $(m+2)$ entre $\mathfrak{M}$ i $\mathfrak{N}$, seria $\gamma^{m+2} > \mathfrak{D}$, *Q. E. A.* Així, serà $\mathfrak{N} = (m+1)$, o sigui, $\dfrac{\mathfrak{B}}{\mathfrak{D}} = \dfrac{\alpha^{m+1}}{\gamma^{m+1}} = \dfrac{\beta^m}{\delta^m}$.

Com que $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1$, $\mathfrak{B}$ serà primer amb $\mathfrak{D}$, i, per una raó similar, β^m primer amb δ^m. D'on es copsa fàcilment que l'equació $\dfrac{\mathfrak{B}}{\mathfrak{D}} = \dfrac{\beta^m}{\delta^m}$ no pot ser consistent, llevat que sigui, o bé $\mathfrak{B} = \beta^m$, $\mathfrak{D} = \delta^m$, o bé $\mathfrak{B} = -\beta^m$, $\mathfrak{D} = -\delta^m$. Ara, com que la forma f, per la substitució pròpia α^m, β^m, γ^m, δ^m, es transforma en la forma f^m, que és $(\pm a^m, b^m, \mp a^{m+1})$, es tindran les equacions $a\alpha^m\alpha^m + 2b\alpha^m\gamma^m - a'\gamma^m\gamma^m = \pm a^m$ … [5]; $a\alpha^m\beta^m + b(\alpha^m\delta^m + \beta^m\gamma^m) - a'\gamma^m\delta^m = b^m$ … [6]; $a\beta^m\beta^m + 2b\beta^m\delta^m - a'\delta^m\delta^m = \mp a^{m+1}$ … [7]; $\alpha^m\delta^m - \beta^m\gamma^m = 1$ … [8]. D'aquí resulta (de les equacions [7] i [3]) $\mp a^{m+1} = -A'$. A més a més, multiplicant l'equació [2] per $\alpha^m\delta^m - \beta^m\gamma^m$, l'equació [6] per $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C}$, i restant, es confirma fàcilment per desenvolupament que és $B - b^m = (\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)(a\mathfrak{B}\beta^m + b(\mathfrak{D}\beta^m + \mathfrak{B}\delta^m) - a'\mathfrak{D}\delta^m) + (\mathfrak{B}\delta^m - \mathfrak{D}\beta^m)(a\mathfrak{A}\alpha^m + b(\mathfrak{C}\alpha^m + \mathfrak{A}\gamma^m) - a'\mathfrak{C}\gamma^m)$ … [9], o

* Aquí no importa que l'ordre de (II), o bé sigui el mateix que en (I), o bé oposat a aquest; *és a dir*, que també en (I), (m) estigui situat, o bé a l'esquerra de L, o bé a la dreta.

sigui, com que, o bé $\beta^m = \mathfrak{B}$, $\delta^m = \mathfrak{D}$, o bé $\beta^m = -\mathfrak{B}$, $\delta^m = -\mathfrak{D}$, és $B - b^m = \pm(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)(a\mathfrak{B}\mathfrak{B} + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}\mathfrak{D}) = \mp(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)A'$. D'aquí, $B \equiv b^m$ (mòd. A'); però, com que tant B com b^m estan situats entre $\sqrt{D}$ i $\sqrt{D} \mp A'$, serà, necessàriament, $B = b^m$, de manera que $\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m = 0$, o sigui, $\dfrac{\mathfrak{A}}{\mathfrak{C}} = \dfrac{\alpha^m}{\gamma^m}$, *és a dir*, $\mathfrak{M} = (m)$.

Així, d'aquesta manera, de la suposició que $\mathfrak{M}$ no és igual a cap de les quantitats (2), (3), (4), etc., hem deduït que aquesta és efectivament igual a alguna. Però si suposem des de l'inici que és $\mathfrak{M} = (m)$, evidentment serà, o bé $\mathfrak{A} = \alpha^m$, $\mathfrak{C} = \gamma^m$, o bé $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$. En ambdós casos resulta de [1] i [5] que $A = \pm a^m$, i, de [9], $B - b^m = \pm(\mathfrak{B}\delta^m - \mathfrak{D}\beta^m)A$, o sigui, $B \equiv b^m$ (mòd. A). D'aquí, de manera similar com més amunt, es conclou que $B = b^m$, i, d'aquí, que $\mathfrak{B}\delta^m = \mathfrak{D}\beta^m$; per tant, com que $\mathfrak{B}$ és primer amb $\mathfrak{D}$, i β^m amb δ^m, o bé serà $\mathfrak{B} = \beta^m$, $\mathfrak{D} = \delta^m$, o bé $-\mathfrak{B} = \beta^m$, $-\mathfrak{D} = \delta^m$, i, en conseqüència, de [7], $-A' = \mp a^{m+1}$. Per la qual cosa, les formes F, f^m, seran idèntiques. Però, amb l'ajut de l'equació $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = \alpha^m\delta^m - \beta^m\gamma^m$, es prova sense cap dificultat que, quan $+\mathfrak{A} = \alpha^m$, $+\mathfrak{C} = \gamma^m$, s'ha de posar $+\mathfrak{B} = \beta^m$, $+\mathfrak{D} = \delta^m$; contràriament, $-\mathfrak{B} = \beta^m$, $-\mathfrak{D} = \delta^m$, quan $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$, *Q. E. D.*

III. Si el signe de la quantitat $\dfrac{\mathfrak{A}}{\mathfrak{C}}$ és oposat al signe de a, la demostració és tan similar a la precedent que és suficient indicar només els punts principals. $\dfrac{-\sqrt{D} + b}{a'}$ estarà situat entre $\dfrac{\mathfrak{C}}{\mathfrak{A}}$ i $\dfrac{\mathfrak{D}}{\mathfrak{B}}$. La fracció $\dfrac{\mathfrak{D}}{\mathfrak{B}}$ serà igual a alguna de les fraccions $\dfrac{'\delta}{'\beta}$, $\dfrac{''\delta}{''\beta}$, $\dfrac{'''\delta}{'''\beta}$, etc., ... (I),

que, posada $= \frac{{}^m\delta}{{}^m\beta}$, serà $= \frac{\mathfrak{C}}{\mathfrak{A}} = \frac{{}^m\gamma}{{}^m\alpha} \ldots$ (II). Però (I) es demostra així. Si se suposa que $\frac{\mathfrak{D}}{\mathfrak{B}}$ no és igual a cap d'aquelles fraccions, haurà d'estar situada entre dues tals $\frac{{}^m\delta}{{}^m\beta}$, $\frac{{}^{m+1}\delta}{{}^{m+1}\beta}$. Però d'aquí es dedueix, de la mateixa manera que més amunt, que, necessàriament, és $\frac{\mathfrak{C}}{\mathfrak{A}} = \frac{{}^{m+1}\delta}{{}^{m+1}\beta} = \frac{{}^m\gamma}{{}^m\alpha}$, i que, o bé $\mathfrak{A} = {}^m\alpha$, $\mathfrak{C} = {}^m\gamma$, o bé $-\mathfrak{A} = {}^m\alpha$, $-\mathfrak{C} = {}^m\gamma$. Però com que f, per la substitució pròpia ${}^m\alpha$, ${}^m\beta$, ${}^m\gamma$, ${}^m\delta$, es transforma en la forma ${}^mf = (\pm{}^ma, {}^mb, \mp{}^{m-1}a)$, d'aquí emergeixen tres equacions, de les quals, conjuntament amb les equacions 1, 2, 3, 4, i la ${}^m\alpha{}^m\delta - {}^m\beta{}^m\gamma = 1$, es dedueix, de la mateixa manera que més amunt, que el primer terme A de la forma F és igual al primer terme de la forma ${}^mf$ i que el terme central d'aquella és congru al central d'aquesta segons el mòdul A; d'on se segueix que, com que les dues formes són reduïdes, de manera que els termes centrals de totes dues estan situats entre $\sqrt{D}$ i $\sqrt{D} \mp A$, aquests dos termes centrals són iguals; d'aquí es dedueix, però, que $\frac{{}^m\delta}{{}^m\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$. Així, la veritat de l'afirmació (I) aquí s'ha derivat de la suposició que aquella és falsa.

Suposant, però, que $\frac{{}^m\delta}{{}^m\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$, de manera enterament similar i per les mateixes equacions, es demostra que també és $\frac{{}^m\gamma}{{}^m\alpha} = \frac{\mathfrak{C}}{\mathfrak{A}}$, que era la segona (II). D'aquí, però, amb l'ajut de les equacions $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1$, ${}^m\alpha{}^m\delta - {}^m\beta{}^m\gamma = 1$, es dedueix que, o bé és $\mathfrak{A} = {}^m\alpha$, $\mathfrak{B} = {}^m\beta$, $\mathfrak{C} = {}^m\gamma$, $\mathfrak{D} = {}^m\delta$, o bé $-\mathfrak{A} = {}^m\alpha$, $-\mathfrak{B} = {}^m\beta$, $-\mathfrak{C} = {}^m\gamma$, $-\mathfrak{D} = {}^m\delta$, i les formes F, ${}^mf$, són idèntiques. *Q. E. D.*

194. Com que les formes que més amunt hem anomenat associades (article 187, 6) sempre són impròpiament equivalents (article 160), es copsa que si les formes reduïdes F, f, són impròpiament equivalents i la forma G, associada a la forma F, les formes f, G, seran pròpiament equivalents, de manera que la forma G [està] continguda en el període de la forma f. Així, si les formes F, f, són equivalents tant pròpiament com impròpiament, és clar que tant F com G s'han de trobar en el període de la forma f. Per tant, aquest període serà un associat de si mateix i contindrà dues formes ambigües (article 187, 7). D'on es confirma excel·lentment el teorema de l'article 165, a partir del qual ja podíem estar segurs que es dóna alguna forma ambigua equivalent a les formes F, f.

195. Problema. *Proposades dues formes qualssevol Φ, ϕ, del mateix determinant, decidir si són equivalents o no.*

Solució. Se cerquen dues formes reduïdes F, f, pròpiament equivalents a les proposades Φ, ϕ, respectivament (article 183). Segons que aquestes equivalguin, o bé només pròpiament, o bé només impròpiament, o bé de les dues maneres, o bé de cap, també les proposades seran equivalents o bé només pròpiament, o bé només impròpiament, o bé de les dues maneres, o bé de cap. Es calcula el període de cadascuna de les formes reduïdes, *per exemple*, el període de la forma f. Si la forma F apareix en aquest període, però no simultàniament la forma associada a F, evidentment tindrà lloc el *primer* cas; contràriament, si aquesta associada és present però no F, el *segon*; si totes dues, el *tercer*; si cap, el *quart*.

Exemple. Siguin proposades les formes (129, 92, 65), (42, 59, 81), de determinant 79. Pròpiament equivalents a elles, es troben les reduïdes (10, 7, −3), (5, 8, −3). El període de la primera forma és aquest: (10, 7, −3), (−3, 8, 5), (5, 7, −6), (−6, 5, 9), (9, 4, −7), (−7, 3, 10). Com que la forma (5, 8, −3) no apareix en ell, sinó, en canvi, l'associada (−3, 8, 5), concloem que les formes proposades només equivalen impròpiament.

Si totes les formes reduïdes de determinant donat es distribueixen de la mateixa manera que més amunt (article 187, 5) en períodes P, Q, R, etc., i de qualsevol període s'elegeix a voluntat alguna forma, F de P, G de Q, H de R, etc., entre les formes F, G, H, etc., no podrà haver-n'hi dues que equivalguin pròpiament. Però qualsevol altra forma del mateix determinant serà pròpiament equivalent a alguna d'aquestes, i, certament, només a una *única*. D'aquí és evident que *totes les formes d'aquest determinant es poden distribuir en tantes classes com períodes es tinguin*, això és, assignant les que equivalen pròpiament a la forma F a la primera classe, les que equivalen pròpiament a la forma G a la segona, etc. D'aquesta manera, totes les formes contingudes a la mateixa classe seran pròpiament equivalents, però formes de classes diferents no podran equivaler pròpiament. Però aquí no ens detenim en aquest argument, que cal explicar més extensament més avall.

196. Problema. *Proposades dues formes pròpiament equivalents, Φ, ϕ, trobar una transformació pròpia de l'una en l'altra.*

Solució. Pel mètode de l'article 183 es podran trobar dues sèries de formes Φ, Φ', Φ'', ..., Φ^n, i ϕ, ϕ', ϕ'', ..., ϕ^ν, tals que qualsevol forma següent equivalgui pròpiament a la precedent i que les últimes Φ^n, ϕ^ν, siguin formes reduïdes; i com que Φ, ϕ, se suposen pròpiament equivalents, necessàriament Φ^n estarà continguda en el període de la forma ϕ^ν. Sigui $\phi^\nu = f$ i el seu període fins a la forma Φ^n aquest: f, f', f'', ..., f^{m-1}, Φ^n, de manera que, en aquest període, l'índex de la forma Φ^n sigui m; i es designen les formes que són oposades a les associades de les formes Φ, Φ', Φ'', ..., Φ^n, per Ψ, Ψ', Ψ'', ..., Ψ^n, respectivament.* Llavors, a la progressió ϕ, ϕ', ϕ'', ..., f, f', f'', ..., f^{m-1}, Ψ^{n-1}, Ψ^{n-2}, ..., Ψ, Φ, qualsevol forma serà contigua per l'última part a la precedent, d'on, per l'article 177, es podrà trobar una transformació pròpia de la primera, ϕ, en l'última, Φ. Allò es copsa sense dificultat per a les restants formes de la progressió; per a f^{m-1} i Ψ^{n-1} es prova així. Sigui $f^{m-1} = (g,\ h,\ i)$; f^m, o sigui, $\Phi^n = (g',\ h',\ i')$, $\Phi^{n-1} = (g'',\ h'',\ i'')$. La forma $(g',\ h',\ i')$ serà contigua per l'última part tant a la forma $(g,\ h,\ i)$ com a la forma $(g'',\ h'',\ i'')$; D'aquí, $i = g' = i''$, $-h \equiv h' \equiv -h''$ (mòd. i o bé g' o bé i''). D'on és evident que la forma $(i'',\ -h'',\ g'')$, és a dir, la forma Ψ^{n-1}, és contigua per l'última part a la forma $(g,\ h,\ i)$, és a dir, a la forma f^{m-1}.

Si les formes Φ, ϕ, són impròpiament equivalents, la forma ϕ equivaldrà pròpiament a la forma a què Φ és oposada. Així, es podrà trobar la transformació pròpia de la forma ϕ en la forma a què Φ és oposada; si se

* De manera que Ψ s'origina de Φ intercanviant el primer terme i l'últim i atribuint al central el signe oposat, i similarment per a les restants.

suposa que aquella resulta per la substitució α, β, γ, δ, es copsa fàcilment que ϕ es transforma impròpiament en Φ per la substitució α, $-\beta$, γ, $-\delta$.

D'aquí, també es copsa que si les formes Φ, ϕ, són equivalents tant pròpiament com impròpiament es poden trobar *dues* transformacions, una pròpia i una impròpia.

Exemple. Se cerca una transformació impròpia de la forma (129, 92, 65) en la forma (42, 59, 81), que hem trobat a l'article precedent que equival impròpiament a aquella. Així, caldrà investigar, primer, una transformació pròpia de la forma (129, 92, 65) en la forma (42, −59, 81). Per a aquest fi, es desenvolupa la progressió de formes: (129, 92, 65), (65, −27, 10), (10, 7, −3), (−3, 8, 5), (5, 22, 81), (81, 59, 42), (42, −59, 81). D'aquí es dedueix la transformació pròpia −47, 56, 73, −87, per la qual (129, 92, 65) es transforma en (42, −59, 81); per tant, per la impròpia −47, −56, 73, 87, es transformarà en (42, 59, 81).

197. Si es té una transformació d'alguna forma $(a, b, c) \ldots \phi$ en una equivalent Φ, es podran deduir d'aquesta *totes* les transformacions similars de la forma ϕ en Φ, sempre que es puguin explicitar totes les solucions de l'equació indeterminada $tt - Duu = mm$, on D designa el determinant de les formes Φ, ϕ; i m, el màxim comú divisor dels nombres a, $2b$, c (article 162). Així, doncs, ataquem aquest problema, que ja hem resolt més amunt per a un valor negatiu de D, per a un de positiu. Però, com que, evidentment, qualsevol valor de t que satisfà l'equació encara la satisfà un cop canviat de signe, i, similarment, qualsevol valor de u, serà suficient

si podem explicitar tots els valors *positius* de t, u, i qualsevol solució per valors positius complirà quatre vegades com a solució. Resolem aquesta tasca de manera que, *primer*, es troben els valors *mínims* de t, u (excepte els obvis $t = m$, $u = 0$), i, *després*, ensenyem a derivar d'aquests tots els restants.

198. PROBLEMA. *Trobar els nombres mínims t, u, que satisfan l'equació indeterminada $tt - Duu = mm$, suposat que es dóna alguna forma (M, N, P), el determinant de la qual és D, i el màxim comú divisor de M, $2N$, P, és m.*

Solució. S'agafa a voluntat una forma reduïda $(a, b, -a')$ ... f, de determinant D, on el màxim comú divisor dels nombres a, $2b$, a', sigui m; que aquesta es dóna, és evident del fet que es pot trobar una forma reduïda equivalent a la forma (M, N, P), que, per l'article 161, estarà proveïda d'aquesta propietat; però, per al propòsit present, es podrà utilitzar qualsevol forma reduïda en què aquesta condició tingui lloc. Es desenvolupa el període de la forma f, que suposem que consta de n formes. Retinguts tots els signes que hem usat a l'article 188, f^n serà $(+a^n, b^n, -a^{n+1})$, ja que n és parell, i f es transformarà en aquesta forma per la substitució pròpia α^n, β^n, γ^n, δ^n. Però, com que f i f^n són idèntiques, f també es transformarà en f^n per la substitució pròpia 1, 0, 0, 1. D'aquestes dues transformacions similars de la forma f en f^n es podrà deduir, per l'article 162, una solució de l'equació $tt - Duu = mm$ *en enters*, això és, $t = \frac{1}{2}(\alpha^n + \delta^n)m$ (equació 18 de l'article 162),

$u = \dfrac{\gamma^n m}{a}$ (equació 19).* Es designen aquests valors, agafats positivament si tal vegada encara no ho són, per T, U, i T, U, seran els valors mínims de t, u, excepte $t = m$, $u = 0$ (dels quals seran necessàriament diferents, ja que, evidentment, γ^n no podrà ser $= 0$).

En efecte, suposem que es donen valors encara menors de t, u, posem $\mathfrak{t}$, $\mathfrak{u}$, que siguin positius i $\mathfrak{u}$ no $= 0$. Llavors, per l'article 162, la forma f es transformaria en una forma idèntica a ella per la substitució pròpia $\dfrac{1}{m}(\mathfrak{t} - b\mathfrak{u})$, $\dfrac{1}{m}a'\mathfrak{u}$, $\dfrac{1}{m}a\mathfrak{u}$, $\dfrac{1}{m}(\mathfrak{t} + b\mathfrak{u})$. Ara, de l'article 193, *II*, se segueix que, *o bé* $\dfrac{1}{m}(\mathfrak{t} - b\mathfrak{u})$, *o bé* $-\dfrac{1}{m}(\mathfrak{t} - b\mathfrak{u})$, ha de ser igual a algun dels nombres α'', α''', α^{IV}, etc., posem $= \alpha^\mu$ (en efecte, com que $\mathfrak{tt} = D\mathfrak{uu} + mm = bb\mathfrak{uu} + aa'\mathfrak{uu} + mm$, serà $\mathfrak{tt} > bb\mathfrak{uu}$, de manera que $\mathfrak{t} - b\mathfrak{u}$, positiu; d'aquí, la fracció $\dfrac{\mathfrak{t} - b\mathfrak{u}}{a\mathfrak{u}}$, que correspon a la fracció $\dfrac{\mathfrak{A}}{\mathfrak{C}}$ de l'article 193, tindrà el mateix signe que a o bé a'); i, en el primer cas, $\dfrac{1}{m}a'\mathfrak{u}$, $\dfrac{1}{m}a\mathfrak{u}$, $\dfrac{1}{m}(\mathfrak{t} + b\mathfrak{u})$, en el segon, les mateixes quantitats, canviats els signes, són, respectivament, $= \beta^\mu$, γ^μ, δ^μ. Però com que és $\mathfrak{u} < U$, és a dir, $\mathfrak{u} < \dfrac{\gamma^n m}{a}$, i > 0, serà $\gamma^\mu < \gamma^n$ i > 0; en conseqüència, com que la progressió γ, γ', γ'', etc., creix contínuament, μ estarà situat, necessàriament, entre 0 i n, exclusivament. Però

* Els que a l'article 162 eren α, β, γ, δ; α', β', γ', δ'; A, B, C; A', B', C'; e, aquí són 1, 0, 0, 1; α^n, β^n, γ^n, δ^n; a, b, $-a'$; a, b, $-a'$; 1.

la forma corresponent, f^μ, serà idèntica a la forma f, *Q. E. A.*, ja que s'ha suposat que totes les formes f, f', etc., fins a la f^{n-1} són diferents. D'això es conclou que T, U, són els valors mínims de t, u (exceptuats els valors m, 0).

Exemple. Si $D = 79$, $m = 1$, es podrà utilitzar la forma $(3,\ 8,\ -5)$, per a la qual $n = 6$ i $\alpha^n = -8$, $\gamma^n = -27$, $\delta^n = -152$ (article 188). D'aquí, $T = 80$, $U = 9$, que són els valors mínims dels nombres t, u, que satisfan l'equació $tt - 79uu = 1$.

199. A la pràctica, es poden trobar fórmules encara més còmodes. Evidentment, serà $2b\gamma^n = -a(\alpha^n - \delta^n)$, que es dedueix fàcilment de l'article 162 multiplicant l'equació [19] per $2b$, la [20] per a, i canviant els caràcters utilitzats allà pels presents. D'aquí resulta $\alpha^n + \delta^n = 2\delta^n - \dfrac{2b}{a}\gamma^n$, de manera que

$$\pm T = m(\delta^n - \frac{b}{a}\gamma^n), \quad \pm U = \frac{\gamma^n m}{a}.$$

Per un mètode similar, obtenim els valors

$$\pm T = m\left(\alpha^n + \frac{b}{a'}\beta^n\right), \quad \pm U = \frac{\beta^n m}{a'}.$$

Tant aquestes fórmules com aquelles surten extremament còmodes, a causa que $\gamma^n = \delta^{n-1}$, $\alpha^n = \beta^{n-1}$, de manera que, si s'utilitzen aquestes, és suficient de calcular només la progressió β', β'', β''', $\ldots$, β^n, i, si es prefereix utilitzar aquelles, només la δ', δ'', δ''', etc. A part d'això, de l'article 189, 3, es dedueix fàcilment que, com que n és necessàriament parell, α^n i $\dfrac{b}{a'}\beta^n$ tenen

el mateix signe; i també δ^n i $\frac{b}{a}\gamma^n$, de manera que, en la primera fórmula, s'ha d'agafar per a T la diferència absoluta, en la darrera, la suma absoluta; i, així, no és necessari en absolut respectar els signes. Recuperats els símbols utilitzats a l'article 189, 4, de la primera fórmula serà

$$T = m[k', k'', k''', \ldots, k^n] - \frac{mb}{a}[k', k'', k''', \ldots, k^{n-1}],$$
$$U = \frac{m}{a}[k', k'', k''', \ldots, k^{n-1}],$$

de la posterior

$$T = m[k'', k''', \ldots, k^{n-1}] - \frac{mb}{a'}[k'', k''', \ldots, k^n],$$
$$U = \frac{m}{a'}[k'', k''', \ldots, k^n],$$

on, per al valor de T, també es podrà escriure $m[k''$, k''', $\ldots$, k^n, $\frac{b}{a'}]$.

Exemple. Per a $D = 61$, $m = 2$, es pot utilitzar la forma (2, 7, −6), per a la qual es troba $n = 6$; k', k'', k''', k^{IV}, k^V, k^{VI}, respectivament, = 2, 2, 7, 2, 2, 7. D'aquí resulta $T = 2[2, 2, 7, 2, 2, 7] - 7[2, 2, 7, 2, 2] = 2888 - 1365 = 1523$ de la primera fórmula; el mateix apareix de la segona, $T = 2[2, 7, 2, 2] + \frac{7}{3}[2, 7, 2, 2, 7]$. Però U resulta $= \frac{1}{3}[2, 2, 7, 2, 2] = [2, 7, 2, 2, 7] = 195$.

D'altra banda, encara es donen més artificis pels quals es pot simplificar el càlcul, però la brevetat no permet parlar-ne més extensament aquí.

200. Perquè dels valors mínims de t, u els obtinguem *tots*, mostrem l'equació $TT - DUU = mm$ així: $\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right) = 1$, d'on també serà $\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e \left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e = 1 \ldots$ [1], on e denota un nombre qualsevol. Ara, per abreujar, designarem els valors de les quantitats

$$\frac{m}{2}\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e + \frac{m}{2}\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e,$$
$$\frac{m}{2\sqrt{D}}\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e - \frac{m}{2\sqrt{D}}\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e,$$

* en general per t^e, u^e, respectivament; *és a dir*, els valors d'aquelles per a $e = 0$, per t^0, u^0 (que seran m, 0); per a $e = 1$, per t', u' (que resulten T, U); per a $e = 2$, per t'', u''; per a $e = 3$, per t''', u''', etc.; i demostrarem que si per a e s'agafen tots els nombres enters no negatius, és a dir, 0 i tots els positius des de 1 fins a ∞, aquelles expressions representen tots els valors positius de t, u; això és, I) tots els valors d'aquelles expressions són realment valors de t, u; II) tots aquells valors són nombres enters; III) no es donen valors positius de t, u, que no estiguin continguts en aquelles fórmules.

I. Substituïts t^e, u^e, pels seus valors, es confirma sense dificultat, amb l'ajut de l'equació [1], que és $(t^e + u^e\sqrt{D})(t^e - u^e\sqrt{D}) = mm$, és a dir, $t^e t^e - Du^e u^e = mm$.

* Només en aquestes quatre expressions i en l'equació [1] e denota *l'exponent* de la potència; en les restants, les lletres afegides a dalt designen sempre *índexs*.

II. De la mateixa manera, es confirma fàcilment que, en general, és $t^{e+1} + t^{e-1} = \frac{2T}{m}t^e$, $u^{e+1} + u^{e-1} = \frac{2T}{m}u^e$. D'aquí, és evident que les dues progressions t^0, t', t'', t''', etc., u^0, u', u'', u''', etc., són recurrents i que l'escala de relació de cadascuna és $\frac{2T}{m}$, -1, això és, $t'' = \frac{2T}{m}t' - t^0$, $t''' = \frac{2T}{m}t'' - t'$, etc.; $u'' = \frac{2T}{m}u'$, etc.

Ara, com que, per hipòtesi, es dóna alguna forma $(M,\ N,\ P)$, de determinant D, en què M, $2N$, P, són divisibles per m, es tindrà $TT = (NN - MP)UU + mm$ i, així, evidentment, $4TT$ serà divisible per mm. D'aquí, $\frac{2T}{m}$ serà un nombre enter i, certament, positiu. Però com que $t^0 = m$, $t' = T$, $u^0 = 0$, $u' = U$, de manera que enters, tots els t'', t''', etc., u'', u''', etc., també seran enters. A més a més, es copsa, ja que $TT > mm$, que tots els t^0, t', t'', t''', etc., són positius i creixents contínuament a l'infinit, i també tots els u^0, u', u'', u''', etc.

III. Suposem que encara es donen altres valors positius de t, u, que no estiguin continguts en la progressió t^0, t', t'', etc., u^0, u', u'', etc., posem $\mathfrak{T}$, $\mathfrak{U}$. És evident que, com que la progressió u^0, u', etc., creix des de 0 fins a infinit, $\mathfrak{U}$ estarà situat necessàriament entre dos termes consecutius u^n i u^{n+1}, de manera que sigui $\mathfrak{U} > u^n$ i $\mathfrak{U} < u^{n+1}$. Perquè demostrem l'absurditat d'aquesta suposició, observem que:

1r) L'equació $tt - Duu = mm$ també serà satisfeta posant $t = \frac{1}{m}(\mathfrak{T}t^n - D\mathfrak{U}u^n)$, $u = \frac{1}{m}(\mathfrak{U}t^n - \mathfrak{T}u^n)$. Això

es confirma, certament sense dificultat, per substitució; però, que aquests valors, que per abreujar posarem = τ, ν, sempre són nombres *enters*, ho mostrem així. Si (M, N, P) és una forma de determinant D, i m un divisor comú dels nombres M, $2N$, P, tant $\mathfrak{T}+N\mathfrak{U}$ com $t^n + Nu^n$ serà divisible per m, de manera que, també, $\mathfrak{U}(t^n + Nu^n) - u^n(\mathfrak{T} + N\mathfrak{U})$, o sigui, $\mathfrak{U}t^n - \mathfrak{T}u^n$. Per tant, ν serà enter, i, en conseqüència, també, τ, ja que $\tau\tau = D\nu\nu + mm$.

2n) És clar que ν no pot ser = 0; en efecte, d'aquí se seguiria $\mathfrak{W}\mathfrak{W}t^nt^n = \mathfrak{T}\mathfrak{T}u^nu^n$, o sigui, $\mathfrak{W}\mathfrak{W}(Du^nu^n + mm) = u^nu^n(D\mathfrak{W}\mathfrak{W} + mm)$, o sigui, $\mathfrak{W}\mathfrak{W} = u^nu^n$, contra la hipòtesi que $\mathfrak{U} > u^n$. Així, doncs, com que, excepte el valor 0, el valor mínim de u és U, ν no serà, certament, menor que U.

3r) Es pot confirmar fàcilment dels valors de t^n, t^{n+1}, u^n, u^{n+1}, que és $mU = u^{n+1}t^n - t^{n+1}u^n$. Per tant, $\mathfrak{U}t^n - \mathfrak{T}u^n$ no serà menor, certament, que $u^{n+1}t^n - t^{n+1}u^n$.

4t) Ara, de l'equació $\mathfrak{T}\mathfrak{T} - D\mathfrak{W}\mathfrak{W} = mm$ es té $\dfrac{\mathfrak{T}}{\mathfrak{U}} = \sqrt{D + \dfrac{mm}{\mathfrak{W}\mathfrak{W}}}$ i, similarment, $\dfrac{t^{n+1}}{u^{n+1}} = \sqrt{D + \dfrac{mm}{u^{n+1}u^{n+1}}}$, d'on es dedueix fàcilment que és $\dfrac{\mathfrak{T}}{\mathfrak{U}} > \dfrac{t^{n+1}}{u^{n+1}}$. Però, d'aquí i de la conclusió de 3r), se segueix que $(\mathfrak{U}t^n - \mathfrak{T}u^n)(t^n + u^n\dfrac{\mathfrak{T}}{\mathfrak{U}}) > (u^{n+1}t^n - t^{n+1}u^n)(t^n + u^n\dfrac{t^{n+1}}{u^{n+1}})$, o sigui, fet el desenvolupament i substituïts en lloc de $\mathfrak{T}\mathfrak{T}$, t^nt^n, $t^{n+1}t^{n+1}$ els seus valors $D\mathfrak{W}\mathfrak{W}+mm$, Du^nu^n+mm, $Du^{n+1}u^{n+1} + mm$,

$$\frac{1}{\mathfrak{U}}(\mathfrak{UU} - u^n u^n) > \frac{1}{u^{n+1}}(u^{n+1}u^{n+1} - u^n u^n),$$

d'on, com que cada una de les quantitats és, evidentment, positiva, resulta, transposant, $\mathfrak{U} + \frac{u^n u^n}{u^{n+1}} > u^{n+1} + \frac{u^n u^n}{\mathfrak{U}}$, *Q. E. A.*, ja que la primera part de la primera quantitat és *menor* que la primera part de la segona quantitat, i també la segona d'aquella és menor que la segona d'aquesta. Per la qual cosa la suposició no pot ser consistent i les progressions t^0, t', t'', etc., u^0, u', u'', etc., representaran tots els valors positius de t, u.

Exemple. Per a $D = 61$, $m = 2$, vàrem trobar els valors positius mínims de t, u, 1523, 195; per tant, *tots* els valors positius s'expressaran per les fórmules $t = \left(\frac{1523}{2} + \frac{195}{2}\sqrt{61}\right)^e + \left(\frac{1523}{2} - \frac{195}{2}\sqrt{61}\right)^e$, $u = \frac{1}{\sqrt{61}}\left(\left(\frac{1523}{2} + \frac{195}{2}\sqrt{61}\right)^e - \left(\frac{1523}{2} - \frac{195}{2}\sqrt{61}\right)^e\right)$. Es troba, però, $t^0 = 2$, $t' = 1523$, $t'' = 1523t' - t^0 = 2319527$, $t''' = 1523t'' - t' = 3532618098$, etc.; $u^0 = 0$, $u' = 195$, $u'' = 1523u' - u^0 = 296985$, $u''' = 1523u'' - u' = 452307960$, etc.

201. Sobre el problema tractat als articles precedents, encara afegim les observacions següents.

1) Com que hem ensenyat a solucionar l'equació $tt - Duu = mm$ per a tots els casos en què m és el màxim comú divisor dels tres nombres M, $2N$, P, tals que $NN - MP = D$, val la pena la feina de determinar tots els nombres que poden ser tals divisors, o sigui,

tots els valors de m per a un valor donat de D. Es posa $D = nnD'$, de manera que D' sigui lliure completament de factors quadrats, cosa que s'obté si per a nn es pren el màxim quadrat que divideix D; però si D, ja per si mateix, no implica cap factor quadrat, s'haurà de fer $n = 1$. Llavors, afirmo que:

Primer, si D' fos de la forma $4k + 1$, qualsevol divisor de $2n$ seria un valor de m, i recíprocament. En efecte, si g és un divisor de $2n$, es tindrà la forma $(g,\ n,\ \frac{nn(D'-1)}{g})$, el determinant de la qual és D, i en la qual el màxim comú divisor dels nombres g, $2n$, $\frac{nn(D'-1)}{g}$, serà, evidentment, g (en efecte, és clar que $\frac{nn(D'-1)}{gg} = \frac{4nn}{gg} \cdot \frac{D'-1}{4}$ és un nombre enter). Però si, recíprocament, se suposa que g és un valor de m, això és, el màxim comú divisor dels nombres M, $2N$, P, i que $NN - MP = D$, evidentment $4D$, o sigui, $4nnD'$, serà divisible per gg. D'aquí se segueix, però, que $2n$ és necessàriament divisible per g. En efecte, si g no dividís $2n$, g i $2n$ tindrien màxim comú divisor menor que g, el qual posat $= \delta$, i $2n = \delta n'$, $g = \delta g'$, seria $n'n'D'$ divisible per $g'g'$; n' primer amb g', de manera que, també, $n'n'$ amb $g'g'$; i, en conseqüència, D' també divisible per $g'g'$, contràriament a la hipòtesi segons la qual D' és lliure de tot factor quadrat.

Segon, si D' fos de la forma $4k + 2$ o bé $4k + 3$, qualsevol divisor de n seria un valor de m; i recíprocament, qualsevol valor de m divideix n. En efecte, si

g és un divisor de n, es tindrà la forma $(g,\ 0,\ \frac{nnD'}{g})$, el determinant de la qual és $= D$, i on, evidentment, el màxim comú divisor dels nombres $g,\ 0,\ \frac{nnD'}{g}$, serà g. Però si se suposa que g és un valor de m, posem el màxim comú divisor dels nombres $M,\ 2N,\ P$, i és $NN - MP = D$, de la mateixa manera que més amunt, g dividirà $2n$, o sigui, $\frac{2n}{g}$ serà enter. Si aquest quocient fos imparell, el quadrat $\frac{4nn}{gg}$ seria $\equiv 1\,(\text{mòd. } 4)$, de manera que $\frac{4nnD'}{gg} \equiv 2$ o bé $\equiv 3\,(\text{mòd. } 4)$. Però $\frac{4nnD'}{gg} = \frac{4D}{gg} = \frac{4NN}{gg} - \frac{4MP}{gg} \equiv \frac{4NN}{gg}\,(\text{mòd. } 4)$ i, en conseqüència, $\frac{4NN}{gg} \equiv 2$ o bé $\equiv 3\,(\text{mòd. } 4)$, *Q. E. A.*, ja que tot quadrat ha de ser congru a zero o a la unitat segons el mòdul 4. Per tant, el quocient $\frac{2n}{g}$ serà necessàriament parell, de manera que $\frac{n}{g}$, enter; o sigui, g divisor de n.

Així, és clar que 1 sempre és valor de m, o sigui, que l'equació $tt - Duu = 1$ és resoluble, pel que precedeix, per a qualsevol valor positiu no quadrat de D; llavors, 2 només és un valor de m si D és de la forma $4k$ o bé $4k + 1$.

2) Si m és més gran que 2, però és un nombre idoni, la resolució de l'equació $tt - Duu = mm$ es pot reduir a la resolució de l'equació similar en què m és o bé 1 o bé 2. Això és, posat, com abans, $D = nnD'$, si

m divideix n, mm dividirà D. Llavors, si se suposa que els valors mínims de p, q, en l'equació $pp - \frac{D}{mm}qq = 1$ són $p = P$, $q = Q$, els valors mínims de t, u, en l'equació $tt - Duu = mm$ seran $t = mP$, $u = Q$. Però, si m no divideix n, almenys dividirà $2n$ i serà, certament, parell; però $\frac{4D}{mm}$, enter. I, llavors, si en l'equació $pp - \frac{4D}{mm}qq = 4$ els valors mínims de p, q, s'han trobat $p = P$, $q = Q$, els valors mínims de t, u, en l'equació $tt - Duu = mm$ seran $t = \frac{m}{2}P$, $u = Q$. Però, en ambdós casos, no solament es podran deduir els valors mínims de t, u, dels valors mínims de p, q, sinó que, evidentment, per aquest mètode, *tots* els valors d'aquests de *tots* els valors d'aquells.

3) Si t^0, u^0; t', u'; t'', u''; etc., designen tots els valors positius de t, u, en l'equació $tt - Duu = mm$, (com a l'article precedent), si succeeix que alguns valors d'aquella sèrie són congrus als seus primers valors segons un mòdul donat qualsevol, r, posem $t^\rho \equiv t^0$ (o sigui, $\equiv m$), $u^\rho \equiv u^0$, o sigui, $\equiv 0\,(\text{mòd.}\,r)$; i simultàniament els valors immediatament següents als segons valors, posem $t^{\rho+1} \equiv t'$, $u^{\rho+1} \equiv u'\,(\text{mòd.}\,r)$, també serà $t^{\rho+2} \equiv t''$, $u^{\rho+2} \equiv u''$; $t^{\rho+3} \equiv t'''$, $u^{\rho+3} \equiv u'''$; etc. D'aquí es dedueix fàcilment això, que cadascuna de les sèries t^0, t', t'', etc.; u^0, u', u'', etc., és de classe recurrent, això és, com que $t'' = \frac{2T}{m}t' - t^0$, $t^{\rho+2} = \frac{2T}{m}t^{\rho+1} - t^\rho$, serà $t'' \equiv t^{\rho+2}$, i similarment per als restants. Però d'aquí se segueix que, en general, serà $t^{h+\rho} \equiv t^h$, $u^{h+\rho} \equiv u^h\,(\text{mòd.}\,r)$, on h denota un nombre qualsevol, i encara, més generalment, si fos $\mu \equiv \nu\,(\text{mòd.}\,\rho)$, seria $t^\mu \equiv t^\nu$, $u^\mu \equiv u^\nu\,(\text{mòd.}\,r)$.

4) Però sempre es poden satisfer les condicions requerides a l'observació precedent, això és, sempre es pot trobar un índex ρ (per a un mòdul qualsevol donat r) per al qual sigui $t^\rho \equiv t^0$, $t^{\rho+1} \equiv t'$, $u^\rho \equiv u^0$, $u^{\rho+1} \equiv u'$. Per a demostrar això, observem

Primer, que la tercera condició sempre es pot satisfer. En efecte, es copsa sense dificultat, pel criteri transmès en 1), que l'equació $pp - rrDqq = mm$ també serà resoluble; i si se suposa que els valors mínims positius de p, q (excepte els m, 0), són P, Q, també, evidentment, $t = P$, $u = rQ$, estaran entre els valors de t, u. Per tant, P, rQ, estaran continguts a les progressions t^0, t', etc.; u^0, u', etc., i, si $P = t^\lambda$, $rQ = u^\lambda$, serà $u^\lambda \equiv 0 \equiv u^0 \,(\text{mòd.}\, r)$. A part d'això, es copsarà fàcilment que entre u^0 i u^λ no hi haurà cap terme congru a u^0 segons el mòdul r.

Segon, és clar que si aquí, a sobre, són complertes les tres condicions restants, posem, si també $u^{\lambda+1} \equiv u'$, $t^\lambda \equiv t^0$, $t^{\lambda+1} \equiv t'$, només s'ha de posar $\rho = \lambda$. Però si una o una altra d'aquelles condicions no té lloc, afirmo que, certament, es pot establir $\rho = 2\lambda$. Efectivament, de l'equació [1], i de les fórmules generals per a t^e, u^e, de l'article precedent, es dedueix que $t^{2\lambda} = \dfrac{1}{m}(t^\lambda t^\lambda + Du^\lambda u^\lambda) = \dfrac{1}{m}(mm + 2Du^\lambda u^\lambda)$, de manera que $\dfrac{t^{2\lambda} - t^0}{t^{2\lambda} - t^0 r} = \dfrac{2Du^\lambda u^\lambda}{mr}$, quantitat que serà un nombre enter, ja que, per hipòtesi, r divideix u^λ, i mm, $4D$, de manera que, amb més raó, m [divideix] $2D$. A més a més, serà $u^{2\lambda} = \dfrac{2}{m} t^\lambda u^\lambda$, i, com que $4t^\lambda t^\lambda = 4Du^\lambda u^\lambda + 4mm$, de manera que divisible per mm, $2t^\lambda$ serà divisible per m i, en conseqüència, $u^{2\lambda}$ per r, o sigui, $u^{2\lambda} \equiv 0 \,(\text{mòd.}\, r)$.

Tercer, es troba que $t^{2\lambda+1} = t' + \dfrac{2Du^\lambda u^{\lambda+1}}{m}$ i, com que, per una raó similar, $\dfrac{2Du^\lambda}{mr}$ és enter, serà $t^{2\lambda+1} \equiv t' \,(\text{mòd.}\, r)$. Finalment, es troba $u^{2\lambda+1} = u' + \dfrac{2t^{\lambda+1}u^\lambda}{m}$, i, com que $2t^{\lambda+1}$ és divisible per m, i u^λ, per r, serà $u^{2\lambda+1} \equiv u' \,(\text{mòd.}\, r)$. *Q. E. D.*

D'altra banda, la utilitat de les dues observacions darreres apareixerà en el que segueix.

202. Un cas particular del problema, a saber, resoldre l'equació $tt - Duu = 1$, ja va ser tractat pels geòmetres del segle precedent. El molt sagaç Fermat va proposar aquest problema als analistes anglesos, i Wallis esmenta Brounker com a descobridor de la solució que transmet a *Alg. Cap.* 98*, Opp. T. II p.* 418 *s.*; Ozanam, a Fermat; i, finalment, l'il·lm. Euler, qui tractà d'allò a *Comm. Petr. VI p.* 175*, Comm. nou. XI p.* 28* *Algebra, P. II, p.* 226*, Opusc. An. I, p.* 310., a Pell, d'on aquell problema ha estat anomenat per alguns autors *de Pell.* Totes aquestes solucions, mirades en essència, concorden amb la que obtenim si a l'article 198 prenem la forma reduïda en què $a = 1$; no obstant això, que les operacions que es descriuen *acaben* necessàriament a la fi, o sigui, que el problema sempre és *realment resoluble*, ningú abans de l'il·lm. La Grange no va demostrar-ho rigorosament,** *Melanges de la Soc. de Turin T. IV p.* 19, i, més elegantment, a *Hist. de l'Ac. de Berlin,*

* En aquest comentari, l'algoritme que vàrem exposar a l'article 32 utilitza notacions similars, cosa que vàrem negligir de notar allà.

** El que, per a aquest fi, Wallis va portar més enllà al lloc citat, p. 427, 428, no té cap importància. El paralogisme consisteix

1767*, p.* 237. Aquesta disquisició també apareix als *suplements a l'Àlgebra d'Euler*, ja elogiats sovint. D'altra banda, el nostre mètode (obtingut de principis totalment diferents, i no restringit al cas $m = 1$) proporciona sovint més camins per a arribar a la solució, ja que en l'article 198 podem partir de qualsevol altra forma reduïda $(a,\ b,\ -a')$.

203. PROBLEMA. *Si les formes* Φ*,* ϕ*, són equivalents, exhibir totes les transformacions de l'una en l'altra.*

Solució. Quan aquestes formes són equivalents només d'una única manera (és a dir, o bé només pròpiament, o bé només impròpiament) se cerca, per l'article 196, una transformació de la forma ϕ en Φ; sigui aquesta, $\alpha,\ \beta,\ \gamma,\ \delta$; i és clar que no se'n poden donar altres que les que siguin similars a aquesta. Però quan ϕ, Φ, equivalen tant pròpiament com impròpiament, se cerquen dues transformacions dissemblants; és a dir, l'una pròpia i l'altra impròpia, posem $\alpha,\ \beta,\ \gamma,\ \delta$ i $\alpha',\ \beta',\ \gamma',\ \delta'$, i qualsevol altra transformació serà similar, o bé a aquesta, o bé a aquella. Així, si la forma ϕ és $(a,\ b,\ c)$; el seu determinant $= D$; el màxim comú divisor dels nombres $a,\ 2b,\ c$ (com sempre en el que precedeix), m; i $t,\ u$, formalment, són tots els nombres que satisfan l'equació $tt - Duu = mm$; en el primer cas, totes les transformacions de la forma ϕ en Φ estaran contingudes en la

---

en què a la p. 428 l. 4 suposa que, proposada una quantitat p, es poden trobar nombres enters a, z, tals que $\frac{z}{a}$ sigui menor que p, però el defecte, menor que un *d'assignat*. Això és veritat quan el defecte *assignat* és una *quantitat donada*, però no quan depèn de a i z, de manera que és variable, com succeeix en el cas present.

primera de les fórmules I següents; en el darrer, o bé en la primera I, o bé en la segona II.

$$\text{(I)}\qquad \begin{array}{ll} \frac{1}{m}(\alpha t-(\alpha b+\gamma c)u), & \frac{1}{m}(\beta t-(\beta b+\delta c)u),\\ \frac{1}{m}(\gamma t+(\alpha a+\gamma b)u), & \frac{1}{m}(\delta t+(\beta a+\delta b)u), \end{array}$$

(II)

$$\begin{array}{ll} \frac{1}{m}(\alpha' t-(\alpha' b+\gamma' c)u), & \frac{1}{m}(\beta' t-(\beta' b+\delta' c)u),\\ \frac{1}{m}(\gamma' t+(\alpha' a+\gamma' b)u), & \frac{1}{m}(\delta' t+(\beta' a+\delta' b)u). \end{array}$$

Exemple. Es desitgen totes les transformacions de la forma (129, 92, 65) en la forma (42, 59, 81). A l'article 195 vàrem trobar que aquestes només són impròpiament equivalents, i a l'article següent vàrem trobar una transformació impròpia d'aquella en aquesta, -47, -56, 73, 87. Per la qual cosa, totes les transformacions de la forma (129, 92, 65) en (42, 59, 81) s'expressaran per la fórmula $-(47t+421u)$, $-(56t+503u)$, $73t+653u$, $87t+780u$, on t, u, són formalment tots els nombres que satisfan l'equació $tt-79uu=1$; aquests, però, s'expressen per les fórmules

$$\pm t=\frac{1}{2}\left((80+9\sqrt{79})^e+(80-9\sqrt{79})^e\right),$$
$$\pm u=\frac{1}{2\sqrt{79}}\left((80+9\sqrt{79})^e-(80-9\sqrt{79})^e\right),$$

on per e s'han d'agafar tots els nombres enters no negatius.

204. Es copsa que la fórmula general que expressa totes les transformacions surt *més simple* com més simple sigui la transformació inicial de la qual s'ha deduït la fórmula. Ara, com que és arbitrària, arribaríem a una transformació que moltes vegades la fórmula general pot transformar en més simple, si de la fórmula trobada primer es dedueix una transformació més simple atribuint a t, u, valors determinats, i després es compon d'aquesta una altra fórmula. Així, *per exemple*, posant $t = 80$, $u = -9$, en la fórmula trobada en l'exemple de l'article precedent, apareix una transformació més simple que aquella de què havíem partit, això és, 29, 47, -37, -60, d'on es dedueix la fórmula general $29t-263u$, $47t - 424u$, $-37t + 337u$, $-60t + 543u$. Així, quan s'ha trobat la fórmula general pels preceptes precedents, es podrà intentar si, atribuint a t, u, valors determinats $\pm t'$, $\pm u'$; $\pm t''$, $\pm u''$, etc., s'obtindria una transformació més simple que aquella de la qual la fórmula fou deduïda, cas en què d'aquella transformació es podrà derivar una fórmula més simple. D'altra banda, quan cal decidir la simplicitat, resta quelcom d'arbitrari, per la qual cosa valdria la pena si ens poguéssim contenir en una norma fixa i assignar *límits* a la progressió t', u'; t'', u''; etc., més enllà dels quals les transformacions apareixerien contínuament menys senzilles, així que no seria necessari progressar més enllà, sinó que seria suficient emprendre l'intent entre aquells; no obstant això, com que, sovint, pels mètodes que hem prescrit, se sol produir la transformació més simple, o bé immediatament, o bé usant els valors $\pm t'$, $\pm u'$, per t, u, per abreujar, suprimim aquesta disquisició.

205. Problema. *Trobar totes les representacions d'un nombre donat M per una fórmula donada $axx +$*

$2bxy + cyy$, el determinant de la qual és positiu i no quadrat $= D$.

Solució. Observem, primer, que la investigació de les representacions per valors de x, y, no primers entre si, completament de la mateixa manera que més amunt (article 181) per a les formes de determinant negatiu, es pot reduir aquí al cas en què se cerquen les representacions per valors de les indeterminades primers entre si, cosa que, doncs, seria superflu repetir aquí. Però, per a la possibilitat de representacions per valors de x, y, primers entre si, es requereix que D sigui residu quadràtic de M, i si tots els valors de l'expressió $\sqrt{D}\,(\text{mòd.}\,M)$ són N, $-N$; N', $-N'$; N'', $-N''$; etc. (que és lícit agafar de manera que cap no sigui $> \frac{1}{2}M$), qualsevol representació del nombre M per la forma proposada pertanyerà a algun d'aquests valors. Així, s'hauran de trobar abans tots aquells valors; i, a continuació, investigar les representacions que pertanyen a cadascun. Només es donaran representacions que pertanyin al valor N si les formes (a, b, c) i $\left(M, N, \frac{NN-D}{M}\right)$ són pròpiament equivalents; si ho són, se cerca alguna transformació pròpia de la primera en la darrera, sigui aquesta α, β, γ, δ. Llavors, es tindrà la representació del nombre M per la forma (a, b, c) pertanyent al valor N, $x = \alpha$, $y = \gamma$, i totes les representacions que pertanyen a aquest valor s'expressaran per la fórmula $x = \frac{1}{m}(\alpha t - (\alpha b + \gamma c)u)$, $y = \frac{1}{m}(\gamma t + (\alpha a + \gamma b)u)$, on m designa el màxim comú divisor dels nombres a, $2b$, c; i t, u, formalment, tots els nombres que satisfan l'equació $tt - Duu = mm$. D'altra banda, és evident que aquesta fórmula general surt més simple com més simple sigui la

transformació α, β, γ, δ, de la qual s'ha deduït; per tant, no serà inútil descobrir abans la transformació més simple de la forma $(a,\ b,\ c)$ en $\left(M,\ N,\ \dfrac{NN-D}{M}\right)$ segons l'article precedent, i deduir la fórmula d'aquesta. Completament de la mateixa manera es poden expressar per fórmules generals les representacions que pertanyen als valors restants, $-N$, N', $-N'$, etc. (si aquestes es donen).

Exemple. Se cerquen totes les representacions del nombre 585 per la fórmula $42xx + 62xy + 21yy$. Pel que pertany a les representacions per valors de x, y, no primers entre si, és clar immediatament que no se'n poden donar altres que les del tipus en què el màxim comú divisor de x, y, sigui 3, ja que 585 només és divisible pel quadrat 9. Així, quan s'han descobert totes les representacions per la forma $42x'x' + 62x'y' + 21y'y'$ del nombre $\dfrac{585}{9}$, és a dir, 65, en què x' és primer amb y', totes les representacions del nombre 585 per la forma $42xx + 62xy + 21yy$ en què x, y, són primers entre si es derivaran d'elles posant $x = 3x'$, $y = 3y'$. Els valors de l'expressió $\sqrt{79}\,(\text{mòd. } 65)$ són ± 12, ± 27. Una representació del nombre 65 que pertany al valor -12, es troba $x' = 2$, $y' = -1$; en conseqüència, totes les representacions de 65 pertanyents a aquest valor s'expressaran per la fórmula $x' = 2t - 41u$, $y' = -t + 53u$, de manera que totes les representacions de 585 originades *d'aquesta*, per la fórmula $x = 6t - 123u$, $y = -3t + 159u$. De manera similar, es troba la fórmula general que expressa totes les representacions del nombre 65 que pertanyen al valor -12, $x' = 22t - 199u$, $y' = -23t + 211u$; i la fórmula que inclou totes les representacions del nombre 585 originades d'aquesta, $x = 66t - 597u$, $y = -69t + 633u$. En canvi,

cap representació del nombre 65 no pertany als valors $+27$ i -27. Per a trobar les representacions del nombre 585 per valors de x, y, primers entre si, primer convé trobar els valors de l'expressió $\sqrt{79}$ (mòd. 585), que són ± 77, ± 103, ± 157, ± 248. Es troba que cap representació no pertany als valors ± 77, ± 103, ± 248; però, al valor -157, pertany la representació $x = 3$, $y = 1$, d'on es dedueix la fórmula general que expressa totes les representacions que pertanyen a aquest valor, $x = 3t - 114u$, $y = t + 157u$; i, similarment, es troba la representació que pertany a -157, $x = 83$, $y = -87$, i la fórmula en què estan contingudes totes les semblants, $x = 83t - 746u$, $y = -87t + 789u$. Així, es tenen quatre fórmules generals en les quals estan contingudes totes les representacions del nombre 585 per la forma $42xx + 62xy + 21yy$,

$$\begin{aligned} &x = 6t - 123u, \qquad && y = -3t + 159u, \\ &x = 66t - 597u, \qquad && y = -69t + 633u, \\ &x = 3t - 114u, \qquad && y = t + 157u, \\ &x = 83t - 746u, \qquad && y = -87t + 789u, \end{aligned}$$

on t, u, denoten formalment tots els nombres enters que satisfan l'equació $tt - 79uu = 1$.

Per abreujar, no ens entretenim en aplicacions especials de les disquisicions precedents de les formes de determinant positiu no quadrat, ja que qualsevol les podrà obtenir sense dificultat, per pròpia iniciativa, de manera similar als articles 176, 182, i passem immediatament a les formes de determinant positiu quadrat, que són les úniques que encara resten.

206. Problema. *Proposada la forma* (a, b, c), *de determinant quadrat* hh, *on* h *designa la seva arrel*

positiva, trobar una forma (A, B, C)*, pròpiament equivalent a ella, en la qual* A *estigui comprès entre els límits* 0 *i* $2h-1$*, inclusivament,* B *sigui* $= h$*,* $C = 0$*.*

Solució. I. Com que $hh = bb - ac$, serà $(h-b) : a = c : -(h+b)$. Sigui aquesta raó igual a la raó $\beta : \delta$ de manera que β sigui primer amb δ, i es determinen α, γ de manera que sigui $\alpha\delta - \beta\gamma = 1$, coses que es podran fer. Per la substitució α, β, γ, δ, la forma (a, b, c) es transforma en (a', b', c'), que, doncs, serà pròpiament equivalent a aquella. Es tindrà, però, $b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = (h-b)\alpha\delta + b(\alpha\delta + \beta\gamma) - (h+b)\beta\gamma = h(\alpha\delta - \beta\gamma) = h$; $c' = a\beta\beta + 2b\beta\delta + c\delta\delta = (h-b)\beta\delta + 2b\beta\delta - (h+b)\beta\delta = 0$. Així, si, a sobre, a' ja està situat entre els límits 0 i $2h-1$, la forma (a', b', c') satisfarà totes les condicions.

II. Però si a' està fora dels límits 0 i $2h-1$, sigui A el residu mínim positiu de a' segons el mòdul $2h$, que, evidentment, estarà situat entre aquests límits, i es posa $A - a' = 2hk$. Llavors, la forma (a', b', c'), és a dir, $(a', h, 0)$, es transformarà, per la substitució $1, 0, k, 1$, en la forma $(A, h, 0)$, que serà pròpiament equivalent a les formes (a', b', c'), (a, b, c) i satisfarà totes les condicions. D'altra banda, es copsa que la forma (a, b, c) es transforma en la forma $(A, h, 0)$ per la substitució $\alpha + \beta k, \beta, \gamma + \delta k, \delta$.

Exemple. Sigui proposada la forma $(27, 15, 8)$, el determinant de la qual és $= 9$. Aquí, $h = 3$; la raó $-12 : 27 = 8 : -18$, en nombres mínims, és igual a la raó $4 : -9$. Així, posats $\beta = 4$, $\delta = -9$, $\alpha = -1$, $\gamma = 2$, la forma (a', b', c') resulta $(-1, 3, 0)$, que es transforma en la forma $(5, 3, 0)$ per la substitució $1, 0, 1, 1$. Així,

doncs, aquesta és la forma buscada, i la proposada es transforma en ella per la substitució pròpia 3, 4, −7, −9.

Anomenarem *formes reduïdes* les tals formes (A, B, C) en què $C = 0$, $B = h$, i A està situat entre els límits 0 i $2h$; les quals, doncs, s'han de distingir curosament de les formes reduïdes de determinant negatiu o bé positiu no quadrat.

207. Teorema. *Dues formes reduïdes* (a, h, 0), (a', h, 0) *no idèntiques, no poden ser pròpiament equivalents.*

Dem. En efecte, si se suposa que equivalen pròpiament, la primera es transformarà en la darrera per una substitució pròpia α, β, γ, δ, i es tindran les quatre equacions $a\alpha\alpha+2h\alpha\gamma = a'$ ... [1], $a\alpha\beta+h(\alpha\delta+\beta\gamma) = h$ ... [2], $a\beta\beta + 2h\beta\delta = 0$ ... [3], $\alpha\delta - \beta\gamma = 1$ ... [4]. Multiplicant la segona equació per β, la tercera per α, i restant, resulta $-h(\alpha\delta-\beta\gamma)\beta = \beta h$, o sigui, per causa de [4], $-\beta h = \beta h$; d'on, necessàriament, $\beta = 0$. Per tant, de [4], $\alpha\delta = 1$ i $\alpha = \pm 1$. D'aquí, de [1], $a \pm 2h\gamma = a'$, equació que només pot ser consistent si $\gamma = 0$ (ja que, per hipòtesi, tant a com a' estan compresos entre 0 i $2h - 1$); *és a dir*, si $a = a'$, o sigui, si les formes (a, h, 0), (a', h, 0) són idèntiques, contràriament a la hipòtesi.

D'aquí, els problemes següents, que per a determinants no quadrats presentaven una dificultat molt més gran, es podran resoldre sense dificultat.

I. *Proposades dues formes F, F', del mateix determinant quadrat, investigar si equivalen pròpiament.* Se

cerquen dues formes reduïdes pròpiament equivalents a les formes F, F', respectivament; si aquestes són idèntiques, les proposades seran pròpiament equivalents; si no, no ho seran.

II. *Posades aquestes, investigar si equivalen impròpiament o no.* Sigui G una forma oposada a alguna de les proposades, *per exemple*, a la forma F; si aquesta equival pròpiament a la forma F', F i F' equivaldran impròpiament, i contràriament.

208. Problema. *Proposades dues formes pròpiament equivalents F, F', de determinant hh, trobar una transformació pròpia de l'una en l'altra.*

Solució. Equivalgui pròpiament la forma reduïda Φ a la forma F, i així, per hipòtesi, aquesta també equivaldrà pròpiament a la forma F'. Se cerca, per l'article 206, una transformació pròpia de la forma F en Φ, sigui aquesta α, β, γ, δ; i una transformació pròpia de la forma F' en Φ, que sigui α', β', γ', δ'. Llavors, Φ es transformarà en F' per la substitució pròpia δ', $-\beta'$, $-\gamma'$, α', i, d'aquí, F en F' per la substitució pròpia $\alpha\delta' - \beta\gamma'$, $\beta\alpha' - \alpha\beta'$, $\gamma\delta' - \delta\gamma'$, $\delta\alpha' - \gamma\beta'$.

Val la pena desenvolupar una altra fórmula per a aquesta transformació de la forma F en F' per a la qual no sigui certament necessari conèixer la forma reduïda Φ. Suposem que la forma F és (a, b, c), $F' = (a', b', c')$, $\Phi = (A, h, 0)$. Com que la raó $\beta : \delta$ és igual a les raons $(h - b) : a$, o bé $c : -(h + b)$, en nombres mínims, es copsa fàcilment que $\dfrac{h-b}{\beta} = \dfrac{a}{\delta}$ serà *enter*,

sigui aquest $= f$; també $\frac{c}{\beta} = \frac{-h-b}{\delta}$ serà enter, que es posa $= g$. Es tindrà, però, $A = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma$, de manera que $\beta A = a\alpha\alpha\beta + 2b\alpha\beta\gamma + c\beta\gamma\gamma$, o sigui (substituïts $\delta(h-b)$ en lloc de $a\beta$ i βg en lloc de c), $\beta A = \alpha\alpha\delta h + b(2\beta\gamma - \alpha\delta)\alpha + \beta\beta\gamma\gamma g$, o sigui (a causa que $b = -h - \delta g$), $\beta A = 2\alpha(\alpha\delta - \beta\gamma)h + (\alpha\delta - \beta\gamma)^2 g = 2\alpha h + g$. De manera similar, $\delta A = a\alpha\alpha\delta + 2b\alpha\gamma\delta + c\gamma\gamma\delta = \alpha\alpha\delta\delta f + b(2\alpha\delta - \beta\gamma)\gamma - \beta\gamma\gamma h = (\alpha\delta - \beta\gamma)^2 f + 2\gamma(\alpha\delta - \beta\gamma)h = 2\gamma h + f$. Per tant, $\alpha = \frac{\beta A - g}{2h}$, $\gamma = \frac{\delta A - f}{2h}$. Completament de la mateixa manera, posats $\frac{h-b'}{\beta'} = \frac{\alpha'}{\delta'} = f'$, $\frac{c'}{\beta'} = \frac{-h-b'}{\delta'} = g'$, resulta $\alpha' = \frac{\beta' A - g'}{2h}$, $\gamma' = \frac{\delta' A - f'}{2h}$. Substituïts aquests valors de α, γ, α', γ', en la fórmula transmesa fa un moment per a la transformació de la forma F en F', es transforma en la $\frac{\beta f' - \delta' g}{2h}$, $\frac{\beta' g - \beta g'}{2h}$, $\frac{\delta f' - \delta' f}{2h}$, $\frac{\beta' f - \delta g'}{2h}$, de la qual A ha desaparegut totalment.

Si es proposen dues formes impròpiament equivalents F, F', i se cerca una transformació impròpia de l'una en l'altra, sigui la forma G oposada a la forma F, i α, β, γ, δ, una transformació pròpia de la forma G en F'. Llavors, és evident que α, β, $-\gamma$, $-\delta$, serà una transformació impròpia de la forma F en F'.

Finalment, és clar que si les formes proposades són equivalents, d'una banda, pròpiament, i, de l'altra, impròpiament, es poden trobar d'aquesta manera dues transformacions, l'una pròpia i l'altra impròpia.

209. Així, ja només resta que ensenyem com es dedueixen d'una transformació totes les restants similars. Això depèn, però, de la solució de l'equació indeterminada $tt - hhuu = mm$, on m designa el màxim comú divisor dels nombres a, $2b$, c, si (a, b, c) és alguna de les formes equivalents. Però aquesta equació sempre es pot resoldre només de dues maneres, a saber, posant, o bé $t = m$, $u = 0$, o bé $t = -m$, $u = 0$. En efecte, suposem que encara es dóna una altra solució $t = T$, $u = U$, de manera que U no és $= 0$. Com que mm divideix certament $4hh$, serà $\frac{4TT}{mm} = \frac{4UUhh}{mm} + 4$, i tant $\frac{4TT}{mm}$ com $\frac{4UUhh}{mm}$, quadrats enters. Però es copsa sense dificultat que el nombre 4 no pot ser la diferència de dos quadrats enters, llevat que el quadrat menor sigui 0, és a dir, $U = 0$, contràriament a la hipòtesi. Així, si la forma F es transforma en la forma F' per la substitució α, β, γ, δ, no es donarà cap altra transformació similar a aquesta excepte la transformació $-\alpha$, $-\beta$, $-\gamma$, $-\delta$. Per tant, si les dues formes equivalen o bé només pròpiament, o bé només impròpiament, només es donaran *dues* transformacions; però si tant pròpiament com impròpiament, *quatre*, a saber, dues pròpies i dues impròpies.

210. Teorema. *Si dues formes reduïdes* $(a,\ h,\ 0)$, $(a',\ h,\ 0)$, *són impròpiament equivalents, serà* $aa' \equiv mm\,(\text{mòd. } 2mh)$, *on* m *designa el màxim comú divisor dels nombres* a, $2h$, *o bé* a', $2h$; *i, recíprocament, si* a, $2h$; a', $2h$, *tenen el mateix màxim comú divisor,* m, *i és* $aa' \equiv mm\,(\text{mòd. } 2mh)$, *les formes* $(a,\ h,\ 0)$, $(a',\ h,\ 0)$, *seran impròpiament equivalents.*

Dem. I. Es transforma la forma $(a,\ h,\ 0)$ en la forma $(a',\ h,\ 0)$ per la substitució impròpia α, β, γ, δ,

de manera que es tinguin les quatre equacions $a\alpha\alpha + 2h\alpha\gamma = a'$ ... [1]; $a\alpha\beta + h(\alpha\delta + \beta\gamma) = h$ ... [2]; $a\beta\beta + 2h\beta\delta = 0$ ... [3]; $\alpha\delta - \beta\gamma = -1$ ... [4]. D'aquí se segueix, multiplicant [4] per h i restant de [2], cosa que expressem així [2] $- h$[4], $(a\alpha + 2h\gamma)\beta = 2h$ ... [5]; similarment, de $\gamma\delta$[2]$-\gamma\gamma$[3]$-(a+a\beta\gamma+h\gamma\delta)$[4], esborrat el que es destrueix, $-a\alpha\delta = a + 2h\gamma\delta$, o sigui, $-(a\alpha + 2h\gamma)\delta = a$ ... [6]; finalment, de a[1], $a\alpha(a\alpha + 2h\gamma) = aa'$, o sigui, $(a\alpha + 2h\gamma)^2 - aa' = 2h\gamma(a\alpha + 2h\gamma)$, o sigui, $(a\alpha + 2h\gamma)^2 \equiv aa' \,(\text{mòd. } 2h(a\alpha + 2h\gamma))$. ... [7]. Ara, de [5] i [6] se segueix que $a\alpha + 2h\gamma$ divideix $2h$ i a, de manera que, també, m, que és el màxim comú divisor de a, $2h$; evidentment, però, m també dividirà $a\alpha + 2h\gamma$; per tant, necessàriament, $a\alpha + 2h\gamma$ serà $= +m$ o bé $= -m$. D'aquí se segueix immediatament, de [7], que $mm \equiv aa' \,(\text{mòd. } 2mh)$, *Q. E. P.*

II. Si a, $2h$; a', $2h$, tenen el mateix màxim comú divisor, m, i, a sobre, és $aa' \equiv mm \,(\text{mòd. } 2mh)$, els $\frac{a}{m}$, $\frac{2h}{m}$, $\frac{a'}{m}$, $\frac{aa' - mm}{2mh}$, seran enters. Però es confirma fàcilment que la forma $(a,\ h,\ 0)$ es transforma en $(a',\ h,\ 0)$ per la substitució $-\frac{a'}{m}$, $-\frac{2h}{m}$, $\frac{aa' - mm}{2mh}$, $\frac{a}{m}$, i que aquesta transformació és impròpia. Per tant, aquelles formes seran impròpiament equivalents. *Q. E. S.*

D'aquí, també es pot decidir immediatament si alguna forma reduïda donada $(a,\ h,\ 0)$ és impròpiament equivalent a ella mateixa. Això és, designat per m el màxim comú divisor dels nombres a, $2h$, haurà de ser $aa \equiv mm \,(\text{mòd. } 2mh)$.

211. S'obtenen totes les formes reduïdes de determinant donat hh, si en la forma indefinida $(A,\ h,\ 0)$ se substitueix A per tots els nombres des de 0 fins a $2h-1$, inclusivament; així, la seva quantitat serà $2h$. Es copsa que totes les formes de determinant hh es poden distribuir en tantes *classes*, i que aquestes tindran les mateixes propietats esmentades, a com hem arribat més amunt (articles 175, 195) per a les classes de formes de determinant negatiu i positiu no quadrat. Així, totes les formes de determinant 25 es distribuiran en deu classes, que es podran distingir per les formes reduïdes contingudes a cadascuna. Aquestes formes reduïdes són (0, 5, 0), (1, 5, 0), (2, 5, 0), (5, 5, 0), (8, 5, 0), (9, 5, 0), que, simultàniament, equivalen impròpiament a si mateixes; (3, 5, 0), a la qual equival impròpiament (7, 5, 0); (4, 5, 0), a la qual equival impròpiament (6, 5, 0).

212. PROBLEMA. *Trobar totes les representacions d'un nombre donat M per una forma donada $axx + 2bxy + cyy$ de determinant hh.*

La solució d'aquest problema es pot atacar a partir dels principis de l'article 168 completament de la mateixa manera que més amunt (articles 180, 181, 205) hem mostrat per a les formes de determinant negatiu i positiu no quadrat; cosa que, com que no està subjecta a cap dificultat, seria superflu repetir aquí. Contràriament, no ho serà deduir la solució d'un altre principi que és propi del cas present.

Posats, com en els articles 206, 208, $(h-b) : a = c : -(h+b) = \beta : \delta$; $\dfrac{h-b}{\beta} = \dfrac{a}{\delta} = f$; $\dfrac{c}{\beta} = \dfrac{-h-b}{\delta} = g$,

es prova sense dificultat que la forma proposada és el producte dels factors $\delta x - \beta y$ i $fx - gy$. D'on és evident que qualsevol representació del nombre M per la forma proposada dóna lloc a una descomposició del nombre M en dos factors. Així, si d, d', d'', etc., són tots els divisors del nombre M (incloent-hi també 1 i M, i cadascun d'ells posat *dues* vegades, tant positivament com negativament), és clar que s'obtenen totes les representacions del nombre M si es posa, successivament, $\delta x - \beta y = d$, $fx - gy = \frac{M}{d}$, $\delta x - \beta y = d'$, $fx - gy = \frac{M}{d'}$, etc., es desenvolupen d'aquí els valors de x, y, i es rebutgen aquelles representacions on x o bé y obtenen valors fraccionaris. Però, evidentment, de les dues primeres equacions se segueix $x = \frac{\beta M - gdd}{(\beta f - \delta g)d}$, $y = \frac{\delta M - fdd}{(\beta f - \delta g)d}$, valors que sempre són *determinats*; d'això és evident que $\beta f - \delta g = 2h$, de manera que el denominador no és, certament, $= 0$. D'altra banda, també s'haurien pogut resoldre els problemes restants a partir del mateix principi, posem la descomposició en dos factors de qualsevol forma de determinant quadrat; però també hem preferit utilitzar aquí un mètode anàleg al que hem transmès més amunt per a les formes de determinant no quadrat.

Exemple. Se cerquen totes les representacions del nombre 12 per la forma $3xx + 4xy - 7yy$. Aquesta es descompon en els factors $x - y$ i $3x + 7y$. Tots els divisors del nombre 12 són ± 1, 2, 3, 4, 6, 12. Posats $x - y = 1$, $3x + 7y = 12$, resulta $x = \frac{19}{10}$, $y = \frac{9}{10}$, valors que s'han de rebutjar perquè són fraccionaris. De la mateixa manera, dels divisors -1, ± 3, ± 4, ± 6, ± 12, s'obtenen valors inútils; del divisor $+2$, però, s'obtenen els valors $x = 2$, $y = 0$, i del divisor -2, els $x = -2$, $y = 0$;

així, doncs, excepte aquestes dues representacions, no se'n donen altres.

Aquest mètode no es pot aplicar si $M = 0$. En aquest cas, és evident que tots els valors de x, y, han de satisfer, o bé l'equació $\delta x - \beta y = 0$, o bé la $fx - gy = 0$. Però totes les solucions de la primera equació es contenen en la fórmula $x = \beta z$, $y = \delta z$, on z designa formalment un nombre enter qualsevol (sempre que, tal com se suposa, β i δ siguin primers entre si); i, similarment, posant $= m$ el màxim comú divisor dels nombres f, g, totes les solucions de la darrera equació s'expressaran per la fórmula $x = \frac{gz}{m}$, $y = \frac{fz}{m}$. Per tant, aquestes dues fórmules generals comprendran, en aquest cas, totes les representacions del nombre M.

* * *

En les [proposicions] que precedeixen, ha estat explicat de manera que sembla que no es pot desitjar res més tot allò que pertany al coneixement de l'equivalència i la recerca de totes les transformacions de formes i també la investigació de totes les representacions de nombres donats per formes donades. Així, només resta que ensenyem a decidir, proposades dues formes que no poden ser equivalents a causa de la *desigualtat dels determinants*, si una està continguda en l'altra i, en aquest cas, a trobar totes les transformacions d'aquella en aquesta.

213. Més amunt, en els articles 157, 158, hem mostrat que si una forma f de determinant D implica una forma F de determinant E i es transforma en ella per la substitució α, β, γ, δ, serà $E = (\alpha\delta - \beta\gamma)^2 D$; i,

que si és $\alpha\delta - \beta\gamma = \pm 1$, la forma f no només implica la forma F, sinó que és equivalent a ella; i, en conseqüència, si f implica F però no equival a ella, el quocient $\frac{E}{D}$ és un enter més gran que 1. Així, el problema que cal resoldre aquí serà *decidir si una forma donada f de determinant D implica una forma donada F de determinant Dee*, on se suposa que e és un nombre positiu més gran que 1. Enllestirem aquesta feina de manera que ensenyem a assignar una quantitat finita de formes contingudes en f que siguin disposades de manera que, si F està continguda en f, necessàriament hagi d'equivaler a alguna d'elles.

I. Suposem que tots els divisors (positius) del nombre e (incloent-hi també 1 i e) són m, m', m'', etc., i que $e = mn = m'n' = m''n''$, etc. Per abreujar, designem per $(m; 0)$ la forma en què f es transforma per la substitució pròpia m, 0, 0, n; per $(m; 1)$ la forma en què f es transforma per la substitució pròpia m, 1, 0, n; etc., i, en general, per $(m; k)$ la forma en què f es transforma per la substitució pròpia m, k, 0, n. De manera similar, f es transforma en $(m'; 0)$ per la substitució pròpia m', 0, 0, n'; en $(m'; 1)$ per la m', 1, 0, n'; en $(m''; 0)$ per la m'', 0, 0, n'', etc. Totes aquestes formes estaran contingudes pròpiament en f, i el determinant de cadascuna serà $= Dee$. Designem per Ω el complex de totes les formes $(m; 0)$, $(m; 1)$, $(m; 2)$, $\ldots$, $(m; m-1)$; $(m'; 0)$, $(m'; 1)$, $\ldots$, $(m'; m'-1)$; $(m''; 0)$, etc., la quantitat de les quals serà $m + m' + m''+$ etc., i de les quals es copsa fàcilment que totes són diferents entre si.

Si, *per exemple*, la forma f és la (2, 5, 7) i $e = 5$, Ω comprendrà les sis formes següents (1; 0), (5; 0), (5;

1), (5; 2), (5; 3), (5; 4), que, si es desenvolupen, són (2, 25, 175), (50, 25, 7), (50, 35, 19), (50, 45, 35), (50, 55, 55), (50, 65, 79).

II. Ara, afirmo que si una forma F de determinant Dee està continguda pròpiament en f, necessàriament serà pròpiament equivalent a alguna de les formes de Ω. Suposem que la forma f es transforma en F per la substitució pròpia α, β, γ, δ, i serà $\alpha\delta - \beta\gamma = e$. Sigui $= n$ el màxim comú divisor pres positivament dels nombres γ, δ (que no poden ser tots dos 0 simultàniament), i $\frac{e}{n} = m$ que, evidentment, serà enter. S'agafen g, h, de manera que sigui $\gamma g + \delta h = n$ i, finalment, sigui k el residu mínim positiu del nombre $\alpha g + \beta h$ segons el mòdul m. Llavors, la forma $(m; k)$, que evidentment serà entre les formes de Ω, equivaldrà pròpiament a la forma F, i, certament, es transformarà en ella per la substitució pròpia $\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h$, $\frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g$, $\frac{\gamma}{n}$, $\frac{\delta}{n}$. Efectivament, *primer*, és evident que aquests quatre nombres són enters; *segon*, es confirma fàcilment que la substitució és pròpia; *tercer*, és clar que la forma en què $(m; k)$ es transforma per aquella substitució és la mateixa en què f es transforma* per la substitució $m\left(\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h\right) + \frac{k\gamma}{n}$, $m\left(\frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g\right) + \frac{k\delta}{n}$, γ, δ; o sigui, com que $mn = e = \alpha\delta - \beta\gamma$, de manera que $\beta\gamma + mn = \alpha\delta$, $\alpha\delta - mn = \beta\gamma$, per la $\frac{1}{n}(\alpha\gamma g + \alpha\delta h)$, $\frac{1}{n}(\beta\gamma g + \beta\delta h)$, γ,

* Ja que aquesta es transforma en $(m; k)$ per la substitució m, k, 0, n. Vegeu l'article 159.

δ; o sigui, finalment, com que $\gamma g + \delta h = n$, per la α, β, γ, δ; és a dir, per hipòtesi, en F. Per tant, $(m;\ k)$ i F seran pròpiament equivalents. *Q. E. D.*

D'això, doncs, sempre es pot decidir si alguna forma donada f de determinant D implica pròpiament una forma F de determinant Dee. Si se cerca, però, si f implica impròpiament F, només s'ha d'investigar si la forma oposada a F està continguda pròpiament en f, article 159.

214. Problema. *Proposades dues formes, f, de determinant D, i F, de determinant Dee, la primera de les quals implica pròpiament la darrera, exhibir totes les transformacions pròpies de la forma f en F.*

Solució. Si Ω designa el mateix complex de formes que a l'article precedent, s'extreuen d'aquest complex totes les formes a què F equival pròpiament, siguin Φ, Φ', Φ'', etc., aquestes. Qualsevol d'aquestes formes proveirà, d'aquesta manera, de transformacions pròpies de la forma f en F, i, certament, [formes] diferents [transformacions] diferents (és a dir, totes diferents), però totes [les formes] totes [les transformacions] (és a dir, no hi haurà cap transformació pròpia de la forma f en F que no sigui originada per una de les formes Φ, Φ', etc.). Com que el mètode és el mateix per a totes les formes Φ, Φ', etc., només parlarem d'una.

Suposem que Φ és $(M;\ K)$ i que $e = MN$, de manera que f es transforma en Φ per la substitució pròpia M, K, 0, N. A més a més, es designen formalment per $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$, totes les transformacions pròpies de la forma Φ en F. Llavors, evidentment, f es transformarà en Φ

per la substitució pròpia $M\mathfrak{a} + K\mathfrak{c}$, $M\mathfrak{b} + K\mathfrak{d}$, $N\mathfrak{c}$, $N\mathfrak{d}$, i, d'aquesta manera, de qualsevol transformació pròpia de la forma Φ en F, se seguirà una transformació pròpia de la forma f en F. Les formes restants, Φ', Φ'', etc., s'han de tractar de la mateixa manera; cada una de les transformacions pròpies de cadascuna en F originarà una transformació pròpia de la forma f en F.

Perquè es vegi que aquesta solució és completa en tots els sentits, s'haurà de mostrar que:

I. *D'aquesta manera, s'obtenen totes les transformacions pròpies possibles de la forma f en F.* Sigui α, β, γ, δ, una transformació pròpia qualsevol de la forma f en F, i, com a l'article precedent, II, n el màxim comú divisor dels nombres γ, δ; també, de la mateixa manera que allà, determinats nombres m, g, h, k. Llavors, la forma $(m;\ k)$ estarà entre les formes Φ, Φ', etc., i $\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h$, $\frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g$, $\frac{\gamma}{n}$, $\frac{\delta}{n}$, serà alguna de les transformacions pròpies d'aquesta forma en F; d'aquesta, però, per la regla transmesa fa un instant, s'obté la transformació α, β, γ, δ; tot això s'ha demostrat a l'article precedent.

II. *Totes les transformacions produïdes d'aquesta manera són diferents entre si; o sigui, cap no es troba dues vegades.* Certament, es copsa sense dificultat que moltes transformacions diferents de les formes Φ o bé Φ' etc. en F no poden produir la mateixa transformació de la forma f en F; però, també, que formes diferents, per exemple Φ i Φ', no poden produir la mateixa transformació, es demostra així. Suposem que la transformació pròpia α, β, γ, δ, de la forma f en F, s'obté *tant* de la transformació pròpia $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$, de la forma Φ en F, *com*

de la transformació pròpia $\mathfrak{a}'$, $\mathfrak{b}'$, $\mathfrak{c}'$, $\mathfrak{d}'$, de la forma Φ' en F. Sigui $\Phi = (M;\ K)$, $\Phi' = (M';\ K')$, $e = MN = M'N'$. Així, es tindran les equacions $\alpha = M\mathfrak{a} + K\mathfrak{c} = M'\mathfrak{a}' + K'\mathfrak{c}'$ ... [1], $\beta = M\mathfrak{b} + K\mathfrak{d} = M'\mathfrak{b}' + K'\mathfrak{d}'$ ... [2], $\gamma = N\mathfrak{c} = N'\mathfrak{c}'$ ... [3], $\delta = N\mathfrak{d} = N'\mathfrak{d}'$ ... [4], $\mathfrak{a}\mathfrak{d} - \mathfrak{b}\mathfrak{c} = \mathfrak{a}'\mathfrak{d}' - \mathfrak{b}'\mathfrak{c}' = 1$ ... [5]. De $\mathfrak{a}$[4] − $\mathfrak{b}$[3], i amb l'ajut de l'equació [5], se segueix que $N = N'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}')$; per tant, que N' divideix N; similarment, de $\mathfrak{a}'$[4] − $\mathfrak{b}'$[3] resulta que $N(\mathfrak{a}'\mathfrak{d} - \mathfrak{b}'\mathfrak{c}) = N'$; per tant, N divideix N'; d'on, com que s'ha suposat que tant N com N' són positius, serà, necessàriament, $N = N'$ i $M = M'$ i, d'aquí, de [3] i [4], $\mathfrak{c} = \mathfrak{c}'$, $\mathfrak{d} = \mathfrak{d}'$. A més a més, de $\mathfrak{a}$[2]−$\mathfrak{b}$[1] resulta que $K = M'(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}') = M(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'$, d'aquí $K \equiv K'$ (mòd. M), que només pot ser si $K = K'$, ja que tant K com K' estan compresos entre els límits 0 i $M - 1$. Per la qual cosa, les formes Φ, Φ', no són diferents, contràriament a la hipòtesi.

D'altra banda, és clar que si D fos negatiu o bé un quadrat positiu, per aquest mètode es podrien trobar, realment, totes les transformacions pròpies de la forma f en F; però si D és positiu no quadrat, es podran assignar certes fórmules generals en les quals estaran contingudes totes les transformacions pròpies (la quantitat de les quals és infinita).

Finalment, si la forma F està continguda impròpiament en la forma f, es podran exhibir fàcilment totes les transformacions impròpies d'aquella en aquesta pel mètode indicat. Això és, si se suposa que α, β, γ, δ, designa formalment totes les transformacions pròpies de la forma f en la forma que és oposada a la forma F, totes les transformacions impròpies de la forma f en F s'exhibiran per α, $-\beta$, γ, $-\delta$.

Exemple. Es desitgen totes les transformacions de la forma (2, 5, 7) en (275, 0, −1), que està continguda en ella tant pròpiament com impròpiament. Ja a l'article precedent hem transmès el complex de les formes Ω per a aquest cas; fet l'examen, es troba que tant (5; 1) com (5; 4) equivalen pròpiament a la forma (275, 0, −1). Totes les transformacions pròpies de la forma (5; 1), *és a dir*, (50, 35, 19), en (275, 0, −1), per la nostra teoria explicada més amunt, es troben contingudes en la fórmula general $16t - 275u$, $-t + 16u$, $-15t + 275u$, $t - 15u$, on t, u, designen formalment tots els nombres enters que satisfan l'equació $tt - 275uu = 1$; per tant, totes les transformacions pròpies de la forma (2, 5, 7) en (275, 0, −1) originades d'aquí estaran contingudes en la fórmula general $65t + 1100u$, $-4t + 65u$, $-15t + 275u$, $t - 15u$. De manera similar, totes les transformacions pròpies de la forma (5; 4), *és a dir*, (50, 65, 79), en (275, 0, −1) es contenen en la fórmula general $14t + 275u$, $t + 14u$ $-15t - 275u$, $-t - 15u$, de manera que totes les transformacions pròpies de la forma (2, 5, 7) en (275, 0, −1) originades d'aquí, en la $10t + 275u$, $t + 10u$, $-15t - 275u$, $-t - 15u$. Aquestes dues fórmules, doncs, inclouen totes les transformacions pròpies buscades. De la mateixa manera, però, es troba que totes les transformacions impròpies de la forma (2, 5, 7) en (275, 0, −1) estan contingudes en les dues fórmules següents: (I) … $65t - 1100u$, $4t - 65u$, $-15t + 275u$, $-t + 15u$; i (II) … $10t + 275u$, $-t - 10u$, $-15t - 275u$, $t + 15u$.

215. Fins aquí, hem exclòs de totes les disquisicions les formes de determinant 0; així, perquè la nostra teoria arribi a ser completa en tots sentits, encara cal afegir quelcom sobre elles. Com que s'ha demostrat en

general que, si alguna forma de determinant D implica una forma de determinant D', D' és múltiple de D, és clar a l'instant que una forma el determinant de la qual és $= 0$ només pot implicar una altra forma el determinant de la qual també sigui $= 0$. Per tant, només resten per resoldre dos problemes, això és: 1r. *Proposades dues formes f, F, la darrera de les quals té determinant* 0*, decidir si la primera implica la posterior o no i, en aquell cas, exhibir totes les transformacions d'aquella en aquesta.* 2n. *Trobar totes les representacions d'un nombre donat per una forma donada de determinant* 0. El primer problema requereix un mètode quan el determinant de la primera forma f també és 0, un altre quan no és 0. Ara exposarem tot això.

I. Abans que res, observem que qualsevol forma $axx+2bxy+cyy$ el determinant de la qual és $bb-ac=0$ es pot expressar així: $m(gx+hy)^2$, on g, h, denoten nombres primers entre si, m un enter. En efecte, sigui m el màxim comú divisor de a, c, agafat amb el mateix signe amb què aquests nombres són afectats (es copsa fàcilment que aquests no poden tenir signes oposats), i $\frac{a}{m}$, $\frac{c}{m}$, seran enters no negatius primers entre si, el seu producte $= \frac{bb}{mm}$, és a dir, quadrat, de manera que ells mateixos quadrats (article 21). Sigui $\frac{a}{m} = gg$, $\frac{c}{m} = hh$, i g, h, també seran primers entre si, $gghh = \frac{bb}{mm}$, i $gh = \pm\frac{b}{m}$. D'aquí, és clar que $m(gx \pm hy)^2$ serà $= axx + 2bxy + cyy$.

Ara, siguin proposades dues formes f, F, totes dues de determinant 0, i, certament, sigui $f = m(gx + hy)^2$, $F = M(GX+HY)^2$, de manera que g sigui primer amb h, G, amb H. Llavors, afirmo que, si la forma f implica la forma F, o bé m és igual a M, o bé, almenys, divideix M i el quocient és un quadrat; i recíprocament, si $\frac{M}{m}$ és un quadrat enter, F està continguda en f. En efecte, si se suposa que f es transforma en F per la substitució $x = \alpha X + \beta Y$, $y = \gamma X + \delta Y$, serà $\frac{M}{m}(GX+HY)^2 = ((\alpha g+\gamma h)X+(\beta g+\delta h)Y)^2$, d'on se segueix fàcilment que $\frac{M}{m}$ és un quadrat. Es posa $= ee$, i serà $e(GX + HY) = \pm((\alpha g + \gamma h)X + (\beta g + \delta h)Y)$; és a dir, $\pm eG = \alpha g + \gamma h$, $\pm eH = \beta g + \delta h$; així, si es determinen $\mathfrak{G}$, $\mathfrak{H}$, de manera que sigui $\mathfrak{G}G + \mathfrak{H}H = 1$, serà $\pm e = \mathfrak{G}(\alpha g+\gamma h)+\mathfrak{H}(\beta g+\delta h)$, de manera que *enter. Q. E. P.* Però si, recíprocament, se suposa que $\frac{M}{m}$ és un quadrat enter $= ee$, la forma f implicarà la forma F. Això és, es podran determinar enters α, β, γ, δ, de manera que resulti $\alpha g + \gamma h = \pm eG$, $\beta g + \delta h = \pm eH$. En efecte, s'agafen enters $\mathfrak{g}$, $\mathfrak{h}$, de manera que resulti $\mathfrak{g}g + \mathfrak{h}h = 1$, i aquelles equacions se satisfaran posant $\alpha = \pm eG\mathfrak{g} + hz$, $\gamma = \pm eG\mathfrak{h} - gz$, $\beta = \pm eH\mathfrak{g} + hz'$, $\delta = \pm eH\mathfrak{h} - gz'$, si s'atribueixen a z, z', valors enters qualssevol; per tant, F estarà continguda en f. *Q. E. S.* Simultàniament, s'entén sense dificultat que aquestes fórmules exhibeixen tots els valors que poden prendre α, β, γ, δ; és a dir, totes les transformacions de la forma f en F, si se suposa que z, z', representen formalment tots els nombres enters.

II. Proposades dues formes $f = axx+2bxy+cyy$, el determinant de la qual no és $= 0$, i $F = M(GX+HY)^2$, el determinant de la qual és $= 0$ (on G, H, designen, com abans, nombres primers entre si), afirmo, *primer*, que si f implica F, el nombre M es pot representar per la forma f; *segon*, que si M es pot representar per f, F està continguda en f; *tercer*, que si, en aquest cas, totes les representacions del nombre M per la forma f s'expressen formalment per $x = \xi$, $y = \nu$, totes les transformacions de la forma f en F s'expressen per $G\xi$, $H\xi$, $G\nu$, $H\nu$. Demostrem tot això de la manera següent.

1r. Suposem que f es transforma en F per la substitució α, β, γ, δ, i s'agafen els nombres $\mathfrak{G}$, $\mathfrak{H}$, de manera que sigui $\mathfrak{G}G + \mathfrak{H}H = 1$. Llavors, és evident que si es posa $x = \alpha\mathfrak{G} + \beta\mathfrak{H}$, $y = \gamma\mathfrak{G} + \delta\mathfrak{H}$, el valor de la forma f resulta M, de manera que M és representable per la forma f.

2n. Si se suposa que és $a\xi\xi + 2b\xi\nu + c\nu\nu = M$, és evident que, per la substitució $G\xi$, $H\xi$, $G\nu$, $H\nu$, la forma f es transforma en F. Però que,

3r, en aquest cas, la substitució $G\xi$, $H\xi$, $G\nu$, $H\nu$, representa *totes* les transformacions de la forma f en F, si se suposa que ξ, ν, representen tots els valors de x, y, que facin $f = M$, es copsa així. Sigui α, β, γ, δ, una transformació qualsevol de la forma f en F i, com abans, $\mathfrak{G}G+\mathfrak{H}H = 1$. Llavors, entre els valors de x, y, també hi haurà els $x = \alpha\mathfrak{G} + \beta\mathfrak{H}$, $y = \gamma\mathfrak{G} + \delta\mathfrak{H}$, dels quals s'obté la substitució $G(\alpha\mathfrak{G} + \beta\mathfrak{H})$, $H(\alpha\mathfrak{G} + \beta\mathfrak{H})$, $G(\gamma\mathfrak{G} + \delta\mathfrak{H})$, $H(\gamma\mathfrak{G} + \delta\mathfrak{H})$; o sigui, $\alpha + \mathfrak{H}(\beta G - \alpha H)$, $\beta + \mathfrak{G}(\alpha H - \beta G)$, $\gamma + \mathfrak{H}(\delta G - \gamma H)$, $\delta + \mathfrak{G}(\gamma H - \delta G)$. Però, com que $a(\alpha X+\beta Y)^2+2b(\alpha X+\beta Y)(\gamma X+\delta Y)+c(\gamma X+\delta Y)^2 =$

$M(GX + HY)^2$, serà $a(\alpha\delta - \beta\gamma)^2 = M(\delta G - \gamma H)^2$, $c(\beta\gamma - \alpha\delta)^2 = M(\beta G - \alpha H)^2$, de manera que (com que el determinant de la forma f multiplicat per $(\alpha\delta - \beta\gamma)^2$ és igual al determinant de la forma F, és a dir, $= 0$, de manera que, també, $\alpha\delta - \beta\gamma = 0$) $\delta G - \gamma H = 0$, $\beta G - \alpha H = 0$. D'aquí, aquella substitució es transforma en la α, β, γ, δ, d'on és clar que la fórmula transmesa proporciona *totes* les transformacions de la forma f en F.

III. Resta que ensenyem a exhibir totes les representacions d'un nombre donat per una forma donada de determinant 0. Sigui $m(gx + hy)^2$ aquesta forma, i és clar immediatament que aquell nombre ha de ser divisible per m i el quocient, un quadrat. Així, si el nombre proposat es considera $= mee$, es copsa que per als valors de x, y, per als quals resulti $m(gx + hy)^2 = mee$, per als mateixos, $gx + hy$ resultarà, o bé $= +e$, o bé $= -e$. Per tant, es tindran totes les representacions si s'han descobert totes les solucions en enters de les equacions lineals $gx + hy = +e$, $gx + hy = -e$. Se sap, però, que aquestes són resolubles (sempre que g, h, són primers entre si, com se suposa). Això és, si es determinen $\mathfrak{g}$, $\mathfrak{h}$, de manera que sigui $\mathfrak{g}g + \mathfrak{h}h = 1$, la primera equació se satisfarà posant $x = \mathfrak{g}e + hz$, $y = \mathfrak{h}e - gz$; la darrera fent $x = -\mathfrak{g}e + hz$, $y = -\mathfrak{h}e - gz$, on z denota un enter qualsevol. Simultàniament, però, aquestes fórmules expressen *tots* els valors enters de x, y, si se suposa que z designa formalment un nombre enter qualsevol.

* * *

A aquestes disquisicions hi afegim, com a colofó,

216. Problema. *Trobar totes les solucions en nombres enters de l'equació general indeterminada* de segon grau que conté dues incògnites* $axx+2bxy+cyy+2dx+2ey+f=0$ *(on a, b, c, etc., són enters donats qualssevol).*

Solució. En lloc de les incògnites x, y, introduïm les altres $p=(bb-ac)x+be-cd$ i $q=(bb-ac)y+bd-ae$, que, evidentment, sempre seran enteres quan x, y, són enteres. Fet això, es tindrà l'equació $app+2bpq+cqq+f(bb-ac)^2+(bb-ac)(aee-2bde+cdd)=0$, o sigui, posat, per abreujar, el nombre $f(bb-ac)^2+(bb-ac)(aee-2bde+cdd)=-M$, la $app+2bpq+cqq=M$. En el que precedeix, ja hem ensenyat a trobar totes les solucions d'aquesta equació, és a dir, totes les representacions del nombre M per la forma $(a,\ b,\ c)$. Però si de cadascun dels valors de p, q, es determinen els valors corresponents de x, y, amb l'ajut de les equacions $x=\dfrac{p+cd-be}{bb-ac}$, $y=\dfrac{q+ae-bd}{bb-ac}$, es copsa fàcilment que tots aquests valors satisfan l'equació proposada i que no es dóna cap valor enter de x, y, que no s'obtingui d'aquesta manera. Per consegüent, si de tots els valors de x, y produïts així rebutgem els valors fraccionaris, quedaran totes les solucions cercades.

Sobre aquesta solució, s'ha d'observar el següent.

* Si es proposés una equació en la qual el coeficient segon, quart, o bé cinquè no fos parell, multiplicada per 2 rebria la forma que suposem aquí.

1r. Si, o bé M no es pot representar per la forma (a, b, c), o bé de cap representació no se segueixen valors *enters* de x, y, l'equació no es podrà resoldre en enters de cap manera.

2n. Quan el determinant de la forma (a, b, c), és a dir, el nombre $bb - ac$, és negatiu, o bé positiu quadrat i, simultàniament, M no és $= 0$, la quantitat de representacions del nombre M per la forma (a, b, c) serà finita i, en conseqüència, també la quantitat de totes les solucions de l'equació proposada (si aquestes, en veritat, es donen) serà finita.

3r. Quan $bb - ac$ és positiu no quadrat, o bé un quadrat i, simultàniament, $M = 0$, el nombre M es podrà representar *d'infinites maneres diferents* per la forma (a, b, c), si [s'hi pot representar] d'alguna manera; però, com que és impossible trobar totes *aquestes* representacions i temptejar si originen valors enters o fraccionaris de x, y, és necessari transmetre una regla per la qual, quan, per casualitat, cap representació no pot proporcionar en absolut valors enters de x, y, puguem estar *segurs* d'aquest fet (efectivament, per moltes representacions que fossin *temptejades* en aquest cas, sense aquesta regla mai no arribaríem a la certesa); però quan algunes representacions donen valors enters de x, y, altres, fraccionaris, s'haurà d'ensenyar de quina manera es poden distingir *a priori*, en general, aquestes d'aquelles.

4t. Quan $bb - ac = 0$, no es poden determinar de cap manera els valors de x, y, per les fórmules precedents; per tant, s'haurà d'investigar *un mètode especial* per a aquest cas.

217. Per al cas en què $bb-ac$ és un nombre positiu no quadrat, hem ensenyat més amunt que totes les representacions del nombre M per la forma $app+2bpq+cqq$ (si se'n dóna alguna) es poden expressar per una o bé per més fórmules tals com $p=\frac{1}{m}(\mathfrak{A}t+\mathfrak{B}u)$, $q=\frac{1}{m}(\mathfrak{C}t+\mathfrak{D}u)$, on $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, denoten nombres enters donats, m el màxim comú divisor dels nombres a, $2b$, c, i, finalment, t, u, formalment, tots els nombres enters que satisfan l'equació $tt-(bb-ac)uu=mm$. Com que tots els valors de t, u, es poden agafar tant positivament com negativament, per a cada una d'aquelles formes podrem substituir de *quatre* maneres $p=\frac{1}{m}(\mathfrak{A}t+\mathfrak{B}u)$, $q=\frac{1}{m}(\mathfrak{C}t+\mathfrak{D}u)$; $p=\frac{1}{m}(\mathfrak{A}t-\mathfrak{B}u)$, $q=\frac{1}{m}(\mathfrak{C}t-\mathfrak{D}u)$; $p=\frac{1}{m}(-\mathfrak{A}t+\mathfrak{B}u)$, $q=\frac{1}{m}(-\mathfrak{C}t+\mathfrak{D}u)$; $p=-\frac{1}{m}(\mathfrak{A}t+\mathfrak{B}u)$, $q=-\frac{1}{m}(\mathfrak{C}t+\mathfrak{D}u)$; de manera que la quantitat de totes les fórmules és ara quatre vegades més gran que abans, però t i u no expressen més tots els nombres que satisfan l'equació $tt-(bb-ac)uu=mm$, sinó només els positius. Així, s'haurà de considerar qualsevol d'aquestes formes separadament, i investigar quins valors de t, u, proporcionen valors enters de x, y.

De la fórmula $p=\frac{1}{m}(\mathfrak{A}t+\mathfrak{B}u)$, $q=\frac{1}{m}(\mathfrak{C}t+\mathfrak{D}u)$, ... [1], se segueixen $x=\frac{\mathfrak{A}\,t+\mathfrak{B}\,u+mcd-mbe}{m(bb-ac)}$, $y=\frac{\mathfrak{C}\,t+\mathfrak{D}\,u+mae-mbd}{m(bb-ac)}$, com a valors de x, y. Però, més amunt, hem mostrat que tots els valors (positius) de t constitueixen una progressió recurrent t^0, t', t'',

etc.; similarment, els valors corresponents de u també formen una sèrie recurrent u^0, u', u'', etc.; a part, es pot assignar un nombre ρ tal que, segons un mòdul donat qualsevol, resulti $t^\rho \equiv t^0$, $t^{\rho+1} \equiv t'$, $t^{\rho+2} \equiv t''$, etc., $u^\rho \equiv u^0$, $u^{\rho+1} \equiv u'$, etc. Per a aquest mòdul, agafarem el nombre $m(bb - ac)$ i, per abreujar, designarem els valors de x, y, que es produeixen posant $t = t^0$, $u = u^0$, i als quals atribuirem l'índex 0, per x^0, y^0; i, similarment, els que es produeixen fent $t = t'$, $u = u'$, per x', y', als quals atribuirem l'índex 1, etc. Llavors, es copsarà sense dificultat que si x^h, y^h, fossin nombres enters i ρ determinat degudament, també $x^{h+\rho}$, $y^{h+\rho}$, no menys $x^{h+2\rho}$, $y^{h+2\rho}$, i, en general, $x^{h+k\rho}$, $y^{h+k\rho}$, seran enters; i, contràriament, si x^h o bé y^h és fracció, també $x^{h+k\rho}$ o bé $y^{h+k\rho}$ serà fracció. D'aquí es conclou fàcilment que si es desenvolupen els valors de x, y, a què corresponen els índexs 0, 1, 2, …, $\rho - 1$, i per a cap d'aquests índexs *ni* x *ni* y no és enter, no es donarà en absolut cap índex per al qual tant x com y rebin valors enters, cas en què, de la fórmula [1], no es podran deduir valors enters de x, y. Però, si entre aquells índexs n'hi ha alguns, posem μ, μ', μ'', etc., als quals corresponen valors enters de x, y, tots els valors enters de x, y, que, certament, es poden obtenir de la fórmula [1] seran aquells els índexs dels quals estiguin continguts en alguna de les fórmules $\mu + k\rho$, $\mu' + k\rho$, $\mu'' + k\rho$, etc., on k denota formalment tots els nombres enters positius, inclòs també el zero.

Les fórmules restants, en què estan continguts els valors de p, q, s'han de tractar exactament de la mateixa manera. Si ocorregués que no s'obtinguessin valors enters de x, y, de cap de totes aquestes fórmules, l'equació proposada no es podria resoldre en absolut en enters de

cap manera; però, quan realment és resoluble, totes les solucions en enters es podran expressar pels preceptes transmesos en el que precedeix.

218. Quan $bb - ac$ és un nombre quadrat i $M = 0$, tots els valors de p, q, estaran compresos en dues fórmules del tipus $p = \mathfrak{A}z$, $q = \mathfrak{B}z$; $p = \mathfrak{A}'z$, $q = \mathfrak{B}'z$, on z designa formalment qualsevol nombre enter, però $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{A}'$, $\mathfrak{B}'$ són enters donats, el primer dels quals amb el segon, el tercer amb el quart, no tenen cap divisor comú (article 212). Així, tots els valors enters de x, y, originats per la primera fórmula estaran continguts en la fórmula

$$[1] \qquad x = \frac{\mathfrak{A}z + cd - be}{bb - ac}, \quad y = \frac{\mathfrak{B}z + ae - bd}{bb - ac},$$

i tots els restants, originats per la segona fórmula, en la

$$[2] \qquad x = \frac{\mathfrak{A}'z + cd - be}{bb - ac}, \quad y = \frac{\mathfrak{B}'z + ae - bd}{bb - ac}.$$

Però com que totes dues fórmules també poden proporcionar valors fraccionaris (llevat que $bb - ac = 1$), és necessari que separem, en cada una de les dues fórmules, els valors de z que transformen en enters tant x com y, dels restants; no obstant això, és suficient considerar només la primera, ja que per a l'altra s'ha d'aplicar exactament el mateix mètode.

Com que $\mathfrak{A}$, $\mathfrak{B}$, són primers entre si, serà lícit determinar dos nombres $\mathfrak{a}$, $\mathfrak{b}$, de manera que resulti $\mathfrak{A}\mathfrak{a} + \mathfrak{B}\mathfrak{b} = 1$. Fet això, es té $(\mathfrak{a}x + \mathfrak{b}y)(bb - ac) = z + \mathfrak{a}(cd - be) + \mathfrak{b}(ae - bd)$, d'on és clar immediatament que tots els valors de z que puguin produir valors enters

de x, y, han de ser congrus necessàriament al nombre $\mathfrak{a}(be-cd)+\mathfrak{b}(bd-ae)$ segons el mòdul $bb-ac$, o sigui, han d'estar continguts en la fórmula $(bb-ac)z'+\mathfrak{a}(be-cd)+\mathfrak{b}(bd-ae)$, on z' designa formalment un nombre enter. D'aquí, fàcilment, en lloc de la fórmula [1], obtenim la següent

$$x=\mathfrak{A}z'+\mathfrak{b}\frac{\mathfrak{A}(bd-ae)-\mathfrak{B}(be-cd)}{bb-ac}$$
$$y=\mathfrak{B}z'-\mathfrak{a}\frac{\mathfrak{A}(bd-ae)-\mathfrak{B}(be-cd)}{bb-ac},$$

que és evident que proporciona, o bé per a tots els valors de z', o bé per a cap, valors enters de x, y; i, certament, el primer cas sempre tindrà lloc quan $\mathfrak{A}(bd-ae)$ i $\mathfrak{B}(be-cd)$ són congrus segons el mòdul $bb-ac$, el darrer quan són incongrus. S'haurà de tractar la fórmula [2] completament de la mateixa manera, i separar les solucions en enters (si pot proporcionar aquestes) de les restants.

219. Quan $bb-ac=0$, la forma $axx+2bxy+cyy$ es podrà expressar així: $m(\alpha x+\beta y)^2$, on m, α, β són enters (article 215). Es posa $\alpha x+\beta y=z$, i l'equació proposada es transforma en la $mzz+2dx+2ey+f=0$, d'on, i de $z=\alpha x+\beta y$, es dedueix que $x=\dfrac{\beta mzz+2ez+\beta f}{2\alpha e-2\beta d}$, $y=\dfrac{\alpha mzz+2dz+\alpha f}{2\beta d-2\alpha e}$. Ara, és clar que, llevat que fos $\alpha e=\beta d$ (cas que considerarem separadament tot seguit), els valors de x, y, deduïts d'aquestes fórmules atribuint a z un valor qualsevol satisfan l'equació proposada; per tant, no resta res més, sinó que ensenyem a determinar aquells valors de z dels quals se segueixen valors enters de x, y.

Com que $\alpha x + \beta y = z$, necessàriament per a z només es poden agafar nombres *enters*; a part, però, és evident que si algun valor de z produeix tant x com y enter, tots els valors de z congrus a ell segons el mòdul $2\alpha e - 2\beta d$ produeixen igualment valors enters. Així, si se substitueix z per tots els nombres enters des de 0 fins a $2\alpha e - 2\beta d - 1$ (quan $\alpha e - \beta d$ és positiu) o bé fins a $2\beta d - 2\alpha e - 1$ (quan $\alpha e - \beta d$ és negatiu) inclusivament, i per a cap d'aquests valors ni x ni y resulten enters, cap valor en absolut de z no produirà valors enters de x, y, i l'equació proposada no es podrà resoldre en enters de cap manera; però, si alguns d'aquells valors de z procuren valors enters de x, y, posem ζ, ζ', ζ'', etc. (que també és lícit trobar per la solució de congruències de segon grau, segons els principis de la Secció IV), es produiran *totes* les solucions posant $z = (2\alpha e - 2\beta d)v + \zeta$, $z' = (2\alpha e - 2\beta d)v + \zeta'$, etc., on v designa formalment tots els nombres enters.

220. Per al cas que hem exclòs, en què $\alpha e = \beta d$, és oportú indagar un mètode peculiar. Suposem que α, β, són primers entre si, que se sap per l'article 215, I, que és lícit, i $\dfrac{d}{\alpha} = \dfrac{e}{\beta}$ serà un nombre enter (article 19), que posarem $= h$. Llavors, l'equació proposada indueix la forma $(m\alpha x + m\beta y + h)^2 - hh + mf = 0$, i, evidentment, no es pot resoldre racionalment llevat que $hh - mf$ sigui un nombre quadrat. Sigui $hh - mf = kk$, i és clar que, a l'equació proposada, equivalen les dues següents: $m\alpha x + m\beta y + h + k = 0$, $m\alpha x + m\beta y + h - k = 0$; *és a dir*, qualsevol solució de l'equació proposada també satisfà alguna d'aquestes equacions, i recíprocament. Evidentment, la primera equació no es pot resoldre en enters llevat que $h + k$ sigui divisible per m, i, similar-

ment, la darrera no admetrà solució en enters llevat que $h - k$ sigui divisible per m. Aquestes dues condicions, però, són suficients per a la resolubilitat d'una i altra equació (ja que se suposa que α, β, són primers entre si), i totes les solucions es podran expressar segons les regles conegudes.

221. Il·lustrem amb un exemple el cas considerat a l'article 217 (ja que és el més difícil de tots). Sigui $xx + 8xy + yy + 2x - 4y + 1 = 0$ l'equació proposada. D'aquesta, en primer lloc, per la introducció de les altres incògnites $p = 15x - 9$, $q = 15y + 6$, es deriva l'equació $pp + 8pq + qq = -540$. Però totes les solucions en enters d'aquesta es troben contingudes en les quatre fórmules següents:

$$\begin{aligned} p &= 6t, \quad & q &= -24t - 90u, \\ p &= 6t, \quad & q &= -24t + 90u, \\ p &= -6t, \quad & q &= 24t - 90u, \\ p &= -6t, \quad & q &= 24t + 90u, \end{aligned}$$

on t, u, denoten formalment tots els nombres enters positius que satisfan l'equació $tt - 15uu = 1$, que estan aplegats a la fórmula $t = \frac{1}{2}((4 + \sqrt{15})^n + (4 - \sqrt{15})^n)$, $u = \frac{1}{2\sqrt{15}}((4+\sqrt{15})^n - (4-\sqrt{15})^n)$, si n designa formalment tots els nombres enters positius (incloent-hi també el zero). Per la qual cosa, tots els valors de x, y, estaran continguts en les fórmules

$$\begin{aligned} x &= \frac{1}{5}(2t + 3), \quad & y &= -\frac{1}{5}(8t + 30u + 2), \\ x &= \frac{1}{5}(2t + 3), \quad & y &= -\frac{1}{5}(8t - 30u + 2), \end{aligned}$$

$$x = \frac{1}{5}(-2t + 3), \quad y = \frac{1}{5}(8t - 30u - 2),$$
$$x = \frac{1}{5}(-2t + 3), \quad y = \frac{1}{5}(8t + 30u - 2).$$

Però, aplicats degudament els nostres preceptes, es troba que perquè es produeixin valors *enters* s'han d'agafar a la primera i la segona fórmules els valors de t, u, que provenen d'un índex *n parell;* però a la tercera i la quarta, els que s'obtenen de *n imparell.* Es tenen les solucions més simples $x = 1, -1, -1$; $y = -2, 0, 12$, respectivament.

D'altra banda, convé observar que la solució del problema explicat en els articles precedents es pot abreujar sovint per multitud d'artificis, sobretot pel que pertany a l'exclusió de les solucions inútils, és a dir, que impliquen fraccions; però, perquè no resultem massa extensos, estem forçats a ometre aquests en aquest lloc.

222. Com que molt del que hem explorat fins aquí també ha estat considerat per altres geòmetres, no podem silenciar el seu mèrit. L'il·lm. La Grange va instituir unes disquisicions generals de *l'equivalència de formes* a *Nouv. Mem. de l'Ac. de Berlin* 1773*, p.* 263*, i* 1775*, p.* 323 *s.*, on va ensenyar principalment que, per a qualsevol determinant donat, es dóna una quantitat finita de formes preparades de manera que qualsevol forma d'aquell determinant sigui equivalent a alguna d'elles, de manera que totes les formes de determinant donat es poden distribuir en classes. Posteriorment, el preclar Le Gendre va descobrir moltes propietats elegants d'aquesta classificació, la major part per indici, les quals transmetrem i proveirem de demostracions més avall. D'altra banda, ningú fins ara havia abordat la

distinció entre equivalència pròpia i impròpia, la utilitat de la qual és conspícua sobretot en les disquisicions més subtils.

El famós problema explicat en l'article 216 i següents va ser resolt completament en primer lloc per l'il·lm. La Grange, *Hist. de l'Ac. de Berlin* 1767*, p.* 165 *i* 1768*, p.* 181 *s.* Una solució (però menys completa) també apareix en els ja sovint lloats *Suppl. ad Euleri Algebram.* Ja abans, l'il·lm. Euler havia atacat el mateix argument, *Comm. Petr. T. VI p.* 175*; Comm. Nou. T. IX p.* 3*; Ibid. T. XVIII p.* 185 *s.*, però sempre va restringir la seva investigació a [veure] com, d'alguna solució que suposa ja coneguda, se'n deriven altres; i, a part, els seus mètodes només valen en pocs casos per a proporcionar *totes* les solucions (vegeu La Grange, *Hist. de l'Ac. de Berlin* 1767*, p.* 237). Com que l'última d'aquestes tres és del comentari donat més recent que la solució La Grangiana, que recull el problema amb tota generalitat i no deixa res a desitjar en aquest respecte, sembla que Euler en aquell moment (el tom XVIII dels Comentaris pertany a l'any 1773, i és publicat l'any 1774) encara no coneixia aquella solució. D'altra banda, la nostra solució (igual que totes les restants que hem transmès fins ara en aquesta secció) és edificada en principis completament diferents.

Les [proposicions] pertanyents a això que s'han transmès per altres com Diofant, Fermat, etc., contemplen casos molt especials; per tant, com que ja s'ha fet menció més amunt de les que han semblat dignes de recordar, evitem enumerar-les totes amb detall.

* * *

Les [proposicions] que hem exposat fins ara de les formes de segon grau s'han de tenir només com a primers elements d'aquesta doctrina; prosseguint més detalladament aquesta disquisició, se'ns ha obert un camp vastíssim, per la qual cosa exposarem en el que segueix el que sembla especialment digne d'atenció. Efectivament, aquest argument és tan fèrtil que convé fer silenci, per abreujar, de moltes altres coses que ja ara hem arribat a trobar; però moltes més, sens dubte, encara resten ocultes i esperen nous intents. D'altra banda, convé remarcar a l'instant, en el principi d'aquestes investigacions, que les formes de determinant 0 n'han estat excloses, si no s'adverteix del contrari.

223. Ja hem mostrat més amunt (articles 175, 195, 211) que, proposat un nombre enter qualsevol D (sigui positiu, sigui negatiu), es pot assignar una quantitat finita de formes F, F', F'', etc., de determinant D establertes de manera que qualsevol forma de determinant D sigui pròpiament equivalent a una d'elles i, certament, només a una única. Així, doncs, totes les formes de determinant D (la quantitat de les quals és infinita) es podran *classificar* segons aquelles formes, això és, formant la primera classe el complex de totes les formes pròpiament equivalents a la forma F, la segona, les formes que equivalen pròpiament a la forma F', etc.

De cadascuna de les classes de formes de determinant donat D s'elegeix alguna forma, i es podrà considerar com a *forma representant* de tota la classe. És completament arbitrari, certament, quina forma s'agafi de cada classe; no obstant això, sempre s'haurà de preferir la que sembla que supera les altres en *simplicitat*. La simplicitat d'alguna forma $(a,\ b,\ c)$ s'haurà d'estimar,

evidentment, per la magnitud dels nombres a, b, c, i amb raó es dirà que la forma (a', b', c') és menys simple que la (a, b, c) si $a' > a$, $b' > b$, $c' > c$. Però, d'aquí, la qüestió encara no és completament determinada i resta al nostre arbitri, *per exemple*, quina de les formes $(17, 0, -45)$, $(5, 0, -153)$ preferim tenir per més simple. No obstant això, sovint serà avantatjós observar la norma següent:

I. Quan el determinant D és negatiu, es prenen les formes reduïdes contingudes en cada classe com a formes representants; però, on en una mateixa classe es trobin dues formes reduïdes (que seran oposades, article 172), es pren aquella el terme central de la qual és positiu.

II. Quan el determinant D és positiu no quadrat, es desenvolupa el període d'alguna forma reduïda continguda en la classe proposada, en què es trobaran o bé dues formes ambigües, o bé cap (article 187).

1) En el primer cas, siguin (A, B, C), (A', B', C'), les formes ambigües; M, M', els residus mínims dels nombres B, B', segons els mòduls A, A', respectivament (que es podran agafar positivament si no són $= 0$); i, finalment, $\frac{D - MM}{A} = N$, $\frac{D - M'M'}{A'} = N'$. Fet això així, de les formes $(A, M, -N)$, $(A', M', -N')$, s'agafa com a forma representant la que sembla més simple. En aquest judici, es prefereix la forma el terme central de la qual és $= 0$; però quan el terme central és 0 o bé en totes dues o bé en cap, s'ha de preferir la que té el primer terme menor que l'altra, i quan els primers termes són iguals en magnitud i de signes diferents, s'ha de posposar el signe negatiu al positiu.

2) Però quan en tot el període no es té cap forma ambigua, s'elegeix de totes les formes del període la que té el primer terme mínim sense respectar el signe, de manera que, certament, si en el mateix període ocorren dues formes en les quals el mateix primer terme és afectat en una de signe positiu, en l'altra, de negatiu, es posposa la darrera a la primera. Sigui (A, B, C) aquesta forma i es dedueix d'ella, de la mateixa manera que en el cas precedent, l'altra $(A, M, -N)$ (posem, agafant per a M el residu mínim absolut de B segons el mòdul A, i fent $N = \frac{D - MM}{A}$), i es pren precisament aquesta com a representant.

Però si s'esdevingués que el mateix primer terme menor A fos comú a més d'una forma del període, totes aquestes formes s'hauran de tractar de la manera que hem prescrit i, de les formes produïdes, s'haurà d'assumir com a forma representant aquella el terme central de la qual ha sortit mínim.

Així, per exemple, per a $D = 305$, es té, entre altres, el període $(17, 4, -17)$, $(-17, 13, 8)$, $(8, 11, -23)$, $(-23, 12, 7)$, $(7, 16, -7)$, $(-7, 12, 23)$, $(23, 11, -8)$, $(-8, 13, 17)$, de les quals, en primer lloc, s'elegeix la forma $(7, 16, -7)$, i d'aquí es dedueix, en segon lloc, la forma representant $(7, 2, -43)$.

III) Quan el determinant és positiu quadrat $= kk$, s'extreu la forma reduïda $(A, k, 0)$ continguda en la classe proposada i, si $A < k$ o bé $= k$, es pren aquesta com a forma representant; però si $A > k$, s'assumeix en el seu lloc la forma $(A - 2k, k, 0)$, el primer terme de la qual serà negatiu però menor que k.

Exemple. D'aquesta manera, totes les formes de determinant -235 es distribueixen en setze classes, de les quals seran representants (1, 0, 235), (2, 1, 118), (4, 1, 59), (4, -1, 59), (5, 0, 47), (10, 5, 26), (13, 5, 20), (13, -5, 20), i les altres vuit diferents de les precedents només en els signes dels termes extrems, (-1, 0, -235), (-2, 1, -118), etc.

Totes les formes de determinant 79 se separen en sis classes, els representants de les quals són (1, 0, -79), (3, 1, -26), (3, -1, -26), (-1, 0, 79), (-3, 1, 26), (-3, -1, 26).

224. Així, per aquesta classificació, les formes que són pròpiament equivalents se separaran completament de les altres. Dues formes del mateix determinant D, si són de la mateixa classe, seran pròpiament equivalents; qualsevol nombre representable per una també es podrà representar per l'altra; i si un nombre qualsevol M es pot representar per la primera forma de manera que les indeterminades tinguin valors primers entre si, el mateix nombre es podrà representar per l'altra forma de la mateixa manera, i, certament, de manera que cada una de les representacions pertanyi al mateix valor de l'expressió $\sqrt{D}$ (mòd. M). Però si les dues formes pertanyen a classes diferents, no seran pròpiament equivalents; de la representabilitat d'algun nombre donat per l'una no es pot concloure la representabilitat del mateix nombre per l'altra; contràriament, si el nombre M es pot representar per una de manera que els valors de les indeterminades siguin primers entre si, immediatament estem segurs que no es dóna cap representació semblant del mateix nombre per una altra forma que pertanyi al

mateix valor de l'expressió $\sqrt{D}\,(\text{mòd. } M)$ (vegeu els articles 167, 168).

Contràriament, perquè pugui resultar que dues formes F, F', de classes diferents K, K', siguin impròpiament equivalents, cas en què *qualsevol* forma d'una classe equivaldrà impròpiament a *qualsevol* forma de l'altra, qualsevol forma de K tindrà una forma oposada a ella en K', i les classes K, K', s'anomenaran *oposades*. Així, en el primer exemple de l'article precedent, la tercera classe de formes de determinant -235 és oposada a la quarta, la setena a l'octava; en el segon exemple, la classe segona a la tercera, la cinquena a la sisena. Així, proposades dues formes qualssevol de classes oposades, qualsevol nombre M que es pot representar per una també es podrà per l'altra; això, si en una resulta per valors de les indeterminades primers entre si, en l'altra es podrà fer igualment, però de manera que aquestes dues representacions pertanyin a valors oposats de l'expressió $\sqrt{D}\,(\text{mòd. } M)$. D'altra banda, les regles transmeses més amunt per a l'elecció de les formes representants s'han establert de manera que per a classes oposades sempre es troben formes representants oposades.

Finalment, també es donen classes *oposades a si mateixes*. Això és, si alguna forma, simultàniament amb la forma oposada, es conté en la mateixa classe, es copsa fàcilment que totes les formes d'aquesta classe són equivalents entre elles tant pròpiament com impròpiament i que tenen amb elles les seves oposades. Tindrà aquest caràcter qualsevol classe en què es contingui una forma ambigua, i, recíprocament, a qualsevol classe oposada a ella mateixa es trobarà necessàriament una forma ambigua (articles 163, 165), per la qual cosa s'anomenarà

classe ambigua. Així, entre les classes de formes de determinant -235 se'n tenen vuit d'ambigües, representants de les quals són $(1, 0, 235)$, $(2, 1, 118)$, $(5, 0, 47)$, $(10, 5, 26)$, $(-1, 0, -235)$, $(-2, 1, -118)$, $(-5, 0, -47)$, $(-10, 5, -26)$; entre les classes de formes de determinant 79, dues, representants de les quals són $(1, 0, -79)$, $(-1, 0, 79)$. D'altra banda, si s'han determinat representants de les formes segons les nostres regles, d'aquí es podran conèixer sense dificultat les classes ambigües. Això és, per a un determinant positiu no quadrat, una classe ambigua obté, certament, una forma representant ambigua (article 194); per a determinant negatiu, la forma representant d'una classe ambigua serà, o bé ella mateixa ambigua, o bé tal que els seus termes externs són iguals (article 172); finalment, per a determinant positiu quadrat, es decideix fàcilment per l'article 210 si la forma representant és impròpiament equivalent a si mateixa, de manera que la classe que representa, ambigua.

225. Ja hem mostrat més amunt (article 175) que en una forma (a, b, c) de determinant negatiu els termes externs tenen els mateixos signes tant entre si com amb els termes externs de qualsevol altra forma equivalent a ella. Si a, c, són positius, anomenarem *positiva* la forma (a, b, c), i també anomenarem *classe positiva* tota la classe en què es conté (a, b, c) i que constarà només de formes positives. Contràriament, (a, b, c) serà una *forma negativa*, i continguda en una *classe negativa*, si a, c, són negatius. Per una forma positiva no es poden representar nombres negatius, ni positius per una de negativa. Si la forma (a, b, c) és representant d'alguna classe positiva, la forma $(-a, b, -c)$ serà representant d'una classe negativa, d'on se segueix que la

quantitat de classes positives és igual a la quantitat de negatives i, simultàniament, quan aquelles siguin determinades, també es tenen aquestes. En conseqüència, en les disquisicions sobre formes de determinant negatiu, sovint serà suficient considerar les classes positives, ja que les seves propietats es transfereixen fàcilment a les classes negatives.

D'altra banda, aquesta distinció només té lloc per a formes de determinant negatiu; per a formes de determinant positiu, es poden representar sense discriminació nombres positius i negatius, de manera que no és rar que, en aquest cas, s'hagin de portar dues formes tals com (a, b, c), $(-a, b, -c)$, a la mateixa classe.

226. Anomenem *primitiva* una forma qualsevol (a, b, c), si els nombres a, b, c, no tenen divisor comú; altrament, s'anomenarà *derivada* i, certament, posat $= m$ el màxim comú divisor dels nombres a, b, c, la forma (a, b, c) serà *derivada de la forma primitiva* $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$. D'aquesta definició és clar immediatament que totes les formes el determinant de les quals no sigui divisible per cap quadrat (excepte 1) són necessàriament primitives. A més a més, de l'article 161 és clar que si en alguna classe donada de formes de determinant D es troba una forma primitiva, totes les formes d'aquesta classe seran primitives, cas en què la mateixa classe s'anomenarà *primitiva*. A més a més, és evident que si una forma F de determinant D és derivada d'una forma primitiva f de determinant $\frac{D}{mm}$ i les classes en què estan contingudes les formes F, f, són K, k, respectivament, totes les formes de la classe K seran derivades de la classe pri-

mitiva k; en conseqüència, en aquest cas, anomenarem la classe K *derivada de la classe primitiva* k.

Si $(a,\ b,\ c)$ és una forma primitiva, però a, c, no són simultàniament parells (és a dir, si o bé tots dos són imparells, o bé almenys un d'ells), s'entén fàcilment que no només a, b, c, sinó també a, $2b$, c, no poden tenir cap divisor comú, cas en què la forma $(a,\ b,\ c)$ s'anomenarà *pròpiament primitiva* o bé, més simplement, *forma pròpia.* Però si $(a,\ b,\ c)$ és una forma primitiva, però ambdós nombres a, c, parells, és clar que els nombres a, $2b$, c, tenen el divisor comú 2 (que simultàniament serà el màxim), i $(a,\ b,\ c)$ s'anomenarà *forma impròpiament primitiva*, o bé, més simplement, *forma impròpia.** En aquest cas, b serà necessàriament imparell (en efecte, altrament, $(a,\ b,\ c)$ no seria una forma primitiva); per tant, serà $bb \equiv 1 \,(\text{mòd.}\, 4)$, de manera que, com que ac és divisible per 4, el determinant $bb - ac \equiv 1 \,(\text{mòd.}\, 4)$. Així, només tenen lloc formes impròpies per a un determinant de la forma $4n+1$, si és positiu, o bé de la forma $-(4n+3)$, si és negatiu. Però és evident de l'article 161 que, si en alguna classe donada es troba una forma pròpiament primitiva, totes les formes d'aquesta classe són pròpiament primitives; contràriament, una classe que implica una forma impròpiament primitiva consta només de formes impròpiament primitives. Per la qual cosa, la mateixa classe s'anomenarà, en el primer cas, *pròpiament primitiva*, o bé, més simplement, *pròpia;* en el darrer, *impròpiament primitiva*, o bé, *impròpia.* Així,

* Aquí hem elegit aquests termes *pròpiament* i *impròpiament* perquè no se'ns n'acudien d'altres més idonis, cosa que advertim perquè ningú no busqui cap nexe ocult entre aquesta significació i la que hem utilitzat a l'article 157, que no hi és. D'altra banda, certament, aquí no s'ha de témer cap ambigüitat.

per exemple, entre les classes positives de formes de determinant -235, sis són pròpies, de les quals posem representants $(1, 0, 235)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(13, 5, 20)$, $(13, -5, 20)$, i la mateixa quantitat entre les negatives; però dues són impròpies entre les unes i les altres. Totes les classes de formes de determinant 79 (com és natural per als nombres de la forma $4n+3$) són pròpies.

Si la forma (a, b, c) és derivada, i, certament, de la primitiva $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$, aquesta podrà ser o bé pròpiament o bé impròpiament primitiva. En el primer cas, m també serà el màxim comú divisor dels nombres a, $2b$, c; en el darrer, el màxim comú divisor d'aquests nombres serà $2m$. D'aquí s'entén la distinció entre *forma derivada d'una forma pròpiament primitiva* i *forma derivada d'una impròpiament primitiva;* i també (com que, a causa de l'article 161, totes les formes d'una mateixa classe es comporten igualment respecte d'això) entre *la classe derivada d'una classe pròpiament primitiva* i *la classe derivada d'una impròpiament primitiva.*

Per aquestes distincions hem obtingut el primer fonament en virtut del qual podem estructurar la distribució de totes les classes de formes de determinant donat en diferents *ordres.* Reunirem dues classes, de les quals les formes (a, b, c), (a', b', c'), són representants, en el *mateix ordre*, *tant* si els nombres a, b, c, tenen el mateix màxim comú divisor que a', b', c', *com* si a, $2b$, c, el mateix que a', $2b'$, c'; però si, d'aquestes condicions, o bé alguna o bé totes dues no tenen lloc, les classes es portaran a *ordres diferents.* D'aquí, és clar immediatament que totes les classes pròpiament primitives constitueixen

un ordre; totes les classes impròpiament primitives, un altre; si mm és un quadrat que divideix el determinant D, les classes derivades de les classes pròpiament primitives de determinant $\frac{D}{mm}$ formaran un ordre particular, i un altre les classes derivades de classes impròpiament primitives de determinant $\frac{D}{mm}$, etc. Si per cas D no és divisible per cap quadrat (excepte 1), no hi haurà ordres de classes derivades, de manera que, o bé només es donarà un ordre (quan $D \equiv 2$ o bé 3 segons el mòdul 4), posem l'ordre de les classes pròpiament primitives, o bé dos (quan $D \equiv 1 \,(\text{mòd. } 4)$), això és, l'ordre de les classes pròpiament primitives i l'ordre de les classes impròpiament primitives. Pels principis del càlcul de combinacions, s'estableix sense dificultat la regla general següent: si se suposa $D = D' 2^{2\mu} a^{2\alpha} b^{2\beta} c^{2\gamma} \cdots$, de manera que D' no impliqui cap factor quadrat i a, b, c, etc., siguin nombres primers imparells diferents (forma a la qual qualsevol nombre es pot reduir fent $\mu = 0$ quan D no és divisible per 4; i α, β, γ, etc., tots $= 0$, o sigui, el que rendeix el mateix, ometent els factors $a^{2\alpha}$, $b^{2\beta}$, $c^{2\gamma}$, etc., quan D no es pot dividir per cap quadrat imparell), es tindran, o bé $(\mu+1)(\alpha+1)(\beta+1)(\gamma+1)\cdots$ ordres, sempre que $D' \equiv 2$ o bé $3 \,(\text{mòd. } 4)$, o bé $(\mu + 2)(\alpha+1)(\beta+1)(\gamma+1)\ldots$ ordres, quan $D' \equiv 1 \,(\text{mòd. } 4)$. Però suprimim la demostració d'aquesta regla, ja que ni és difícil ni aquí tampoc necessària.

Exemple 1. Per a $D = 45 = 5 \cdot 3^2$, es tenen sis classes, representants de les quals són $(1,\ 0,\ -45)$, $(-1,\ 0,\ 45)$, $(2,\ 1,\ -22)$, $(-2,\ 1,\ 22)$, $(3,\ 0,\ -15)$, $(6,\ 3,\ -6)$. Aquestes es distribueixen en quatre ordres, això és, l'ordre I comprèn dues classes pròpies de les quals són representants $(1,\ 0,\ -45)$, $(-1,\ 0,\ 45)$; l'ordre II contin-

drà dues classes impròpies, de les quals són representants $(2, 1, -22)$, $(-2, 1, 22)$; l'ordre III contindrà una classe derivada de la pròpia de determinant 5, posem com a representant de la qual $(3, 0, -15)$; l'ordre IV constarà d'una classe derivada de la impròpia de determinant 5, posem com a representant de la qual $(6, 3, -6)$.

Exemple 2. Les classes positives de determinant $-99 = -11 \cdot 3^2$ es distribuiran entre quatre ordres: l'ordre I comprendrà les classes pròpiament primitives següents:* $(1, 0, 99)$, $(4, 1, 25)$, $(4, -1, 25)$, $(5, 1, 20)$, $(5, -1, 20)$, $(9, 0, 11)$; l'ordre II contindrà les classes impròpies $(2, 1, 50)$, $(10, 1, 10)$; l'ordre III, les classes derivades de les pròpies de determinant -11, $(3, 0, 33)$, $(9, 3, 12)$, $(9, -3, 12)$; l'ordre IV, l'única classe derivada de la impròpia de determinant -11, $(6, 3, 18)$. Les classes negatives d'aquest determinant es podran distribuir en ordres completament de la mateixa manera.

Observem que *classes oposades sempre es porten al mateix ordre*, teorema del qual la raó es copsa sense dificultat.

227. D'aquests diferents ordres, mereix sobretot la màxima atenció l'ordre de les classes pròpiament primitives. Efectivament, cada una de les classes derivades té per origen una certa classe primitiva (de determinant menor), de la consideració de les quals sovint se segueix espontàniament el que es refereix a aquelles. Més avall, però, ensenyarem que qualsevol classe impròpiament primitiva és associada quasi de la mateixa

* Mostrant, per abreujar, les formes representants en lloc de les classes que representen.

manera, o bé a una única classe pròpiament primitiva, o bé a tres (del mateix determinant). A més a més, per a determinants negatius, es podran passar per alt les classes negatives, ja que a cadascuna d'aquestes sempre corresponen certes classes positives. Així, perquè penetrem més profundament en la natura de les classes pròpiament primitives, abans que res explicarem una certa diferència essencial en virtut de la qual tot ordre de classes pròpies es pot subdividir en molts *gèneres*. Com que, fins ara, encara no hem abordat aquest importantíssim argument, ens caldrà atacar-lo íntegrament.

228. Teorema. *Per una forma pròpiament primitiva qualsevol, F, es poden representar infinits nombres no divisibles per qualsevol nombre primer donat p.*

Dem. És evident que si la forma F és $= axx + 2bxy + cyy$, p no pot dividir simultàniament tots tres nombres a, $2b$, c. Ara, quan a no és divisible per p, és clar que si per x es pren un nombre qualsevol no divisible per p, però per y un nombre divisible per p, el valor de la forma F resulta no divisible per p; quan c no és divisible per p, s'obté el mateix atribuint a x un valor divisible i a y un valor no divisible; finalment, quan tant a com c són divisibles per p, de manera que $2b$ no divisible, la forma F induirà un valor no divisible per p atribuint tant a x com a y valors qualssevol no divisibles per p. *Q. E. D.*

És evident que el teorema també té lloc per a formes *impròpiament primitives*, sempre que no sigui $p = 2$.

Com que moltes condicions d'aquest tipus, que el mateix nombre sigui divisible per alguns nombres primers donats, no divisible per altres (vegeu l'article 32), poden ser consistents simultàniament, es copsa fàcilment que es poden determinar d'infinites maneres nombres x, y, de manera que la forma primitiva $axx+2bxy+cyy$ assoleixi un valor no divisible per nombres primers donats qualssevol, dels quals únicament cal excloure 2 quan la forma és impròpiament primitiva. D'aquí és clar que es pot proposar un teorema més general així: *Per una forma primitiva qualsevol es poden representar infinits nombres que siguin primers amb un nombre qualsevol donat (imparell quan la forma és impròpiament primitiva).*

229. Teorema. *Sigui F una forma primitiva de determinant D, p un nombre primer que divideix D; llavors, els nombres no divisibles per p que es poden representar per la forma F coincideixen en què, o bé tots són residus quadràtics de p, o bé tots no-residus.*

Dem. Sigui $F = (a, b, c)$; m, m', dos nombres qualssevol no divisibles per p que es poden representar per la forma F, això és, $m = agg + 2bgh + chh$, $m' = ag'g'+2bg'h'+ch'h'$. Llavors, serà $mm' = (agg'+b(gh'+hg')+chh')^2 - D(gh'-hg')^2$; per tant, mm' serà congru a un quadrat segons el mòdul D, de manera que, també, segons p, és a dir, mm' serà un residu quadràtic de p. D'aquí se segueix que, o bé tots dos m, m', són residus quadràtics de p, o bé tots dos no-residus. *Q. E. D.*

Es prova de manera similar que quan el determinant D és divisible per 4 els nombres imparells repre-

sentables per F o bé tots són $\equiv 1$ o bé tots $\equiv 3\,(\text{mòd. } 4)$. Això és, en aquest cas, el producte de dos tals nombres sempre serà un residu quadràtic de 4, de manera que $\equiv 1\,(\text{mòd. } 4)$; per tant, o bé tots dos seran $\equiv 1$, o bé tots dos $\equiv 3$.

Finalment, quan D és divisible per 8, el producte de dos nombres imparells qualssevol que es poden representar per F serà residu quadràtic de 8 i, en conseqüència, $\equiv 1\,(\text{mòd. } 8)$. Per tant, en aquest cas, els nombres imparells representables per F, o bé tots seran $\equiv 1$, o bé tots $\equiv 3$, o bé tots $\equiv 5$, o bé tots $\equiv 7\,(\text{mòd. } 8)$.

Així, per exemple, com que el nombre 10, que és no-residu de 7, es pot representar per la forma (10, 3, 17), tots els nombres no divisibles per 7 que es poden representar per aquella forma seran no-residus de 7. Com que -3 és representable per la forma $(-3,\ 1,\ 49)$, i segons el mòdul 4 és $\equiv 1$, tots els nombres imparells representables per aquesta forma es comportaran igualment.

D'altra banda, si fos necessari per al propòsit present, podríem demostrar fàcilment que els nombres representables per la forma F no tenen tal relació fixa amb cap nombre primer que no divideixi D, sinó que, per la forma F, es poden representar indistintament tant residus com no-residus d'un nombre primer qualsevol que no divideixi D. Contràriament, respecte dels nombres 4 i 8 també té lloc en altres casos una certa analogia, que no podem ometre.

I. *Quan el determinant D d'una forma primitiva F és* $\equiv 3\,(\text{mòd. } 4)$*, els nombres imparells representables per la forma F, o bé tots seran* $\equiv 1$*, o bé tots* $\equiv 3\,(\text{mòd. } 4)$. En efecte, si m, m', són dos nombres representables per F, el producte mm' es podrà reduir a la forma $pp - Dqq$ de la mateixa manera que més amunt. Així, quan cadascun dels m, m', és imparell, necessàriament un dels nombres p, q, serà parell i l'altre imparell, de manera que un dels quadrats pp, $qq \equiv 0$, l'altre $\equiv 1\,(\text{mòd. } 4)$. D'on es dedueix fàcilment que, certament, $pp - Dqq$ és $\equiv 1\,(\text{mòd. } 4)$, de manera que, o bé tots dos m, $m' \equiv 1$, o bé tots dos $\equiv 3\,(\text{mòd. } 4)$. Així, *per exemple*, per la forma (10, 3, 17) no es poden representar altres nombres imparells que els que són de la forma $4n + 1$.

II. *Quan el determinant D d'una forma primitiva F és* $\equiv 2\,(\text{mòd. } 8)$*, tots els nombres imparells representables per F seran o bé en part* $\equiv 1$ *i en part* $\equiv 7$*, o bé en part* $\equiv 3$ *i en part* $\equiv 5\,(\text{mòd. } 8)$. En efecte, suposem que m, m', són dos nombres imparells representables per F; així, doncs, el seu producte mm' es podrà reduir a la forma $pp - Dqq$. Doncs, quan cada un dels m, m', és imparell, p haurà de ser necessàriament imparell (ja que D és parell), de manera que $pp \equiv 1\,(\text{mòd. } 8)$; però qq serà o bé $\equiv 0$, o bé $\equiv 1$, o bé $\equiv 4$, i, en conseqüència, Dqq o bé $\equiv 0$ o bé $\equiv 2$. D'aquí, $mm' = pp - Dqq$ resulta o bé $\equiv 1$ o bé $\equiv 7\,(\text{mòd. } 8)$; així, si m és o bé $\equiv 1$ o bé $\equiv 7$, m' també serà o bé $\equiv 1$ o bé $\equiv 7$; però si m és o bé $\equiv 3$ o bé $\equiv 5$, m' també serà o bé $\equiv 3$ o bé $\equiv 5$. *Per exemple*, tots els nombres imparells representables per la forma (3, 1, 5) són o bé $\equiv 3$ o bé $\equiv 5\,(\text{mòd. } 8)$, i cap nombre de la forma $8n + 1$ o bé $8n + 7$ no es pot representar per aquella forma.

III. *Quan el determinant D de la forma primitiva F és* $\equiv 6\,(\text{mòd. } 8)$*, es poden representar per aquesta forma nombres imparells, o bé només tals que són* $\equiv 1$ *i* $\equiv 3\,(\text{mòd. } 8)$*, o bé només tals que són* $\equiv 5$ *i* $\equiv 7\,(\text{mòd. } 8)$. Qualsevol podrà desenvolupar sense dificultat una demostració completament similar a la precedent (en II). Així, *per exemple*, per la forma (5, 1, 7) únicament es poden representar nombres imparells tals que són o bé $\equiv 5$ o bé $\equiv 7\,(\text{mòd. } 8)$.

230. Així, doncs, tots els nombres que es poden representar per una forma primitiva donada F de determinant D tindran una relació fixa amb cadascun dels divisors primers de D (pels quals ells mateixos no són, certament, divisibles), però els nombres imparells que es poden representar per F en cadascun dels casos també tindran una relació fixa amb els nombres 4 i 8; això és, amb 4 quan D és, o bé $\equiv 0$, o bé $\equiv 3\,(\text{mòd. } 4)$, i amb 8 quan D és, o bé $\equiv 0$, o bé $\equiv 2$, o bé $\equiv 6\,(\text{mòd. } 8)$.* Anomenarem *caràcter* o bé *caràcter particular* de la forma F la tal relació amb cadascun d'aquests nombres, i l'expressarem de la manera següent. Quan per la forma F només es poden representar residus quadràtics del nombre primer p, li atribuirem el caràcter Rp, en el cas oposat, el caràcter Np; similarment, escriurem 1, 4, quan per la forma F no es poden representar altres nombres imparells que els que són $\equiv 1\,(\text{mòd. } 4)$, d'on és clar immediatament quins caràcters s'expressaran pels símbols 3, 4; 1, 8; 3, 8; 5, 8; 7, 8. Finalment, atribuirem el caràcter 1 *i* 7, 8, a les formes per les quals només es poden represen-

* Per als determinants divisibles per 8 es pot negligir la relació amb el nombre 4, perquè, en aquest cas, ja està continguda en la relació amb 8.

tar nombres imparells tals que segons el mòdul 8 són o bé $\equiv 1$ o bé $\equiv 7$; d'això se segueix espontàniament el significat dels caràcters 3 *i* 5, 8; 1 *i* 3, 8; 5 *i* 7, 8.

Cadascun dels caràcters d'una forma primitiva donada (a, b, c) de determinant D sempre es pot conèixer per almenys un dels nombres a, c (que, evidentment, tots dos són representables per aquella forma). Efectivament, quan p és un divisor primer de D, certament un dels nombres a, c, no serà divisible per p; en efecte, si tots dos fossin divisibles per p, p també dividiria bb $(= D + ac)$ i, en conseqüència, també b, *és a dir*, la forma (a, b, c) no seria primitiva. De manera similar, en els casos en què la forma (a, b, c) té una relació fixa amb els nombres 4 o bé 8, certament, com a mínim, un dels nombres a, c, serà imparell; així, doncs, aquella relació es podrà desprendre d'això. Així, per exemple, el caràcter de la forma (7, 0, 23) respecte del nombre 23 es conclou, del nombre 7, que és $N23$; el caràcter de la mateixa forma respecte del nombre 7 es té que és $R7$, del nombre 23; finalment, el caràcter d'aquesta forma respecte del nombre 4, que és 3, 4, es pot concloure o bé del nombre 7 o bé del nombre 23.

Com que tots els nombres que es poden representar per alguna forma F continguda en una classe K també són representables per qualsevol altra forma d'aquesta classe, evidentment cadascun dels caràcters de la forma F també correspon a totes les formes restants d'aquesta classe; per això serà lícit considerar aquells com a caràcters de tota la classe. Així, cadascun dels caràcters d'una classe primitiva donada qualsevol es coneix de la seva forma representant. Classes oposades sempre tindran tots els mateixos caràcters.

231. El complex de *tots* els caràcters particulars d'una forma o bé d'una classe donada constituirà el caràcter íntegre d'aquesta forma o bé classe. Així, per exemple, el caràcter íntegre de la forma (10, 3, 17) o bé de tota la classe que representa serà 1, 4; $N7$; $N23$. De manera similar, el caràcter íntegre de la forma (7, 1, -17) serà 7, 8; $R3$; $N5$; efectivament, en aquest cas, el caràcter particular 3, 4, s'ha omès, perquè ja està contingut en el caràcter 7, 8. D'aquesta font obtenim una subdivisió de tot l'ordre de les classes pròpiament primitives (positives quan el determinant és negatiu) de determinant donat, en molts *gèneres* diferents, consignant en el mateix gènere totes les classes que tenen el mateix caràcter íntegre; i en gèneres diferents aquelles els caràcters íntegres de les quals són diferents. Però a cada gènere li atribuïm els caràcters íntegres que tenen les classes contingudes en ell. Així, per exemple, per al determinant -161 es tenen setze classes positives pròpiament primitives, que es distribueixen en quatre gèneres de la manera següent:

Caràcters	Formes representants de les classes
$1, 4; R7; R23$	$(1, 0, 161)$, $(2, 1, 81)$, $(9, 1, 18)$, $(9, -1, 18)$.
$1, 4; N7; N23$	$(5, 2, 33)$, $(5, -2, 33)$, $(10, 3, 17)$, $(10, -3, 17)$.
$3, 4; R7; N23$	$(7, 0, 23)$, $(11, 2, 15)$, $(11, -2, 15)$, $(14, 7, 15)$.
$3, 4; N7; R23$	$(3, 1, 54)$, $(3, -1, 54)$, $(6, 1, 27)$, $(6, -1, 27)$.

De la quantitat de caràcters íntegres diferents que, certament, són possibles *a priori*, es tenen les [proposicions] següents:

I. Quan el determinant D és divisible per 8, són possibles quatre caràcters particulars diferents respecte del nombre 8; el nombre 4 no proporciona cap caràcter particular (nota de l'article precedent). A part, es donen dos caràcters respecte de cada un dels divisors primers imparells de D; per tant, si la quantitat d'aquells és m, es donaran en total 2^{m+2} caràcters íntegres diferents (considerant $m = 0$ quan D és una potència de 2).

II. Quan el determinant D no és divisible per 8, però, en canvi, ho és per 4, i, a sobre, per m nombres primers imparells, es tindran, en total, 2^{m+1} caràcters íntegres diferents.

III. Quan el determinant D és parell però no divisible per 4, serà o bé $\equiv 2 \,(\text{mòd. } 8)$ o bé $\equiv 6$. En el primer cas, es donaran dos caràcters particulars respecte del nombre 8, posem 1 *i* 7, 8; i 3 *i* 5, 8; i la mateixa quantitat en el darrer cas. Així, doncs, posada $= m$ la quantitat de divisors primers imparells de D, es tindran en total 2^{m+1} caràcters íntegres diferents.

IV. Quan D és imparell, serà o bé $\equiv 1$ o bé $\equiv 3 \,(\text{mòd. } 4)$. En el darrer cas, es donen dos caràcters diferents respecte del nombre 4; en el primer cas, una tal relació no entra en el caràcter íntegre. Per tant, si m designa el mateix que abans, en el primer cas es donaran 2^m caràcters íntegres diferents; en el darrer, 2^{m+1}.

S'ha de notar molt bé, però, que d'aquí no se segueix de cap manera que realment es donin tants gèneres com caràcters diferents siguin possibles *a priori*. Certament, en el nostre exemple només la meitat d'ells corresponen efectivament a classes o sigui, a gèneres, i no es donen classes positives a les quals corresponguin els caràcters 1, 4; $R7$; $N23$ o bé 1, 4; $N7$; $R23$ o bé 3, 4; $R7$; $R23$ o bé 3, 4; $N7$; $N23$. Més avall, es tractarà més abundantment d'aquest seriosíssim argument.

Atribuirem, des d'ara, el nom de *forma principal* a la forma $(1, 0, -D)$, que, sens dubte, s'ha de tenir per la més simple entre totes les formes de determinant D; anomenarem *classe principal* tota la classe en què ella es troba; i, finalment, tot el gènere en què la classe principal està continguda s'anomenarà *gènere principal*. Així, s'han de distingir molt bé la forma principal, una forma de la classe principal i una forma del gènere principal; i també una classe principal i una classe del gènere principal. Utilitzarem sempre aquestes denominacions encara que potser, per a algun determinant, no es donin altres classes excepte la principal, o bé altres gèneres excepte el gènere principal, com, per exemple, succeeix sovint quan D és un nombre primer positiu de la forma $4n+1$.

232. Encara que el que s'ha explicat dels caràcters de les formes ha anat dirigit a la finalitat més pròxima que d'això s'obtingui la subdivisió de l'ordre *positiu pròpiament primitiu*, no obstant això res no impedeix que el mateix també s'apliqui a formes i classes negatives o bé a les impròpiament primitives; i pel mateix principi se subdivideixen en gèneres tant un ordre impròpiament primitiu positiu, com un ordre pròpiament primitiu ne-

gatiu, com un ordre impròpiament primitiu negatiu. Així, per exemple, després que l'ordre pròpiament primitiu de les formes de determinant 145 s'ha subdividit en els dos gèneres següents,

$$\begin{array}{r|l} R5, R29 & (1,0,-145),(5,0,-29) \\ N5, N29 & (3,1,-48),(3,-1,-48), \end{array}$$

també l'ordre impròpiament primitiu es pot subdividir igualment en els dos gèneres

$$\begin{array}{r|l} R5, R29 & (4,1,-36),(4,-1,-36) \\ N5, N29 & (2,1,-72),(10,5,-12); \end{array}$$

o bé, així com les classes positives de les formes de determinant -129 es distribueixen en els quatre gèneres

$$\begin{array}{r|l} 1,4;R3;N43 & (1,0,129),(10,1,13),(10,-1,13) \\ 1,4;N3;N43 & (2,1,65),(5,1,26),(5,-1,26) \\ 3,4;R3;N43 & (3,0,43),(7,2,19),(7,-2,19) \\ 3,4;N3;R43 & (6,3,23),(11,5,14),(11,-5,14), \end{array}$$

les classes negatives també se separen en els quatre ordres

$$\begin{array}{r|l} 3,4;N3;N43 & (-1,0,-129),(-10,1,-13), \\ & (-10,-1,-13) \\ 3,4;R3;R43 & (-2,1,-65),(-5,1,-26), \\ & (-5,-1,-26) \\ 1,4;N3;R43 & (-3,0,-43),(-7,2,-19), \\ & (-7,-2,-19) \\ 1,4;R3;N43 & (-6,3,-23),(-11,5,-14), \\ & (-11,-5,-14). \end{array}$$

No obstant això, com que el sistema de les classes negatives sempre surt tan similar al sistema de les positives, sovint semblarà superflu construir-los separadament. Més

avall, però, ensenyarem a reduir un ordre impròpiament primitiu a un pròpiament primitiu.

Finalment, pel que ateny als ordres derivats, no són necessàries regles noves per a la seva subdivisió. En efecte, com que qualsevol ordre derivat té l'origen en algun ordre primitiu (de determinant menor), i cada una de les classes d'aquell es correspon espontàniament a cada una d'aquest, evidentment es podrà obtenir la subdivisió de l'ordre derivat de la subdivisió de l'ordre primitiu.

233. Si la forma (primitiva) $F = (a,\ b,\ c)$ s'ha establert de manera que es puguin trobar dos nombres g, h, tals que resulti $gg \equiv a$, $gh \equiv b$, $hh \equiv c$, segons un mòdul donat m, direm que aquella forma és un residu quadràtic del nombre m, i $gx+hy$, un valor de l'expressió $\sqrt{axx + 2bxy + cyy}\,(\text{mòd.}\,m)$, o sigui, més breument, direm que $(g,\ h)$ és un valor de l'expressió $\sqrt{(a,b,c)}$, o bé $\sqrt{F}\,(\text{mòd.}\,m)$. Més generalment, si el multiplicador M, primer amb el mòdul m, és de tal naturalesa que pugui resultar $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM\,(\text{mòd.}\,m)$, direm que $M(a,\ b,\ c)$, o sigui, MF, és un residu quadràtic de m, i $(g,\ h)$, un valor de l'expressió $\sqrt{M(a,b,c)}$, o bé $\sqrt{MF}\,(\text{mòd.}\,m)$. Així, per exemple, la forma (3, 1, 54) és un residu quadràtic de 23 i (7, 10) un valor de l'expressió $\sqrt{(3,1,54)}\,(\text{mòd.}\,23)$; similarment, $(2,\ -4)$, un valor de l'expressió $\sqrt{5(10,3,17)}\,(\text{mòd.}\,23)$. L'ús d'aquestes definicions es mostrarà més avall; notin-se aquí les proposicions següents:

I. Si $M(a,\ b,\ c)$ és residu quadràtic del nombre m, aquest dividirà el determinant de la forma $(a,\ b,\ c)$. En

efecte, si $(g,\ h)$ és un valor de l'expressió $\sqrt{M(a,b,c)}$ (mòd. m), o sigui, $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM$ (mòd. m), serà $bbMM - acMM \equiv 0$, o sigui, $(bb - ac)MM$ divisible per m. Però com que se suposa que M és primer amb m, també $bb - ac$ serà divisible per m.

II. Si $M(a,\ b,\ c)$ és residu quadràtic de m, i m o bé un nombre primer o bé una potència d'un nombre primer, posem $= p^{\mu}$, el caràcter particular de la forma $(a,\ b,\ c)$ respecte del nombre p serà o bé Rp, o bé Np, segons si M és residu o bé no-residu de p. Això se segueix immediatament del fet que tant aM com cM són residus de m, o sigui, de p, i, com a mínim, un dels nombres a, c no és divisible per p (article 230).

De manera similar, si (mantenint les [hipòtesis] restants) $m = 4$, el caràcter particular de la forma $(a,\ b,\ c)$ serà o bé 1, 4, o bé 3, 4, segons que $M \equiv 1$, o bé $M \equiv 3$; i també, si $m = 8$ o bé una potència més alta del nombre 2, el caràcter particular de la forma $(a,\ b,\ c)$ serà 1, 8; 3, 8; 5, 8; 7, 8, segons que $M \equiv 1;\ 3;\ 5;\ 7$ (mòd. 8), respectivament.

III. Recíprocament, si m és un nombre primer o bé una potència d'un nombre primer imparell $= p^{\mu}$ que divideix el determinant $bb - ac$, i M o bé un residu o bé un no-residu de p segons si el caràcter de la forma $(a,\ b,\ c)$ respecte de p és Rp o bé Np, respectivament, $M(a,\ b,\ c)$ serà un residu quadràtic de m. En efecte, quan a no és divisible per p, aM serà un residu de p, de manera que també de m; així, si g és un valor de l'expressió $\sqrt{aM}$ (mòd. m), h, un valor de l'expressió $\dfrac{bg}{a}$ (mòd. m),

serà $gg \equiv aM$, $ah \equiv bg$, de manera que $agh \equiv bgg \equiv abM$ i $gh \equiv bM$; finalment, $ahh \equiv bgh \equiv bbM \equiv bbM - (bb - ac)M \equiv acM$, de manera que $hh \equiv cM$, és a dir, (g, h) un valor de l'expressió $\sqrt{M(a, b, c)}$. Però quan a és divisible per m, c certament no ho serà; d'on es copsa fàcilment que resulta el mateix si es pren per a h un valor de l'expressió $\sqrt{cM}$ (mòd. m), per a g, un valor de l'expressió $\frac{bh}{c}$ (mòd. m).

De manera similar es demostra que si m fos $= 4$ i dividís $bb - ac$, i si s'agafés el nombre M o bé $\equiv 1$ o bé $\equiv 3$ segons que el caràcter particular de la forma (a, b, c) fos 1, 4 o bé 3, 4, $M(a, b, c)$ seria un residu quadràtic de m. I també, si m fos $= 8$ o bé una potència més alta de 2 per la qual $bb - ac$ fos divisible, i si M s'agafés $\equiv 1; 3; 5; 7$ (mòd. 8) segons el que postula el caràcter particular de la forma (a, b, c) respecte del nombre 8, $M(a, b, c)$ seria un residu quadràtic de m.

IV. Si el determinant de la forma (a, b, c) és $= D$ i $M(a, b, c)$, un residu quadràtic de D, es poden conèixer immediatament a partir del nombre M tots els caràcters particulars de la forma (a, b, c) tant respecte de cadascun dels divisors primers imparells de D com respecte del nombre 4 o bé del nombre 8 (si divideixen D). Així, per exemple, com que $3(20, 10, 27)$ és un residu quadràtic de 440, això és, (150, 9) un valor de l'expressió $\sqrt{3(20, 10, 27)}$ segons el mòdul 440; i $3N5$, $3R11$; els caràcters de la forma (20, 10, 27) són 3, 8; $N5$; $R11$. Només els caràcters particulars respecte dels nombres 4 i 8, quan no divideixin el determinant, no tenen necessàriament un nexe amb el nombre M.

V. Recíprocament, si un nombre M primer amb D recull en ell tots els caràcters particulars de la forma (a, b, c) (exceptuant-ne els caràcters respecte dels nombres 4, 8, quan no divideixen D), $M(a, b, c)$ serà un residu quadràtic de D. Efectivament, de III és clar que si es converteix D en la forma $\pm A^\alpha B^\beta C^\gamma \cdots$ de manera que A, B, C, etc., siguin nombres primers diferents, $M(a, b, c)$ serà un residu quadràtic de cadascun dels A^α, B^β, C^γ, etc. Així, doncs, si un valor de l'expressió $\sqrt{M(a,b,c)}$ segons el mòdul A^α és ($\mathfrak{A}$, $\mathfrak{A}'$); segons el mòdul B^β, ($\mathfrak{B}$, $\mathfrak{B}'$); segons el mòdul C^γ, ($\mathfrak{C}$, $\mathfrak{C}'$); etc., i es determinen nombres g, h, de manera que sigui $g \equiv \mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., $h \equiv \mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, etc., segons els mòduls A^α, B^β, C^γ, etc., respectivament (article 32), es copsarà fàcilment que és $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM$, segons tots els mòduls A^α, B^β, C^γ, etc., de manera que també segons el mòdul D, que és el seu producte.

VI. Per aquestes raons, els nombres tals com M s'anomenaran *nombres característics* de la forma (a, b, c), i, per V, es podran trobar sense dificultat molts nombres d'aquesta forma al mateix temps que són descoberts tots els caràcters particulars d'aquesta forma; però els més simples sovint es troben més fàcilment temptejant. És evident que si M és un nombre característic d'una forma primitiva donada de determinant D, tots els nombres congrus a M segons el mòdul D seran nombres característics de la mateixa forma; formes contingudes en una mateixa classe, o també en classes diferents del mateix gènere, tenen els mateixos nombres característics, per la qual cosa qualsevol nombre característic d'una forma donada també es pot atribuir a tota la classe i el gènere; finalment, 1 sempre és nombre carac-

terístic de les formes de la classe i del gènere principal, o sigui, qualsevol forma del gènere principal és residu del seu determinant.

VII. Si (g, h) és un valor de l'expressió $\sqrt{M(a,b,c)}$ (mòd. m) i $g' \equiv g$, $h' \equiv h$ (mòd. m), (g', h') també serà un valor d'aquesta expressió. Tals valors es poden tenir per *equivalents;* contràriament, si (g, h), (g', h'), són valors de la mateixa expressió $\sqrt{M(a,b,c)}$, però no és $g \equiv g'$, $h \equiv h'$ (mòd. M), simultàniament, cal jutjar que són *diferents.* Evidentment, quan (g, h) és un valor de tal expressió, també ho serà $(-g, -h)$, i es demostra fàcilment que aquests valors sempre són diferents llevat que $m = 2$. Es demostra de manera igualment fàcil que l'expressió $\sqrt{M(a,b,c)}$ (mòd. m) no pot tenir més valors diferents que dos tals (oposats) quan m sigui, o bé un nombre primer imparell, o bé una potència d'un nombre primer imparell, o bé $= 4$; però quan m sigui $= 8$ o bé una potència més alta del nombre 2, en total se'n donen quatre. D'aquí es dedueix fàcilment, per VI, que si el determinant D de la forma (a, b, c) és $= \pm 2^{\mu} A^{\alpha} B^{\beta} \cdots$, on A, B, etc., designen nombres primers imparells diferents la quantitat dels quals és $= n$, i M, un nombre característic d'aquella forma, es donen en total, o bé 2^n, o bé 2^{n+1}, o bé 2^{n+2}, valors diferents de l'expressió $\sqrt{M(a,b,c)}$ (mòd. D) segons que μ sigui, o bé < 2, o bé $= 2$, o bé > 2. Així, per exemple, es tenen setze valors de l'expressió $\sqrt{7(12,6,-17)}$ (mòd. 240), posem $(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$, $(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61)$, $(\pm 78, \mp 101)$. Per abreujar, no afegim una demostració més àmplia, sobretot, ja que no és necessària per al que segueix.

VIII. Finalment, observem que si D és el determinant de dues formes equivalents $(a,\ b,\ c)$, $(a',\ b',\ c')$, M un nombre característic, i la primera es transforma en la darrera per la substitució $\alpha,\ \beta,\ \gamma,\ \delta$, de qualsevol valor de l'expressió $\sqrt{M(a,b,c)}$, com $(g,\ h)$, se segueix un valor de l'expressió $\sqrt{M(a',b',c')}$, posem $(\alpha g + \gamma h,\ \beta g + \delta h)$. Qualsevol podrà trobar la demostració sense dificultat.

234. Després que hem presentat aquestes [proposicions] de la distribució de formes en classes, gèneres i ordres, i que hem explicat les propietats generals que sorgeixen immediatament d'aquestes distincions, passem a un altre argument importantíssim, no atacat fins ara per ningú, de la *composició* de formes. En el començament d'aquesta disquisició, i perquè en endavant no calgui interrompre la sèrie contínua de demostracions, intercalem immediatament el

LEMA. *Es tenen quatre sèries de nombres enters* $a,\ a',\ a'',\ \ldots,\ a^n;\ b,\ b',\ b'',\ \ldots,\ b^n;\ c,\ c',\ c'',\ \ldots,\ c^n;$ $d,\ d',\ d'',\ \ldots,\ d^n$, *que consten de la mateixa quantitat de termes (posem* $n+1$*), i relacionades de manera que* $cd' - dc'$, $cd'' - dc''$, *etc.,* $c'd'' - d'c''$, *etc., etc., siguin respectivament iguals a* $k(ab' - ba')$, $k(ab'' - ba'')$, *etc.,* $k(a'b'' - b'a'')$, *etc., etc., o sigui, en general,* $c^\lambda d^\mu - d^\lambda c^\mu = k(a^\lambda b^\mu - b^\lambda a^\mu)$, *on* k *denota un nombre enter donat;* $\lambda,\ \mu$, *enters diferents qualssevol entre* 0 *i* n, *inclusivament, el més gran dels quals és* μ;* i que, *a part,*

* Considerant a com a^0, b com b^0, etc. D'altra banda, evidentment, també valdrà la mateixa equació quan $\lambda = \mu$ o bé $\lambda > \mu$.

tots els $a^\lambda b^\mu - b^\lambda a^\mu$ *no tinguin cap divisor comú. Llavors, es poden trobar quatre nombres enters* α, β, γ, δ, *tals que sigui* $\alpha a+\beta b = c$, $\alpha a'+\beta b' = c'$, $\alpha a''+\beta b'' = c''$, *etc.;* $\gamma a + \delta b = d$, $\gamma a' + \delta b' = d'$, $\gamma a'' + \delta b'' = d''$, *etc., o sigui, en general,* $\alpha a^\nu + \beta b^\nu = c^\nu$, $\gamma a^\nu + \delta b^\nu = d^\nu$*; fet això, serà* $\alpha\delta - \beta\gamma = k$.

Com que, per hipòtesi, els nombres $ab' - ba'$, $ab'' - ba''$, etc.; $a'b'' - b'a''$, etc. (la quantitat dels quals serà $= \frac{1}{2}(n+1)n$), no tenen cap divisor comú, es podran trobar tants altres nombres enters que, multiplicats respectivament per ells, la suma dels productes resulti = 1 (article 40). Aquests multiplicadors es designen per (0, 1), (0, 2), etc., (1, 2), etc., o sigui, en general, el multiplicador de $a^\lambda b^\mu - b^\lambda a^\mu$ per (λ, μ), de manera que sigui

$$\sum(\lambda, \mu)(a^\lambda b^\mu - b^\lambda a^\mu) = 1.$$

(Per la lletra Σ denotem la suma de tots els valors de l'expressió a la qual és prefixada que s'originen atribuint a λ, μ, tots els valors diferents entre 0 i n, de manera que sigui $\mu > \lambda$.) Fet això, si es considera $\sum(\lambda, \mu)(c^\lambda b^\mu - b^\lambda c^\mu) = \alpha$, $\sum(\lambda, \mu)(a^\lambda c^\mu - c^\lambda a^\mu) = \beta$, $\sum(\lambda, \mu)(d^\lambda b^\mu - b^\lambda d^\mu) = \gamma$, $\sum(\lambda, \mu)(a^\lambda d^\mu - d^\lambda a^\mu) = \delta$, els α, β, γ, δ, estaran dotats de les propietats prescrites.

Dem. I. Si ν denota un nombre enter qualsevol entre 0 i n, serà $\alpha a^\nu + \beta b^\nu = \sum(\lambda, \mu)(c^\lambda b^\mu a^\nu - b^\lambda c^\mu a^\nu + a^\lambda c^\mu b^\nu - c^\lambda a^\mu b^\nu) = \frac{1}{k}\sum(\lambda, \mu)(c^\lambda d^\mu c^\nu - d^\lambda c^\mu c^\nu) = \frac{1}{k}c^\nu \sum(\lambda, \mu)(c^\lambda d^\mu - d^\lambda c^\mu) = c^\nu \sum(\lambda, \mu)(a^\lambda b^\mu - b^\lambda a^\mu) = c^\nu$. I per un càlcul similar, es troba $\gamma a^\nu + \delta b^\nu = d^\nu$, *Q. E. P.*

II. Així, doncs, com que $c^\lambda = \alpha a^\lambda + \beta b^\lambda$, $c^\mu = \alpha a^\mu + \beta b^\mu$, resulta $c^\lambda b^\mu - b^\lambda c^\mu = \alpha(a^\lambda b^\mu - b^\lambda a^\mu)$, i, de manera similar, $a^\lambda c^\mu - c^\lambda a^\mu = \beta(a^\lambda b^\mu - b^\lambda a^\mu)$, $d^\lambda b^\mu - b^\lambda d^\mu = \gamma(a^\lambda b^\mu - b^\lambda a^\mu)$, $a^\lambda d^\mu - d^\lambda a^\mu = \delta(a^\lambda b^\mu - b^\lambda a^\mu)$, fórmules de les quals es poden trobar molt més fàcilment els valors de α, β, γ, δ, sempre que s'agafin λ, μ, de manera que $a^\lambda b^\mu - b^\lambda a^\mu$ no sigui $= 0$, que certament es podrà fer, ja que, per hipòtesi, tots els $a^\lambda b^\mu - b^\lambda a^\mu$ no tenen divisor comú, de manera que *tots* no poden ser $= 0$. D'aquestes mateixes equacions es dedueix, multiplicant la primera per la quarta, la segona per la tercera, i restant, que $(\alpha\delta - \beta\gamma)(a^\lambda b^\mu - b^\lambda a^\mu)^2 = (a^\lambda b^\mu - b^\lambda a^\mu)(c^\lambda d^\mu - d^\lambda c^\mu) = k(a^\lambda b^\mu - b^\lambda a^\mu)^2$, d'on, necessàriament, $\alpha\delta - \beta\gamma = k$. *Q. E. S.*

235. Si la forma $AXX + 2BXY + CYY \ldots F$ es transforma en el producte de dues formes $axx + 2bxy + cyy \ldots f$, i $a'x'x' + 2b'x'y' + c'y'y' \ldots f'$ per una substitució tal com $X = pxx' + p'xy' + p''yx' + p'''yy'$, $Y = qxx' + q'xy' + q''yx' + q'''yy'$ (cosa que, per abreujar, en el que segueix sempre expressarem així: si F es transforma en ff' per la substitució p, p', p'', p'''; q, q', q'', q'''),* direm més simplement que la forma F és *transformable* en ff'; si, a sobre, aquesta transformació s'ha construït de manera que els sis nombres $pq' - qp'$, $pq'' - qp''$, $pq''' - qp'''$, $p'q'' - q'p''$, $p'q''' - q'p'''$, $p''q''' - q''p'''$, no tinguin divisor comú, anomenarem la forma F *composta* de les formes f, f'.

* Així, doncs, en aquesta designació convé respectar perfectament l'ordre, tant dels coeficients p, p', etc., com de les formes f, f'. Però es copsa fàcilment que si s'inverteix l'ordre de les formes de manera que la primera resulti la darrera, els coeficients p', q', s'han de commutar amb els p'', q'', i qualsevol dels altres manté el seu lloc.

Emprenem aquesta disquisició amb la suposició més general que la forma F es transforma en ff' per la substitució p, p', p'', p'''; q, q', q'', q''', i desenvoluparem el que se segueixi d'això. Evidentment, les nou equacions següents equivaldran en total a aquesta suposició (és a dir, si aquestes equacions tenen lloc simultàniament, F es transformarà en ff' per la substitució dita, i recíprocament):

$$App + 2Bpq + Cqq = aa', \quad [1]$$
$$Ap'p' + 2Bp'q' + Cq'q' = ac', \quad [2]$$
$$Ap''p'' + 2Bp''q'' + Cq''q'' = ca', \quad [3]$$
$$Ap'''p''' + 2Bp'''q''' + Cq'''q''' = cc', \quad [4]$$
$$App' + B(pq' + qp') + Cqq' = ab', \quad [5]$$
$$App'' + B(pq'' + qp'') + Cqq'' = ba', \quad [6]$$
$$Ap'p''' + B(p'q''' + q'p''') + Cq'q''' = bc', \quad [7]$$
$$Ap''p''' + B(p''q''' + q''p''') + Cq''q''' = cb', \quad [8]$$
$$A(pp''' + p'p'') + B(pq''' + qp''' + p'q'' + q'p'') + C(qq''' + q'q'') = 2bb'. \quad [9]$$

Siguin D, d, d', els determinants de les formes F, f, f', respectivament; M, m, m' (que suposem tots agafats positivament), els màxims comuns divisors dels nombres A, $2B$, C; a, $2b$, c; a', $2b'$, c', respectivament. A més a més, es determinen sis nombres enters $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, de manera que sigui $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, $\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m'$. Finalment, es designen els nombres $pq' - qp'$, $pq'' - qp''$, $pq''' - qp'''$, $p'q'' - q'p''$, $p'q''' - q'p'''$, $p''q''' - q''p'''$, per P, Q, R, S, T, U, respectivament, i sigui $= k$ el seu màxim comú divisor pres positivament. Ara, posant

$$App''' + B(pq''' + qp''') + Cqq''' = bb' + \Delta, \quad [10]$$

de l'equació [9] resulta

$$Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta. \qquad [11]$$

D'aquestes onze equacions, 1, ..., 11 hem desenvolupat les noves següents:*

$$DPP = d'aa, \qquad [12]$$
$$DP(R-S) = 2d'ab, \qquad [13]$$
$$DPU = d'ac - (\Delta\Delta - dd'), \qquad [14]$$
$$D(R-S)^2 = 4d'bb + 2(\Delta\Delta - dd'), \qquad [15]$$
$$D(R-S)U = 2d'bc, \qquad [16]$$
$$DUU = d'cc, \qquad [17]$$
$$DQQ = da'a', \qquad [18]$$
$$DQ(R+S) = 2da'b', \qquad [19]$$
$$DQT = da'c' - (\Delta\Delta - dd'), \qquad [20]$$
$$D(R+S)^2 = 4db'b' + 2(\Delta\Delta - dd'), \qquad [21]$$
$$D(R+S)T = 2db'c', \qquad [22]$$
$$DTT = dc'c'. \qquad [23]$$

Contràriament, d'aquí es dedueixen les dues

$$0 = 2d'aa(\Delta\Delta - dd'),$$
$$0 = (\Delta\Delta - dd')^2 - 2d'ac(\Delta\Delta - dd'),$$

això és, la primera de $12 \cdot 15 - 13 \cdot 13$, la darrera de $14 \cdot 14 - 12 \cdot 17$; d'on es copsa fàcilment que és necessàriament $\Delta\Delta - dd' = 0$, tant si a és $= 0$ com si no és $= 0$.** Així,

* L'origen d'aquestes equacions és aquest: 12 de $5 \cdot 5 - 1 \cdot 2$; 13 de $5 \cdot 9 - 1 \cdot 7 - 2 \cdot 6$; 14 de $10 \cdot 11 - 6 \cdot 7$; 15 de $5 \cdot 8 + 5 \cdot 8 + 10 \cdot 10 + 11 \cdot 11 - 1 \cdot 4 - 2 \cdot 3 - 6 \cdot 7 - 6 \cdot 7$; 16 de $8 \cdot 9 - 3 \cdot 7 - 4 \cdot 6$; 17 de $8 \cdot 8 - 3 \cdot 4$. La deducció de les sis restants es disposa de la mateixa manera, sempre que les equacions 2, 5, 7, es commutin respectivament amb les equacions 3, 6, 8, i es mantinguin a continuació les restants 1, 4, 9, 10, 11, en el mateix lloc; posem 18 de $6 \cdot 6 - 1 \cdot 3$, etc.

** Sigui suficient aquesta derivació de l'equació $\Delta\Delta = dd'$ per al projecte present; altrament, hauríem pogut tractar alguna

suposarem que a les equacions 14, 15, 20, 21, s'esborra $\Delta\Delta - dd'$ a la dreta.

Ara, establint

$$\mathfrak{A}P + \mathfrak{B}(R - S) + \mathfrak{C}U = mn',$$
$$\mathfrak{A}'Q + \mathfrak{B}'(R + S) + \mathfrak{C}'T = m'n,$$

(on s'ha d'observar perfectament que n, n', poden sortir també fraccions, encara que necessàriament mn', $m'n$, siguin enters), de les equacions 12, ..., 17, es dedueix fàcilment

$$Dmmn'n' = d'(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)^2 = d'mm,$$

i, semblantment, de les equacions 18 ..., 23,

$$Dm'm'nn = d(\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c')^2 = dm'm'.$$

Així, doncs, serà $d = Dnn$, $d' = Dn'n'$, d'on obtenim la PRIMERA CONCLUSIÓ: *La raó que els determinants de les formes F, f, f', tenen entre si és, necessàriament, un quadrat*; i la SEGONA: *D sempre divideix els nombres $dm'm'$, $d'mm$.* Així, és clar que D, d, d', tenen el mateix signe i que cap forma el determinant de la qual és més gran que el màxim comú divisor dels nombres $dm'm'$, $d'mm$, no pot ser transformable en el producte ff'.

Es multipliquen les equacions 12, 13, 14, per $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, respectivament; i, similarment, pels mateixos nombres, les equacions 13, 15, 16, i 14, 16, 17; se sumen els

---

anàlisi més elegant, però massa llarga aquí, deduint directament de les equacions 1 ..., 11 la $0 = (\Delta\Delta - dd')^2$.

tres productes, i es divideix la suma per Dmn', escrit $Dn'n'$ per d'. Llavors, surt

$$P = an', \quad R - S = 2bn', \quad U = cn'.$$

De manera similar, multiplicades les equacions 18, 19, 20, i també 19, 21, 22 i 20, 22, 23, per $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, respectivament, s'obté

$$Q = a'n, \quad R + S = 2b'n, \quad T = c'n.$$

D'aquí es té la TERCERA CONCLUSIÓ: *Els nombres* a, $2b$, c, *són proporcionals als nombres* P, $R - S$, U, *i posada la raó d'aquells amb aquests com* 1 *a* n', n' *serà l'arrel quadrada de* $\dfrac{d'}{D}$; *i, similarment, els nombres* a', $2b'$, c', *tenen la mateixa raó amb* Q, $R + S$, T, *i si aquesta es posa que és com* 1 *a* n, n *serà l'arrel quadrada de* $\dfrac{d}{D}$.

D'altra banda, les quantitats n, n', poden ser arrels positives o bé negatives de $\dfrac{d}{D}$, $\dfrac{d'}{D}$, d'on en reclamem la distinció, que semblarà estèril a primera vista, però l'ús de la qual apareixerà suficientment en el que segueix. Això és, en la transformació de la forma F en ff' direm que la forma f s'agafa *directament* quan n és positiva, *inversament* quan n és negativa; i, similarment, que f' s'agafa directament o inversament segons que n' sigui positiva o bé negativa. Però, afegint la condició que k sigui $= 1$, la forma F s'anomenarà, *o bé* composta directament de cada una de les dues formes f, f', *o bé* inversament de cada una de les dues, *o bé* directament de f i inversament de f', *o bé* inversament de f i directament de f', segons que n, n', siguin o bé totes dues

positives, o bé totes dues negatives, o bé la primera positiva, la darrera negativa, o bé la primera negativa, la darrera positiva. D'altra banda, qualsevol entendrà fàcilment que aquestes relacions no depenen de l'ordre en què es col·loquen les formes f, f' (vegeu la primera nota del present article).

A més a més, observem que el màxim comú divisor dels nombres P, Q, R, S, T, U, posem k, divideix els nombres mn', $m'n$ (com és evident dels valors establerts més amunt), de manera que el seu quadrat kk els $mmn'n'$, $m'm'nn$, i Dkk els $d'mm$, $dm'm'$. Però, també, recíprocament, qualsevol divisor comú de mn', $m'n$, dividirà k. En efecte, sigui e un tal divisor, el qual, evidentment, també dividirà els nombres an', $2bn'$, cn', $a'n$, $2b'n$, $c'n$, és a dir, els nombres P, $R-S$, U, Q, $R+S$, T; i, en conseqüència, també $2R$ i $2S$. Ara, si $\frac{2R}{e}$ fos un nombre imparell, també $\frac{2S}{e}$ hauria de ser imparell (ja que la suma i la diferència són parelles), de manera que el seu producte també imparell. Però aquest producte resulta $= \frac{4}{ee}(b'b'nn - bbn'n') = \frac{4}{ee}(d'nn+a'c'nn-dn'n'-acn'n') = \frac{4}{ee}(a'c'nn-acn'n')$, de manera que parell, ja que e divideix $a'n$, $c'n$, an', cn'. Per tant, $\frac{2R}{e}$ serà necessàriament parell i, en conseqüència, R, i també S, divisible per e. Així, doncs, com que e divideix tots sis P, Q, R, S, T, U, també dividirà el seu màxim comú divisor k. *Q. E. D.* D'aquí es conclou que k és el màxim comú divisor dels nombres mn', $m'n$; d'on es copsa fàcilment que *Dkk serà el màxim comú divisor dels nombres $dm'm'$, $d'mm$.* Aquesta és la QUARTA CONCLUSIÓ. Així, és clar que sempre que F

sigui composta de f i f', D serà el màxim comú divisor dels nombres $dm'm'$, $d'mm$, i recíprocament; aquesta propietat també s'hauria pogut adoptar com a definició de forma composta. Així, doncs, la forma composta de les formes f, f', té el determinant màxim possible entre totes les formes transformables en el producte ff'.

Prèviament que puguem progressar més enllà, convé definir acuradament, abans que res, el valor de Δ, el qual hem mostrat que és $= \sqrt{dd'} = \sqrt{DDnnn'n'}$, certament, però el *signe* del qual encara no s'ha determinat aquí. Per a aquest fi, de les equacions fonamentals 1, ..., 11, hem trobat $DPQ = \Delta aa'$ (equació que s'obté de $5 \cdot 6 - 1 \cdot 11$), de manera que $Daa'nn' = \Delta aa'$, d'on, si cap dels nombres a, a' no és $= 0$, resulta $\Delta = Dnn'$. Però, de manera completament similar, de les equacions fonamentals se'n poden deduir unes altres vuit, en les quals es tenen a l'esquerra Dnn', a la dreta Δ, multiplicats per $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc',* d'on es conclou fàcilment, del fet que ni tots els a, $2b$, c, ni tots els a', $2b'$, c', poden ser $= 0$, que en tots els casos resulta $\Delta = Dnn'$, de manera que Δ té el mateix signe que D, d, d', o bé l'oposat, segons que n, n', tinguin el mateix signe, o bé diferent.

A més a més, observem que els nombres aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc', $2bb' + 2\Delta$, $2bb' - 2\Delta$, són tots divisibles per mm'. Per als nou primers, això és evident per si mateix, però per als dos restants es pot demostrar de manera similar a com abans hem mostrat que R i S són divisibles per e. Això és, és clar que $4bb' + 4\Delta$ i $4bb' - 4\Delta$ són divisibles per mm' (ja que

*Per abreujar, convé suprimir l'anàlisi, que els lectors podran detectar fàcilment.

$4\Delta = \sqrt{16dd'}$, $4d$ és divisible per mm, i $4d'$ per $m'm'$, de manera que $16dd'$ per $mmm'm'$ i 4Δ per mm') i la diferència dels quocients, parella; es demostra fàcilment que el producte dels quocients és parell, d'on cada un dels quocients, parell, i $2bb' + 2\Delta$ i $2bb' - 2\Delta$, divisibles per mm'.

Ara, de les onze equacions fonamentals es dedueixen fàcilment les sis següents:

$APP = aa'q'q' - 2ab'qq' + ac'qq,$
$AQQ = aa'q''q'' - 2ba'qq'' + ca'qq,$
$ARR = aa'q'''q''' - 2(bb' + \Delta)qq''' + cc'qq,$
$ASS = ac'q''q'' - 2(bb' - \Delta)q'q'' + ca'q'q',$
$ATT = ac'q'''q''' - 2bc'q'q''' + cc'q'q',$
$AUU = ca'q'''q''' - 2cb'q''q''' + cc'q''q''.$

D'aquí se segueix que tots els APP, AQQ, etc., són divisibles per mm', d'on, com que kk és el màxim comú divisor dels nombres PP, QQ, RR, etc., es deriva fàcilment que també Akk és divisible per mm'. Però substituïts a, $2b$, c, a', $2b'$, c', pels seus valors $\frac{P}{n'}$, etc., o sigui, $\frac{1}{n'}(pq' - qp')$, etc., es transformaran en unes altres sis equacions, en les quals es tindran a la dreta els productes de la quantitat $\frac{1}{nn'}(q'q'' - qq''')$ per PP, QQ, RR, etc. Deixem el càlcul, fàcil, als lectors. D'aquí se segueix (ja que tots els PP, QQ, etc., no poden ser $= 0$) que $Ann' = q'q'' - qq'''$.

De manera similar, de les equacions fonamentals es deriven unes altres sis equacions, que només difereixen de les precedents en què a tot arreu per A es té C, i per q, q', q'', q''', respectivament p, p', p'', p''', les

quals, per abreujar, no escrivim. D'aquí se segueix, de la mateixa manera, que Ckk és divisible per mm' i que $Cnn' = p'p'' - pp'''$.

Finalment, de la mateixa font s'obtenen les sis equacions

$$BPP = -aa'p'q' + ab'(pq' + qp') - ac'pq,$$
$$BQQ = -aa'p''q'' + ba'(pq'' + qp'') - ca'pq,$$
$$BRR = -aa'p'''q''' + (bb' + \Delta)(pq''' + qp''') - cc'pq,$$
$$BSS = -ac'p''q'' + (bb' - \Delta)(p'q'' + q'p'') - ca'p'q',$$
$$BTT = -ac'p'''q''' + bc'(p'q''' + q'p''') - cc'p'q',$$
$$BUU = -ca'p'''q''' + cb'(p''q''' + q''p''') - cc'p''q'',$$

d'on, igualment com abans, es conclou que $2Bkk$ és divisible per mm' i que $2Bnn' = pq''' + qp''' - p'q'' - q'p''$.

Així, com que Akk, $2Bkk$, Ckk, són divisibles per mm', es copsarà fàcilment que Mkk també ha de ser divisible per mm'. Però de les equacions fonamentals es conclou que M divideix aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc', de manera que també am', $2bm'$, cm' (que són els màxims comuns divisors dels tres primers, dels tres del mig i dels tres últims, respectivament); finalment, també mm', que és el màxim comú divisor d'aquests. D'aquí és clar que en el cas en què la forma F és composta de les formes f, f', o sigui, $k = 1$, necessàriament és $M = mm'$. Aquesta és la CINQUENA CONCLUSIÓ.

Si el màxim comú divisor dels nombres A, B, C, és $\mathfrak{M}$, aquest serà, o bé $= M$ (quan la forma F és pròpiament primitiva o bé derivada d'una pròpiament primitiva), o bé $= \frac{1}{2}M$ (quan F és una forma impròpiament

primitiva o bé derivada d'una impròpiament primitiva); similarment, designant per $\mathfrak{m}$, $\mathfrak{m}'$, respectivament, els màxims comuns divisors dels nombres a, b, c; a', b', c', $\mathfrak{m}$ serà, o bé $= m$, o bé $= \frac{1}{2}m$, i $\mathfrak{m}'$, o bé $= m'$, o bé $= \frac{1}{2}m'$. Ara, és clar que $\mathfrak{mm}$ divideix d, i $\mathfrak{m}'\mathfrak{m}'$, d', de manera que $\mathfrak{mmm}'\mathfrak{m}'$, dd', o sigui, $\Delta\Delta$, i $\mathfrak{mm}'$, Δ. D'aquí, i de les sis últimes equacions per a BPP, etc., se segueix que $\mathfrak{mm}'$ divideix Bkk, de manera que (com que també divideix Akk, Ckk) també $\mathfrak{M}kk$. Així, doncs, sempre que F és composta de f, f', $\mathfrak{mm}'$ dividirà $\mathfrak{M}$. Així, quan, en aquest cas, cadascuna de les f, f', és pròpiament primitiva o bé derivada d'una pròpiament primitiva, o sigui, $\mathfrak{mm}' = mm' = M$, serà $\mathfrak{M} = M$, o sigui, F una forma similar. Però, quan, en la mateixa suposició, o bé cada una de les f, f', o bé almenys alguna, és impròpiament primitiva o bé derivada d'una impròpiament primitiva, *per exemple*, la forma f, de les equacions fonamentals, se segueix que aa', $2ab'$, ac', ba', $2bb'$, bc', ca', $2cb'$, cc', són divisibles per $\mathfrak{M}$, de manera que també am', bm', cm', i, d'aquí, també $\mathfrak{m}m' = \frac{1}{2}mm' = \frac{1}{2}M$; d'on, necessàriament, en aquest cas, serà $\mathfrak{M} = \frac{1}{2}M$, o sigui, la forma F també impròpiament primitiva o bé derivada d'una impròpiament primitiva. Això proporciona la SISENA CONCLUSIÓ.

Finalment, observem que si *se suposa* que tenen lloc les nou equacions $an' = P$, $2bn' = R - S$, $cn' = U$, $a'n = Q$, $2b'n = R + S$, $c'n = T$, $Ann' = q'q'' - qq'''$, $2Bnn' = pq''' + qp''' - p'q'' - q'p''$, $Cnn' = p'p'' - pp'''$ (que, com que sovint convindrà referir-nos a elles en el que segueix, designarem per Ω), mirats n, n', com a incògnites, però cap dels quals $= 0$, es confirma fàcil-

ment per substitució que les equacions fonamentals 1, ..., 9, també són vertaderes necessàriament, o sigui, que la forma (A, B, C) es transforma en el producte de les formes (a, b, c), (a', b', c'), per la substitució p, p', p'', p'''; q, q', q'', q'''; i, a part, és $bb - ac = nn(BB - AC)$, $b'b' - a'c' = n'n'(BB - AC)$. Confiem a la diligència dels lectors el càlcul, que seria massa llarg afegir aquí.

236. PROBLEMA. *Proposades dues formes els determinants de les quals o bé són iguals o bé, almenys, la raó entre ells és un quadrat, trobar una forma composta d'elles.*

Solució. Siguin $(a, b, c) \ldots f$, $(a', b', c') \ldots f'$, les formes que s'han de compondre; d, d', els seus determinants; m, m', els màxims comuns divisors dels nombres a, $2b$, c; a', $2b'$, c', respectivament; D el màxim comú divisor dels nombres $dm'm'$, $d'mm$, afectat pel mateix signe que d, d'. Llavors, $\frac{dm'm'}{D}$, $\frac{d'mm}{D}$, seran nombres positius primers entre si i el seu producte un quadrat; per tant, ells mateixos seran quadrats (article 21). D'aquí, $\sqrt{\frac{d}{D}}$, $\sqrt{\frac{d'}{D}}$, seran quantitats racionals, que posarem $= n$, n', i, certament, agafarem per a n el valor positiu o bé el negatiu segons que la forma f hagi d'entrar en la composició o bé directament o bé inversament, i, similarment, determinarem el signe de n' per la raó amb què f' hagi d'entrar en la composició. Així, mn', $m'n$, seran nombres enters primers entre si; però n i n' també poden ser fraccions. Fet això així, observem que an', cn', $a'n$, $c'n$, $bn' + b'n$, $bn' - b'n$, són

enters, cosa que és evident en si per als quatre primers (ja que $an' = \frac{a}{m}mn'$, etc.); per als altres dos, es demostra de la mateixa manera que en l'article precedent s'ha demostrat que R i S són divisibles per e.

Ara, s'agafen a voluntat quatre nombres enters $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$, amb l'única condició que les quatre quantitats posades a l'esquerra en les equacions (I) següents no resultin totes simultàniament $= 0$, i es posa ... (I)

$$\begin{aligned}
&\mathfrak{Q}'an' + \mathfrak{Q}''a'n + \mathfrak{Q}'''(bn' + b'n) = \mu q,\\
&-\mathfrak{Q}an' + \mathfrak{Q}'''c'n - \mathfrak{Q}''(bn' - b'n) = \mu q',\\
&\mathfrak{Q}'''cn' - \mathfrak{Q}a'n + \mathfrak{Q}'(bn' - b'n) = \mu q'',\\
&-\mathfrak{Q}''cn' - \mathfrak{Q}'c'n - \mathfrak{Q}(bn' + b'n) = \mu q''',
\end{aligned}$$

de manera que q, q', q'', q''', resultin enters que no tinguin divisor comú, cosa que s'obté agafant per a μ el màxim comú divisor dels quatre nombres que estan a l'esquerra en aquestes equacions. Llavors, doncs, per l'article 40, es podran trobar quatre nombres enters $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$, tals que resulti $\mathfrak{P}q+\mathfrak{P}'q'+\mathfrak{P}''q''+\mathfrak{P}'''q''' = 1$. Fet això, es determinen els nombres p, p', p'', p''', per les equacions següents ... (II):

$$\begin{aligned}
&\mathfrak{P}'an' + \mathfrak{P}''a'n + \mathfrak{P}'''(bn' + b'n) = p,\\
&-\mathfrak{P}an' + \mathfrak{P}'''c'n - \mathfrak{P}''(bn' - b'n) = p',\\
&\mathfrak{P}'''cn' - \mathfrak{P}a'n + \mathfrak{P}'(bn' - b'n) = p'',\\
&-\mathfrak{P}''cn' - \mathfrak{P}'c'n - \mathfrak{P}(bn' + b'n) = p'''.
\end{aligned}$$

Finalment, es posa $q'q''-qq''' = Ann'$, $pq'''+qp'''-p'q''-q'p'' = 2Bnn'$, $p'p''-pp''' = Cnn'$. Llavors, A, B, C seran nombres enters i la forma $(A,\ B,\ C)$ ... F, composta de les formes f, f'.

Dem. I. De les equacions I i II es confirmen sense dificultat les quatre equacions següents ... (III):

$$0 = q'cn' - q''c'n - q'''(bn' - b'n),$$
$$0 = qcn' + q'''a'n - q''(bn' + b'n),$$
$$0 = q'''an' + qc'n - q'(bn' + b'n),$$
$$0 = q''an' - q'a'n - q(bn' - b'n).$$

II. Ara, suposem que s'han determinat nombres enters $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, $\mathfrak{N}$, $\mathfrak{N}'$, de manera que resulti $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, $\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m'$, $\mathfrak{N}m'n + \mathfrak{N}'mn' = 1$. Llavors, serà $\mathfrak{A}a\mathfrak{N}'n' + 2\mathfrak{B}b\mathfrak{N}'n' + \mathfrak{C}c\mathfrak{N}'n' + \mathfrak{A}'a'\mathfrak{N}n + 2\mathfrak{B}'b'\mathfrak{N}n + \mathfrak{C}'c'\mathfrak{N}n = 1$. D'aquí, i de les equacions (III), es confirma fàcilment que si es posa

$$-q'\mathfrak{A}\mathfrak{N}' - q''\mathfrak{A}'\mathfrak{N} - q'''(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) = \mathfrak{q},$$
$$q\mathfrak{A}\mathfrak{N}' - q'''\mathfrak{C}'\mathfrak{N} + q''(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) = \mathfrak{q}',$$
$$-q'''\mathfrak{C}\mathfrak{N}' + q\mathfrak{A}'\mathfrak{N} - q'(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) = \mathfrak{q}'',$$
$$q''\mathfrak{C}\mathfrak{N}' + q'\mathfrak{C}'\mathfrak{N} + q(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) = \mathfrak{q}''',$$

serà ... (IV)

$$\mathfrak{q}'an' + \mathfrak{q}''a'n + \mathfrak{q}'''(bn' + b'n) = q,$$
$$-\mathfrak{q}an' + \mathfrak{q}'''c'n - \mathfrak{q}''(bn' - b'n) = q',$$
$$\mathfrak{q}'''cn' - \mathfrak{q}a'n + \mathfrak{q}'(bn' - b'n) = q'',$$
$$-\mathfrak{q}''cn' - \mathfrak{q}'c'n - \mathfrak{q}(bn' + b'n) = q'''.$$

Quan $\mu = 1$, aquestes equacions no són necessàries, però en el seu lloc es poden retenir les equacions (I), a les quals són completament anàlogues. Ara, si de les equacions (II), (IV), es desenvolupen els valors dels Ann', $2Bnn'$, Cnn' (és a dir, dels nombres $q'q'' - qq'''$, etc.), i s'esborren els que es destrueixen mútuament, es trobarà que les parts de cadascun són, o bé productes d'enters per nn', o bé d'enters per $dn'n'$, o bé d'enters

per $d'nn$, i, a sobre, que totes les parts que constitueixen $2Bnn'$ impliquen el factor 2. D'aquí es conclou (ja que $dn'n' = d'nn$ i, en conseqüència, $\frac{dn'n'}{nn'} = \frac{d'nn}{nn'} = \sqrt{dd'}$ són enters) que A, B, C, són nombres enters. *Q. E. P.*

III. Substituint els valors de p, p', p'', p''', de les equacions (II), es comprova fàcilment, amb l'ajut de les equacions (III) i de la $\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$, que és $pq' - qp' = an'$, $pq''' - qp''' - p'q'' + q'p'' = 2bn'$, $p''q''' - q''p''' = cn'$, $pq'' - qp'' = a'n$, $pq''' - qp''' + p'q'' - q'p'' = 2b'n$, $p'q''' - q'p''' = c'n$, equacions que són idèntiques a les sis primeres de (Ω) de l'article precedent; però les tres restants ja tenen lloc per hipòtesi. Per tant (*aquí mateix, al final*), la forma F es transformarà en ff' per la substitució p, p', p'', p'''; q, q', q'', q''', i el seu determinant serà $= D$, o sigui, igual al màxim comú divisor dels nombres $dm'm'$, $d'mm$; per la qual cosa, per la conclusió quarta de l'article precedent, F serà composta de f, f'. *Q. E. S.* Finalment, es copsarà fàcilment que F és composta de f, f', de la *manera* que s'ha prescrit, ja que els signes de les quantitats n, n', ja s'han determinat correctament des de l'inici.

237. Teorema. *Si la forma F és transformable en el producte de dues formes f, f', i la forma f' implica la forma f'', F també serà transformable en el producte de les formes f, f''.*

Dem. Es retenen tots els símbols de l'article 235 per a les formes F, f, f'; sigui $= (a'', b'', c'')$ la forma f'', i es transforma f' en f'' per la substitució α, β, γ, δ. Llavors, es copsarà sense dificultat que F es transforma

en ff'' per la substitució $\alpha p+\gamma p'$, $\beta p+\delta p'$, $\alpha p''+\gamma p'''$, $\beta p''+\delta p'''$; $\alpha q+\gamma q'$, $\beta q+\delta q'$, $\alpha q''+\gamma q'''$, $\beta q''+\delta q'''$. *Q. E. D.*

Per abreujar, posats els coeficients $\alpha p+\gamma p'$, $\beta p+\delta p'$, etc. $=\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$; $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$, i el nombre $\alpha\delta-\beta\gamma=e$, es confirma fàcilment de les equacions (Ω) de l'article 235 que és $\mathfrak{P}\mathfrak{Q}'-\mathfrak{Q}\mathfrak{P}'=an'e$, $\mathfrak{P}\mathfrak{Q}'''-\mathfrak{Q}\mathfrak{P}'''-\mathfrak{P}'\mathfrak{Q}''+\mathfrak{Q}'\mathfrak{P}''=2bn'e$, $\mathfrak{P}''\mathfrak{Q}'''-\mathfrak{Q}''\mathfrak{P}'''=cn'e$; $\mathfrak{P}\mathfrak{Q}''-\mathfrak{Q}\mathfrak{P}''=\alpha\alpha a'n+2\alpha\gamma b'n+\gamma\gamma c'n=a''n$, $\mathfrak{P}\mathfrak{Q}'''-\mathfrak{Q}\mathfrak{P}'''+\mathfrak{P}'\mathfrak{Q}''-\mathfrak{Q}'\mathfrak{P}''=2b''n$, $\mathfrak{P}'\mathfrak{Q}'''-\mathfrak{Q}'\mathfrak{P}'''=c''n$; $\mathfrak{Q}'\mathfrak{Q}''-\mathfrak{Q}\mathfrak{Q}'''=Ann'e$, $\mathfrak{P}\mathfrak{Q}'''+\mathfrak{Q}\mathfrak{P}'''-\mathfrak{P}'\mathfrak{Q}''-\mathfrak{Q}'\mathfrak{P}''=2Bnn'e$, $\mathfrak{P}'\mathfrak{P}''-\mathfrak{P}\mathfrak{P}'''=Cnn'e$. Ara, designat per d'' el determinant de la forma f'', e serà l'arrel quadrada de $\dfrac{d''}{d'}$, i, certament, positiva o bé negativa segons que la forma f' impliqui la forma f'' o bé pròpiament o bé impròpiament. Per tant, $n'e$ serà l'arrel quadrada de $\dfrac{d''}{D}$; d'on és clar que les nou equacions precedents són completament anàlogues a les equacions (Ω) de l'article 235, i la forma f s'agafa en la transformació de la forma F en ff'' de la mateixa manera que en la transformació de la forma F en ff'; en canvi, la forma f'' en aquella o bé de la mateixa manera que f' en aquesta, o bé oposada, segons que f' impliqui f'' pròpiament o bé impròpiament.

238. Teorema. *Si la forma F està continguda en la forma F' i és transformable en el producte de les formes f, f', la forma F' també serà transformable en el mateix producte.*

Dem. Retinguts per a les formes F, f, f', els mateixos símbols que més amunt, i suposant que la forma F' es transforma en F per la substitució α, β, γ, δ, es copsarà fàcilment que resulta el mateix de F' per la substitució $\alpha p+\beta q$, $\alpha p'+\beta q'$, $\alpha p''+\beta q''$, $\alpha p'''+\beta q'''$, $\gamma p+\delta q$, $\gamma p'+\delta q'$, $\gamma p''+\delta q''$, $\gamma p'''+\delta q'''$, que de F per la substitució p, p', p'', p'''; q, q', q'', q''', de manera que F' es transforma en ff' per aquella substitució. *Q. E. D.*

A part, com a l'article precedent, es confirma fàcilment per un càlcul similar que F' és transformable en ff' de la mateixa manera que F, quan F' implica F pròpiament; però quan F estigui continguda impròpiament en F', les transformacions de la forma F en ff' i de la forma F' en ff' són oposades respecte de cadascuna de les formes f, f'; això és, d'aquestes formes, la que entri directament en una transformació s'agafa inversament en l'altra.

De la combinació del teorema present amb el teorema de l'article precedent obtenim el següent més general: *Si la forma F és transformable en el producte ff', i les formes f, f', impliquen, respectivament, les formes g, g', però la forma F està continguda en la forma G, G serà transformable en el producte gg'.* Efectivament, pel teorema de l'article present, G serà transformable en ff'; d'aquí, pel teorema de l'article precedent, en fg'; i, pel mateix teorema, també en gg'. A més a més, és clar que si totes tres formes f, f', G, impliquen pròpiament les formes g, g', F, G serà transformable en gg' respecte de les formes g, g', de la mateixa manera que F en ff' respecte de les formes f, f'; que succeeix el mateix si aquelles tres implicacions són totes impròpies; finalment, que es podrà determinar de manera igual-

ment fàcil *de quina manera* G és transformable en gg' si alguna d'aquelles implicacions és diferent de les dues restants.

Si les formes F, f, f', són equivalents a les formes G, g, g', respectivament, aquestes tindran els mateixos determinants que aquelles, i el que són els nombres m, m', per a les formes f, f', seran el mateix per a les formes g, g' (article 161). D'aquí es dedueix sense dificultat, per la conclusió quarta de l'article 235, que, en aquest cas, G serà *composta* de g, g', si F és composta de f, f'; i, certament, que la forma g entra en aquella composició de la mateixa manera que f en aquesta, quan F equivalgui a G de la mateixa manera que f a g, i recíprocament; i, similarment, cal agafar g' en la primera composició de la mateixa manera o bé de manera oposada que f' en la darrera, segons que l'equivalència de les formes f', g', sigui similar o bé diferent a l'equivalència de les formes F, G.

239. Teorema. *Si la forma F és composta de les formes f, f', qualsevol altra forma transformable en el producte ff' de la mateixa manera que F implicarà pròpiament F.*

Dem. Retinguts per a F, f, f', tots els símbols de l'article 235, les equacions Ω també tindran lloc aquí. Suposem que la forma $F' = (A', B', C')$, el determinant de la qual és $= D'$, es transforma en el producte ff' per la substitució $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, $\mathfrak{p}'''$; $\mathfrak{q}$, $\mathfrak{q}'$, $\mathfrak{q}''$, $\mathfrak{q}'''$, i designem els nombres $\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}'$, $\mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}''$, $\mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}'''$, $\mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}''$, $\mathfrak{p}'\mathfrak{q}''' - \mathfrak{q}'\mathfrak{p}'''$, $\mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}'''$, per P', Q', R', S', T', U', respectivament. Llavors, es tindran nou equacions

completament similars a les Ω, posem $P' = a\mathfrak{n}'$, $R' - S' = 2b\mathfrak{n}'$, $U' = c\mathfrak{n}'$, $Q' = a'\mathfrak{n}$, $R' + S' = 2b'\mathfrak{n}$, $T' = c'\mathfrak{n}$, $\mathfrak{q}'\mathfrak{q}'' - \mathfrak{q}\mathfrak{q}''' = A'\mathfrak{n}\mathfrak{n}'$, $\mathfrak{p}\mathfrak{q}''' + \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'' = 2B'\mathfrak{n}\mathfrak{n}'$, $\mathfrak{p}'\mathfrak{p}'' - \mathfrak{p}\mathfrak{p}''' = C'\mathfrak{n}\mathfrak{n}'$, que designarem per Ω'. Aquí, les quantitats $\mathfrak{n}$, $\mathfrak{n}'$, seran les arrels quadrades de $\frac{d}{D'}$, $\frac{d'}{D'}$, i, certament, afectades dels mateixos signes que n, n', respectivament; així, doncs, si es posa $= k$ l'arrel quadrada de $\frac{D}{D'}$ (que serà un nombre enter) agafada positivament, serà $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$. D'aquí, i de les sis primeres equacions en Ω i Ω', és evident que serà $P' = kP$, $Q' = kQ$, $R' = kR$, $S' = kS$, $T' = kT$, $U' = kU$. Per tant, pel lema de l'article 234, es podran determinar quatre nombres enters α, β, γ, δ, tals que resulti $\alpha p + \beta q = \mathfrak{p}$, $\gamma p + \delta q = \mathfrak{q}$, $\alpha p' + \beta q' = \mathfrak{p}'$, $\gamma p' + \delta q' = \mathfrak{q}'$, etc., i $\alpha\delta - \beta\gamma = k$. Substituïts aquests valors de $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{p}'$, $\mathfrak{q}'$, etc., en les tres últimes equacions de Ω', es confirma fàcilment, amb l'ajut de les equacions $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$ i les tres últimes de Ω, que serà $A'\alpha\alpha + 2B'\alpha\gamma + C'\gamma\gamma = A$, $A'\alpha\beta + B'(\alpha\delta + \beta\gamma) + C'\gamma\delta = B$, $A'\beta\beta + 2B'\beta\delta + C'\delta\delta = C$, causa per la qual la forma F' es transformarà en F per la substitució α, β, γ, δ (que serà pròpia, ja que $\alpha\delta - \beta\gamma = k$ és positiu), és a dir, implicarà pròpiament la forma F. *Q. E. D.*

Així, si F' també és composta de les formes f, f' (de la mateixa manera que F d'elles mateixes), les formes F, F', tindran el mateix determinant, i, encara més, seran pròpiament equivalents. Més generalment, si la forma G és composta de les formes g, g', de la mateixa manera que F de f, f', respectivament, i les formes g, g', equivalen pròpiament a f, f', les formes F, G, equivaldran pròpiament.

Com que aquest cas, en què les dues formes que cal compondre entren directament en la composició, és el més simple, i els restants es redueixen fàcilment a aquest, en el que segueix només tindrem en compte aquell, de manera que si es diu simplement que alguna forma és composta de dues altres, sempre convindrà sobreentendre que aquella és composta pròpiament de totes dues.* Valdrà la mateixa restricció quan es digui que una forma és transformable en el producte de dues altres.

240. Teorema. *Si la forma F és composta de les formes f, f', la forma $\mathfrak{F}$ de F i f'', la forma F' de f, f'', la forma $\mathfrak{F}'$ de F' i f', les formes $\mathfrak{F}$, $\mathfrak{F}'$, seran pròpiament equivalents.*

Dem. I. Sigui $f = axx + 2bxy + cyy$, $f' = a'x'x' + 2b'x'y' + c'y'y'$, $f'' = a''x''x'' + 2b''x''y'' + c''y''y''$, $F = AXX + 2BXY + CYY$, $F' = A'X'X' + 2B'X'Y' + C'Y'Y'$, $\mathfrak{F} = \mathfrak{A}\mathfrak{X}\mathfrak{X} + 2\mathfrak{B}\mathfrak{X}\mathfrak{Y} + \mathfrak{C}\mathfrak{Y}\mathfrak{Y}$, $\mathfrak{F}' = \mathfrak{A}'\mathfrak{X}'\mathfrak{X}' + 2\mathfrak{B}'\mathfrak{X}'\mathfrak{Y}' + \mathfrak{C}'\mathfrak{Y}'\mathfrak{Y}'$; d, d', d'', D, D', $\mathfrak{D}$, $\mathfrak{D}'$, respectivament, els determinants d'aquestes set formes, que tots tindran els mateixos signes i la seva raó serà un quadrat. A més a més, sigui m el màxim comú divisor dels nombres a, $2b$, c, i tinguin m', m'', M, un significat similar relativament a les formes f', f'', F. Llavors, per la conclusió 4 de l'article 235, D serà el màxim comú divisor dels nombres $dm'm'$, $d'mm$, de manera que $Dm''m''$, el màxim comú divisor dels nom-

* Similarment, se sol sobreentendre com en la composició de raons (que té una gran analogia amb la composició de formes) que les raons que cal compondre s'han d'agafar directament, llevat que allà s'adverteixi del contrari.

bres $dm'm'm''m''$, $d'mmm''m''$; $M = mm'$; $\mathfrak{D}$, el màxim comú divisor dels nombres $Dm''m''$, $d''MM$, o sigui, dels nombres $Dm''m''$, $d''mmm'm'$. D'aquí es conclou que $\mathfrak{D}$ és el màxim comú divisor dels tres nombres $dm'm'm''m''$, $d'mmm''m''$, $d''mmm'm'$; però, per una raó similar, $\mathfrak{D}'$ serà el màxim comú divisor dels tres mateixos nombres; per tant, com que $\mathfrak{D}$, $\mathfrak{D}'$, tenen els mateixos signes, serà $\mathfrak{D} = \mathfrak{D}'$, o sigui, les formes $\mathfrak{F}$, $\mathfrak{F}'$, tindran el mateix determinant.

II. Ara, es transforma F en ff' per la substitució $X = pxx' + p'xy' + p''yx' + p'''yy'$, $Y = qxx' + q'xy' + q''yx' + q'''yy'$, i $\mathfrak{F}$ en Ff'' per la substitució $\mathfrak{X} = \mathfrak{p}Xx'' + \mathfrak{p}'Xy'' + \mathfrak{p}''Yx'' + \mathfrak{p}'''Yy''$, $\mathfrak{Y} = \mathfrak{q}Xx'' + \mathfrak{q}'Xy'' + \mathfrak{q}''Yx'' + \mathfrak{q}'''Yy''$, i es designen per n, n', $\mathfrak{N}$, n'', les arrels quadrades positives de $\frac{d}{D}$, $\frac{d'}{D}$, $\frac{D}{\mathfrak{D}}$, $\frac{d''}{\mathfrak{D}}$. Llavors, per l'article 235, es tindran divuit equacions, una meitat de les quals pertanyerà a la transformació de la forma F en ff', l'altra a la transformació de la forma $\mathfrak{F}$ en Ff''. La primera serà $pq' - qp' = an'$, a la manera de la qual es podran formar fàcilment les restants, que cal ometre aquí per abreujar. D'altra banda, les quantitats n, n', $\mathfrak{N}$, n'', seran, certament, racionals, però no necessàriament nombres enters.

III. Si els valors de X, Y, se substitueixen en els valors de $\mathfrak{X}$, $\mathfrak{Y}$, surt una substitució com $\mathfrak{X} = (1)xx'x'' + (2)xx'y'' + (3)xy'x'' + (4)xy'y'' + (5)yx'x'' + (6)yx'y'' + (7)yy'x'' + (8)yy'y''$, $\mathfrak{Y} = (9)xx'x'' + (10)xx'y'' + (11)xy'x'' + (12)xy'y'' + (13)yx'x'' + (14)yx'y'' + (15)yy'x'' + (16)yy'y''$, per la qual, evidentment, $\mathfrak{F}$ es transformarà en el producte $ff'f''$. El coeficient (1) serà

$= p\mathfrak{p} + q\mathfrak{p}''$; no afegim els valors dels quinze restants ja que qualsevol els desenvoluparà sense dificultat. Designem el nombre $(1)(10) - (2)(9)$ per $(1, 2)$, el nombre $(1)(11) - (3)(9)$ per $(1, 3)$, i, en general, $(g)(8 + h) - (h)(8 + g)$ per (g, h), suposant que g, h, són enters diferents entre 1 i 16, dels quals h és el més gran;* d'aquesta manera es tindran en total vint-i-vuit símbols. Ara, denotades per $\mathfrak{n}$, $\mathfrak{n}'$, les arrels quadrades positives de $\frac{d}{\mathfrak{D}}$, $\frac{d'}{\mathfrak{D}}$ (que seran $= n\mathfrak{N}$, $n'\mathfrak{N}$), es trobaran les 28 equacions següents: $(1,2) = aa'\mathfrak{n}''$, $(1,3) = aa''\mathfrak{n}'$, $(1,4) = ab'\mathfrak{n}'' + ab''\mathfrak{n}'$, $(1,5) = a'a''\mathfrak{n}$, $(1,6) = a'b\mathfrak{n}'' + a'b''\mathfrak{n}$, $(1,7) = a''b\mathfrak{n}' + a''b'\mathfrak{n}$, $(1,8) = bb'\mathfrak{n}'' + bb''\mathfrak{n}' + b'b''\mathfrak{n} + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$, $(2,3) = ab''\mathfrak{n}' - ab'\mathfrak{n}''$, $(2,4) = ac''\mathfrak{n}'$, $(2,5) = a'b''\mathfrak{n} - a'b\mathfrak{n}''$, $(2,6) = a'c''\mathfrak{n}$, $(2,7) = bb''\mathfrak{n}' + b'b''\mathfrak{n} - bb'\mathfrak{n}'' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$, $(2,8) = bc''\mathfrak{n}' + b'c''\mathfrak{n}$, $(3,4) = ac'\mathfrak{n}''$, $(3,5) = a''b'\mathfrak{n} - a''b\mathfrak{n}'$, $(3,6) = bb'\mathfrak{n}'' + b'b''\mathfrak{n} - bb''\mathfrak{n}' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$, $(3,7) = a''c'\mathfrak{n}$, $(3,8) = bc'\mathfrak{n}'' + b''c'\mathfrak{n}$, $(4,5) = b'b''\mathfrak{n} - bb'\mathfrak{n}'' - bb''\mathfrak{n}' + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$, $(4,6) = b'c''\mathfrak{n} - bc''\mathfrak{n}'$, $(4,7) = b''c'\mathfrak{n} - bc'\mathfrak{n}''$, $(4,8) = c'c''\mathfrak{n}$, $(5,6) = ca'\mathfrak{n}''$, $(5,7) = ca''\mathfrak{n}'$, $(5,8) = b'c\mathfrak{n}'' + b''c\mathfrak{n}'$, $(6,7) = b''c\mathfrak{n}' - b'c\mathfrak{n}''$, $(6,8) = cc''\mathfrak{n}'$, $(7,8) = cc'\mathfrak{n}''$, que designarem per Φ, i les altres nou: $(10)(11) - (9)(12) = a\mathfrak{n}'\mathfrak{n}''\mathfrak{A}$, $(1)(12) - (2)(11) - (3)(10) + (4)(9) = 2a\mathfrak{n}'\mathfrak{n}''\mathfrak{B}$, $(2)(3) - (1)(4) = a\mathfrak{n}'\mathfrak{n}''\mathfrak{C}$, $-(9)(16) + (10)(15) + (11)(14) - (12)(13) = 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{A}$, $(1)(16) - (2)(15) - (3)(14) + (4)(13) + (5)(12) - (6)(11) - (7)(10) + (8)(9) = 4b\mathfrak{n}'\mathfrak{n}''\mathfrak{B}$, $-(1)(8) + (2)(7) + (3)(6) - (4)(5) = 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{C}$, $(14)(15) - (13)(16) = c\mathfrak{n}'\mathfrak{n}''\mathfrak{A}$,

* No s'ha de confondre el significat present d'aquests símbols amb el que havien pres en l'article 234; efectivament, els nombres expressats *aquí* per aquests símbols corresponen especialment als que en l'article 234 es multiplicaven per nombres indicats allà per símbols similars.

$(5)(16)-(6)(15)-(7)(14)+(8)(13) = 2c\mathfrak{n}'\mathfrak{n}''\mathfrak{B}$, $(6)(7)-(5)(8) = c\mathfrak{n}'\mathfrak{n}''\mathfrak{C}$, que designarem per Ψ.*

IV. Seria massa llarg deduir l'origen de totes les 37 equacions; serà suficient de confirmar-ne algunes, a la manera de les quals es podran demostrar les restants sense dificultat.

1) Es té $(1,2) = (1)(10)-(2)(9) = (\mathfrak{p}\mathfrak{q}'-\mathfrak{q}\mathfrak{p}')pp+(\mathfrak{p}\mathfrak{q}'''-\mathfrak{q}\mathfrak{p}'''-\mathfrak{p}'\mathfrak{q}''+\mathfrak{q}'\mathfrak{p}'')pq+(\mathfrak{p}''\mathfrak{q}'''-\mathfrak{q}''\mathfrak{p}''')qq = \mathfrak{n}''(App+2Bpq+Cqq) = \mathfrak{n}''aa'$, que és la primera equació.

2) La segona equació resulta $(1,3) = (1)(11)-(3)(9) = (\mathfrak{p}\mathfrak{q}''-\mathfrak{q}\mathfrak{p}'')(pq'-qp') = a''\mathfrak{N}an' = aa''\mathfrak{n}'$.

3) L'octava equació en Φ serà $(1,8) = (1)(16)-(8)(9) = (\mathfrak{p}\mathfrak{q}'-\mathfrak{q}\mathfrak{p}')pp'''+(\mathfrak{p}\mathfrak{q}'''-\mathfrak{q}\mathfrak{p}''')pq'''-(\mathfrak{p}'\mathfrak{q}''-\mathfrak{q}'\mathfrak{p}'')qp'''+(\mathfrak{p}''\mathfrak{q}'''-\mathfrak{q}''\mathfrak{p}''')qq''' = \mathfrak{n}''(App'''+B(pq'''+qp''')+Cqq''')+b''\mathfrak{N}(pq'''-qp''') = \mathfrak{n}''(bb'+\sqrt{dd'})+b''\mathfrak{N}(bn'+b'n)$** $= \mathfrak{n}''bb'+\mathfrak{n}'bb''+\mathfrak{n}b'b''+\mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$. Deixem als lectors la confirmació de les equacions restants.

V. De les equacions Φ se segueix, de la manera següent, que els 28 nombres (1, 2), (1, 3), etc., no tenen cap divisor comú. Primer, observem els vint-i-set productes de tres factors, el primer dels quals és $\mathfrak{n}$, el segon,

---

* Convé observar que es poden descobrir unes altres 18 equacions similars a aquestes Ψ en les quals, a la dreta, en lloc dels factors a, $2b$, c, es tinguin a', $2b'$, c'; a'', $2b''$, c''; però ometem aquestes, ja que no són necessàries per al nostre propòsit.

** Això se segueix de l'equació 10 dels articles 235 i següents. La quantitat radical $\sqrt{dd'}$ resulta $= Dnn' = \mathfrak{D}nn'\mathfrak{M}\mathfrak{N} = \mathfrak{D}\mathfrak{n}\mathfrak{n}'$.

algun dels nombres a', $2b'$, c', i el tercer, algun dels nombres a'', $2b''$, c''; o bé el primer $\mathfrak{n}'$, el segon, algun dels nombres a, $2b$, c, el tercer, algun dels nombres a'', $2b''$, c''; o bé, finalment, el primer $\mathfrak{n}''$, el segon, algun dels nombres a, $2b$, c i el tercer, algun dels nombres a', $2b'$, c'; cadascun d'aquests vint-i-set productes, a causa de les equacions Φ, és igual, o bé a algun dels 28 nombres $(1, 2)$, $(1, 3)$, etc., o bé a la suma o la diferència d'uns quants (per exemple, $\mathfrak{n}a'a'' = (1, 5)$, $2\mathfrak{n}a'b'' = (1, 6) + (2, 5)$, $4\mathfrak{n}b'b'' = (1, 8) + (2, 7) + (3, 6) + (4, 5)$ i així els restants); per la qual cosa, si aquests nombres tinguessin un divisor comú, aquest també hauria de dividir necessàriament tots aquells productes. D'aquí, però, es dedueix fàcilment, amb l'ajut de l'article 40 i pel mètode aplicat més sovint en el que precedeix, que el mateix divisor també hauria de dividir els nombres $\mathfrak{n}m'm''$, $\mathfrak{n}'mm''$, $\mathfrak{n}''mm'$, de manera que els quadrats d'aquests, $\frac{dm'm'm''m''}{\mathfrak{D}}$, $\frac{d'mmm''m''}{\mathfrak{D}}$, $\frac{d''mmm'm'}{\mathfrak{D}}$, són divisibles pel quadrat d'aquell, *Q. E. A.*, ja que, per I, el màxim comú divisor dels tres numeradors és $\mathfrak{D}$, de manera que aquests quadrats no poden tenir cap divisor comú.

VI. Totes aquestes [proposicions] pertanyen a la transformació de la forma $\mathfrak{F}$ en $ff'f''$, i s'han deduït de les transformacions de la forma F en ff' i de la forma $\mathfrak{F}$ en Ff''. Però, de manera completament similar, de les transformacions de la forma F' en ff'' i de la forma $\mathfrak{F}'$ en $F'f'$ es derivarà una transformació de la forma $\mathfrak{F}'$ en $ff'f''$ com $\mathfrak{X}' = (1)'xx'x'' + (2)'xx'y'' + (3)'xy'x'' + etc.$, $\mathfrak{Y}' = (9)'xx'x'' + (10)'xx'y'' + (11)'xy'x'' + etc.$ (designant tots els coeficients similarment com a la transformació de la forma $\mathfrak{F}$ en $ff'f''$, i enganxant a cadascun una

prima per a distingir-los) de la qual, igual com abans, es deduiran 28 equacions anàlogues a les Φ, que designarem per Φ', i unes altres 9 anàlogues a les Ψ, que expressarem per Ψ'. Això és, denotant $(1)'(10)' - (2)'(9)'$ per $(1,\,2)'$, $(1)'(11)' - (3)'(9)'$ per $(1,\,3)'$, etc., les equacions Φ' seran $(1,2)' = aa'\mathfrak{n}''$, $(1,3)' = aa''\mathfrak{n}'$, etc.; en canvi, les equacions Ψ', $(10)'(11)' - (9)'(12)' = a'\mathfrak{n}'\mathfrak{n}''\mathfrak{A}'$, etc. (Deixem als lectors un desenvolupament més extens per raó de brevetat; d'altra banda, per als experts no és, certament, necessari un nou càlcul, sinó que trobaran que aquí es pot transferir fàcilment per analogia la primera anàlisi.) Fetes aquestes així, de Φ i Φ' se segueix immediatament $(1,2) = (1,2)'$, $(1,3) = (1,3)'$, $(1,4) = (1,4)'$, $(2,3) = (2,3)'$, etc.; d'aquí, però, i del fet que tots els $(1,\,2)$, $(1,\,3)$, $(2,\,3)$, etc., no tenen cap divisor comú (per V), es conclou, amb l'ajut del lema de l'article 234, que es poden determinar quatre nombres enters α, β, γ, δ, de manera que resulti $\alpha(1)' + \beta(9)' = (1)$, $\alpha(2)' + \beta(10)' = (2)$, $\alpha(3)' + \beta(11)' = (3)$, etc.; $\gamma(1)' + \delta(9)' = (9)$, $\gamma(2)' + \delta(10)' = (10)$, $\gamma(3)' + \delta(11)' = (11)$, etc., i $\alpha\delta - \beta\gamma = 1$.

VII. D'aquí, i substituint de les tres primeres equacions de Ψ els valors de $a\mathfrak{A}$, $a\mathfrak{B}$, $a\mathfrak{C}$, i de les tres primeres equacions de Ψ' els valors de $a\mathfrak{A}'$, $a\mathfrak{B}'$, $a\mathfrak{C}'$, es confirma fàcilment que serà $a(\mathfrak{A}\alpha\alpha + 2\mathfrak{B}\alpha\gamma + \mathfrak{C}\gamma\gamma) = a\mathfrak{A}'$, $a(\mathfrak{A}\alpha\beta + \mathfrak{B}(\alpha\delta + \beta\gamma) + \mathfrak{C}\gamma\delta) = a\mathfrak{B}'$, $a(\mathfrak{A}\beta\beta + 2\mathfrak{B}\beta\delta + \mathfrak{C}\delta\delta) = a\mathfrak{C}'$, d'on, evidentment, se segueix, llevat que $a = 0$, que la forma $\mathfrak{F}$ es transforma en $\mathfrak{F}'$ per la substitució pròpia α, β, γ, δ. Però, aplicant en lloc de les tres primeres equacions de Ψ i Ψ' les tres següents, es confirmaran fàcilment tres equacions completament similars a les transmeses fa un moment, en les quals, en lloc del

factor a, es troba per tot arreu b; d'on és clar que també val ara la mateixa conclusió sempre que no sigui $b = 0$. Finalment, aplicant les tres últimes equacions de Ψ, Ψ', es trobarà, de la mateixa manera, que la conclusió és veritat llevat que $c = 0$. En conseqüència, com que, certament, tot els a, b, c, no poden ser simultàniament $= 0$, la forma $\mathfrak{F}$ es transformarà necessàriament en $\mathfrak{F}'$ per la substitució α, β, γ, δ, de manera que equivaldrà pròpiament a aquesta forma. *Q. E. D.*

241. Una forma tal com $\mathfrak{F}$ o bé $\mathfrak{F}'$, que s'origina si es compon una de les tres formes donades amb la que resulta de la composició de les dues restants, l'anomenarem *composta d'aquestes tres formes*, i és clar, de l'article precedent, que aquí no interessa gens en quin ordre es componguin les tres formes. De manera similar, proposades qualssevol formes f, f', f'', f''', etc. (de les quals les raons entre els determinants han de ser quadrats), si la forma f es compon amb f', la que resulta, amb f'', la que s'origina d'aquí, amb f''', etc., la forma que es produeix al final d'aquesta operació s'anomenarà composta *de totes les formes f, f', f'', f''', etc.* Però es demostra fàcilment que aquí també és arbitrari en quin ordre es componen les formes; *és a dir*, qualsevol ordre en què es componguin aquestes formes, les formes originades de la composició sempre són pròpiament equivalents. A més a més, és evident que si a les formes f, f', f'', etc. equivalen pròpiament les formes g, g', g'', etc., respectivament, la forma composta d'aquestes serà pròpiament equivalent a la forma composta d'aquelles.

242. Les proposicions precedents recullen la composició de formes amb la màxima generalitat; passem ara a aplicacions més particulars per les quals no hem volgut interrompre l'ordre d'aquelles. Primerament, certament, reprendrem el problema de l'article 236, que limitarem per les condicions següents: *primer*, que les formes que cal compondre tinguin el mateix determinant, o sigui, que sigui $d = d'$; *segon*, que m, m', siguin primers entre si; *tercer*, que la forma cercada sigui composta directament de cadascuna de les f, f'. D'aquí, mm, $m'm'$, també seran primers entre si; per tant, el màxim comú divisor dels nombres $dm'm'$, $d'mm$, és a dir, D, resultarà $= d = d'$, i $n = n' = 1$. Les quatre quantitats $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$, que es poden prendre a voluntat, les posarem $= -1$, 0, 0, 0, respectivament, cosa que serà lícita sempre, exceptuant-ne l'únic cas en què a, a', $b + b'$ són simultàniament $= 0$, el qual, doncs, no considerarem aquí; però, evidentment, aquest cas només pot ocórrer en formes de determinant positiu quadrat. Llavors, és clar que μ resulta el màxim comú divisor dels nombres a, a', $b+b'$; s'han d'agafar els nombres $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$, de manera que resulti $\mathfrak{P}'a+\mathfrak{P}''a'+\mathfrak{P}'''(b+b') = \mu$; però $\mathfrak{P}$ és completament arbitrari. D'aquí, substituint en els llocs citats p, q, p', q', etc., pels seus valors, prové $A = \dfrac{aa'}{\mu\mu}$, $B = \dfrac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D))$; però C es podrà determinar per l'equació $AC = BB - D$, sempre que a i a' no siguin simultàniament $= 0$.

Així, doncs, en aquesta solució, el valor de A no depèn dels valors dels $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ (que es poden determinar d'infinites maneres diferents); però, atribuint a aquests nombres altres valors, B obtindrà altres valors, i val la pena investigar de quina manera tots els valors

de B estan connectats entre si. Per a aquesta finalitat, observem que:

I. Sigui com sigui que es determinin $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$, els valors de B procedents d'això són tots congrus segons el mòdul A. Suposem que, si es posa $\mathfrak{P} = \mathfrak{p}$, $\mathfrak{P}' = \mathfrak{p}'$, $\mathfrak{P}'' = \mathfrak{p}''$, $\mathfrak{P}''' = \mathfrak{p}'''$, resulta $B = \mathfrak{B}$; però que, fent $\mathfrak{P} = \mathfrak{p} + \mathfrak{d}$, $\mathfrak{P}' = \mathfrak{p}' + \mathfrak{d}'$, $\mathfrak{P}'' = \mathfrak{p}'' + \mathfrak{d}''$, $\mathfrak{P}''' = \mathfrak{p}''' + \mathfrak{d}'''$, es produeix $B = \mathfrak{B} + \mathfrak{D}$. Llavors, doncs, serà $a\mathfrak{d}' + a'\mathfrak{d}'' + (b + b')\mathfrak{d}''' = 0$, $aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\mathfrak{d}''' = \mu\mathfrak{D}$. Multiplicant la primera part de la darrera equació per $a\mathfrak{p}' + a'\mathfrak{p}'' + (b + b')\mathfrak{p}'''$, la segona per μ, i restant al primer producte la quantitat $(ab'\mathfrak{p}' + a'b\mathfrak{p}'' + (b'b' + D)\mathfrak{p}''')(a\mathfrak{d}' + a'\mathfrak{d}'' + (b + b')\mathfrak{d}''')$, que, a causa de la primera equació, serà, evidentment, $= 0$, es tindrà, fet el desenvolupament i suprimit allò que es destrueix, $aa'(\mu\mathfrak{d} + ((b' - b)\mathfrak{p}'' + c'\mathfrak{p}''')\mathfrak{d}' + ((b - b')\mathfrak{p}' + c\mathfrak{p}''')\mathfrak{d}'' - (c'\mathfrak{p}' + c\mathfrak{p}'')\mathfrak{d}''') = \mu\mu\mathfrak{D}$, d'on, evidentment, $\mu\mu\mathfrak{D}$ serà divisible per aa', o sigui, $\mathfrak{D}$ per $\dfrac{aa'}{\mu\mu}$, és a dir, per A, i $\mathfrak{B} \equiv \mathfrak{B} + \mathfrak{D}$ (mòd. A).

II. Si els valors $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, $\mathfrak{p}'''$, de $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$, donen $B = \mathfrak{B}$, es poden trobar altres valors d'aquests nombres per als quals B obtingui un valor donat qualsevol congru a $\mathfrak{B}$ segons el mòdul A, posem $\mathfrak{B} + kA$. Primer, observem que els quatre nombres μ, c, c', $b - b'$, no poden tenir divisor comú; efectivament, si el tinguessin, aquest dividiria els sis nombres a, a', $b + b'$, c, c', $b - b'$, de manera que tant els a, $2b$, c, com els a', $2b'$, c', i, en conseqüència, també els m, m', que, per hipòtesi, són primers entre si. Per la qual cosa, es podran assignar quatre nombres enters h, h', h'', h''', tals que resulti $h\mu + h'c + h''c' + h'''(b - b') = 1$. Fet

això, si s'estableix $kh = \mathfrak{d}$, $k(h''(b+b') - h'''a') = \mu\mathfrak{d}'$, $k(h'(b+b') + h'''a) = \mu\mathfrak{d}''$, $-k(h'a' + h''a) = \mu\mathfrak{d}'''$, és clar que $\mathfrak{d}$, $\mathfrak{d}'$, $\mathfrak{d}''$, $\mathfrak{d}'''$, són enters; a més a més, es confirma fàcilment que resulta $a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''' = 0$, $aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb'+D)\mathfrak{d}''' = \dfrac{aa'k}{\mu}(\mu h + ch' + c'h'' + (b-b')h''') = \mu kA$. De la primera equació és clar que $\mathfrak{p}+\mathfrak{d}$, $\mathfrak{p}'+\mathfrak{d}'$, $\mathfrak{p}''+\mathfrak{d}''$, $\mathfrak{p}'''+\mathfrak{d}'''$, també són valors de $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$; de la darrera, que aquests valors produeixen $B = \mathfrak{B} + kA$. *Q. E. D.* D'aquí es copsa que sempre es pot determinar B de manera que estigui comprès entre 0 i $A-1$, inclusivament, suposat que A és positiu; o bé entre 0 i $-A-1$, si A és negatiu.

243. De les equacions $\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b+b') = \mu$, $B = \dfrac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb'+D))$, es dedueix $B = b + \dfrac{a}{\mu}(\mathfrak{P}a' + \mathfrak{P}'(b'-b) - \mathfrak{P}'''c) = b' + \dfrac{a'}{\mu}(\mathfrak{P}a + \mathfrak{P}''(b-b') - \mathfrak{P}'''c')$; per tant, $B \equiv b \left(\text{mòd. } \dfrac{a}{\mu}\right)$ i $B \equiv b' \left(\text{mòd. } \dfrac{a'}{\mu}\right)$. Quan $\dfrac{a}{\mu}$, $\dfrac{a'}{\mu}$, són primers entre si, entre 0 i $A-1$ (o sigui, entre 0 i $-A-1$, quan A és negatiu), només hi haurà comprès un únic nombre que sigui $\equiv b$ segons el mòdul $\dfrac{a}{\mu}$ i $\equiv b'$ segons el mòdul $\dfrac{a'}{\mu}$; si aquest es posa $= B$ i $\dfrac{B\mathfrak{B} - D}{A} = C$, és palès que ($A$, B, C) serà composta de les formes (a, b, c), (a', b', c'). Així, en aquest cas, per a trobar la forma composta, no convé considerar més els nombres $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$. Així, per exemple, si se cerca la forma composta de les formes (10, 3, 11), (15, 2, 7), a, a', $b+b'$ seran, respectivament,

$= 10,\ 15,\ 5$; $\mu = 5$; d'aquí, $A = 6$, $B \equiv 3\,(\text{mòd. } 2)$ i $\equiv 2\,(\text{mòd. } 3)$, d'on $B = 5$, i $(6,\ 5,\ 21)$, la forma buscada. D'altra banda, la condició que $\frac{a}{\mu}$, $\frac{a'}{\mu}$, siguin primers entre si equival completament que els dos nombres a, a', no tinguin divisor comú més gran que els tres a, a', $b+b'$, o sigui, el que rendeix el mateix, que el màxim comú divisor dels nombres a, a', també divideixi el nombre $b + b'$. Abans que res, es noten els casos particulars següents:

1) Proposades dues formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, del mateix determinant D, preparades de manera que el màxim comú divisor dels nombres a, $2b$, c, sigui primer amb el màxim comú divisor dels nombres a', $2b'$, c', i a primer amb a', la forma $(A,\ B,\ C)$ composta d'elles es troba fent $A = aa'$, $B \equiv b\,(\text{mòd. } a)$, i $\equiv b'\,(\text{mòd. } a')$, $C = \frac{BB - D}{A}$. Aquest cas té lloc sempre que una de les formes que cal compondre és la forma principal, posem $a = 1$, $b = 0$, $c = -D$. Llavors, serà $A = a'$, B es podrà establir $= b'$, d'on resultarà $C = c'$; per tant, *la composta de la forma principal i qualsevol altra forma del mateix determinant és aquesta mateixa forma.*

2) Si s'han de compondre dues formes *oposades* pròpiament primitives, posem $(a,\ b,\ c)$ i $(a,\ -b,\ c)$, serà $\mu = a$. D'aquí, es copsa fàcilment que la forma principal $(1,\ 0,\ -D)$ és composta d'aquelles.

3) Proposades qualssevol formes pròpiament primitives $(a,\ b,\ c)$, $(a',\ b',\ c')$, $(a'',\ b'',\ c'')$, etc., del mateix determinant D, els primers termes de les quals, a, a',

a'', etc., són nombres primers entre si, es troba la forma $(A,\ B,\ C)$ composta de totes elles establint A igual al producte de tots els a, a', a'', etc.; B congru a b, b', b'', etc., segons els mòduls a, a', a'', etc., respectivament; $C = \dfrac{BB - D}{A}$. En efecte, es copsa fàcilment que la composta de dues formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, serà la forma $(aa',\ B,\ \dfrac{BB - D}{aa'})$; d'aquesta i $(a'',\ b'',\ c'')$, la forma $(aa'a'',\ B,\ \dfrac{BB - D}{aa'a''})$, etc. Recíprocament,

4) Proposada una forma pròpiament primitiva $(A,\ B,\ C)$ de determinant D, si el terme A es descompon en factors qualssevol primers entre si a, a', a'', etc., s'agafen els nombres b, b', b'', etc., o bé iguals a B o almenys congrus segons els mòduls a, a', a'', etc., respectivament, i resulta $ac = bb - D$, $a'c' = b'b' - D$, $a''c'' = b''b'' - D$, etc., la forma $(A,\ B,\ C)$ serà composta de les formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, $(a'',\ b'',\ c'')$, etc., o sigui, *descomponible en aquestes formes*. Es prova sense dificultat que la mateixa proposició val encara que la forma $(A,\ B,\ C)$ sigui impròpiament primitiva o bé derivada. Així, d'aquesta manera, qualsevol forma es pot descompondre en altres del mateix determinant, tots els primers termes de les quals siguin o bé nombres primers o bé potències de nombres primers. Una tal descomposició es pot aplicar còmodament molt sovint si de moltes formes donades se n'ha de compondre una. Així, per exemple, si se cerca la forma composta de les formes (3, 1, 134), (10, 3, 41), (15, 2, 27), es descompon la segona en les (2, 1, 201), (5, −2, 81), la tercera en les (3, −1, 134), (5, 2, 81), i és clar que la forma composta de les cinc formes (3, 1, 134), (2, 1, 201), (5, −2, 81), (3, −1, 134), (5, 2, 81), qualsevol que sigui l'ordre en què s'agafin,

també serà la composta de les tres donades. Però de la composició de la primera amb la quarta s'origina la forma principal (1, 0, 401); aquesta mateixa prové de la composició de la tercera amb la cinquena; per tant, de la composició de totes es forma la forma (2, 1, 201).

5) A causa de la seva utilitat, val la pena explicar aquest mètode encara més àmpliament. De l'observació precedent, el problema de compondre qualssevol formes donades pròpiament primitives del mateix determinant, és evident que es pot reduir a la composició de formes els termes inicials de les quals siguin potències de nombres primers (ja que un nombre primer es pot considerar com la seva pròpia potència primera). Per la qual cosa, convé contemplar principalment el cas en què s'han de compondre dues formes pròpiament primitives $(a,\ b,\ c)$, $(a',\ b',\ c')$, en les quals a i a' són potències del *mateix* nombre primer. Així, sigui $a = h^\kappa$, $a' = h^\lambda$, on h designa un nombre primer, i suposem (la qual cosa és lícita) que κ no és menor que λ. Així, h^λ serà el màxim comú divisor dels nombres a, a', i si, a sobre, aquest divideix $b+b'$, es tindrà el cas considerat a l'inici d'aquest article i $(A,\ B,\ C)$ serà la composta de les donades si es posa $A = h^{\kappa-\lambda}$, $B \equiv b \left(\text{mòd. } h^{\kappa-\lambda}\right)$ i $\equiv b' \left(\text{mòd. } 1\right)$, condició, aquesta darrera, que, evidentment, es pot ometre, i $C = \dfrac{BB-D}{A}$. Però si h^λ no divideix $b+b'$, el màxim comú divisor d'aquests nombres i ell mateix serà necessàriament una potència de h; sigui, doncs, $= h^\nu$, i serà $\nu < \lambda$ (s'ha de posar $\nu = 0$ si, per casualitat, h^λ i $b+b'$ són primers entre si). Així, si es determinen $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$, de manera que resulti $\mathfrak{P}'h^\kappa + \mathfrak{P}''h^\lambda + \mathfrak{P}'''(b+b') = h^\nu$, però $\mathfrak{P}$ es pren a voluntat, la forma $(A,\ B,\ C)$ serà la composta de les donades si es posa $A = h^{\kappa+\lambda-2\nu}$,

$B = b + h^{\kappa-\nu}(\mathfrak{P}h^{\lambda} - \mathfrak{P}'(b-b') - \mathfrak{P}'''c)$, $C = \dfrac{BB-D}{A}$. Però es copsa fàcilment que, en aquest cas, també es pot prendre $\mathfrak{P}'$ a voluntat; per tant, posant $\mathfrak{P} = \mathfrak{P}' = 0$, resulta $B = b - \mathfrak{P}'''ch^{\kappa-\nu}$, o sigui, més generalment, $B = kA + b - \mathfrak{P}'''ch^{\kappa-\nu}$, on k designa un nombre arbitrari (article precedent). En aquesta fórmula senzillíssima només intervé $\mathfrak{P}'''$, que és el valor de l'expressió $\dfrac{h^{\nu}}{b+b'}\,(\text{mòd.}\,h^{\lambda})$. Si, per exemple, se cerca la forma composta de (16, 3, 19) i (8, 1, 37), és $h = 2$, $\kappa = 4$, $\lambda = 3$, $\nu = 2$. D'aquí, $A = 8$, $\mathfrak{P}'''$ és el valor de l'expressió $\dfrac{4}{4}\,(\text{mòd.}\,8)$, el qual és 1, d'on $B = 8k - 73$, de manera que, fent $k = 9$, és $B = -1$ i $C = 37$, o sigui, la forma cercada és (8, −1, 37).

Així, proposades formes qualssevol els termes inicials de les quals són tots potències de nombres primers, s'haurà de mirar en primer lloc si els termes inicials d'algunes són potències d'un *mateix* nombre primer i compondre-les entre elles respectivament d'acord amb la regla donada. D'aquesta manera s'obtindran formes els termes inicials de les quals seran encara potències de nombres primers, però tots diferents; per tant, la forma composta d'aquestes es podrà definir seguint la tercera observació. Per exemple, donades les formes (3, 1, 47), (4, 0, 35), (5, 0, 28), (16, 2, 9), (9, 7, 21), (16, 6, 11), de la primera i la cinquena resulta la forma (27, 7, 7); de la segona i la quarta resulta (16, −6, 11); d'aquesta i la sisena (1, 0, 140), de la qual es pot prescindir. Queden, per tant, les (5, 0, 28) i (27, 7, 7), de les quals resulta (135, −20, 4), i, en lloc d'ella, es pot prendre la forma pròpiament equivalent (4, 0, 35). Aquesta és, per tant, la resultant de la composició de les sis donades.

D'altra banda, d'aquesta font poden sorgir molts altres artificis útils en la pràctica; però, per no allargarnos massa, suprimim un tractament més extens d'aquesta qüestió, per a seguir amb consideracions més difícils.

244. Si per alguna forma f es pot representar un nombre a, per la forma f', un nombre a', i la forma F és transformable en ff', es copsa sense dificultat que el producte aa' serà representable per la forma F. D'aquí se segueix immediatament que, quan els determinants d'aquestes formes siguin negatius, la forma F serà positiva si, o bé f, f', són totes dues positives o bé totes dues negatives; contràriament, F resulta negativa si una de les formes f, f', és positiva i l'altra negativa. Mantinguem-nos, principalment, en el cas que hem considerat en l'article precedent, en què F és composta de f, f', i f, f' i F tenen el mateix determinant D. Suposem, a sobre, que les representacions dels nombres a, a', per les formes f, f', resulten per valors de les indeterminades primers entre si, i que la primera pertany al valor b de l'expressió $\sqrt{D}\,(\text{mòd.}\,a)$, la darrera al valor b' de l'expressió $\sqrt{D}\,(\text{mòd.}\,a')$, i es posa $bb - D = ac$, $b'b' - D = a'c'$. Llavors, per l'article 168, les formes $(a,\ b,\ c)$, $(a',\ b',\ c')$, equivaldran pròpiament a les formes f, f'; per tant, F també serà composta d'aquelles dues formes. Però la forma $(A,\ B,\ C)$ serà composta d'aquestes mateixes formes si, posat $= \mu$ el màxim comú divisor dels nombres a, a', $b+b'$, s'estableix $A = \dfrac{aa'}{\mu\mu}$, $B \equiv b$ i b', segons els mòduls $\dfrac{a}{\mu}$, $\dfrac{a'}{\mu}$, respectivament, $AC = BB - D$; per tant, aquesta forma equivaldrà pròpiament a la forma F. Ara, el nombre aa' es representa per la forma $Axx + 2Bxy + Cyy$ fent $x = \mu$, $y = 0$, valors dels quals el màxim comú divi-

sor és μ; per tant, aa' també es podrà representar per la forma F de manera que els valors de les indeterminades tinguin màxim comú divisor μ (article 166). Així, doncs, quan surti $\mu = 1$, aa' es podrà representar per la forma F atribuint a les indeterminades valors primers entre si, i aquesta representació pertanyerà al valor B de l'expressió $\sqrt{D}\,(\text{mòd.}\, aa')$, congru a b, b' segons els mòduls a, a', respectivament. La condició $\mu = 1$ sempre té lloc quan a, a', són primers entre si; en general, però, quan el màxim comú divisor de a, a', es primer amb $b + b'$.

245. Teorema. *Si la forma f s'ha de referir al mateix ordre que g, i, similarment, f' és del mateix ordre que g', la forma F composta de f, f', tindrà el mateix determinant i serà del mateix ordre que la forma G composta de g, g'.*

Dem. Siguin $= (a,\ b,\ c)$, $(a',\ b',\ c')$, $(A,\ B,\ C)$, respectivament, les formes f, f', F, i $= d$, d', D, els seus determinants. A més a més, sigui $= m$ el màxim comú divisor dels nombres a, $2b$, c; i $= \mathfrak{m}$ el màxim comú divisor dels nombres a, b, c; i tinguin m', $\mathfrak{m}'$, significats similars respecte de la forma f', i M, $\mathfrak{M}$, respecte de la forma F. Llavors, l'ordre de la forma f es determinarà pels nombres d, m, $\mathfrak{m}$, d'on els mateixos nombres també valdran per a la forma g; per la mateixa raó, els nombres d', m', $\mathfrak{m}'$, seran el mateix per a la forma g' que són per a la forma f'. Ara, per l'article 235, els nombres D, M, $\mathfrak{M}$, són determinats per d, d', m, m', $\mathfrak{m}$, $\mathfrak{m}'$; això és, D serà el màxim comú divisor de $dm'm'$, $d'mm$; $M = mm'$ i $\mathfrak{M} = \mathfrak{m}\mathfrak{m}'$ (si, simultàniament, $m = \mathfrak{m}$, $m' = \mathfrak{m}'$) o bé $= 2\mathfrak{m}\mathfrak{m}'$ (si $m = 2\mathfrak{m}$ o bé $m' = 2\mathfrak{m}'$). Aquestes propietats de D, M, $\mathfrak{M}$, com que se segueixen

del fet que F és composta de f, f', es copsa fàcilment que D, M, i $\mathfrak{M}$ també valen per a la forma G, de manera que G és del mateix ordre que F. *Q. E. D.*

Per aquesta raó, anomenarem compost dels ordres en què són les formes f, f', l'ordre en què és la forma F. Així, per exemple, el compost de dos ordres pròpiament primitius sempre és un ordre similar; i d'un pròpiament primitiu i un impròpiament primitiu, un impròpiament primitiu. S'haurà d'entendre de manera similar quan algun ordre s'anomenarà compost de molts d'altres ordres.

246. Problema. *Proposades dues formes primitives qualssevol f, f', de la composició de les quals s'origina F, definir el gènere a què s'haurà de referir F a partir dels gèneres a què pertanyen f, f'.*

Solució. I. Considerem, primer, el cas en què, com a mínim, una de les formes f, f', *per exemple*, la primera, és pròpiament primitiva, i designem per d, d', D, els determinants de les formes f, f', F. Llavors, D serà el màxim comú divisor dels nombres $dm'm'$, d', on m' és o bé 1 o bé 2 segons si la forma f' és pròpiament o bé impròpiament primitiva; en aquell cas, però, F pertanyerà a un ordre pròpiament primitiu, en aquest, a un impròpiament primitiu. Ara, es definirà el gènere de la forma F pels seus caràcters particulars, naturalment, tant respecte de cadascun dels divisors primers imparells de D, com, en alguns casos, respecte dels nombres 4 o bé 8. Així, doncs, convindrà determinar cada un d'aquests.

1r. Si p és un divisor primer imparell qualsevol de D, necessàriament també dividirà d, d', de manera que entre els caràcters de les formes f, f', també ocorreran les seves relacions amb p. Ara, si per f es pot representar un nombre a, per f', un nombre a', el producte aa' es podrà representar per F. Així, si els residus quadràtics de p (no divisibles per p) es poden representar tant per f com per f', també es podran representar per F els residus quadràtics de p; és a dir, si totes dues f, f', tenen el caràcter Rp, la forma F tindrà el mateix caràcter. Per una raó similar, F tindrà el caràcter Rp si totes dues f, f', tenen el caràcter Np; contràriament, F tindrà el caràcter Np si una de les formes f, f', té Rp, l'altra, Np.

2n. Si en el caràcter íntegre de la forma F hi intervé una relació amb el nombre 4, la tal relació també ha d'intervenir en els caràcters de les formes f, f'. Llavors, efectivament, allò només s'esdevindrà quan $D \equiv 0$ o bé $\equiv 3 \,(\text{mòd. } 4)$. Quan D és divisible per 4, també $dm'm'$ i d' seran divisibles per 4, d'on és clar immediatament que f' no pot ser impròpiament primitiva, de manera que és $m' = 1$; d'aquí, tant d com d' seran divisibles per 4, i en tots dos caràcters hi intervindrà la relació amb 4. Quan $D \equiv 3 \,(\text{mòd. } 4)$, D dividirà d, d'; els quocients seran quadrats, de manera que, necessàriament, d, d', també, o bé $\equiv 0$ o bé $\equiv 3 \,(\text{mòd. } 4)$; i entre els caràcters de f, f', [hi haurà] una relació amb 4. D'aquí se segueix, de la mateixa manera que en (1r), que el caràcter de la forma F serà 1, 4, si o bé totes dues f, f', tenen 1, 4, o bé totes dues 3, 4; contràriament, el caràcter de la forma F serà 3, 4, si una de les formes f, f', té 1, 4, l'altra, 3, 4.

3r. Quan D és divisible per 8, també ho serà d'; d'aquí, certament, f' [serà] pròpiament primitiva, $m' = 1$, i d també divisible per 8; per tant, entre els caràcters de la forma F, només pot tenir lloc, llavors, algun dels caràcters 1, 8; 3, 8; 5, 8; 7, 8, si també apareix la tal relació amb 8 en el caràcter tant de la forma f com de la forma f'. Però, de la mateixa manera que abans, es confirma fàcilment que el caràcter de la forma F serà 1, 8, si f, f', tenen el mateix respecte de 8; el caràcter de la forma F serà 3, 8, si una de les formes f, f', té 1, 8, l'altra 3, 8, o bé una 5, 8, l'altra 7, 8; que F té 5, 8, si f, f', tenen 1, 8, i 5, 8, o bé 3, 8, i 7, 8; que F té 7, 8, si f, f', tenen 1, 8, i 7, 8, o bé 3, 8, i 5, 8.

4t. Quan $D \equiv 2\,(\text{mòd.}\,8)$, d' serà o bé $\equiv 0$ o bé $\equiv 2\,(\text{mòd.}\,8)$; d'aquí, $m' = 1$, de manera que d també o bé $\equiv 0$ o bé $\equiv 2\,(\text{mòd.}\,8)$; no obstant això, tots dos d, d', no poden ser divisibles per 8, ja que D és el seu *màxim* comú divisor. Per tant, només s'haurà d'atribuir a la forma F algun dels caràcters 1 *i* 7, 8; 3 *i* 5, 8, en el cas en què, o bé totes dues formes f, f', en tenen algun d'aquests, o bé l'un, algun d'aquells i l'altre, un dels 1, 8; 3, 8; 5, 8; 7, 8. D'aquí es dedueix fàcilment que el caràcter de la forma F es determina per la taula següent, si el caràcter posat en el marge pertany a una de les formes f, f', però el caràcter en la capçalera, a l'altra.

	1 *i* 7,8 o bé 1,8 o bé 7,8	3 *i* 5,8 o bé 3,8 o bé 5,8
1 *i* 7,8	1 *i* 7,8	3 *i* 5,8
3 *i* 5,8	3 *i* 5,8	1 *i* 7,8

5è. Es prova de la mateixa manera que no es pot atribuir a F cap dels caràcters 1 i 3, 8, o bé 5 i 7, 8, llevat que, almenys, algun d'aquests també correspongui a una de les formes f, f', i, a l'altra, o bé algun d'aquests mateixos o bé un dels 1, 8; 3, 8; 5, 8; 7, 8. I, certament, el caràcter de la forma F es determinarà per aquesta taula, en el marge i en la capçalera de la qual hi ha els caràcters de les formes f, f'.

	1 i 3,8 o bé 1,8 o bé 3,8	5 i 7,8 o bé 5,8 o bé 7,8
1 i 3,8	1 i 3,8	5 i 7,8
5 i 7,8	5 i 7,8	1 i 3,8

II. Si cada una de les dues formes f, f', és impròpiament primitiva, D serà el màxim comú divisor dels nombres $4d$, $4d'$; o sigui, $\frac{1}{4}D$ el màxim comú divisor dels nombres d, d'. D'aquí se segueix fàcilment que tant d com d' com $\frac{1}{4}D$ seran $\equiv 1 \,(\text{mòd. } 4)$. Però, posant $F = (A, B, C)$, el màxim comú divisor dels nombres A, B, C, serà $= 2$ i el màxim comú divisor dels nombres A, $2B$, C, serà 4. Per tant, F serà una forma derivada de la impròpiament primitiva $\left(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C\right)$, el determinant de la qual serà $\frac{1}{4}D$, i el gènere de la qual determinarà el gènere de la forma F. Però, el caràcter d'aquella forma, com a impròpiament primitiva, no implicarà relacions amb 4 i 8, sinó només relacions amb cadascun dels divisors primers imparells de $\frac{1}{4}D$. Ara,

com que, evidentment, tots aquests divisors també divideixen d, d', i la meitat de qualsevol producte de dos factors dels quals un és representable per f, l'altre per f', es pot representar per la forma $\left(\frac{1}{2}A,\ \frac{1}{2}B,\ \frac{1}{2}C\right)$, es copsarà fàcilment que el caràcter d'aquesta forma respecte de qualsevol nombre primer imparell p que divideix $\frac{1}{4}D$ serà Rp, *tant* si fos $2Rp$ i les formes f, f', tinguessin el mateix caràcter respecte de p, *com* si fos $2Np$ i els caràcters de les formes f, f', respecte de p, oposats; contràriament, el caràcter d'aquella forma serà Np, *tant* si f, f', tenen el caràcters iguals respecte de p i és $2Np$, *com* si f, f', els tenen oposats i és $2Rp$.

247. De la solució del problema precedent, és evident que si g és una forma primitiva del mateix ordre i gènere que f, i g' una forma primitiva del mateix ordre i gènere que f', la forma composta de g i g' pertany al mateix gènere a què pertanyi la forma composta de f i f'. D'aquí se segueix espontàniament el significat de *gènere compost* de dos altres gèneres (o també de més de dos). A més a més, d'allò és clar que si f, f', tenen el mateix determinant i f és una forma del gènere principal, però F és composta de f i f', F serà del mateix gènere que f'; en conseqüència, sempre es podrà ometre el gènere principal en la composició amb altres gèneres del mateix determinant. Però, si mantingudes les restants [hipòtesis], f no és del gènere principal, però f' és una forma primitiva, F serà, certament, d'un altre gènere que f'. Finalment, si f, f', són formes pròpiament primitives del mateix gènere, F serà del gènere principal; però si f, f', són totes dues pròpiament primitives del mateix determinant, però de gèneres diferents,

F no podrà pertànyer al gènere principal. Així, si una forma pròpiament primitiva qualsevol es compon *amb ella mateixa*, la forma resultant d'això, que també serà pròpiament primitiva i del mateix determinant, pertanyerà necessàriament al gènere principal.

248. Problema. *Proposades dues formes qualssevol f, f', la composta de les quals és F, definir el gènere de la forma F a partir dels gèneres de les formes f, f'.*

Solució. Sigui $f = (a, b, c)$, $f' = (a', b', c')$, $F = (A, B, C)$; a més a més, $\mathfrak{m}$ el màxim comú divisor dels nombres a, b, c, i $\mathfrak{m}'$ el màxim comú divisor dels nombres a', b', c', de manera que f, f', siguin derivades de les primitives $\left(\frac{a}{\mathfrak{m}}, \frac{b}{\mathfrak{m}}, \frac{c}{\mathfrak{m}}\right)$, $\left(\frac{a'}{\mathfrak{m}'}, \frac{b'}{\mathfrak{m}'}, \frac{c'}{\mathfrak{m}'}\right)$, que denotarem per $\mathfrak{f}$, $\mathfrak{f}'$, respectivament. Ara, si almenys una de les formes $\mathfrak{f}$, $\mathfrak{f}'$, és pròpiament primitiva, el màxim comú divisor dels nombres A, B, C, serà $\mathfrak{m}\mathfrak{m}'$, de manera que F, derivada de la forma primitiva $\left(\frac{A}{\mathfrak{m}\mathfrak{m}'}, \frac{B}{\mathfrak{m}\mathfrak{m}'}, \frac{C}{\mathfrak{m}\mathfrak{m}'}\right)$ ... $\mathfrak{F}$, d'on és clar que el gènere de la forma F depèn del gènere de la forma $\mathfrak{F}$. Però es copsarà fàcilment que $\mathfrak{F}$ es transforma en $\mathfrak{f}\mathfrak{f}'$ per la mateixa substitució per la qual F es transforma en ff', de manera que $\mathfrak{F}$ és composta de $\mathfrak{f}$, $\mathfrak{f}'$, i el seu gènere es pot determinar pel problema de l'article 246. Però si cada una de les $\mathfrak{f}$, $\mathfrak{f}'$, és impròpiament primitiva, el màxim comú divisor dels nombres A, B, C, serà $2\mathfrak{m}\mathfrak{m}'$, i la forma $\mathfrak{F}$ també composta de $\mathfrak{f}$, $\mathfrak{f}'$, i, evidentment, derivada de la pròpiament primitiva $\left(\frac{A}{2\mathfrak{m}\mathfrak{m}'}, \frac{B}{2\mathfrak{m}\mathfrak{m}'}, \frac{C}{2\mathfrak{m}\mathfrak{m}'}\right)$. Així, el gènere

d'aquesta forma es podrà determinar per l'article 246, i, com que F és derivada d'aquesta mateixa forma, d'aquí es distingeix espontàniament el seu gènere.

D'aquesta solució, és evident que el teorema explicat a l'article precedent per a formes primitives, això és, *si f', g', són dels mateixos gèneres respectivament que f, g, la forma $f'g'$ serà del mateix gènere que sigui la forma composta de f, g*, val en general per a formes qualssevol.

249. Teorema. *Si les formes f, f', són dels mateixos ordres, gèneres i classes que g, g', respectivament, la forma composta de f i f' serà de la mateixa classe que la forma composta de g i g'.*

D'aquest teorema (la veritat del qual se segueix directament de l'article 239) serà clar espontàniament el significat de *classe composta de dues classes donades*, o també *de més de dues*.

Si es compon una classe qualsevol K amb la classe principal, es produirà la mateixa classe K, o sigui, la classe principal es pot negligir en la composició amb altres classes del mateix determinant. De la composició de dues classes pròpiament primitives oposades, sempre s'origina la classe principal del mateix determinant (vegeu l'article 243). Així, com que qualsevol classe ambigua és oposada a si mateixa, de la composició de qualsevol classe ambigua pròpiament primitiva amb si mateixa s'obté la classe principal del mateix determinant.

De l'última proposició també val el recíproc. Això és, *si de la composició d'una classe pròpiament primi-*

tiva K amb si mateixa s'obté la classe principal H del mateix determinant, K serà necessàriament una classe ambigua. En efecte, si K' és la classe oposada a K, la composta de les tres classes K, K, K', serà la mateixa classe que s'origina de H i K'; d'aquelles prové K (ja que K i K' produeixen H, i aquesta amb K la mateixa K), i, d'aquestes, K'; per tant, K coincidirà amb K' i la classe serà, certament, ambigua.

A més a més, noteu aquesta proposició: *Si les classes K, L, són oposades a les classes K', L', respectivament, la classe composta de K i L serà l'oposada de la classe composta de K' i L'.* Siguin f, g, f', g', formes de les classes K, L, K', L'; F, la forma composta de f, g; i F', la composta de f', g'. Com que f' equival impròpiament a f, i g' a g, però F és composta directament de f, g, F també serà composta de f', g', però de totes dues inversament. Per tant, qualsevol forma que equivalgui impròpiament a F serà composta directament de f', g', de manera que equivaldrà pròpiament a F' (articles 238, 239), d'on F, F', equivaldran impròpiament i les classes a què pertanyen seran oposades.

D'aquí se segueix que si una classe ambigua K es compon amb una classe ambigua L, sempre es produeix una classe ambigua. Efectivament, la classe serà oposada a la que és composta de les classes oposades a K, L, de manera que a si mateixa, ja que aquestes classes són oposades a si mateixes.

Finalment, observem que si són proposades dues classes qualssevol K, L, del mateix determinant, la primera de les quals és pròpiament primitiva, sempre es pot trobar una classe M del mateix determinant la com-

posta de la qual i K sigui L. Evidentment, això s'obté agafant per a M la classe que és composta de L i la classe oposada a K; simultàniament, es copsarà facilíssimament que aquesta classe és l'única proveïda d'aquesta propietat, o sigui, que classes diferents del mateix determinant compostes amb la mateixa classe pròpiament primitiva produeixen classes diferents.

La composició de classes es pot denotar còmodament pel signe d'addició, +, així com la identitat de classes pel signe d'igualtat. Amb aquests signes, la proposició transmesa fa un moment es pot expressar així: Si K' és la classe oposada a K, $K+K'$ serà la classe principal del mateix determinant, d'on $K+K'+L=L$; així, posada $K'+L=M$, serà $K+M=L$, com es desitjava; però si, a part de M, es donés una altra M' proveïda de la mateixa propietat, o sigui, $K+M'=L$, seria $K+K'+M'=L+K'=M$, d'on $M=M'$. Si es componen moltes classes idèntiques, això (a la manera de multiplicació) es pot denotar, fent-les precedir del seu nombre, de manera que $2K$ designarà el mateix que $K+K$, $3K$ el mateix que $K+K+K$, etc. Els mateixos signes també es podrien transferir a les formes, de manera que $(a,\ b,\ c)+(a',\ b',\ c')$ designés la forma composta de $(a,\ b,\ c)$, $(a',\ b',\ c')$; però, perquè no es pugui originar cap mena d'ambigüitat, preferim abstenir-nos d'aquesta abreviatura, sobretot perquè ja hem atribuït un significat peculiar a un signe com $\sqrt{M\cdot(a,b,c)}$. Direm que la classe $2K$ s'origina de la *duplicació* de la classe K, la classe $3K$ de la *triplicació*, etc.

250. Si D és un nombre divisible per mm (on suposem m positiu), es donarà un ordre de formes de determinant D derivat d'un ordre pròpiament primitiu

de determinant $\frac{D}{mm}$ (o bé *dos*, certament, quan D és negatiu, un positiu i un negatiu); evidentment, la forma $(m, 0, -\frac{D}{m})$ pertanyerà a aquell ordre (això és, al positiu) i amb raó es pot considerar com *la forma més simple* en ell (igualment, $\left(-m, 0, \frac{D}{m}\right)$ serà la més simple de l'ordre negatiu quan D és negatiu). Si, a sobre, és $\frac{D}{mm} \equiv 1 \,(\text{mòd. } 4)$, també es donarà un ordre de formes de determinant D derivat de l'ordre impròpiament primitiu de determinant $\frac{D}{mm}$, al qual pertanyerà, evidentment, la forma $\left(2m, m, \frac{mm - D}{2m}\right)$, que es tindrà com la més simple en ell. (Quan D és negatiu, es donaran novament dos ordres i, en el negatiu, es tindrà la forma $\left(-2m, -m, \frac{D - mm}{2m}\right)$ com la més simple.) Així, per exemple, si també es vol considerar aquí el cas en què $m = 1$, en els quatre ordres de formes de determinant 45 les més simples seran les següents: $(1, 0, -45)$, $(2, 1, -22)$, $(3, 0, -15)$, $(6, 3, -6)$. Enteses aquestes així, es presenta el

PROBLEMA. *Proposada una forma qualsevol F de l'ordre O, trobar una forma pròpiament primitiva (positiva) del mateix determinant, la composició de la qual amb la forma més simple de O origini F.*

Solució. Sigui la forma $F = (ma, mb, mc)$ derivada de la primitiva $f = (a, b, c)$, el determinant de la qual és $= d$, i suposem, *primer*, que f és pròpiament primitiva. Observem, primerament, que si per cas a no

és primer amb $2dm$, es donen, certament, altres formes pròpiament equivalents a $(a,\ b,\ c)$ els primers termes de les quals estan proveïts d'aquesta propietat. Efectivament, per l'article 228, es donen nombres primers amb $2dm$ representables per aquella forma; sigui $a' = a\alpha\alpha + 2b\alpha\gamma + c\gamma\gamma$ un tal nombre, i suposem (que és lícit) que α, γ, són primers entre si; llavors, agafats β, δ, de manera que resulti $\alpha\delta - \beta\gamma = 1$, f es transformarà, per la substitució α, β, γ, δ, en la forma $(a',\ b',\ c')$, que equivaldrà pròpiament a aquella i estarà proveïda de la propietat predita. Ara, com que F i $(a'm,\ b'm,\ c'm)$ també equivalen pròpiament, es copsarà fàcilment que és suficient considerar el cas en què a és primer amb $2dm$. Llavors, $(a,\ bm,\ cmm)$ serà una forma pròpiament primitiva (en efecte, si a, $2bm$, cmm, tinguessin un divisor comú, aquest també dividiria $2dm = 2bbm - 2acm$) del mateix determinant que F, i es confirma fàcilment que F es transforma en el producte de la forma $(m,\ 0,\ -dm)$, que, llevat que F sigui una forma negativa, serà la més simple de l'ordre O, per $(a,\ bm,\ cmm)$, per la substitució $1,\ 0,\ -b,\ -cm;\ 0,\ m,\ a,\ bm$; d'on es conclou, pel criteri de l'observació 4 de l'article 235, que F és composta de $(m,\ 0,\ -dm)$ i $(a,\ bm,\ cmm)$. Però, quan F és una forma negativa, es transformarà en el producte de la forma més simple del mateix ordre, $(-m,\ 0,\ dm)$, per la positiva $(-a,\ bm,\ -cmm)$ per la substitució $1,\ 0,\ b,\ -cm;\ 0,\ -m,\ -a,\ bm$; de manera que serà la forma composta d'elles.

Segon, si f és una forma impròpiament primitiva, serà lícit suposar que $\frac{1}{2}a$ és primer amb $2dm$; en efecte, si aquesta propietat encara no té lloc en la forma f, es pot trobar una forma pròpiament equivalent a f i

proveïda d'aquesta propietat. D'aquí, però, se segueix fàcilment que $\left(\frac{1}{2}a,\ bm,\ 2cmm\right)$ és una forma pròpiament primitiva del mateix determinant que F; de manera igualment fàcil, es confirma que F es transforma en el producte de les formes $\left(\pm 2m,\ \pm m,\ \pm\frac{1}{2}(m-dm)\right)$, $\left(\pm\frac{1}{2}a,\ bm,\ \pm 2cmm\right)$ per la substitució $1,\ 0,\ \frac{1}{2}(1\mp b),\ -cm;$ $0,\ \pm 2m,\ \pm\frac{1}{2}a,\ (b\pm 1)m$, on s'han d'agafar els signes inferiors quan F és una forma negativa, els superiors en els casos restants, de manera que és composta d'aquestes dues formes de les quals la primera serà la més simple de l'ordre O, la darrera una forma pròpiament primitiva (positiva).

251. Problema. *Proposades dues formes F, f, del mateix determinant D i que pertanyen al mateix ordre O, trobar una forma pròpiament primitiva de determinant D que, composta amb f, produeixi F.*

Solució. Sigui ϕ la forma més simple de l'ordre O; $\mathfrak{F}$, $\mathfrak{f}$ les formes pròpiament primitives de determinant D que, compostes amb ϕ, produeixin F, f, respectivament; finalment, f' una forma pròpiament primitiva que, composta amb $\mathfrak{f}$, produeixi $\mathfrak{F}$. Llavors, la forma F serà composta de les tres formes ϕ, $\mathfrak{f}$, f', o sigui, de les dues f, f', *Q. E. I.*

Així, qualsevol classe d'un ordre donat es pot considerar com a composta de qualsevol classe donada del mateix ordre i alguna classe pròpiament primitiva del mateix determinant.

252. Teorema. *Per a un determinant donat, a cada un dels gèneres d'un mateix ordre hi ha contingudes la mateixa quantitat de classes.*

Dem. Pertanyin els gèneres G i H al mateix ordre, consti G de les n classes K, K', K'', $\ldots$, K^{n-1}, i sigui L alguna classe del gènere H. S'investiga, per l'article precedent, la classe pròpiament primitiva M del mateix determinant, la composició de la qual amb K produeixi L, i es designen per L', L'', $\ldots$, L^{n-1}, les classes que s'originen de la composició de la classe M amb K', K'', $\ldots$, K^{n-1}, respectivament. Llavors, de l'última observació de l'article 249 se segueix que totes les classes L, L', L'', $\ldots$, L^{n-1}, són diferents, i, per l'article 248, totes pertanyeran al mateix gènere, és a dir, al gènere H. Finalment, es copsarà fàcilment que H no pot contenir altres classes a part d'aquestes, ja que qualsevol classe del gènere H es pot considerar com a composta de M i una altra classe del mateix determinant, que, necessàriament, serà sempre del gènere G. En conseqüència, H, igual que G, conté n classes diferents. *Q. E. D.*

253. El teorema precedent suposa la identitat de l'ordre i no s'ha d'estendre a ordres diferents. Així, per exemple, per al determinant -171, es donen 20 classes positives que es redueixen a quatre ordres; en l'ordre pròpiament primitiu es contenen dos gèneres, cadascun dels quals comprèn sis classes; en l'ordre impròpiament primitiu, els dos gèneres posseeixen quatre classes, dues cadascun; en l'ordre derivat de l'ordre pròpiament primitiu de determinant -19 hi ha un únic gènere que conté tres classes; finalment, l'ordre derivat de l'impròpiament primitiu de determinant -19 té un únic gènere que consta d'una classe; es comporten igualment les classes ne-

gatives. Així, val la pena esbrinar un principi general del qual depengui el nexe entre la quantitat de classes en diferents ordres. Suposem que K, L són dues classes del mateix ordre (positiu) O de determinant D, i M una classe pròpiament primitiva del mateix determinant de la composició de la qual amb K s'origini L, que, per l'article 251, sempre es pot assignar. Ara, en alguns casos pot resultar que M sigui *l'única* classe pròpiament primitiva que composta amb K produeixi L; en altres, poden existir moltes classes pròpiament primitives diferents proveïdes d'aquesta propietat. Suposem, en general, que es donen r classes pròpiament primitives d'aquest tipus, M, M', M'', $\ldots$, M^{r-1}, cadascuna de les quals composta amb K produeixi la mateixa classe L, i designem el seu complex per W. A més a més, sigui L' una altra classe (diferent de la classe L) de l'ordre O, i N' la classe pròpiament primitiva de determinant D que composta amb L doni com a resultat L', i es designa per W' el complex de les classes $N'+M$, $N'+M'$, $N'+M''$, $\ldots$, $N'+M^{r-1}$ (que seran totes pròpiament primitives i diferents entre si). Llavors, es copsarà fàcilment que K composta amb qualsevol classe de W' produeix L', d'on es conclou que W i W' no tenen cap classe comuna; a part d'això, es comprova sense dificultat que no es dóna cap classe pròpiament primitiva no continguda en el complex W' que, composta amb K, produeixi L'. De la mateixa manera, és clar que si L'' és una altra classe de l'ordre O diferent de les classes L, L', es donen r formes pròpiament primitives diferents tant entre si com de les formes W, W', que, compostes cadascuna amb K, produeixin L'', i igualment es tindrà això per a totes les classes restants de l'ordre O. Però, com que qualsevol classe pròpiament primitiva (positiva) de determinant D composta amb K produeix una classe de

l'ordre O, d'aquí es conclou fàcilment que, si la quantitat de totes les classes de l'ordre O és n, la quantitat de totes les classes pròpiament primitives (positives) del mateix determinant serà rn. Així tenim la regla general: Si K, L, denoten classes qualssevol de l'ordre O, i r la quantitat de classes pròpiament primitives diferents del mateix determinant, cadascuna de les quals composta amb K produeix L, la quantitat de totes les classes en l'ordre pròpiament primitiu (positiu) serà r vegades més gran que la quantitat de classes de l'ordre O.

Com que les classes K, L, es poden prendre completament a voluntat en l'ordre O, també serà lícit agafar classes idèntiques, i, certament, per a això serà útil la classe en què es conté la forma més simple d'aquest ordre. Així, prenent aquesta per K i L, la qüestió és reduïda que s'assignin totes les classes pròpiament primitives que compostes amb K reprodueixin K. Això aplana el camí mitjançant el següent

254. Teorema. *Si $F = (A, B, C)$ és la forma més simple de l'ordre O de determinant D, i $f = (a, b, c)$ una forma pròpiament primitiva del mateix determinant, el nombre AA es podrà representar per aquesta forma f, si F s'origina per composició de les formes f, F; i, recíprocament, F serà composta d'ella mateixa i f, si AA es pot representar per f.*

Dem. I. Si F es transforma en el producte fF per la substitució p, p', p'', p'''; q, q', q'', q''', per l'article 235, tenim $A(aq''q'' - 2bqq'' + cqq) = A^3$, d'on $AA = aq''q'' - 2bqq'' + cqq$. *Q. E. P.*

II. *Si se suposa* que AA es pot representar per f, es designen per q'', $-q$, els valors de les indeterminades pels quals això s'efectua, o sigui, sigui $AA = aq''q'' - 2bqq'' + cqq$, i es posa $q''a - q(b+B) = Ap$, $-qC = Ap'$, $q''(b-B) - qc = Ap''$, $-q''C = Ap'''$, $q''a - q(b-B) = Aq'$, $q''(b+B) - qc = Aq'''$. Fet això, es confirma fàcilment que F es transforma en el producte fF per la substitució p, p', p'', p'''; q, q', q'', q''', i, encara més, és composta de f i F sempre que tots els nombres p, p', etc., siguin enters. Ara, per la descripció de la forma més simple, B és o bé 0 o bé $\frac{1}{2}A$, de manera que $\frac{2B}{A}$, enter; d'això és clar que $\frac{C}{A}$ sempre és enter. D'aquí, $q' - p$, p', $q''' - p''$, p''', seran enters; i, en especial, només resta que es provi que p i p'' són enters. Però resulta $pp + \frac{2pqB}{A} = a - \frac{qqC}{A}$, $p''p'' + \frac{2p''q''B}{A} = c - \frac{q''q''C}{A}$; per la qual cosa, si $B = 0$, resulta $pp = a - \frac{qqC}{A}$, $p''p'' = c - \frac{q''q''C}{A}$, i, en conseqüència, p, p'', enters; però, si $B = \frac{1}{2}A$, resulta $pp + pq = a - \frac{qqC}{A}$, $p''p'' + p''q'' = c - \frac{q''q''C}{A}$, d'on es conclou de manera igualment fàcil que p i p'', també en aquest cas, són enters. D'això es conclou que F és composta de f i F. *Q. E. S.*

255. Així, el problema s'ha reduït que convé assignar totes les classes pròpiament primitives de determinant D, per les formes de les quals es pot representar AA. Evidentment, AA es pot representar per qualsevol forma el primer terme de la qual és o bé AA o bé el quadrat d'una part alíquota de A; però, recíprocament, si AA es pot representar per la forma f, atribuint a les

indeterminades els valors αe, γe, el màxim comú divisor dels quals és e, la forma f es transformarà per la substitució α, β, γ, δ, en una forma el primer terme de la qual és $\frac{AA}{ee}$, i aquesta forma equivaldrà pròpiament a la forma f si s'agafen β, δ, de manera que resulti $\alpha\delta - \beta\gamma = 1$; d'on és clar que, en qualsevol classe per les formes de la qual es pugui representar AA, es troben formes el primer terme de les quals és AA o bé el quadrat d'una part alíquota de A. Així, la qüestió consisteix a trobar totes les classes pròpiament primitives de determinant D en les quals ocorrin formes d'aquest tipus, que s'obté de la manera següent: Siguin a, a', a'', etc., tots els divisors (positius) de A; s'investiguen tots els valors de l'expressió $\sqrt{D}\,(\text{mòd. } aa)$ situats entre 0 i $aa - 1$, inclusivament, que són b, b', b'', etc., i es posa $bb - D = aac$, $b'b' - D = aac'$, $b''b'' - D = aac''$, etc.; es designa per V el complex de les formes (aa, b, c), (aa, b', c'), etc. Llavors, es copsa fàcilment que en qualsevol classe de determinant D en què ocorri una forma el primer terme de la qual és aa, també hi ha d'estar continguda alguna forma de V. De manera similar, es troben totes les formes de determinant D el primer terme de les quals és $a'a'$ i el central situat entre 0 i $a'a' - 1$, inclusivament, i es designa el seu complex per V'; per la mateixa raó, sigui V'' el complex de les formes similars el primer terme de les quals sigui $a''a''$, etc. De V, V', V'', etc., es rebutgen totes les formes que no són pròpiament primitives, es redueixen les restants a classes, i, si per cas en queden moltes pertanyents a la mateixa classe, se'n reté només una a cada classe. D'aquesta manera es tindran totes les classes buscades, i la quantitat d'aquestes a la unitat serà com la de totes les classes pròpiament primitives (positives) a la quantitat de classes en l'ordre O.

Exemple. Sigui $D = -531$ i O l'ordre positiu derivat de l'ordre impròpiament primitiu de determinant -59, en el qual la forma més simple és (6, 3, 90), o sigui, $A = 6$. Aquí, a, a', a'', a''', seran 1, 2, 3, 6; V contindrà la forma (1, 0, 531); V', les (4, 1, 133), (4, 3, 135); V'', les (9, 0, 59), (9, 3, 60), (9, 6, 63), i, finalment, V''', les (36, 3, 15), (36, 9, 17), (36, 15, 21), (36, 21, 27), (36, 27, 35), (36, 33, 45); d'aquestes dotze formes, però, se n'han de rebutjar sis: posem, de V'', la segona i la tercera; de V''', la primera, la tercera, la quarta i la sisena, que són totes formes derivades; es troba que les sis restants pertanyen totes a classes diferents. Realment, la quantitat de classes pròpiament primitives (positives) de determinant -531 és 18, i la quantitat de classes impròpiament primitives (positives) de determinant -59 (o sigui, la quantitat de classes de determinant -531 derivades d'elles), 3, de manera que aquella a aquesta com 6 a 1.

256. Aquesta solució encara s'il·lustrarà més per les observacions generals següents.

I. Si l'ordre O és derivat d'un ordre pròpiament primitiu, AA dividirà D; però si O és impròpiament primitiu o bé derivat d'un impròpiament primitiu, A serà parell, D divisible per $\frac{1}{2}AA$, i el quocient $\equiv 1 \pmod 4$. D'aquí, el quadrat de qualsevol divisor de A, o bé dividirà D, o bé, almenys, $4D$, i en el darrer cas el quocient sempre serà $\equiv 1 \pmod 4$.

II. Si aa dividex D, tots els valors de l'expressió $\sqrt{D} \pmod{aa}$ que, certament, estan compresos entre 0 i $aa - 1$, seran 0, a, $2a$, $\ldots$, $aa - a$, de manera que la

quantitat de formes en V, a; però entre aquestes només seran pròpiament primitives tantes com nombres de $\frac{D}{aa}$, $\frac{D}{aa}-1$, $\frac{D}{aa}-4$, …, $\frac{D}{aa}-(a-1)^2$, no tenen divisor comú amb a. Quan $a=1$, V constarà d'una única forma, $(1, 0, -D)$, que sempre serà pròpiament primitiva. Quan a és 2 o bé una potència qualsevol de 2, la meitat d'aquells a nombres seran parells, l'altra meitat, imparells; per tant, en V hi haurà $\frac{1}{2}a$ formes pròpiament primitives. Quan a és un altre nombre primer p o bé una potència del nombre primer p, s'han de distingir tres casos: això és, tots aquells a nombres seran primers amb a, de manera que totes les formes en V, pròpiament primitives, si $\frac{D}{aa}$ no és divisible per p i, simultàniament, és no-residu quadràtic de p; però si p divideix $\frac{D}{aa}$, en V hi haurà $\frac{(p-1)a}{p}$ formes pròpiament primitives; finalment, si $\frac{D}{aa}$ és un residu quadràtic de p no divisible per p, en V hi haurà $\frac{(p-2)a}{p}$ formes pròpiament primitives. Totes aquestes [proposicions] es demostren sense dificultat. Però, en general, posat $a=2^\nu p^\pi q^\kappa r^\rho, \ldots$, on p, q, r, etc., designen nombres primers imparells diferents, la quantitat de formes pròpiament primitives en V serà $NPQR\cdots$, on s'ha de posar $N=1$ (si $\nu=0$) o bé $N=2^{\nu-1}$ (si $\nu>0$); $P=p^\pi$ (si $\frac{D}{aa}$ és un no-residu quadràtic de p), o bé $P=(p-1)p^{\pi-1}$ (si $\frac{D}{aa}$ és divisible per p), o bé $P=(p-2)p^{\pi-1}$ (si $\frac{D}{aa}$ és un residu

quadràtic de p no divisible per p); però Q, R, etc., s'han de definir de q, r, etc., de la mateixa manera que P de p.

III. Si aa no divideix D, $\frac{4D}{aa}$ serà enter i $\equiv 1 \pmod 4$, i els valors de l'expressió $\sqrt{D} \pmod{aa}$, els $\frac{1}{2}a$, $\frac{3}{2}a$, $\frac{5}{2}a$, $\ldots$, $aa-\frac{1}{2}a$, d'on la quantitat de formes en V serà a; però, entre aquestes, tantes seran pròpiament primitives com nombres dels $\frac{D}{aa}-\frac{1}{4}$, $\frac{D}{aa}-\frac{9}{4}$, $\frac{D}{aa}-\frac{25}{4}$, $\ldots$, $\frac{D}{aa}-\left(a-\frac{1}{2}\right)^2$, siguin primers amb a. Quan $\frac{4D}{aa} \equiv 1 \pmod 8$, tots aquests nombres seran parells, de manera que en V [no hi haurà] cap forma pròpiament primitiva; però quan $\frac{4D}{aa} \equiv 5 \pmod 8$, tots aquells nombres seran imparells, de manera que totes les formes en V, pròpiament primitives, si a és 2 o bé una potència de 2; en general, però, en aquest cas, hi haurà tantes formes pròpiament primitives en V com nombres d'aquells que no siguin divisibles per cap divisor primer imparell de a. La seva quantitat serà $NPQR\cdots$, si $a = 2^\nu p^\pi q^\kappa r^\rho \cdots$, on convé establir $N = 2^\nu$, però derivar P, Q, R, etc., de p, q, r, etc., de la mateixa manera que en el cas precedent.

IV. Així, d'aquesta manera, es poden definir les quantitats de formes pròpiament primitives en V, V', V'', $\ldots$; per a la suma de totes aquestes quantitats es descobreix sense dificultat la regla general següent: Si $A = 2^\nu \mathfrak{A}^\alpha \mathfrak{B}^\beta \mathfrak{C}^\gamma \cdots$, on $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\ldots$, designen nombres primers imparells diferents, la quantitat total de totes les formes pròpiament primitives en V, V', V'', etc.,

serà $\frac{A\mathfrak{n}\mathfrak{a}\mathfrak{b}\mathfrak{c}\cdots}{2\mathfrak{A}\mathfrak{B}\mathfrak{C}\cdots}$, on s'ha de establir $\mathfrak{n} = 1$ (si $\frac{4D}{AA} \equiv 1\,(\text{mòd. } 8)$), o bé $\mathfrak{n} = 2$ (si $\nu > 0$ i, simultàniament, $\frac{D}{AA}$ enter), o bé $\mathfrak{n} = 3$ (si $\frac{4D}{AA} \equiv 5\,(\text{mòd. } 8)$); a més a més, $\mathfrak{a} = \mathfrak{A}$ (si $\mathfrak{A}$ divideix $\frac{4D}{AA}$), o bé $\mathfrak{a} = \mathfrak{A} \pm 1$ (si $\mathfrak{A}$ no divideix $\frac{4D}{AA}$, agafant el signe superior o bé l'inferior segons si $\frac{4D}{AA}$ és un no-residu o bé un residu quadràtic de $\mathfrak{A}$), i, finalment, $\mathfrak{b}$, $\mathfrak{c}$, etc., es deriven de $\mathfrak{B}$, $\mathfrak{C}$, de la mateixa manera com $\mathfrak{a}$ de $\mathfrak{A}$. La brevetat no permet explicar aquí la demostració més extensament.

V. Ara, pel que fa a la quantitat de classes que proporcionen les formes pròpiament primitives en V, V', V'', etc., s'han de distingir els tres casos següents.

Primer, quan D és un nombre negatiu, cada una de les formes pròpiament primitives en V, V', etc., constitueixen una classe peculiar, o sigui, aquesta quantitat de classes cercades s'expressarà per la fórmula transmesa en l'observació precedent, exceptuant-ne dos casos; això és, on $\frac{4D}{AA}$ és, o bé $= -4$, o bé $= -3$, o sigui, on D és o bé $= -AA$, o bé $= -\frac{3}{4}AA$. Evidentment, per a la demostració d'aquest teorema només s'ha de mostrar que no pot ser que dues formes diferents de V, V', V'', etc., siguin pròpiament equivalents. Així, suposem que $(hh,\ i,\ k)$, $(h'h',\ i',\ k')$, són dues formes pròpiament primitives diferents de V, V', V'', etc., que pertanyin a la mateixa classe, i que la primera es transforma en la darrera per la substitució pròpia α, β, γ, δ; d'on es tindran les equacions $\alpha\delta - \beta\gamma = 1$,

$hh\alpha\alpha+2i\alpha\gamma+k\gamma\gamma = h'h'$, $hh\alpha\beta+i(\alpha\delta+\beta\gamma)+k\gamma\delta = i'$. D'aquí es conclou fàcilment, *primer*, que γ no és, certament, $= 0$ (d'on se seguiria que és $\alpha = \pm 1$, $hh = h'h'$, $i \equiv i'$ (mòd. hh), de manera que les formes proposades, idèntiques, contràriament a la hipòtesi); *segon*, que γ és divisible pel màxim comú divisor dels nombres h, h' (en efecte, posant aquest divisor $= r$, evidentment aquest també dividirà $2i$, $2i'$, però serà primer amb k; a part, rr dividirà $hhk - h'h'k' = ii - i'i'$; d'on es dedueix fàcilment que r també divideix $i - i'$; es té, però, $\alpha i' - \beta h'h' = \alpha i + \gamma k$, d'on γk, i, en conseqüència, γ, també serà divisible per r); *tercer*, que és $(\alpha hh + \gamma i)^2 - D\gamma\gamma = hhh'h'$. Així, posant $\alpha hh + \gamma i = rp$, $\gamma = rq$, p i q seran enters, el darrer dels quals no $= 0$, i $pp - Dqq = \dfrac{hhh'h'}{rr}$. Però $\dfrac{hhh'h'}{rr}$ serà el nombre mínim divisible simultàniament per hh i $h'h'$, de manera que dividirà AA i, en conseqüència, també $4D$; per tant, $\dfrac{4Drr}{hhh'h'}$ serà enter (negatiu) que, posant-lo $= -e$, serà $pp - Dqq = -\dfrac{4D}{e}$, o sigui, $4 = \left(\dfrac{2rp}{hh'}\right)^2 + eqq$, equació en la qual la part $\left(\dfrac{2rp}{hh'}\right)^2$, en tant que quadrat més petit que 4, serà necessàriament o bé 0 o bé 1. En el primer cas, serà $eqq = 4$ i $D = -\left(\dfrac{hh'}{rq}\right)^2$, d'on se segueix que $\dfrac{4D}{AA}$ és un quadrat afectat del signe negatiu, de manera que, certament, no $\equiv 1$ (mòd. 4); així, O no és ni un ordre impròpiament primitiu, ni derivat d'un impròpiament primitiu. D'aquí, $\dfrac{D}{AA}$ serà enter, d'on es dedueix fàcilment

que e és divisible per 4, $qq = 1$, $D = -\left(\frac{hh'}{r}\right)^2$, i $\frac{AA}{D}$, també enter. D'aquí serà necessàriament $D = -AA$, o sigui, $\frac{D}{AA} = -1$, que és la primera excepció. En el darrer cas, serà $eqq = 3$, d'on $e = 3$ i $4D = -3\left(\frac{hh'}{r}\right)^2$; d'aquí $3\left(\frac{hh'}{rA}\right)^2$ serà un enter que, com que multiplicat pel quadrat enter $\left(\frac{rA}{hh'}\right)^2$ produeix 3, no podrà ser un altre que 3; d'aquí, $4D = -3AA$, o sigui, $D = -\frac{3}{4}AA$, que és la segona excepció. Així, doncs, en tots els casos restants, totes les formes pròpiament primitives de V, V', V'', etc., pertanyeran a classes diferents. Per als casos exceptuats, és suficient afegir allò que ha resultat d'una disquisició no difícil, però que, per abreujar, aquí s'ha de suprimir. Això és, en el primer, de les formes pròpiament primitives de V, V', V'', etc., sempre pertanyeran a la mateixa classe de dues en dues; en el darrer, de tres en tres, de manera que la quantitat de totes les classes cercades resulta, en aquell cas, la meitat, en aquest, la tercera part, del valor de l'expressió transmesa en l'observació precedent.

Segon, quan D és un nombre positiu quadrat, cada una de les formes pròpiament primitives en V, V', V'', etc., sense excepció, constitueix una classe peculiar. En efecte, suposem que $(hh,\ i,\ k)$, $(h'h',\ i',\ k')$, són dues tals formes pròpiament equivalents diferents, i que la primera es transforma en la darrera per la substitució pròpia $\alpha, \beta, \gamma, \delta$. Llavors, és clar que tots els raonaments

aplicats per al cas precedent en què no se suposés que D és negatiu també valen aquí. Així, si p, q, r, designen el mateix que allà, també aquí $\frac{4Drr}{hhh'h'}$ serà enter, però ja no negatiu, sinó positiu i, a sobre, quadrat, que, posat $= gg$, serà $\left(\frac{2rp}{hh'}\right)^2 - ggqq = 4$, *Q. E. A.*, ja que la diferència de dos quadrats no pot ser 4 llevat que el quadrat més petit fos 0; per la qual cosa, la suposició no pot ser consistent.

Per al *tercer* cas, però, en què D és un nombre positiu no quadrat, fins ara no tenim cap regla general per a comparar la quantitat de formes pròpiament primitives en V, V', V'', etc., amb la quantitat de classes diferents que en resulten. Certament, podem asseverar que aquesta, o bé és igual a aquella, o bé a una part alíquota seva; encara més, també hem detectat una connexió singular entre el quocient d'aquests nombres i els valors mínims t, u, que satisfan l'equació $tt - Duu = AA$, que seria massa llarg explicar aquí; però no podem dir res cert del fet de si és possible, de la sola inspecció dels nombres D, A, conèixer aquest quocient en tots els casos (com en els casos precedents). Heus aquí alguns exemples, el nombre dels quals qualsevol podrà augmentar fàcilment. Per a $D = 13$, $A = 2$, la quantitat de formes pròpiament primitives en V, etc., és 3, les quals són totes equivalents, o sigui, produeixen una única classe; per a $D = 37$, $A = 2$, també es tenen tres formes pròpiament primitives en V, etc., les quals pertanyen a tres classes diferents; per a $D = 588$, $A = 7$, es tenen vuit formes pròpiament primitives en V, etc., les quals produeixen quatre classes; per a $D = 867$, $A = 17$, en V, etc., hi ha 18 formes pròpiament primitives, tantes com per a

$D = 1445$, $A = 17$, però que per a aquell determinant es distribueixen en dues classes, per a aquest, en sis.

VI. De l'aplicació d'aquesta teoria general al cas en què O és un ordre impròpiament primitiu, es conclou que la quantitat de classes contingudes en aquest ordre serà a la quantitat de totes les classes en l'ordre pròpiament primitiu com 1 a la quantitat de classes diferents que produeixen aquestes tres formes: $(1,\ 0,\ -D)$, $\left(4,\ 1,\ \frac{1-D}{4}\right)$, $\left(4,\ 3,\ \frac{9-D}{4}\right)$. I, certament, d'aquí resultarà una única classe quan $D \equiv 1 \pmod 8$, ja que, en aquest cas, la forma segona i la tercera són impròpiament primitives; però quan $D \equiv 5 \pmod 8$, totes tres formes seran pròpiament primitives i produiran la mateixa quantitat de classes diferents si D és negatiu, exceptuant-ne l'únic cas en què $D = -3$, en què constitueixen una única classe; finalment, el cas en què D és positiu (de la forma $8n + 5$) pertany a aquells per als quals encara es desitja una regla general. Però podem asseverar que en aquest cas aquestes tres formes o bé pertanyen a tres classes diferents o bé a una única, mai a dues; en efecte, es copsa fàcilment que, si les formes $(1,\ 0,\ -D)$, $\left(4,\ 1,\ \frac{1-D}{4}\right)$, $\left(4,\ 3,\ \frac{9-D}{4}\right)$, pertanyen a les classes K, K', K'', respectivament, serà $K + K' = K'$, $K' + K' = K''$, de manera que si se suposa que K i K' són idèntiques, també K' i K'' seran idèntiques; per una raó similar, si se suposa que K i K'' són idèntiques, també ho seran K' i K''; finalment, com que és $K' + K'' = K$, de la suposició que K' i K'' són idèntiques se segueix que K i K'' també coincideixen; d'on es conclou que, o bé

totes tres classes K, K', K'', són diferents, o bé totes tres idèntiques. Per exemple, per sota de 600 es donen 75 nombres de la forma $8n + 5$, entre els quals 17 són determinants per als quals té lloc el primer cas, o sigui, la quantitat de classes de l'ordre pròpiament primitiu és tres vegades més gran que en l'impròpiament primitiu, posem 37, 101, 141, 189, 197, 269, 325, 333, 349, 373, 381, 389, 397, 405, 485, 557, 573; per als 59 casos restants, val el darrer, o sigui, que la quantitat de classes és igual en tots dos ordres.

VII. A penes serà necessari observar que, per la disquisició precedent, no només es poden comparar les quantitats de classes en ordres diferents del mateix determinant, sinó que aquella també és aplicable a qualssevol determinants diferents la raó dels quals sigui un quadrat. Això és, si O designa un ordre qualsevol de determinant dmm, O' un ordre de determinant $dm'm'$, O es podrà comparar amb un ordre pròpiament primitiu de determinant dmm i aquest amb un ordre derivat d'un ordre pròpiament primitiu de determinant d, o sigui, el que rendeix el mateix, respecte de la quantitat de classes, en aquest mateix ordre; i, per una raó similar, l'ordre O' es podrà comparar directament amb aquell mateix.

257. Entre totes les classes d'un ordre donat de determinant donat, demanen una disquisició més detallada, sobretot, les classes ambigües; la determinació de la quantitat d'aquestes classes ens obrirà camí a moltes altres coses. Però és suficient assignar aquesta quantitat per a un sol ordre pròpiament primitiu, ja que els casos restants es poden reduir a aquest fàcilment. Resoldrem aquesta qüestió de manera que, primer, ensenyarem a

descobrir totes les formes ambigües pròpiament primitives (A, B, C) de determinant proposat D en les quals o bé $B = 0$ o bé $B = \frac{1}{2}A$; després, a trobar a partir de la quantitat d'aquestes la quantitat de totes les classes ambigües pròpiament primitives de determinant D.

I. Evidentment, totes les formes pròpiament primitives $(A, 0, C)$ de determinant D es troben agafant per a A cadascun dels divisors de D (tant positivament com negativament) per als quals $C = -\frac{D}{A}$ resulta primer amb A. Així, quan $D = 1$, es donen dues formes d'aquest tipus, $(1, 0, -1)$ i $(-1, 0, 1)$; la mateixa quantitat quan $D = -1$, posem $(1, 0, 1)$, $(-1, 0, -1)$; quan D és un nombre primer o bé una potència d'un nombre primer (sigui el signe positiu, sigui negatiu) es donaran les quatre $(1, 0, -D)$, $(-1, 0, D)$, $(D, 0, -1)$, $(-D, 0, 1)$. En general, però, quan D és divisible per n nombres primers diferents (entre els quals, en aquest lloc, també 2 ha d'entrar en el còmput), es donaran en total 2^{n+1} formes d'aquest tipus; això és, posat $D = \pm PQR\cdots$, on P, Q, R, etc., designen nombres primers diferents o bé potències de nombres primers diferents, la quantitat dels quals és $= n$, els valors de A seran 1, P, Q, R, etc., i els productes de qualssevol d'aquests nombres; la quantitat d'aquests valors, per la teoria de combinacions, resulta 2^n, però s'ha de duplicar, ja que a cadascun d'aquests valors convé atribuir-li tant el signe positiu com el negatiu.

II. De manera similar, és clar que s'obtenen totes les formes pròpiament primitives $(2B, B, C)$ de determinant D, si per a B s'agafen tots els divisors de D (posi-

tivament i negativament) per als quals $C = \frac{1}{2}\left(B - \frac{D}{B}\right)$ resulta enter i primer amb $2B$. Així, com que C ha de ser necessàriament imparell, de manera que $CC \equiv 1\,(\text{mòd. } 8)$, de $D = BB - 2BC = (B-C)^2 - CC$ se segueix que D és, o bé $\equiv 3\,(\text{mòd. } 4)$, quan B és imparell, o bé $\equiv 0\,(\text{mòd. } 8)$, quan B és parell; així, quan D és congru a algun dels nombres 1, 2, 4, 5, 6, segons el mòdul 8, no es donarà cap forma d'aquest tipus. Quan $D \equiv 3\,(\text{mòd. } 4)$, C resulta enter i imparell, sigui quin sigui el divisor de D que s'agafi per a B; però perquè C no tingui cap divisor comú amb $2B$, B s'haurà d'agafar de manera que $\frac{D}{B}$ resulti primer amb B; d'aquí, per a $D = -1$ es tenen les dues formes (2, 1, 1), (−2, −1, −1), i, en general, es copsa fàcilment que, si la quantitat de tots els nombres primers que divideixen D és n, apareixen en total 2^{n+1} formes. Quan D és divisible per 8, C resulta enter agafant per a B qualsevol divisor parell de $\frac{1}{2}D$; l'altra condició, però, que $C = \frac{1}{2}B - \frac{D}{2B}$ sigui primer amb $2B$, se satisfà, *primer*, agafant imparellament per a B tots els divisors parells de D per als quals $\frac{D}{B}$ no té cap divisor comú amb B, la quantitat dels quals (tinguda raó de la diferència de signes) serà 2^{n+1}, si se suposa que D és divisible per n nombres primers imparells diferents; *segon*, agafant parellament per a B tots els divisors parells de $\frac{1}{2}D$ per als quals $\frac{D}{2B}$ resulta primer amb B, la quantitat dels quals també serà 2^{n+1}, de manera que, en aquest cas, en total, es tindran 2^{n+2} formes d'aquest tipus. Això és, posant $D = \pm 2^{\mu} PQR\cdots$, on μ designa un exponent més gran que 2; P, Q, R, etc., nombres primers imparells diferents

o bé potències de tals nombres primers la quantitat dels quals és n, *tant per a* $\frac{1}{2}B$ *com per a* $\frac{D}{2B}$ es poden agafar els valors 1, P, Q, R, etc., i els productes de qualssevol d'aquests nombres, tant amb signe positiu com negatiu.

De tot això es conclou que, si se suposa que D és divisible per n nombres primers imparells diferents (posant $n = 0$ quan $D = \pm 1$ o bé ± 2 o bé una potència de 2), la quantitat de totes les formes pròpiament primitives (A, B, C) en les quals B és o bé $= 0$ o bé $= \frac{1}{2}A$, serà 2^{n+1} quan D és o bé $\equiv 1$ o bé $\equiv 5 \,(\text{mòd. } 8)$; 2^{n+2} quan $D \equiv 2, 3, 4, 6$, o bé $7 \,(\text{mòd. } 8)$ i, finalment, 2^{n+3} quan $D \equiv 0 \,(\text{mòd. } 8)$. Observem que, comparant amb les que hem transmès a l'article 231 per a la quantitat de tots els caràcters possibles de formes primitives de determinant D, aquella, en tots els casos, és precisament el doble més gran que aquesta. D'altra banda, és evident que quan D és negatiu, entre aquelles formes n'hi haurà tantes de positives com de negatives.

258. Evidentment, totes les formes que han sortit a l'article precedent pertanyen a classes ambigües, i recíprocament, a qualsevol classe ambigua pròpiament primitiva de determinant D ha d'haver-hi continguda almenys una d'aquelles formes; en efecte, en tal classe certament hi ha formes ambigües, i a qualsevol forma ambigua pròpiament primitiva (a, b, c) de determinant D equival alguna de les formes de l'article precedent, això és, o bé $\left(a, 0, \frac{-D}{A}\right)$, o bé $\left(a, \frac{1}{2}a, \frac{1}{4}a - \frac{D}{A}\right)$, segons que b és o bé $\equiv 0$ o bé $b \equiv \frac{1}{2}a \,(\text{mòd. } a)$. Així,

el problema s'ha reduït que investiguem quantes classes diferents constitueixen aquelles formes.

Si la forma $(a,\ 0,\ c)$ és entre les formes de l'article precedent, la forma $(c,\ 0,\ a)$ també ocorrerà entre elles, i sempre serà diferent d'aquella, exceptuant-ne l'únic cas en què $a = c = \pm 1$, de manera que $D = -1$, que de moment apartarem. Però, com que, evidentment, aquestes formes pertanyen a la mateixa classe, és suficient retenir-ne una, i, certament, rebutjarem aquella el primer terme de la qual és més gran que el tercer; el cas en què $a = -c = \pm 1$, o sigui, $D = 1$, també l'apartarem. D'aquesta manera, podem reduir a la meitat totes les formes $(A,\ 0,\ C)$, retenint-ne sempre una de cada dues; i en totes les restants serà $A < \sqrt{\pm D}$.

De manera similar, si entre les formes de l'article precedent ocorre la forma $(2b,\ b,\ c)$, entre elles es trobarà $(4c-2b,\ 2c-b,\ c) = \left(-\frac{2D}{b},\ -\frac{D}{b},\ c\right)$, que és equivalent pròpiament a aquella i en serà diferent, exceptuant-ne l'únic cas, que apartem, en què $c = b = \pm 1$, o sigui, $D = -1$. D'aquestes dues formes és suficient retenir aquesta, el primer terme de la qual és menor que el primer terme de l'altra (en aquest cas, no poden ser iguals en magnitud i de signes diferents); d'on és clar que també es poden reduir a la meitat totes les formes $(2B,\ B,\ C)$, rebutjant-ne sempre una de cada dues; i en les restants és $B < \frac{D}{B}$, o sigui, $B < \sqrt{\pm D}$. D'aquesta manera, de totes les formes de l'article precedent, només en roman la meitat, el complex de les quals designarem per W, i només resta que mostrem quantes classes diferents s'originen d'aquestes formes. D'altra banda, és

evident, en el cas en què D és negatiu, que en W hi ha tantes formes positives com negatives.

I. Quan D és negatiu, cadascuna de les formes de W pertanyeran a classes diferents. Efectivament, totes les formes $(A,\ 0,\ C)$ seran reduïdes; similarment, totes les formes $(2B,\ B,\ C)$ seran reduïdes, excepte aquelles en les quals $C < 2B$; en una tal forma, però, serà $2C < 2B + C$; d'on (com que $B < \frac{D}{B}$, és a dir, $B < 2C - B$, de manera que $2B < 2C$, o sigui, $B < C$), $2C - 2B < C$ i $C - B < \frac{1}{2}C$ i, en conseqüència, $(C,\ C - B,\ C)$, que, evidentment, equival a aquella, una forma reduïda. D'aquesta manera, es tenen tantes formes reduïdes com formes es tenen en W, i com que es copsarà fàcilment que entre aquelles no n'hi poden ocórrer ni d'idèntiques ni d'oposades (exceptuat l'únic cas en què $C - B = 0$, en el qual serà $B = C = \pm 1$, de manera que $D = -1$, que ja hem apartat), totes pertanyeran a classes diferents. D'aquí es conclou que la quantitat de totes les classes ambigües pròpiament primitives de determinant D és igual a la quantitat de formes en W, o bé a la meitat de la quantitat de formes de l'article precedent; però en el cas exceptuat, $D = -1$, per compensació passa el mateix, això és, es tenen dues classes, a una de les quals pertanyen les formes $(1,\ 0,\ 1)$, $(2,\ 1,\ 1)$, i, a l'altra, les $(-1,\ 0,\ -1)$, $(-2,\ -1,\ -1)$. Així, en general, per a un determinant negatiu, la quantitat de totes les classes ambigües pròpiament primitives és igual a la quantitat de tots els caràcters assignables de formes primitives d'aquest determinant; però la quantitat de classes ambigües pròpiament primitives positives serà la meitat.

II. Quan D és un quadrat positiu $= hh$, es demostra sense dificultat que cadascuna de les formes de W pertanyen a classes diferents; però, en aquest cas, podem arribar encara més breument a la solució del problema de la manera següent. Com que, per l'article 210, en qualsevol classe ambigua pròpiament primitiva de determinant hh, però no en cap altra, es conté una forma reduïda $(a,\ h,\ 0)$, en la qual a és el valor de l'expressió $\sqrt{1}\,(\text{mòd.}\,2h)$ situat entre 0 i $2h-1$ inclusivament, es copsa que es donen tantes classes ambigües pròpiament primitives de determinant hh com valors tingui aquella expressió. Però de l'article 105 es dedueix sense cap dificultat que la quantitat d'aquests valors és 2^n, o bé 2^{n+1}, o bé 2^{n+2}, segons que h sigui imparell, o bé imparellament parell, o bé parellament parell, o sigui, segons que $D \equiv 1$, o bé $\equiv 4$, o bé $\equiv 0\,(\text{mòd.}\,8)$, on n designa la quantitat de divisors primers imparells de h, o sigui, de D. D'aquí es conclou que la quantitat de classes ambigües pròpiament primitives sempre és la meitat de la quantitat de totes les formes que han sortit a l'article precedent, o sigui, igual a la quantitat de formes en W, o bé de tots els caràcters possibles.

III. Quan D és positiu no quadrat, de cada forma $(A,\ B,\ C)$ continguda en W en deduïm altres $(A,\ B',\ C')$ agafant $B' \equiv B\,(\text{mòd.}\,A)$ i entre els límits $\sqrt{D}$ i $\sqrt{D}\mp A$ (on s'ha d'aplicar el signe superior o bé l'inferior, segons si A és positiu o bé negatiu) i $C' = \dfrac{B'B' - D}{A}$; i designem per W' el complex d'aquestes. Evidentment, aquestes formes seran pròpiament primitives, ambigües, de determinant D, i totes diferents entre si; però, a part d'això, totes seran formes reduïdes. En efecte, quan $A < \sqrt{D}$, B' serà, evidentment, $< \sqrt{D}$ i positiu; a part

d'això, $B' > \sqrt{D} \mp A$, de manera que $A > \sqrt{D} - B'$, i, en conseqüència, A, agafat positivament, estarà situat certament entre $\sqrt{D}+B'$ i $\sqrt{D}-B'$. Però quan $A > \sqrt{D}$, no podrà ser $B = 0$ (ja que hem rebutjat aquestes formes), sinó que, necessàriament, serà $B = \frac{1}{2}A$; d'aquí, B' igual en magnitud a $\frac{1}{2}A$, amb signe positiu (en efecte, com que $A < 2\sqrt{D}$, $\pm\frac{1}{2}A$ estarà comprès entre els límits assignats a B' i serà congru a B segons el mòdul A; per tant, $B' = \pm\frac{1}{2}A$); en conseqüència, $B' < \sqrt{D}$, d'on $2B' < \sqrt{D} + B'$, o sigui, $A < \sqrt{D} + B'$; per la qual cosa, $\pm A$ estarà comprès, necessàriament, entre els límits $\sqrt{D} + B'$ i $\sqrt{D} - B'$. Finalment, W' contindrà totes les formes reduïdes pròpiament primitives ambigües de determinant D; en efecte, si $(a,\ b,\ c)$ és una forma d'aquest tipus, serà o bé $b \equiv 0$ o bé $b \equiv \frac{1}{2}a\,(\text{mòd. } a)$. En el primer cas, evidentment, no podrà ser $b < a$ ni, tampoc, $a > \sqrt{D}$; a causa d'això, la forma $\left(a,\ 0,\ -\frac{D}{a}\right)$ estarà continguda, certament, en W, i la corresponent $(a,\ b,\ c)$ en W'; en el darrer, certament, serà $a < 2\sqrt{D}$, de manera que $\left(a,\ \frac{1}{2}a,\ \frac{1}{4}a - \frac{D}{a}\right)$ continguda en W, i la corresponent $(a,\ b,\ c)$ en W'. D'això es conclou que la quantitat de formes en W és igual que la quantitat de totes les formes reduïdes ambigües pròpiament primitives de determinant D; però, com que en cadascuna de les classes ambigües es contenen *dues* formes reduïdes ambigües (articles 187, 194), la quantitat de totes les classes ambigües pròpiament primitives de determinant D serà la meitat de la quantitat

de formes en W, o sigui, la meitat de tots els caràcters assignables.

259. La quantitat de classes ambigües impròpiament primitives de determinant donat D sempre és igual a la quantitat de pròpiament primitives del mateix determinant. Sigui K la classe principal, i K', K'', etc., les classes ambigües pròpiament primitives restants d'aquest determinant; L alguna classe ambigua impròpiament primitiva del mateix determinant, per exemple, aquella en què hi ha la forma $\left(2,\ 1,\ \frac{1}{2} - \frac{1}{2}D\right)$. Així, de la composició de la classe L amb K es produirà la mateixa classe L; suposem que de la composició de la classe L amb les classes K', K'', etc., provenen les classes L', L'', etc., respectivament, que, evidentment, totes pertanyeran al mateix determinant D i seran impròpiament primitives i ambigües. Així, és clar que el teorema seria demostrat en el moment que es provés que totes les classes L, L', L'', etc., són diferents, i que, excepte elles, no se'n donen altres d'ambigües impròpiament primitives de determinant D. Per a aquesta finalitat, distingim els casos següents:

I. Quan la quantitat de classes impròpiament primitives és igual a la quantitat de pròpiament primitives, qualsevol d'aquelles s'origina de la composició de la classe L amb una classe pròpiament primitiva determinada, d'on, necessàriament, totes les L, L', L'', etc., seran diferents. Però, si es designa per $\mathfrak{L}$ una classe ambigua impròpiament primitiva qualsevol de determinant D, es donarà una classe pròpiament primitiva $\mathfrak{K}$ tal que sigui $\mathfrak{K}+L=\mathfrak{L}$; si la classe $\mathfrak{K}'$ és oposada a la classe $\mathfrak{K}$, també

serà $\mathfrak{K}' + L = \mathfrak{L}$ (ja que les classes L, $\mathfrak{L}$ són oposades a si mateixes), d'on, necessàriament, $\mathfrak{K}$ serà idèntica a $\mathfrak{K}'$, de manera que una classe ambigua; d'aquí, $\mathfrak{K}$ es trobarà entre les classes K, K', K'', etc., i $\mathfrak{L}$ entre les L, L', L'', etc.

II. Quan la quantitat de classes impròpiament primitives és tres vegades més gran que la quantitat de classes pròpiament primitives, sigui H la classe en què hi ha la forma $\left(4, 1, \frac{1-D}{4}\right)$, H' aquella en la qual hi ha la forma $\left(4, 3, \frac{9-D}{4}\right)$, i H, H', seran pròpiament primitives i diferents tant entre si com de la classe principal K, i $H + H' = K$, $2H = H'$, $2H' = H$; i si $\mathfrak{L}$ és una classe impròpiament primitiva qualsevol de determinant D, que s'origina de la composició de la classe L amb la pròpiament primitiva $\mathfrak{K}$, també serà $\mathfrak{L} = L+\mathfrak{K}+H$ i $\mathfrak{L} = L+\mathfrak{K}+H'$; excepte les tres classes (pròpiament primitives i diferents) $\mathfrak{K}$, $\mathfrak{K}+H$, $\mathfrak{K}+H'$, no se'n donaran altres que compostes amb L produeixin $\mathfrak{L}$. Així, doncs, com que, si $\mathfrak{L}$ és ambigua i $\mathfrak{K}'$ oposada a $\mathfrak{K}$, també $L+\mathfrak{K}' = \mathfrak{L}$, $\mathfrak{K}'$ serà, necessàriament, idèntica a alguna d'aquelles tres classes. Si $\mathfrak{K}' = \mathfrak{K}$, $\mathfrak{K}$ serà ambigua; si $\mathfrak{K}' = \mathfrak{K} + H$, serà $K = \mathfrak{K} + \mathfrak{K}' = 2\mathfrak{K} + H = 2(\mathfrak{K} + H')$, de manera que $\mathfrak{K} + H'$, ambigua; i, similarment, si $\mathfrak{K}' = \mathfrak{K} + H'$, $\mathfrak{K} + H$ serà ambigua; d'on es conclou que $\mathfrak{L}$ es troba, necessàriament, entre les classes L, L', L'', etc. Però es copsa fàcilment que entre les tres classes $\mathfrak{K}$, $\mathfrak{K} + H$, $\mathfrak{K} + H'$ no pot haver-n'hi més d'ambigües; en efecte, si tant $\mathfrak{K}$ com $\mathfrak{K} + H$ fossin ambigües, o sigui, idèntiques respectivament a les seves oposades $\mathfrak{K}'$, $\mathfrak{K}' + H'$, seria $\mathfrak{K} + H = \mathfrak{K} + H'$; de la suposició que $\mathfrak{K}$ i $\mathfrak{K} + H'$ són ambigües resulta la mateixa conclusió; finalment, si $\mathfrak{K}+$

H, $\mathfrak{K}+H'$ fossin ambigües, o sigui, idèntiques a les seves oposades $\mathfrak{K}'+H'$, $\mathfrak{K}'+H$, resultaria $\mathfrak{K}+H+\mathfrak{K}'+H=\mathfrak{K}'+H'+\mathfrak{K}+H'$, d'on $2H=2H'$, o sigui, $H'=H$. Per la qual cosa, només es dóna una única classe ambigua pròpiament primitiva que, composta amb L, produeix $\mathfrak{L}$, de manera que L, L', L'', etc., seran totes diferents.

La quantitat de classes ambigües en un ordre *derivat* és evidentment igual a la quantitat de classes ambigües de l'ordre primitiu del qual és derivat, de manera que, pel que precedeix, sempre es podrà assignar.

260. Problema. *La classe pròpiament primitiva K de determinant D s'origina de la duplicació de la classe pròpiament primitiva k del mateix determinant: se cerquen totes les classes similars, de la duplicació de les quals s'origina la classe K.*

Solució. Sigui H la classe principal de determinant D i H', H'', H''', etc., les classes ambigües pròpiament primitives restants del mateix determinant; es designaran per k', k'', k''', etc., les classes $k+H'$, $k+H''$, $k+H'''$, etc., que s'originen de la composició d'aquestes amb k. Llavors, totes les classes k, k', k'', etc., seran classes pròpiament primitives de determinant D i diferents entre si; es copsa de manera igualment fàcil que de la duplicació de cadascuna d'elles s'origina la classe K. Però, si $\mathfrak{K}$ denota una classe pròpiament primitiva qualsevol de determinant D que, duplicada, produeix la classe K, estarà continguda necessàriament entre les classes k, k', k'', etc. En efecte, es posa $\mathfrak{K}=k+\mathfrak{H}$, de manera que $\mathfrak{H}$ sigui una classe pròpiament primitiva de determinant D (article 249), i serà $2k+2\mathfrak{H}=2\mathfrak{K}=K=2k$, d'on es conclou fàcilment que $2\mathfrak{H}$ coincideix

amb la classe principal, que $\mathfrak{H}$ és ambigua, o sigui, que està continguda entre les H, H', H'', etc., i $\mathfrak{K}$ entre les k, k', k'', etc.; per la qual cosa, aquestes classes mostren la solució completa del problema.

D'altra banda, és evident que en el cas en què D és negatiu, de les classes k, k', k'', etc., la meitat seran classes positives, la meitat, negatives.

Així, doncs, com que qualsevol classe pròpiament primitiva de determinant D que es pot originar de la duplicació d'alguna classe semblant prové de la duplicació de tantes classes similars en total com classes ambigües pròpiament primitives de determinant D es donen, es copsa que, si r és la quantitat de totes les classes pròpiament primitives de determinant D, la quantitat de totes les classes pròpiament primitives ambigües d'aquest determinant, n, la quantitat de totes les classes pròpiament primitives del mateix determinant que es poden produir per la duplicació d'una classe similar serà $\frac{r}{n}$. Resulta la mateixa fórmula si, per a determinant negatiu, els caràcters r, n, designen la quantitat de classes *positives*, aquell la de *totes* les pròpiament primitives, aquest, només de les ambigües. Així, per exemple, per al determinant $D = -161$, la quantitat de totes les classes pròpiament primitives positives és 16, la quantitat d'ambigües, 4, d'on la quantitat de totes les classes que es poden originar per duplicació d'alguna classe haurà de ser 4. I, realment, es troba que totes les classes contingudes en el gènere principal estan proveïdes d'aquesta propietat; això és, la classe principal (1, 0, 161) s'origina de la duplicació de les quatre classes ambigües; (2, 1, 81), de la duplicació de les classes (9, 1, 18), (9, −1, 18), (11, 2,

15), (11, −2, 15); (9, 1, 18) de la duplicació de les classes (3, 1, 54), (6, 1, 27), (5, −2, 33), (10, 3, 17); finalment, (9, −1, 18) de la duplicació de les classes (3, −1, 54), (6, −1, 27), (5, 2, 33), (10, −3, 17).

261. Teorema. *A la meitat de tots els caràcters assignables per a un determinant positiu no quadrat no pot correspondre cap gènere pròpiament primitiu; en canvi, per a un determinant negatiu, cap gènere pròpiament primitiu positiu.*

Dem. Sigui m la quantitat de tots els gèneres pròpiament primitius (positius) de determinant D; k la quantitat de classes contingudes en cada gènere, de manera que km sigui la quantitat de totes les classes pròpiament primitives (positives); n la quantitat de tots els caràcters diferents assignables per a aquest determinant. Llavors, per l'article 258, la quantitat de totes les classes pròpiament primitives ambigües (positives) serà $\frac{1}{2}n$; d'aquí, per l'article precedent, la quantitat de totes les classes pròpiament primitives que es poden originar per duplicació d'una classe similar serà $\frac{2km}{n}$. Però, per l'article 267, totes aquestes classes pertanyen al gènere principal, en què es contenen k classes; així, si totes les classes del gènere principal poden provenir de la duplicació d'alguna classe (cosa que es demostrarà en el que segueix que realment sempre té lloc), serà $\frac{2km}{n} = k$, o sigui, $m = \frac{1}{2}n$; però, certament, no pot ser $\frac{2km}{n} > k$, ni tampoc $m > \frac{1}{2}n$. Així, com que la quantitat de tots els gèneres pròpiament primitius (positius) no és, cer-

tament, més gran que la meitat de tots els caràcters assignables, la meitat d'aquests, com a mínim, no poden correspondre a tals gèneres. *Q. E. D.* D'altra banda, cal notar molt bé que d'aquí encara no se segueix que la meitat de tots els caràcters assignables corresponguin realment a gèneres pròpiament primitius (positius), però més avall, per fi, es podrà aclarir la veritat d'aquesta profundíssima proposició sobre els misteris més recòndits dels nombres.

Com que, per a un determinant negatiu, sempre existeixen tants gèneres negatius com positius, de tots els caràcters assignables no més de la meitat poden correspondre, evidentment, a gèneres pròpiament primitius negatius; de la qual cosa, com també dels gèneres impròpiament primitius, en parlarem més avall. Finalment, observem que el teorema no s'estén a determinants positius quadrats, per als quals es copsa sense cap dificultat que cadascun dels caràcters assignables correspon realment a un gènere.

262. Així, en aquest cas, on per a un determinant no quadrat donat D només es poden assignar dos caràcters diferents, només en correspondrà un únic a un gènere pròpiament primitiu (positiu) (que no podrà ser un altre que el gènere principal); l'altre no correspondrà a cap forma pròpiament primitiva (positiva) d'aquell determinant. Això succeeix per als determinants -1, 2, -2, -4, per als nombres primers de la forma $4n+1$ presos positivament, i per als de la forma $4n+3$, negativament, i, finalment, per a totes les potències d'exponent imparell de nombres primers de la forma $4n+1$ preses positivament, i per a les potències de nombres primers de la forma $4n+3$ preses positivament o bé negativament

segons que els exponents siguin parells o bé imparells. A partir d'aquest principi, podem extreure un nou mètode per a demostrar no només el teorema fonamental, sinó també els teoremes restants de la secció precedent que pertanyen als residus -1, $+2$, -2; aquest és completament diferent dels mètodes aplicats en la secció precedent, i sembla que no s'ha d'estimar la seva elegància inferior a cap d'aquells. Però passarem per alt el determinant -4, i els que són potències de nombres primers, ja que no ensenyen res nou.

Així, per al determinant -1 no es dóna cap forma positiva el caràcter de la qual sigui 3, 4; per al determinant $+2$, cap forma en absolut el caràcter de la qual sigui 3 *i* 5, 8; per al determinant -2, el caràcter 5 *i* 7, 8 no correspondrà a cap forma positiva; per al determinant $+p$, si p és un nombre primer de la forma $4n+1$, o bé per al determinant $-p$, si p és un nombre primer de la forma $4n+3$, el caràcter Np no correspondrà a cap forma pròpiament primitiva (positiva en el darrer cas). D'aquí, demostrem els teoremes de la secció precedent de la manera següent.

I. -1 és no-residu de qualsevol nombre (positiu) de la forma $4n+3$. En efecte, si -1 fos un residu d'un tal nombre A, fent $-1 = BB - AC$, $(A,\ B,\ C)$ seria una forma positiva de determinant -1, i el caràcter d'aquesta, 3, 4.

II. -1 és residu de qualsevol nombre primer p de la forma $4n+1$. Efectivament, el caràcter de la forma $(-1,\ 0,\ p)$, i també el de totes les pròpiament primitives de determinant p, serà Rp, de manera que $-1Rp$.

III. Tant $+2$ com -2 són residus de qualsevol nombre primer p de la forma $8n+1$. Efectivament, o bé les formes $\left(8,\ 1,\ \frac{1-p}{8}\right)$, $\left(-8,\ 1,\ \frac{p-1}{8}\right)$, o bé les $\left(8,\ 3,\ \frac{9-p}{8}\right)$, $\left(-8,\ 3,\ \frac{p-9}{8}\right)$ seran pròpiament primitives (segons que n sigui imparell o bé parell), de manera que els seus caràcters, Rp; d'aquí, $+8Rp$ i $-8Rp$, d'on també $2Rp$, $-2Rp$.

IV. $+2$ és no-residu de qualsevol nombre de la forma $8n+3$ o bé $8n+5$. En efecte, si fos residu d'un tal nombre A, es donaria una forma $(A,\ B,\ C)$ de determinant $+2$, el caràcter de la qual seria $3\ i\ 5,\ 8$.

V. De manera similar, -2 és no-residu de qualsevol nombre de la forma $8n+5$ o bé $8n+7$; en efecte, altrament, es donaria una forma $(A,\ B,\ C)$ de determinant -2, el caràcter de la qual seria $5\ i\ 7,\ 8$.

VI. -2 és residu de qualsevol nombre primer p de la forma $8n+3$. Aquesta proposició es pot demostrar per dos mètodes. *Primer*, com que, per IV, és $+2Np$, i, per I, $-1Np$, serà necessàriament $-2Rp$. La *segona* demostració s'obté de la consideració del determinant $+2p$, per al qual són assignables quatre caràcters, posem $Rp,\ 1\ i\ 3,\ 8$; $Rp,\ 5\ i\ 7,\ 8$; $Np,\ 1\ i\ 3,\ 8$; $Np,\ 5\ i\ 7,\ 8$; dels quals, doncs, almenys dos no correspondran a cap gènere. Ara, el primer caràcter correspon a la forma $(1,\ 0,\ 2p)$; el quart, a la forma $(-1,\ 0,\ 2p)$; per tant, els que s'han de rebutjar són el segon i el tercer. Així, com que el caràcter de la forma $(p,\ 0,\ -2)$ relatiu al nombre 8 és $1\ i\ 3,\ 8$, el seu caràcter relatiu a p no podrà ser un altre que Rp, d'on $-2Rp$.

VII. $+2$ és residu de qualsevol nombre primer p de la forma $8n+7$, que es pot demostrar per dos mètodes. *Primer*, com que, de I i V és $-1Np$, $-2Np$, serà $+2Rp$. *Segon*, com que o bé $\left(8,\, 1,\, \frac{1+p}{8}\right)$ o bé $\left(8,\, 3,\, \frac{9+p}{8}\right)$ és una forma pròpiament primitiva de determinant $-p$ (segons si n és parell o bé imparell), el seu caràcter serà Rp, de manera que $8Rp$ i $2Rp$.

VIII. Qualsevol nombre primer p de la forma $4n+1$ és no-residu de qualsevol nombre imparell q que és no-residu de p. En efecte, és clar que si p fos un residu de q, es donaria una forma pròpiament primitiva de determinant p, i el caràcter de la qual, Np.

IX. De manera similar, si un nombre imparell qualsevol q és no-residu d'un nombre primer p de la forma $4n+3$, $-p$ serà no-residu de q; en efecte, altrament, es donaria una forma pròpiament primitiva positiva de determinant $-p$, i el caràcter de la qual, Np.

X. Qualsevol nombre primer p de la forma $4n+1$ és residu de qualsevol altre nombre primer q que és residu de p. Si q també és de la forma $4n+1$, això se segueix immediatament de VIII; però si q és de la forma $4n+3$, $-q$ també serà residu de p (a causa de II), de manera que pRq (per IX).

XI. Si un nombre primer qualsevol q és residu d'un altre nombre primer p de la forma $4n+3$, $-p$ serà residu de q. En efecte, si q és de la forma $4n+1$, de VIII se segueix que pRq, de manera que (per II), $-pRq$; el cas, però, en què q també és de la forma $4n+3$ se sostreu a aquest mètode, no obstant això, es pot acabar fàcil-

ment de la consideració del determinant $+pq$. Això és, com que dels quatre caràctes assignables a aquest determinant, Rp, Rq; Rp, Nq; Np, Rq; Np, Nq, dos no poden correspondre a cap gènere, i els caràcters de les formes $(1,\ 0,\ -pq)$, $(-1,\ 0,\ pq)$, són respectivament el primer i el quart, els caràcters segon i tercer no poden correspondre a cap forma pròpiament primitiva de determinant pq. Així, com que el caràcter de la forma $(q,\ 0,\ -p)$ respecte del nombre p és, per hipòtesi, Rp, el caràcter de la mateixa forma respecte del nombre q ha de ser Rq, de manera que $-pRq$. *Q. E. D.*

Si en les proposicions VIII i IX se suposa que q designa un nombre primer, aquestes, juntament amb les X i XI, mostren el teorema fonamental de la secció precedent.

263. Després que hem comprovat el teorema fonamental amb una nova demostració, mostrarem com distingir la meitat dels caràcters als quals no pot correspondre cap forma pròpiament primitiva (positiva) per a un determinant no quadrat qualsevol donat, qüestió que es podrà acabar molt breument, ja que el seu fonament ja està contingut a la disquisició dels articles 147-150. Sigui ee el quadrat màxim que divideix el determinant proposat D, i $D = D'ee$, de manera que D' no implica cap factor quadrat; a més a més, siguin a, b, c, etc., tots els divisors primers imparells de D', de manera que D', sense respecte del seu signe, o bé és el producte d'aquests nombres o bé el doble d'aquest producte. Es designa per Ω el complex dels caràcters particulars Na, Nb, Nc, etc., sols, quan $D' \equiv 1\,(\text{mòd. } 4)$; adjuntat el caràcter 3, 4 quan $D' \equiv 3$ i e imparell o bé imparellament parell; adjuntats els 3, 8 i 7, 8 quan $D' \equiv 3$ i e

parellament parell; adjuntat o bé el caràcter 3 *i* 5, 8, o bé els dos 3, 8 i 5, 8 quan $D' \equiv 2 \,(\text{mòd. } 8)$ i e és o bé imparell o bé parell; finalment, adjuntat o bé el caràcter 5 *i* 7, 8, o bé els dos 5, 8 i 7, 8 quan $D' \equiv 6 \,(\text{mòd. } 8)$ i e o bé parell o bé imparell. Fet això així, a tots els caràcters íntegres en què es conté una quantitat imparella de caràcters particulars de Ω no podrà correspondre cap gènere pròpiament primitiu (positiu) de determinant D. En tots els casos, els caràcters particulars que expressen una relació amb els divisors primers de D tals que no divideixen D' no aporten res a la possibilitat o bé impossibilitat dels gèneres. Però, per la teoria de combinacions, es copsa facilíssimament que, d'aquesta manera, s'exclou realment la meitat de tots els caràcters íntegres assignables.

La demostració d'aquests preceptes s'acaba de la manera següent. Dels principis de la secció precedent, o sigui, dels teoremes demostrats de nou a l'article precedent, es dedueix sense cap dificultat que si p és un nombre primer (imparell, positiu) que no divideix D, al qual li correspon algun dels caràcters rebutjats, D' implica una quantitat imparella de factors que són no-residus de p, i, així, D', i d'aquí també D, és no-residu de p; a més a més, es copsa fàcilment que el producte de qualssevol nombres imparells primers amb D, a cap dels quals no correspon algun dels caràcters rebutjats, tampoc no pot correspondre a un tal caràcter; d'aquí, recíprocament, es copsa que qualsevol nombre imparell positiu primer amb D, al qual correspon algun dels caràcters rebutjats, implica certament algun factor primer amb aquesta qualitat, de manera que D n'és un no-residu. Així, si es donés una forma pròpiament primitiva (positiva) de

determinant D que correspongués a algun dels caràcters rebutjats, D seria no-residu de qualsevol nombre positiu imparell primer amb ell representable per una tal forma, la qual cosa, evidentment, no pot ser consistent amb el teorema de l'article 154.

Com a exemple, es comparen les classificacions transmeses en els articles 231, 232, el nombre de les quals qualsevol podrà augmentar a voluntat.

264. Així, d'aquesta manera, per a qualsevol determinant no quadrat donat es distribueixen per igual tots els caràcters assignables en dues espècies P, Q, de manera que a cap dels caràcters Q no pugui correspondre una forma pròpiament primitiva (positiva), però, per als restants P, certament, pel que sabem fins ara, res no obsta que pertanyin a tals formes. Respecte d'aquestes espècies de caràcters, es notarà en primer lloc la proposició següent, que es dedueix fàcilment del mateix criteri: Si es compon un caràcter de P amb un caràcter de Q (segons la norma de l'article 246, igual com si a aquest també li correspongués un gènere), es produirà un caràcter de Q; però, si es componen dos caràcters de P o bé dos caràcters de Q, el caràcter resultant pertanyerà a P. Amb l'ajut d'aquest teorema, també es pot excloure la meitat de tots els caràcters assignables per als gèneres negatius i impròpiament primitius de la manera següent.

I. Per a un determinant negatiu D, els gèneres negatius seran respecte d'això completament contraris als positius, això és, cap dels caràcters de P no pertanyerà a un gènere pròpiament primitiu negatiu, però tots aquests gèneres tindran els caràcters de Q. En efecte,

quan $D' \equiv 1 \,(\text{mòd. } 4)$, $-D'$ serà un nombre positiu de la forma $4n + 3$, de manera que, entre a, b, c, etc., [hi haurà] una quantitat imparella de nombres de la forma $4n + 3$, dels quals -1 serà no-residu de cada un, d'on és clar que en el caràcter íntegre de la forma $(-1,\ 0,\ D)$ hi intervé, en aquest cas, una quantitat imparella de caràcters particulars de Ω, o sigui, que ell mateix pertany a Q; quan $D' \equiv 3 \,(\text{mòd. } 4)$, per una raó similar, entre a, b, c, etc., o bé no es trobarà cap nombre de la forma $4n+3$, o bé dos, o bé quatre, etc.; però, com que, en aquest cas, entre els caràcters particulars de la forma $(-1,\ 0,\ D)$ ocorre, o bé 3, 4, o bé 3, 8, o bé 7, 8, és clar que el caràcter íntegre d'aquesta forma també pertany aquí a Q. La mateixa conclusió s'obté de manera igualment fàcil en els restants casos, de manera que la forma negativa $(-1,\ 0,\ D)$ sempre té un caràcter de Q. Però, com que aquesta forma, composta amb qualsevol altra pròpiament primitiva negativa del mateix determinant, produeix una forma positiva similar, es copsa fàcilment que cap forma pròpiament primitiva negativa no pot tenir un caràcter de P.

II. Per a gèneres impròpiament primitius (positius), es prova de manera similar que la qüestió es comporta o bé de la mateixa manera o bé contràriament que per als pròpiament primitius, segons que $D \equiv 1$ o bé $\equiv 5 \,(\text{mòd. } 8)$. Efectivament, en el primer cas, també serà $D' \equiv 1 \,(\text{mòd. } 8)$, d'on es conclou fàcilment que entre els nombres a, b, c, etc., o bé no es troba cap nombre de la forma $8n + 3$ i $8n + 5$, o bé dos, o bé quatre, etc. (això és, el producte de qualssevol nombres imparells entre els quals la quantitat conjunta de nombres de la forma $8n + 3$ i $8n + 5$ resulta imparella sempre surt $\equiv 3$ o bé $\equiv 5 \,(\text{mòd. } 8)$, però el producte de tots els a, b, c,

etc., ha de ser igual o bé a D' o bé a $-D'$); d'aquí, és clar que el caràcter íntegre de la forma $\left(2,\, 1,\, \frac{1-D}{2}\right)$, o bé no inclou cap caràcter particular de Ω, o bé dos, o bé quatre, etc., de manera que pertany a P. Ara, com que qualsevol forma impròpiament primitiva (positiva) de determinant D es pot mirar com a composta de $\left(2,\, 1,\, \frac{1-D}{2}\right)$ i una forma pròpiament primitiva (positiva) del mateix determinant, es copsa que cap forma impròpiament primitiva (positiva) no pot tenir, en aquest cas, un caràcter de Q. En l'altre cas, $D \equiv 5\,(\text{mòd. } 8)$, tot és al contrari; això és, D', que també serà $\equiv 5$, implicarà certament una quantitat imparella de factors de la forma $8n+3$ i $8n+5$, d'on es conclou que el caràcter de la forma $\left(2,\, 1,\, \frac{1-D}{2}\right)$, i, d'aquí, també el caràcter de qualsevol forma impròpiament primitiva (positiva) de determinant D, pertany a Q, de manera que un gènere impròpiament primitiu positiu no pot correspondre a cap caràcter de P.

III. Finalment, per a un determinant negatiu, els gèneres impròpiament primitius negatius són, a la inversa, contraris als gèneres impròpiament primitius positius; això és, aquells no podran tenir un caràcter de P o bé de Q segons que $D \equiv 1$ o bé $D \equiv 5\,(\text{mòd. } 8)$, o sigui, segons que $-D$ sigui de la forma $8n+7$ o bé $8n+3$. Això es dedueix sense cap dificultat del fet que de la composició de la forma $(-1,\, 0,\, D)$, el caràcter de la qual és de Q, amb formes impròpiament primitives negatives del mateix determinant es produeixen formes impròpiament primitives positives, de manera que quan

s'han exclòs d'aquestes els caràcters de Q, necessàriament s'han d'excloure d'aquelles els caràcters de P, i recíprocament.

265. De les disquisicions dels articles 257, 258, sobre la quantitat de classes ambigües, de les quals s'han construït totes les [proposicions] precedents, es poden deduir moltes altres conclusions dignes d'atenció, que, per abreujar, convé suprimir; però no podem ometre la següent, per la seva gran elegància. Hem mostrat que per a un determinant positiu p que és un nombre primer de la forma $4n + 1$ només es dóna una única classe ambigua pròpiament primitiva; per la qual cosa, totes les formes ambigües pròpiament primitives d'un tal determinant seran pròpiament equivalents. Així, si b és el nombre enter positiu més pròxim menor que $\sqrt{p}$, i $p - bb = a'$, les formes $(1,\ b,\ -a')$, $(-1,\ b,\ a')$, equivaldran pròpiament, de manera que, com que, evidentment, totes dues són formes reduïdes, una estarà continguda en el període de l'altra. Atribuint a la primera forma en el seu període l'índex 0, l'índex de la darrera serà necessàriament imparell (ja que els primers termes d'aquestes dues formes tenen signes oposats); així, es posa $= 2m + 1$. A més a més, es copsa fàcilment que si les formes dels índexs 1, 2, 3, etc., són, respectivament, $(-a',\ b',\ a'')$, $(a'',\ b'',\ -a''')$, $(-a''',\ b''',\ a^{IV})$, etc., les corresponents als índexs $2m$, $2m-1$, $2m-2$, $2m-3$, etc., són, respectivament, les formes $(a',\ b,\ -1)$, $(-a'',\ b',\ a')$, $(a''',\ b'',\ -a'')$, $(-a^{IV},\ b''',\ a''')$, etc. D'aquí es conclou que si la forma d'índex m és $(A,\ B,\ C)$, $(-C,\ B,\ -A)$ serà la mateixa, de manera que $C = -A$ i $p = BB + AA$. Per tant, qualsevol nombre primer de la forma $4n+1$ es pot descompondre en dos quadrats (hem deduït aquesta

proposició més amunt, article 182, de principis completament diferents), i podem arribar a una tal descomposició per un mètode molt simple i completament uniforme, això és, per desenvolupament del període de la forma reduïda el determinant de la qual és aquell nombre primer i el primer terme de la qual és 1, fins a una forma els termes externs de la qual són iguals en magnitud, oposats en els signes. Així, per exemple, per a $p = 233$, es té $(1, 15, -8)$, $(-8, 9, 19)$, $(19, 10, -7)$, $(-7, 11, 16)$, $(16, 5, -13)$, $(-13, 8, 13)$ i $233 = 64 + 169$. D'altra banda, és clar que A resulta necessàriament imparell (ja que $(A, B, -A)$ ha de ser una forma pròpiament primitiva) i, en conseqüència, B parell. Com que, per a un determinant positiu p que és un nombre primer de la forma $4n + 1$, en l'ordre impròpiament primitiu també es conté només una única classe ambigua, es copsa que, si g és el nombre imparell més pròxim menor que $\sqrt{p}$ i $p - gg = 4h$, les formes reduïdes impròpiament primitives $(2, g, -2h)$, $(-2, g, 2h)$, equivalen pròpiament, de manera que una està continguda en el període de l'altra. D'aquí es conclou, per raonaments completament similars als precedents, que en el període de la forma $(2, g, -2h)$ es troba una forma els termes externs de la qual són iguals en magnitud i tenen signes oposats, de manera que també es pot obtenir d'aquí la descomposició de p en dos quadrats. Però és clar que els termes externs d'aquesta forma seran parells, de manera que el central, imparell; i com que se sap que un nombre primer només es pot descompondre en dos quadrats d'una única manera, la forma trobada per aquest darrer mètode serà o bé $(B, \pm A, -B)$ o bé $(-B, \pm A, B)$. Així, en el nostre exemple, per a $p = 233$, es té $(2, 15, -4)$, $(-4, 13, 16)$, $(16, 3, -14)$, $(-14, 11, 8)$, $(8, 13, -8)$ i $233 = 169 + 64$ com més amunt.

266. Fins aquí hem restringit la nostra disquisició a les funcions de segon grau tals que impliquen *dues* indeterminades i no ha estat necessari que els atribuïm una denominació especial. Però és evident que podem considerar aquest argument com una secció molt particular d'una disquisició més general *de les funcions algebraiques racionals enteres homogènies de més d'una indeterminada i més d'una dimensió*, i podem distingir còmodament les tals funcions segons la quantitat de dimensions en *formes de segon, tercer, quart grau, etc.*, però segons la quantitat d'indeterminades en *formes binàries, ternàries, quaternàries, etc.* Doncs, les formes que fins ara s'han anomenat més simplement així s'anomenaran *formes binàries de segon grau*; però funcions tals com $Axx + 2Bxy + Cyy + 2Dxz + 2Eyz + Fzz$ (on A, B, C, D, E, F, denoten enters donats) s'anomenaran *formes ternàries de segon grau*, i així successivament. Certament, la secció present només ha estat dedicada a les formes binàries de segon grau; però com que la major part de les veritats referents a aquestes, i les més boniques, la font de les quals s'ha de cercar més pròpiament en la teoria de les formes ternàries de segon grau, encara es mantenen, aquí intercalem una breu digressió sobre aquesta teoria, en la qual transmetrem, sobre els seus primers elements, el que és necessari per a la perfecció de la teoria de les formes binàries, cosa que esperem que serà més acceptada pels geòmetres que si les suprimíssim, o bé les descobríssim per mètodes menys genuïns. Ens hem de reservar, però, per a una altra ocasió, una disquisició més exacta d'aquest importantíssim argument; d'una banda, perquè la seva riquesa excedeix els límits d'aquesta obra, ja ara llarga, i, de l'altra, perquè hi ha l'esperança que encara serà enriquida posteriorment amb increments brillants. Però,

certament, en aquest lloc s'exclouen absolutament del nostre programa tant les formes quaternàries, quinàries, etc., de segon grau, com totes les de graus superiors,* i sigui suficient encomanar a l'atenció dels geòmetres aquest camp vastíssim, en el qual trobaran matèria ingent per a exercitar les seves forces i enriquir l'Aritmètica superior amb aportacions significatives.

267. Serà molt útil per a la claredat establir un ordre fix entre les tres indeterminades que intervenen en les formes ternàries, de manera similar com en les formes binàries, de manera que *la primera, la segona i la tercera indeterminades* es distingeixin mútuament; però, en la disposició de cadascuna de les parts de la forma, sempre observarem aquest ordre, que obtingui el primer lloc la part que implica el quadrat de la primera indeterminada; a continuació, se segueixin successivament les que impliquen el quadrat de la segona indeterminada, el quadrat de la tercera, el doble producte de la segona per la tercera, el doble producte de la primera per la tercera, el doble producte de la primera per la segona; finalment, anomenarem *coeficient primer, segon, tercer, quart, cinquè, sisè*, els nombres enters determinats pels quals estan multiplicats aquests quadrats i dobles productes en el mateix ordre. Així, $axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$ serà una forma ternària ordenada correctament, la primera indeterminada de la qual és x, la segona, x', la tercera, x'', el primer coeficient, a, etc., el quart, b, etc. Però com que serà molt convenient per a la brevetat si no és necessari sempre denotar les indetermi-

* Per aquesta raó, sempre que a continuació parlem simplement de formes d'aquest tipus, les formes s'han d'entendre binàries o bé ternàries de *segon grau*.

nades de la forma ternària per lletres peculiars, també designarem aquesta forma, en la mesura que no considerem les indeterminades, de la manera $\left(\begin{array}{ccc} a, & a', & a'' \\ b, & b', & b'' \end{array}\right)$.

Posant $bb - a'a'' = A$, $b'b' - aa'' = A'$, $b''b'' - aa' = A''$, $ab - b'b'' = B$, $a'b' - bb'' = B'$, $a''b'' - bb' = B''$, s'origina una altra forma $\left(\begin{array}{ccc} A, & A', & A'' \\ B, & B', & B'' \end{array}\right) \cdots F$, que anomenarem *adjunta* a la *forma* $\left(\begin{array}{ccc} a, & a', & a'' \\ b, & b', & b'' \end{array}\right) \cdots f$. D'aquí es troba, novament, denotant per abreujar el nombre $abb + a'b'b' + a''b''b'' - aa'a'' - 2bb'b''$ per D, que $BB - A'A'' = aD$, $B'B' - AA'' = a'D$, $B''B'' - AA' = a''D$, $B'B' - AA'' = a'D$, $AB - B'B'' = bD$, $A'B' - BB'' = b'D$, $A''B'' - BB' = b''D$; d'on és clar que la forma F és adjunta a la forma $\left(\begin{array}{ccc} aD, & a'D, & a''D \\ bD, & b'D, & b''D \end{array}\right)$. Anomenarem *determinant* d'aquesta forma el nombre D, de la naturalesa del qual depenen principalment les propietats de la forma ternària f; d'aquesta manera, el determinant de la forma F resulta $= DD$, o sigui, igual al quadrat del determinant de la forma f, de la qual és adjunta.

Així, per exemple, l'adjunta a la forma ternària $\left(\begin{array}{ccc} 29, & 13, & 9 \\ 7, & -1, & 14 \end{array}\right)$ és la $\left(\begin{array}{ccc} -68, & -260, & -181 \\ 217, & -111, & 133 \end{array}\right)$, i el determinant d'ambdues és $= 1$.

Les formes ternàries de determinant 0 s'exclouran totalment de la investigació següent, ja que aquestes, com es mostrarà en la teoria de les formes ternàries, que cal transmetre en una altra ocasió més extensa-

ment, només són ternàries *d'aparença*, i equipol·lents, realment, a binàries.

268. Si alguna forma ternària f de determinant D, les indeterminades de la qual són x, x', x'' (posem la primera $= x$, etc.), es transforma en la forma ternària g de determinant E, les indeterminades de la qual són y, y', y'', per una substitució tal com

$$\begin{aligned} x &= \alpha y + \beta y' + \gamma y'', \\ x' &= \alpha' y + \beta' y' + \gamma' y'', \\ x'' &= \alpha'' y + \beta'' y' + \gamma'' y'', \end{aligned}$$

on se suposa que els nou coeficients α, β, etc., són tots nombres enters, negligides, per abreujar, les indeterminades, direm simplement que f es transforma en g per la substitució (S)

$$\begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

i que f *implica* g, o sigui, que g *està continguda en* f. Així, d'aquesta suposició se segueixen espontàniament sis equacions per als sis coeficients de g, que no serà necessari afegir; però d'aquí, per un càlcul fàcil, es treuen les conclusions següents.

I. Designat, per abreujar, el nombre $\alpha\beta'\gamma'' + \beta\gamma'\alpha'' + \gamma\alpha'\beta'' - \gamma\beta'\alpha'' - \alpha\gamma'\beta'' - \beta\alpha'\gamma''$ per k, es troba, després de les degudes reduccions, $E = kkD$, d'on és clar que D divideix E i el quocient és quadrat. Així, és clar que el nombre k, per a les transformacions de les formes ternàries, és similar al nombre $\alpha\delta - \beta\gamma$ de l'article 157

per a les transformacions de les formes binàries, posem l'arrel quadrada del quocient dels determinants, d'on podríem conjecturar que la diferència de signe de k també estableix aquí una diferència essencial entre transformacions i implicacions pròpies i impròpies. Però, contemplant la qüestió més de prop, es copsa que f també es transforma en g per la substitució

$$\begin{array}{ccc} -\alpha, & -\beta, & -\gamma \\ -\alpha', & -\beta', & -\gamma' \\ -\alpha'', & -\beta'', & -\gamma''; \end{array}$$

posant, però, en el valor de k, $-\alpha$ per α, $-\beta$ per β, etc., s'obtindrà $-k$, per tant, aquesta substitució seria diferent de la substitució S, i qualsevol forma ternària que n'impliqués una altra d'alguna manera també la implicaria de l'altra manera. Així, aquí es desterrarà completament una tal distinció, ja que no té cap utilitat en les formes ternàries.

II. Denotant per F, G, les formes adjuntes a f, g, respectivament, els coeficients de F es determinen pels coeficients de f, i els coeficients de G pels valors dels coeficients de la forma g coneguts de les equacions que proporciona la substitució S. Expressant els coeficients de la forma f per lletres, es confirma sense cap dificultat, per comparació dels valors dels coeficients de les formes F, G, que F implica la forma G, i que es transforma en ella per la substitució (S')

$$\begin{array}{ccc} \beta'\gamma'' - \beta''\gamma', & \gamma'\alpha'' - \gamma''\alpha', & \alpha'\beta'' - \alpha''\beta' \\ \beta''\gamma - \beta\gamma'', & \gamma''\alpha - \gamma\alpha'', & \alpha''\beta - \alpha\beta'' \\ \beta\gamma' - \beta'\gamma, & \gamma\alpha' - \gamma'\alpha, & \alpha\beta' - \alpha'\beta. \end{array}$$

No escrivim el càlcul, no sotmès a cap dificultat.

III. La forma g, per la substitució (S'')

$$\begin{array}{lll} \beta'\gamma'' - \beta''\gamma', & \beta''\gamma - \beta\gamma'', & \beta\gamma' - \beta'\gamma \\ \gamma'\alpha'' - \gamma''\alpha', & \gamma''\alpha - \gamma\alpha'', & \gamma\alpha' - \gamma'\alpha \\ \alpha'\beta'' - \alpha''\beta', & \alpha''\beta - \alpha\beta'', & \alpha\beta' - \alpha'\beta, \end{array}$$

es transforma evidentment en la mateixa forma en què es transforma f per la

$$\begin{array}{lll} k, & 0, & 0 \\ 0, & k, & 0 \\ 0, & 0, & k, \end{array}$$

o sigui, en la que s'origina multiplicant cadascun dels coeficients de la forma f per kk. Designarem aquesta forma per f'.

IV. Es prova completament de manera similar que la forma G, per la substitució (S''')

$$\begin{array}{lll} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'', \end{array}$$

es transforma en la forma que s'origina de F multiplicant cadascun dels coeficients per kk. Expressarem aquesta forma per F'.

Direm que la substitució S''' s'origina *per transposició* de la substitució S; llavors, evidentment, S apareix novament per transposició de la substitució S'''; i S', S'', l'una de l'altra per transposició. La substitució S' es pot anomenar, per comoditat, *adjunta* de la substitució S, d'on la substitució S''' serà adjunta de S''.

269. Si no només la forma f implica g, sinó que també aquesta, aquella, les formes f, g, s'anomenaran *equivalents*. Així, en aquest cas, no només D dividirà E, sinó també E, D; d'on es conclou fàcilment que ha de ser $D = E$. Recíprocament, però, si la forma f implica una forma g del mateix determinant, aquestes dues formes seran equivalents. En efecte (utilitzant els mateixos signes que a l'article precedent i exceptuant el cas en què $D = 0$), serà $k = \pm 1$, de manera que la forma f', en la qual es transforma g per la substitució S'', idèntica a f, o sigui, f continguda en g. A més a més, és clar que en aquest cas també les formes F, G, adjuntes a f, g, seran equivalents entre si, i la darrera es transformarà en la primera per la substitució S'''. Finalment, a la inversa, si se *suposa* que les formes F, G, són equivalents, i que la primera es transforma en la darrera per la substitució T, també les formes f, g, seran equivalents, i f es transformarà en g per la substitució adjunta a T, i g en f per la que s'origina de la transposició de la substitució T. Efectivament, per aquestes dues substitucions, respectivament, la forma adjunta a F es transforma en la forma adjunta a G, i aquesta en aquella; aquestes dues formes, però, s'originen de f, g, multiplicant cadascun dels coeficients per D; d'on es conclou sense cap dificultat que per les mateixes substitucions f es transforma en g i g en f, respectivament.

270. Si una forma ternària f implica una forma ternària f', i aquesta una forma f'', també f implicarà f''. En efecte, es copsarà molt fàcilment que, si es transforma

f en f' per la substitució	f' en f'' per la substitució
$\alpha,\ \beta,\ \gamma$	$\delta,\ \varepsilon,\ \zeta$
$\alpha',\ \beta',\ \gamma'$	$\delta',\ \varepsilon',\ \zeta'$
$\alpha'', \beta'', \gamma'',$	$\delta'',\ \varepsilon'',\ \zeta'',$

f es transformarà en f'' per la substitució $\alpha\delta + \beta\delta' + \gamma\delta''$, $\alpha\varepsilon + \beta\varepsilon' + \gamma\varepsilon''$, $\alpha\zeta + \beta\zeta' + \gamma\zeta''$; $\alpha'\delta + \beta'\delta' + \gamma'\delta''$, $\alpha'\varepsilon + \beta'\varepsilon' + \gamma'\varepsilon''$, $\alpha'\zeta + \beta'\zeta' + \gamma'\zeta''$; $\alpha''\delta + \beta''\delta' + \gamma''\delta''$, $\alpha''\varepsilon + \beta''\varepsilon' + \gamma''\varepsilon''$, $\alpha''\zeta + \beta''\zeta' + \gamma''\zeta''$.

Així, en el cas en què f equivalgui a f', i f' a f'', la forma f també equivaldrà a la forma f''. D'altra banda, és manifest espontàniament de quina manera s'haurien d'aplicar aquests teoremes a més formes.

271. Ara, d'aquí és clar que totes les formes ternàries, igual com les binàries, es poden distribuir en *classes*, duent formes equivalents a la mateixa classe, no equivalents a diferents. Així, formes de determinants diferents pertanyeran certament a classes diferents i, en conseqüència, es donaran infinites classes de formes ternàries; però formes ternàries del mateix determinant produeixen un nombre ja menor ja més gran de classes; això, però, s'ha de considerar com la propietat mereixedora de la palma d'aquestes formes: *totes les formes del mateix determinant donat sempre constitueixen una quantitat finita de classes.* Per al desenvolupament més extens d'aquest importantíssim teorema s'ha de donar abans l'explicació de la diferència essencial següent, que es té entre les formes ternàries.

Algunes formes ternàries són construïdes de manera que per elles es poden representar sense discriminació nombres positius i negatius, *per exemple*, la forma

$xx + yy - zz$, per la qual cosa, s'anomenaran *formes indefinides*. Contràriament, per altres no es poden representar nombres negatius, sinó (excepte zero, que s'obté posant cadascuna de les indeterminades = 0) només positius, com $xx + yy + zz$; per tant, s'anomenaran *formes positives*; finalment, per altres, com $-xx - yy - zz$, no es poden representar nombres positius, d'on s'anomenaran *formes negatives*; les formes positives i les negatives s'anomenaran amb la denominació comuna de *formes definides*. Ara, heus aquí uns criteris generals pels quals es podrà discernir la naturalesa d'aquestes formes.

Multiplicant per a la forma ternària $f = axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$ de determinant D, i denotant els coeficients de la forma adjunta a f, igual com a l'article 267, per A, A', A'', B, B', B'', s'obté $(ax + b''x' + b'x'')^2 - A''x'x' + 2Bx'x'' - A'x''x'' = g$, i multiplicant de nou per A', surt $A'(ax + b''x' + b'x'')^2 - (A'x'' - Bx')^2 + aDx'x' = h$. D'aquí es conclou immediatament que, si tant A' com aD són nombres negatius, tots els valors de h són negatius, d'on és evident que per una tal forma f només es podran representar nombres el signe dels quals és oposat al signe de aA', és a dir, idèntic al signe de a, o sigui, oposat al signe de D. Així, en aquest cas, f serà una forma definida, i certament positiva o bé negativa segons que a sigui positiu o bé negatiu, o sigui, segons que D sigui negatiu o bé positiu.

Però si o bé cada un dels aD, A' és positiu o bé l'un positiu i l'altre negatiu (cap = 0), es copsarà fàcilment que h pot obtenir valors tant positius com negatius mitjançant la determinació adequada de les quantitats x, x', x''. Per tant, en aquest cas, f podrà obtenir valors

tant afectats del mateix signe que aA' com oposats, i, així, f serà una forma indefinida.

Per al cas en què $A' = 0$ però no $a = 0$, resulta $g = (ax+b''x'+b'x'')^2 - x'(A''x' - 2Bx'')$. Atribuint a x' un valor arbitrari (però aquest no $= 0$) i agafant x'' de manera que $\dfrac{A''x'}{2B} - x''$ obtingui el mateix signe que Bx' (cosa que es copsa fàcilment que pot ser, ja que B no pot ser $= 0$; en efecte, d'aquí seria $BB - A'A'' = aD = 0$, de manera que també $D = 0$, cas que hem exclòs), $x'(A''x' - 2Bx'')$ serà una quantitat positiva, d'on és clar fàcilment que es pot determinar x de manera que g obtingui un valor negatiu. Evidentment, si es desitja, aquests valors es podran agafar també de manera que tots siguin enters. Finalment, és clar que si s'atribueixen valors qualssevol a x', x'', es pot agafar x tan gran que g resulti positiu. D'aquí es conclou que, en aquest cas, la forma f és indefinida.

Finalment, si $a = 0$, serà $f = a'x'x' + 2bx'x'' + a''x''x'' + 2x(b''x' + b'x'')$. Així, agafant x', x'', a voluntat, però de manera que $b''x' + b'x''$ no sigui $= 0$ (cosa que, evidentment, es podrà fer, llevat que b' i b'' siguin simultàniament $= 0$; però llavors seria $D = 0$), es copsa sense cap dificultat que x es pot determinar de manera que f obtingui valors tant positius com negatius. Per tant, també en aquest cas f serà una forma indefinida.

De la mateixa manera que aquí hem decidit la naturalesa de la forma f dels nombres aD, A', també es poden utilitzar aD i A'', de manera que f és una forma definida si tant aD com A'' són negatius; indefinida en tots els casos restants. I també, de manera completament similar, pot servir per a aquesta finalitat la con-

sideració dels nombres $a'D$ i A, o bé dels $a'D$ i A'', o bé dels $a''D$ i A, o bé, finalment, dels $a''D$ i A'.

De tot això es conclou que, en una forma definida, els sis nombres A, A', A'', aD, $a'D$, $a''D$, són negatius, i, certament, en una forma positiva, a, a', a'', seran positius, D negatiu; però, en una negativa, a, a', a'', seran negatius, D positiu. D'aquí és clar que totes les formes ternàries de determinant positiu donat es distribueixen en negatives i indefinides; però totes les de determinant negatiu, en positives i indefinides; finalment, no es donen en absolut formes positives de determinant positiu o bé negatives de determinant negatiu. D'aquí es copsa fàcilment que l'adjunta d'una forma definida sempre és definida i *negativa*, la d'una indefinida, indefinida.

Com que tots els nombres representables per una forma ternària donada, evidentment, també es poden representar per totes les formes equivalents a ella, les formes ternàries contingudes en una mateixa classe seran, o bé totes indefinides, o bé totes positives, o bé totes negatives. Per la qual cosa, serà lícit transferir aquestes denominacions de les formes també a les classes íntegres.

272. El teorema proposat a l'article precedent, que totes les formes ternàries de determinant donat es distribueixen en una quantitat *finita* de classes, el transmetrem per un mètode anàleg al que hem utilitzat en les formes binàries, això és, mostrant, primer, com es pot reduir qualsevol forma ternària a una forma més simple, després, que la quantitat de formes més simples (a les quals s'arriba per tals reduccions) per a qualsevol determinant donat és finita. Suposem, en general, que

és proposada la forma ternària $f = \left(\begin{array}{ccc} a, & a', & a'' \\ b, & b', & b'' \end{array} \right)$ de determinant D (diferent de 0) que, per la substitució (S)

$$\begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'', \end{array}$$

es transforma en l'equivalent $g = \left(\begin{array}{ccc} m, & m', & m'' \\ n, & n', & n'' \end{array} \right)$; i la nostra tasca consistirà a definir α, β, γ, etc., de manera que la forma g surti més simple que f. Siguin $\left(\begin{array}{ccc} A, & A', & A'' \\ B, & B', & B'' \end{array} \right)$, $\left(\begin{array}{ccc} M, & M', & M'' \\ N, & N', & N'' \end{array} \right)$, les formes adjuntes a f, g, respectivament, que es designaran per F, G. Llavors, per l'article 269, F es transformarà en G per la substitució adjunta a S però G en F per la substitució originada de la transposició de S. Denotarem per k el nombre $\alpha\beta'\gamma'' + \alpha'\beta''\gamma + \alpha''\beta\gamma' - \alpha''\beta'\gamma - \alpha\beta''\gamma' - \alpha'\beta\gamma''$, que haurà de ser o bé $= +1$ o bé $= -1$. Fet això així, observem que

I. Si resulta $\gamma = 0$, $\gamma' = 0$, $\alpha'' = 0$, $\beta'' = 0$, $\gamma'' = 1$, serà

$$\begin{array}{l} m = a\alpha\alpha + 2b''\alpha\alpha' + a'\alpha'\alpha', \\ m' = a\beta\beta + 2b''\beta\beta' + a'\beta'\beta', \\ m'' = a'', \quad n = b\beta' + b'\beta, \quad n' = b\alpha' + b'\alpha, \\ n'' = a\alpha\beta + b''(\alpha\beta' + \beta\alpha') + a'\alpha'\beta'. \end{array}$$

A part d'això, $\alpha\beta' - \beta\alpha'$ haurà de ser o bé $= +1$ o bé $= -1$. D'aquí és evident que la forma binària (a, b'', a'), el determinant de la qual és A'', per la substitució α, β, α', β', es transforma en la forma binària (m, n'', m') de determinant M'', i, en conseqüència, equival a ella a causa que $\alpha\beta' - \beta\alpha' = \pm 1$, d'on serà $M'' = A''$, cosa

que també es confirma directament fàcilment. Així, si (a, b'', a') ja no és la forma més simple de la seva classe, es podran determinar $\alpha, \beta, \alpha', \beta'$, de manera que (m, n'', m') sigui una forma més simple; i, certament, es conclou fàcilment de la teoria d'equivalència de formes binàries, que això es pot fer de manera que m no sigui més gran que $\sqrt{-\frac{4}{3}A''}$ si A'' fos negatiu, o bé no més gran que $\sqrt{A''}$ si A'' fos positiu, o bé que $m = 0$ si $A'' = 0$; de manera que, en tots els casos, el valor (absolut) de m es pot rebaixar certament, o bé almenys, fins a $\sqrt{\pm\frac{4}{3}A''}$. Així, d'aquesta manera, la forma f es redueix a una altra que té el primer coeficient menor, si pot ser, i la forma adjunta a la qual té el mateix tercer coeficient que la forma F adjunta a f. En això consisteix la *primera reducció*.

II. Però si resulta $\alpha = 1$, $\beta = 0$, $\gamma = 0$, $\alpha' = 0$, $\alpha'' = 0$, serà $k = \beta'\gamma'' - \beta''\gamma' = \pm 1$; així, la substitució adjunta a S serà

$$\begin{array}{rrr} \pm 1, & 0, & 0 \\ 0, & \gamma'', & -\beta'' \\ 0, & -\gamma', & \beta', \end{array}$$

per la qual F es transformarà en G. Així, es tindrà

$$\begin{array}{l} m = a, \quad n' = b'\gamma'' + b''\gamma', \quad n'' = b'\beta'' + b''\beta', \\ m' = a'\beta'\beta' + 2b\beta'\beta'' + a''\beta''\beta'', \\ m'' = a'\gamma'\gamma' + 2b\gamma'\gamma'' + a''\gamma''\gamma'', \\ n = a'\beta'\gamma' + b(\beta'\gamma'' + \gamma'\beta'') + a''\beta''\gamma'', \\ M' = A'\gamma''\gamma'' - 2B\gamma'\gamma'' + A''\gamma'\gamma', \\ N = -A'\beta''\gamma'' + B(\beta'\gamma'' + \gamma'\beta'') - A''\beta'\gamma', \\ M'' = A'\beta''\beta'' - 2B\beta'\beta'' + A''\beta'\beta'. \end{array}$$

D'aquí, és clar que la forma binària (A'', B, A'), el determinant de la qual és Da, es transforma per la substitució $\beta', -\gamma', -\beta'', \gamma''$, en la forma (M'', N, M') de determinant Dm, de manera que (a causa que $\beta'\gamma''-\gamma'\beta'' = \pm 1$, o bé a causa que $Da = Dm$) equival a ella. Així, llevat que (A'', B, A') ja sigui la forma més simple de la seva classe, es podran determinar els coeficients β', γ', β'', γ'', de manera que (M'', N, M') sigui més simple i, certament, això sempre es podrà fer de manera que, sense respectar el signe, M'' no sigui més gran que $\sqrt{\pm\frac{4}{3}Da}$. Així, d'aquesta manera, la forma f es redueix a una altra que té el mateix primer coeficient, però que la forma adjunta a aquesta tingui el tercer coeficient, si pot ser, menor que [el tercer coeficient de] la forma F adjunta a f. En això consisteix la *segona reducció.*

III. Així, si f és una forma ternària a la qual no és aplicable ni la primera ni la segona reducció, és a dir, per cap de les dues no es pot transformar en una forma més simple, necessàriament serà tant $aa <$ o bé $= \frac{4}{3}A''$, com $A''A'' <$ o bé $= \frac{4}{3}aD$, sense respecte del signe. D'aquí, a^4 serà $<$ o bé $= \frac{16}{9}A''A''$, de manera que $a^4 <$ o bé $= \frac{64}{27}aD$, $a^3 <$ o bé $= \frac{64}{27}D$, i $a <$ o bé $= \frac{4}{3}\sqrt[3]{D}$; d'aquí, novament, $A''A'' <$ o bé $= \frac{16}{9}\sqrt[3]{D^4}$, i $A'' <$ o bé $= \frac{4}{3}\sqrt[3]{D^2}$. Per la qual cosa, sempre que a o bé A'' encara superen aquests límits, necessàriament es podrà aplicar a la forma f l'una o l'altra de les reduccions precedents. D'altra banda, aquesta conclusió no es pot invertir, ja que força sovint succeeix que una forma

ternària, el primer coeficient de la qual i el tercer coeficient de la forma adjunta ja estan per sota d'aquests límits, no obstant això, encara es pot retre més simple per una o altra reducció.

IV. Però, si a una forma ternària donada qualsevol de determinant D s'apliquen alternativament la primera i la segona reducció, és a dir, a ella la primera o la segona; a la que resulta d'aquí, la segona o la primera; a la que prové d'aquí, de nou la primera o la segona; etc., és evident que, finalment, s'arribarà necessàriament a una forma a la qual no se li podrà aplicar més cap de les dues. En efecte, com que el valor absolut tant dels primers coeficients de les formes produïdes d'aquesta manera com dels tercers coeficients de les seves formes adjuntes alternativament es manté igual i decreix contínuament, finalment, aquest progrés acabarà necessàriament en algun lloc, ja que, altrament, es tindrien dues sèries infinites de nombres contínuament decreixents. D'aquí, ara hem obtingut l'egregi teorema: *Qualsevol forma ternària de determinant D es pot reduir a una altra equivalent, el primer coeficient de la qual no és més gran que $\frac{4}{3}\sqrt[3]{D}$; i el tercer coeficient de la seva forma adjunta no més gran que $\frac{4}{3}\sqrt[3]{D^2}$, sense respecte del signe, sempre que la forma proposada encara no estigui proveïda d'aquesta propietat.* D'altra banda, en lloc del primer coeficient de la forma f i el tercer de la forma adjunta a f hauríem pogut tractar de manera completament similar o bé el primer coeficient de la forma i el segon de l'adjunta; o bé el segon de la forma i el primer, o bé el tercer de l'adjunta; o bé el tercer de la forma i el primer, o bé el segon de l'adjunta; volguts aquests, hauríem arribat igualment a la finalitat proposada per nosaltres; però és

convenient adherir-se constantment a un mètode, perquè les operacions que pertanyen a aquest es puguin reduir més fàcilment a un algoritme fix. Finalment, observem que, si se separen les formes definides de les indefinides, per als dos coeficients que hem ensenyat a rebaixar per sota de límits fixos es poden fixar límits encara menors; això, però, no és necessari per al nostre projecte present.

273. Ara, heus aquí alguns exemples, pels quals s'il·lustraran més els preceptes precedents.

Exemple 1. Sigui $f = \begin{pmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{pmatrix}$, i serà

$$F = \begin{pmatrix} -825, & -166, & -398 \\ 257, & 573, & -370 \end{pmatrix},$$

$D = -1$. Com que (19, 1, 21) és una forma binària reduïda, a la qual no equival cap altra amb el primer terme menor que 19, aquí no és aplicable la primera reducció; però la forma binària $(A'', B, A') = (-398, 257, -166)$, per la teoria de l'equivalència de formes binàries, es troba transformable en l'equivalent més simple $(-2, 1, -10)$, en la qual es transforma per la substitució 2, 7, 3, 11. Així, fent $\beta' = 2$, $\gamma' = -7$, $\beta'' = -3$, $\gamma'' = 11$, s'haurà d'aplicar a la forma f la substitució

$$\begin{matrix} 1, & 0, & 0 \\ 0, & 2, & -7 \\ 0, & -3, & 11, \end{matrix}$$

per la qual es troba que es transforma en la

$$\begin{pmatrix} 19, & 354, & 4769 \\ -1299, & 301, & -82 \end{pmatrix}. \qquad (f')$$

El tercer coeficient de la forma adjunta a aquesta és -2; a aquest respecte, f' s'ha de considerar més simple que f.

Es pot aplicar la primera reducció a la forma f'. Això és, com que la forma binària $(19,\ -82,\ 354)$ es transforma en $(1,\ 0,\ 2)$ per la substitució $13,\ 4,\ 3,\ 1$, s'haurà d'aplicar a la forma f' la substitució

$$\begin{array}{rrr} 13, & 4, & 0 \\ 3, & 1, & 0 \\ 0, & 0, & 1, \end{array}$$

per la qual es transforma en la $\begin{pmatrix} 1, & 2, & 4769 \\ -95, & 16, & 0 \end{pmatrix}$ $\cdots$ f''.

A la forma f'', a la qual és adjunta

$$\begin{pmatrix} -513, & -4513, & -2 \\ -95, & 32, & 1520 \end{pmatrix},$$

se li pot aplicar de nou la segona reducció. Això és, $(-2,\ -95,\ -4513)$ es transforma en $(-1,\ 1,\ -2)$ per la substitució $47,\ 1,\ -1,\ 0$; per la qual cosa, s'haurà d'aplicar a f'' la substitució

$$\begin{array}{rrr} 1, & 0, & 0 \\ 0, & 47, & -1 \\ 0, & 1, & 0, \end{array}$$

per la qual es transforma en

$$\begin{pmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{pmatrix}. \qquad (f''')$$

El primer coeficient d'aquesta no es pot disminuir més per la primera reducció, ni el tercer de la seva adjunta per la segona.

Exemple 2. Sigui proposada la forma

$$\begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix}, \qquad (f)$$

l'adjunta de la qual és $\begin{pmatrix} -3, & -20, & -244 \\ 70, & -28, & 8 \end{pmatrix}$, i el determinat de la qual, $= 2$. Aquí es troben successivament, aplicant alternativament la segona i la primera reducció,

substitucions per les quals	la forma	es transforma en
$\begin{matrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 4, & -1 \end{matrix}$	f	$\begin{pmatrix} 10, & 2, & 2 \\ -1, & 0, & -4 \end{pmatrix} = f'$
$\begin{matrix} 0, & -1, & 0 \\ 1, & -2, & 0 \\ 0, & 0, & 1 \end{matrix}$	f'	$\begin{pmatrix} 2, & 2, & 2 \\ 2, & -1, & 0 \end{pmatrix} = f''$
$\begin{matrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 2, & -1 \end{matrix}$	f''	$\begin{pmatrix} 2, & 2, & 2 \\ -2, & 1, & -2 \end{pmatrix} = f'''$
$\begin{matrix} 1, & 0, & 0 \\ 1, & 1, & 0 \\ 0, & 0, & 1 \end{matrix}$	f'''	$\begin{pmatrix} 0, & 2, & 2 \\ -2, & -1, & 0 \end{pmatrix} = f^{IV}.$

La forma f^{IV} no es pot reduir més enllà ni per la primera ni per la segona reducció.

274. Quan es té una forma ternària, el primer coeficient de la qual i el tercer de la forma adjunta s'han reduït tant com es pot fer pels mètodes precedents, el mètode següent proporciona una ulterior reducció.

Aplicant els mateixos signes que en l'article 272, i posant $\alpha = 1$, $\alpha' = 0$, $\beta' = 1$, $\alpha'' = 0$, $\beta'' = 0$, $\gamma'' = 1$, és a dir, aplicant la substitució

$$\begin{array}{ccc} 1, & \beta, & \gamma \\ 0, & 1, & \gamma' \\ 0, & 0, & 1, \end{array}$$

serà $m = a$, $m' = a' + 2b''\beta + a\beta\beta$, $m'' = a'' + 2b\gamma' + 2b'\gamma + a\gamma\gamma + 2b''\gamma\gamma' + a'\gamma'\gamma'$, $n = b + a'\gamma' + b'\beta + b''(\gamma + \beta\gamma') + a\beta\gamma$, $n' = b' + a\gamma + b''\gamma'$, $n'' = b'' + a\beta$; a part d'això, $M'' = A''$, $N = B - A''\gamma'$, $N' = B' - N\beta - A''\gamma$. Així, per una tal substitució, els coeficients a, A'', que per les reduccions precedents han estat disminuïts, no canvien; per la qual cosa, la feina consistirà a obtenir disminucions en els coeficients restants per una determinació idònia de β, γ, γ'. Per a aquesta finalitat observem, primer, que si fos $A'' = 0$, es pot suposar que també és $a = 0$; en efecte, si a no $= 0$, encara seria aplicable la primera reducció per una vegada, ja que qualsevol forma binària de determinant 0 equival a una forma tal com $(0, 0, h)$, o sigui, el seu primer terme $= 0$ (vegeu l'article 215). És lícit suposar, per una raó completament similar, que també és $A'' = 0$ si fos $a = 0$, de manera que, o bé cap dels nombres a, A'' és 0, o bé ho són tots dos.

En el primer cas, és evident que es poden determinar els β, γ, γ', de manera que, sense respecte al signe, n'', N, N', no siguin més grans que $\frac{1}{2}a$, $\frac{1}{2}A''$, $\frac{1}{2}A''$,

respectivament. Així, en el primer exemple de l'article precedent, l'última forma $\begin{pmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{pmatrix}$, l'adjunta de la qual és $\begin{pmatrix} -513, & -2, & -1 \\ 1, & -16, & 32 \end{pmatrix}$, es transformarà en la

$$\begin{pmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \qquad (f^{IV})$$

l'adjunta de la qual és $\begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$, per la substitució

$$\begin{matrix} 1, & -16, & 16 \\ 0, & 1, & -1 \\ 0, & 0, & 1. \end{matrix}$$

En el darrer cas, en què $a = A'' = 0$, de manera que també $b'' = 0$, serà $m = 0$, $m' = a'$, $m'' = a''+2b\gamma'+2b'\gamma+a'\gamma'\gamma'$, $n = b+a'\gamma'+b'\beta$, $n' = b'$, $n'' = 0$. Així, serà $D = a'b'b' = m'n'n'$; i es copsarà fàcilment que es poden determinar β i γ' de manera que n resulti igual al residu mínim absolut de b segons el mòdul que és màxim comú divisor de a', b'; és a dir, que, sense respecte al signe, n no resulti més gran que la meitat d'aquest divisor, de manera que $n = 0$, sempre que a', b' siguin primers entre si. Determinats β, γ', d'aquesta manera, el valor de γ es podrà agafar de manera que m'', sense respecte al signe, no sigui més gran que b'; això és, certament, impossible quan $b' = 0$; llavors, però, seria $D = 0$, cas que hem exclòs. Així, per a l'última forma del segon exemple de l'article precedent, resulta $n = -2 - \beta + 2\gamma'$, d'on, posant $\beta = -2$, $\gamma' = 0$, resulta $n = 0$; a més a més, $m'' = 2 - 2\gamma$ i, posant $\gamma = 1$, $m'' = 0$. Així, tenim la substitució

$$\begin{matrix} 1, & -2, & 1 \\ 0, & 1, & 0 \\ 0, & 0, & 1, \end{matrix}$$

per la qual aquella forma es transforma en

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix}. \qquad (f^V)$$

275. Si es té una sèrie de formes ternàries equivalents f, f', f'', f''', etc., i les transformacions de cadascuna d'aquestes formes en la següent, de les transformacions de la forma f en f' i de la forma f' en f'' es dedueix, per l'article 270, la transformació de la forma f en f''; d'aquesta, i de la transformació de f'' en f''', se segueix la transformació de la forma f en f''', etc., i, evidentment, d'aquesta manera es podrà trobar la transformació de la forma f en qualsevol altra de la sèrie. I com que de la transformació de la forma f en qualsevol altra equivalent g es pot deduir la transformació de la forma g en f (S'' de S, articles 268, 269) d'aquesta manera es podrà trobar la transformació de qualsevol de les formes de la sèrie f', f'', etc., en la primera f. Així, per a les formes del primer exemple de l'article precedent, es troben les substitucions

13,	4,	0	13,	188,	-4	13,	-20,	16
6,	2,	-7	6,	87,	-2	6,	-9,	7
-9,	-3,	11,	-9,	-130,	3,	-9,	14,	-11,

per les quals f es transforma en f'', f''', f^{IV}, respectivament, i de l'última substitució, la

$$\begin{matrix} 1, & 4, & 4 \\ 3, & 1, & 5 \\ 3, & -2, & 3, \end{matrix}$$

per la qual f^{IV} es transforma en f. De manera similar, per a l'exemple 2 de l'article precedent, es produeixen les substitucions

$$\begin{array}{rrr} 1, & -1, & 1 \\ -3, & 4, & -3 \\ 10, & -14, & 11, \end{array} \qquad \begin{array}{rrr} 2, & -3, & -1 \\ 3, & 1, & 0 \\ 2, & 4, & 1, \end{array}$$

per les quals, respectivament, la forma $\begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix}$ es transforma en $\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix}$, i aquesta en aquella.

276. Teorema. *La quantitat de classes en què es distribueixen totes les formes ternàries de determinant donat sempre és finita.*

Dem. I. La quantitat de totes les formes

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

de determinant donat D, en les quals $a = 0$, $b'' = 0$, b no més gran que la meitat del màxim comú divisor dels nombres a', b'; a'' no més gran que b', és, evidentment, finita. En efecte, com que ha de ser $a'b'b' = D$, per a b' no es poden agafar altres valors que $+1$, -1 i les arrels dels quadrats que divideixen D (si d'aquests se'n donen altres, a part de 1) afectades de signe positiu i negatiu, valors dels quals la quantitat és finita. Però per a cada un dels valors de b' el valor de a' és determinat, i, evidentment, els valors de b, a'', es limiten a una quantitat finita.

II. De manera similar, és finita la quantitat de totes les formes $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ de determinant D, en les quals a no és $= 0$, ni més gran que $\frac{4}{3}\sqrt[3]{\pm D}$; $b''b'' - aa' = A''$ no $= 0$ ni més gran que $\frac{4}{3}\sqrt[3]{D^2}$; b'' no més gran que $\frac{1}{2}a$; $ab - b'b'' = B$ i $a'b' - bb'' = B'$ no més grans que $\frac{1}{2}A''$. Efectivament, la quantitat de totes les combinacions dels valors de a, b'', A'', B, B', serà finita; però, determinats cadascun d'ells, també els coeficients restants a', b, b', a'', de la forma i els coeficients de la forma adjunta $bb - a'a'' = A$, $b'b' - aa'' = A'$, $a''b'' - bb' = B''$ seran determinats per les equacions $a' = \frac{b''b'' - A''}{a}$, $A' = \frac{BB - aD}{A''}$, $A = \frac{B'B' - a'D}{A''}$, $B'' = \frac{BB' + b''D}{A''}$, $b = \frac{AB - B'B''}{D} = -\frac{Ba' + B'b''}{A''}$, $b' = \frac{A'B' - BB''}{D} = -\frac{Bb'' + B'a}{A''}$, $a'' = \frac{b'b' - A'}{a} = \frac{bb - A}{a'} = \frac{bb' + B''}{b''}$. Ara, com que totes aquelles formes s'obtenen elegint de totes les combinacions dels valors de a, b'', A'', B, B', aquelles per a les quals també s'obtenen valors enters per a a', a'', b, b', la seva quantitat serà, evidentment, finita.

III. Així, totes les formes en I i II constitueixen una quantitat finita de classes, que també podrà ser menor que la quantitat de formes, si algunes d'aquelles són equivalents entre si. Ara, com que per les disquisicions precedents qualsevol forma ternària de determinant D equival necessàriament a alguna d'aquelles formes, és a dir, pertany a alguna de les classes que constitueixen

aquelles formes, aquestes classes comprendran totes les formes de determinant D; és a dir, totes les formes ternàries de determinant D es distribuiran en una quantitat finita de classes. *Q. E. D.*

277. De l'explicació d'aquestes, sorgeixen espontàniament regles per les quals es poden trobar totes les formes en I i II de l'article precedent; per tant, serà suficient afegir-ne alguns exemples. Per a $D = 1$, les formes I produeixen (per l'ambigüitat dels signes) aquestes sis:

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0, & 1, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix};$$

en les formes II, a i A'' no poden tenir altres valors que $+1$ i -1; per a cada una de les quatre combinacions que s'originen d'aquí, b'', B i B' s'han de posar $= 0$, d'on surten les quatre formes

$$\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}.$$

De manera similar, per a $D = -1$, es tenen les sis formes I i les quatre II

$$\begin{pmatrix} 0, & -1, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0, & -1, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix},$$
$$\begin{pmatrix} -1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}.$$

Per a $D = 2$, surten les sis formes I

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & \pm 1, & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0, & 2, & \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix},$$

i les vuit formes II:

$$\begin{pmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1, & 1, & 2 \\ 0, & 0, & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1, & -1, & -2 \\ 0, & 0, & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1, & -2, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1, & 2, & 1 \\ 0, & 0, & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1, & 2, & -1 \\ 0, & 0, & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1, & -2, & -1 \\ 0, & 0, & 0 \end{pmatrix}.$$

D'altra banda, la quantitat de classes d'aquestes formes és molt menor que la quantitat de formes produïdes en aquests tres casos. Això és, es confirma fàcilment que

I. La forma $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$ es transforma en

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & -1, & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0, & 1, & 1 \\ 0, & \pm 1, & 0 \end{pmatrix},$$
$$\begin{pmatrix} 0, & 1, & -1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix},$$

respectivament, per les substitucions

$$\begin{matrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & -1, \end{matrix} \qquad \begin{matrix} 0, & 0, & 1 \\ 0, & 1, & -1 \\ \pm 1, & 1, & 0, \end{matrix}$$

$$\begin{array}{rrr} 0, & 0, & 1 \\ 0, & 1, & 1 \\ \pm 1, & -1, & -1, \end{array} \qquad \begin{array}{rrr} 1, & 0, & -1 \\ 1, & 1, & -1 \\ 0, & -1, & 1, \end{array}$$

però la forma $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$, en

$$\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix},$$

per la sola permutació de les indeterminades. Per tant, aquelles deu formes ternàries de determinant 1 es redueixen a les dues

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}, \qquad \begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix};$$

per a la primera, si agrada més, també es pot agafar la $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$. Com que la primera forma és indefinida, la darrera definida, és evident que qualsevol forma ternària indefinida de determinant 1 equival a la forma $xx + 2yz$, i qualsevol definida, a la $-xx - yy - zz$.

II. De manera completament similar, es troba que qualsevol forma ternària indefinida de determinant -1 equival a la forma $-xx + 2yz$; qualsevol definida, a la $xx + yy + zz$.

III. Per al determinant 2, de les vuit formes (II) es poden rebutjar immediatament la segona, la sisena i la setena, ja que aquestes s'originen de la primera per la sola permutació de les indeterminades, i per una raó similar, també la cinquena, que prové de la tercera, i la vuitena, igualment de la quarta; les tres restants constitueixen, amb les sis formes de I, tres classes; això és,

$\begin{pmatrix} 0, & 2, & 0 \\ 0, & 1, & 0 \end{pmatrix}$ es transforma en $\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix}$ per la substitució

$$\begin{matrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & -1, \end{matrix}$$

i la forma $\begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}$ en

$$\begin{pmatrix} 0, & 2, & 1 \\ 0, & 1, & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0, & 2, & 1 \\ 0, & -1, & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0, & 2, & -1 \\ 0, & 1, & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0, & 2, & -1 \\ 0, & -1, & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{pmatrix},$$

respectivament, per les substitucions

$$\begin{matrix} 1, & 0, & 1 \\ 1, & 2, & 0 \\ 1, & 1, & 0, \end{matrix} \qquad \begin{matrix} 1, & 0, & -1 \\ 1, & 2, & 0 \\ 1, & 1, & 0, \end{matrix} \qquad \begin{matrix} 1, & 0, & 0 \\ 1, & 2, & -1 \\ 1, & 1, & -1, \end{matrix}$$

$$\begin{matrix} 1, & 0, & 0 \\ 1, & 2, & 1 \\ 1, & 1, & 1, \end{matrix} \qquad \begin{matrix} 1, & 0, & 0 \\ 0, & 1, & 2 \\ 0, & 1, & 1. \end{matrix}$$

Així, qualsevol forma ternària de determinant 2 és reductible a alguna de les tres

$$\begin{pmatrix} 0, & 2, & 0 \\ 0, & 1, & 0 \end{pmatrix}, \begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}, \begin{pmatrix} -1, & -1, & -2 \\ 0, & 0, & 0 \end{pmatrix};$$

en lloc de la primera, si plau més, també es pot agafar $\begin{pmatrix} 2, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$. Però és evident que qualsevol forma

ternària definida equivaldrà necessàriament a la tercera $-xx-yy-2zz$, ja que les dues primeres són indefinides; qualsevol indefinida a la primera o bé a la segona, i, certament, a la primera $2xx + 2yz$ si els seus coeficients primer, segon i tercer són simultàniament parells (ja que es copsa fàcilment que una tal forma es transforma per qualsevol substitució en una forma similar, de manera que no pot equivaler a la segona forma), a la segona $xx + yy - 2zz$ si els seus coeficients primer, segon i tercer no són simultàniament parells, sinó un, dos, o bé tots, imparells (en efecte, per una raó similar, la primera forma $2xx + 2yz$ no podrà ser transformable en una tal forma per cap substitució).

Així, doncs, el que va succeir en els exemples dels articles 273, 274, que la forma definida $\begin{pmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{pmatrix}$ de determinant -1 es reduïa a la $xx + yy + zz$ i que la forma indefinida $\begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix}$ de determinant 2 a $2xx-2yz$, o sigui (el que rendeix el mateix), a $2xx+2yz$, s'hauria pogut preveure *a priori* per les disquisicions precedents.

278. Per una forma ternària, les indeterminades de la qual són x, x', x'', *es representen* tant nombres, atribuint a x, x', x'', valors determinats, com formes binàries, per substitucions del tipus $x = mt + nu$, $x' = m't + n'u$, $x'' = m''t + n''u$, on m, n, m', etc., designen nombres determinats; i t, u, indeterminades de la forma representada. Així, per a una teoria completa de les formes ternàries es requeriria la solució dels problemes següents: I. Trobar totes les representacions d'un nombre donat per una forma ternària donada. II. Tro-

bar totes les representacions d'una forma binària donada per una ternària donada. III. Decidir si dues formes ternàries donades del mateix determinant són o no equivalents i, en el primer cas, trobar totes les transformacions de l'una en l'altra. IV. Decidir si una forma ternària donada n'implica una altra donada de determinant més gran o no i, en el primer cas, assignar totes les transformacions d'aquella en aquesta. D'aquests problemes, més difícils que els anàlegs en les formes binàries, en tractarem més en un altre lloc; aquí, restringim la nostra disquisició a mostrar de quina manera el primer problema es pot reduir al segon i el segon al tercer; però, el tercer, ensenyarem a resoldre'l per a alguns dels casos més simples i que il·lustren principalment la teoria de les formes binàries; exclourem aquí completament el quart.

279. Lema. *Proposats tres nombres enters qualssevol* a, a', a'' *(però que no són tots simultàniament* $= 0$*), trobar-ne uns altres sis* B, B', B'', C, C', C'', *disposats de manera que resulti* $B'C'' - B''C' = a$, $B''C - BC'' = a'$, $BC' - B'C = a''$.

Solució. Sigui α el màxim comú divisor de a, a', a'', i s'agafen enters A, A', A'', de manera que resulti $Aa + A'a' + A''a'' = \alpha$. A més a més, s'agafen a voluntat tres enters $\mathfrak{C}$, $\mathfrak{C}'$, $\mathfrak{C}''$, amb l'única condició que els tres nombres $\mathfrak{C}'A'' - \mathfrak{C}''A'$, $\mathfrak{C}''A - \mathfrak{C}A''$, $\mathfrak{C}A' - \mathfrak{C}'A$, que designarem per b, b', b'', respectivament, i el seu màxim comú divisor per β, no resultin simultàniament $= 0$. Llavors, es posa $a'b'' - a''b' = \alpha\beta C$, $a''b - ab'' = \alpha\beta C'$, $ab' - a'b = \alpha\beta C''$, i és clar que els C, C', C'', seran enters. Finalment, agafant enters $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$, de manera que resulti $\mathfrak{B}b + \mathfrak{B}'b' + \mathfrak{B}''b'' = \beta$, posant $\mathfrak{B}a + \mathfrak{B}'a' + \mathfrak{B}''a'' = h$ i establint $B = \alpha\mathfrak{B} - hA$, $B' = \alpha\mathfrak{B}' - hA'$,

$B'' = \alpha\mathfrak{B}'' - hA''$, aquests valors de B, B', B'', C, C', C'', satisfaran les equacions prescrites.

En efecte, es troba que $aB + a'B' + a''B'' = 0$, $bA + b'A' + b''A'' = 0$, d'on $bB + b'B' + b''B'' = \alpha\beta$. Ara, dels valors de C', C'', resulta $\alpha\beta(B'C'' - B''C') = ab'B' - a'bB' - a''bB'' + ab''B'' = a(bB + b'B' + b''B'') - b(aB + a'B' + a''B'') = \alpha\beta a$, de manera que $B'C'' - B''C' = a$; de manera similar es troba $B''C - BC'' = a'$, $BC' - B'C = a''$. *Q. E. F.* D'altra banda, aquí s'han de suprimir l'anàlisi per la qual s'ha trobat aquesta solució i també el mètode per a trobar, a partir d'una solució, totes.

280. Suposem que la forma binària $att + 2btu + cuu \cdots \phi$, el determinant de la qual és $= D$, es representa per la forma ternària f, les indeterminades de la qual són x, x', x'', posant $x = mt + nu$, $x' = m't + n'u$, $x'' = m''t + n''u$, i que l'adjunta a f és la forma F, les indeterminades de la qual són X, X', X''. Llavors, es confirma fàcilment per càlcul (designant els coeficients de les formes f, F, per lletres peculiars), o bé es dedueix directament de l'article 268, II, que el nombre D es representa per F posant $X = m'n'' - m''n'$, $X' = m''n - mn''$, $X'' = mn' - m'n$, i aquesta representació del nombre D es pot anomenar apropiadament *adjunta* de la representació de la forma ϕ per f. Per abreujar, si els valors de X, X', X'', no tenen cap divisor comú, anomenarem *pròpia* aquesta representació de D, si no, *impròpia*, i també atribuirem les mateixes denominacions a la representació de la forma ϕ per f, a la qual és adjunta aquella representació de D. Ara, la trobada de totes les representacions pròpies del nombre D per la forma F se sustenta en les consideracions següents.

I. No es dóna cap representació de D per F que no es pugui deduir d'alguna representació d'alguna forma de determinant D per la forma f, és a dir, que és adjunta a tal representació.

En efecte, sigui $X = L$, $X' = L'$, $X'' = L''$, una representació qualsevol de D per F; pel lema de l'article precedent, s'agafen m, m', m'', n, n', n'', de manera que resulti $m'n''-n'm'' = L$, $m''n-mn'' = L'$, $mn'-m'n = L''$, i f es transformarà en la forma binària $\phi = att + 2btu+cuu$ per la substitució $x = mt+nu$, $x' = m't+n'u$, $x'' = m''t + n''u$. Llavors, es copsarà fàcilment que D és el determinant de la forma ϕ i la representació proposada de D per F l'adjunta a la representació de ϕ per f.

Exemple. Sigui $f = xx + x'x' + x''x''$, de manera que $F = -XX - X'X' - X''X''$; $D = -209$, i la seva representació per F, la $X = 1$, $X' = 8$, $X'' = 12$; d'aquí es troben com a valors de m, m', m'', n, n', n'', respectivament, els -20, 1, 1, -12, 0, 1, i $\phi = 402tt + 482tu + 145uu$.

II. Si ϕ, χ, són formes binàries pròpiament equivalents, qualsevol representació de D per F adjunta a alguna representació de la forma ϕ per f també serà adjunta a alguna representació de la forma χ per f.

Siguin p, q, les indeterminades de la forma χ; ϕ es transforma en χ per la substitució pròpia $t = \alpha p + \beta q$, $u = \gamma p + \delta q$, i sigui $x = mt + nu$, $x' = m't + n'u$, $x'' = m''t+n''u \cdots (R)$ alguna representació de la forma ϕ per f. Llavors, es copsa sense cap dificultat que si es posa $\alpha m + \gamma n = g$, $\alpha m' + \gamma n' = g'$, $\alpha m'' + \gamma n'' = g''$,

$\beta m + \delta n = h$, $\beta m' + \delta n' = h'$, $\beta m'' + \delta n'' = h''$, la forma χ serà representada per f establint $x = gp + hq$, $x' = g'p + h'q$, $x'' = g''p + h''q \cdots (R')$ i, fet el càlcul, es troba (a causa que $\alpha\delta - \beta\gamma = 1$) que és $g'h'' - g''h' = m'n'' - m''n'$, $g''h - gh'' = m''n - mn''$, $gh' - g'h = mn' - m'n$; és a dir, aquesta representació de D per F és adjunta a les representacions R, R'.

Així, en l'exemple precedent, es troba que $\chi = 13pp - 10pq + 18qq$ equival a la forma ϕ i aquesta es transforma en aquella per la substitució pròpia $t = -3p + q$, $u = 5p - 2q$; d'aquí es troba la representació $x = 4q$, $x' = -3p + q$, $x'' = 2p - q$ de la forma χ per f, de la qual es dedueix la mateixa representació del nombre -209 de la qual havíem partit.

III. Finalment, si dues formes binàries ϕ, χ, de determinant D, les indeterminades de les quals són t, u; p, q, es poden representar per f i una mateixa representació pròpia de D per F és adjunta a alguna representació de l'una i a alguna representació de l'altra, aquelles formes seran, necessàriament, pròpiament equivalents. Suposem que ϕ es representa per f posant $x = mt + nu$, $x' = m't + n'u$, $x'' = m''t + n''u$, però χ establint $x = gp + hq$, $x' = g'p + h'q$, $x'' = g''p + h''q$, i que és $m'n'' - m''n' = g'h'' - g''h' = L$, $m''n - mn'' = g''h - gh'' = L'$, $mn' - m'n = gh' - g'h = L''$. S'agafen enters l, l', l'', de manera que resulti $Ll + L'l' + L''l'' = 1$ i es posa $n'l'' - n''l' = M$, $n''l - nl'' = M'$, $nl' - n'l = M''$, $l'm'' - l''m' = N$, $l''m - lm'' = N'$, $lm' - l'm = N''$; finalment, s'estableix $gM + g'M' + g''M'' = \alpha$, $hM + h'M' + h''M'' = \beta$, $gN + g'N' + g''N'' = \gamma$, $hN + h'N' + h''N'' = \delta$. D'aquí es dedueix fàcilment

$$\alpha m + \gamma n = g - l(gL + g'L' + g''L'') = g$$
$$\beta m + \delta n = h - l(hL + h'L' + h''L'') = h$$

i, de manera similar, $\alpha m' + \gamma n' = g'$, $\beta m' + \delta n' = h'$, $\alpha m'' + \gamma n'' = g''$, $\beta m'' + \delta n'' = h''$. D'aquí és clar que $mt+nu$, $m't+n'u$, $m''t+n''u$ es transformen en $gp+hq$, $g'p + h'q$, $g''p + h''q$, respectivament, per la substitució $t = \alpha p+\beta q$, $u = \gamma p+\delta q \cdots (S)$, d'on és evident que ϕ es transforma per la substitució S en la mateixa forma en què es transforma f posant $x = gp + hq$, $x' = g'p + h'q$, $x'' = g''p + h''q$; de manera que en la forma χ, a la qual, així, equival. Finalment, per les degudes substitucions, es troba fàcilment $\alpha\delta - \beta\gamma = (Ll + L'l' + L''l'')^2 = 1$; conseqüentment, la substitució S és pròpia i les formes ϕ, χ, pròpiament equivalents.

D'aquestes observacions es deriven les regles següents per a trobar totes les representacions pròpies de D per F. Es desenvolupen totes les classes de formes binàries de determinant D i de cadascuna s'elegeix a voluntat una forma; se cerquen totes les representacions pròpies de cadascuna d'aquestes formes per f (rebutjades les que casualment no es poden representar per f), i de cadascuna d'aquestes representacions es dedueixen representacions del nombre D per F. De I i II, és evident que, d'aquesta manera, s'obtenen totes les representacions pròpies possibles, de manera que la solució és completa; de III, que transformacions de formes de classes diferents produeixen, certament, representacions diferents.

281. La investigació de les representacions *impròpies* d'un nombre donat D per una forma F es redueix

fàcilment al cas precedent. Això és, és evident que si D no és divisible per cap quadrat (excepte 1) no es donen en absolut tals representacions; si no, si els quadrats $\lambda\lambda$, $\mu\mu$, $\nu\nu$, etc., divideixen D, es troben totes les representacions impròpies de D per F, si es desenvolupen totes les representacions pròpies dels nombres $\frac{D}{\lambda\lambda}$, $\frac{D}{\mu\mu}$, $\frac{D}{\nu\nu}$, etc., per la mateixa forma F, i es multipliquen els valors de les indeterminades per λ, μ, ν, etc., respectivament.

Així, d'aquesta manera, la trobada de totes les representacions d'un nombre donat per una forma ternària donada, *que és adjunta a alguna forma ternària*, depèn del segon problema; a aquest cas, però, que a primera vista podria semblar menys clar, es redueixen els restants així. Sigui D el nombre que cal representar per la forma $\left(\begin{array}{ccc} g, & g', & g'' \\ h, & h', & h'' \end{array}\right)$, el determinant de la qual és Δ, i a la qual l'adjunta és la forma $\left(\begin{array}{ccc} G, & G', & G'' \\ H, & H', & H'' \end{array}\right) = f$. Llavors, $\left(\begin{array}{ccc} \Delta g, & \Delta g', & \Delta g'' \\ \Delta h, & \Delta h', & \Delta h'' \end{array}\right) = F$ serà novament l'adjunta a aquesta, i és clar que les representacions del nombre ΔD per F (la investigació de les quals depèn de les precedents) són completament idèntiques a les representacions del nombre D per la forma proposada. D'altra banda, quan tots els coeficients de la forma f tenen un divisor comú μ, es copsa que tots els coeficients de la forma F són divisibles per $\mu\mu$; en conseqüència, també ΔD haurà de ser divisible per $\mu\mu$ (altrament no es donaria cap representació); i les representacions del nombre D per la forma proposada coincidiran amb les representacions del nombre $\frac{\Delta D}{\mu\mu}$ per la forma que

s'origina de F en dividir cadascun dels coeficients per $\mu\mu$, forma a la qual serà adjunta la que s'origina de f en dividir cadascun dels coeficients per μ.

Finalment, observem que aquesta solució del primer problema no és aplicable en l'únic cas en què $D = 0$; en efecte, aquí, totes les formes binàries de determinant D no es distribueixen en una quantitat finita de classes; més avall, però, resoldrem aquest cas a partir d'uns altres principis.

282. La investigació de les representacions d'una forma binària donada el determinant de la qual no és $= 0$* per una ternària donada, depèn de les observacions següents.

I. De qualsevol representació pròpia d'una forma binària $(p, q, r) = \phi$ de determinant D per una ternària f de determinant Δ es poden deduir enters B, B' tals que sigui $BB \equiv \Delta p$, $BB' \equiv -\Delta q$, $B'B' \equiv \Delta r$ (mòd. D); és a dir, el valor de l'expressió $\sqrt{\Delta(p, -q, r)}$ (mòd. D). Es té la representació pròpia de la forma ϕ per f, $x = \alpha t + \beta u$, $x' = \alpha' t + \beta' u$, $x'' = \alpha'' t + \beta'' u$, (on x, x', x''; t, u, designen les indeterminades de les formes f, ϕ); s'agafen enters γ, γ', γ'', de manera que $(\alpha'\beta'' - \alpha''\beta')\gamma + (\alpha''\beta - \alpha\beta'')\gamma' + (\alpha\beta' - \alpha'\beta)\gamma'' = k$ resulti o bé $= +1$ o bé $= -1$, i es transforma f per la substitució

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

* Per abreujar, en aquest lloc ometem aquest cas, que cal tractar per un mètode bastant diferent.

en la forma $\left(\begin{array}{ccc} a, & a', & a'' \\ b, & b', & b'' \end{array}\right) = g$, l'adjunta de la qual sigui $\left(\begin{array}{ccc} A, & A', & A'' \\ B, & B', & B'' \end{array}\right) = G$. Llavors, és evident que serà $a = p$, $b'' = q$, $a' = r$, $A'' = D$, i Δ el determinant de la forma g; d'on $BB = \Delta p + A'D$, $BB' = -\Delta q + B''D$, $B'B' = \Delta r + AD$. Així, *per exemple*, la forma $19tt + 6tu + 41uu$ es representa per $xx + x'x' + x''x''$ posant $x = 3t + 5u$, $x' = 3t - 4u$, $x'' = t$; d'on, establint $\gamma = -1$, $\gamma' = 1$, $\gamma'' = 0$, es descobreix $B = -171$, $B' = 27$; o sigui, $(-171, 27)$ és un valor de l'expressió $\sqrt{-1(19, -3, 41)}$ (mòd. 770).

Ara, d'aquí se segueix que, si $\Delta(p, -q, r)$ no és residu quadràtic de D, ϕ no pot ser pròpiament representable per cap forma ternària de determinant Δ; així, en el cas en què Δ, D són primers entre si, Δ haurà de ser el nombre característic de la forma ϕ.

II. Com que γ, γ', γ'', es poden determinar d'infinites maneres diferents, d'això també es produiran altres i altres valors de B, B', dels quals vegem quin nexe tenen entre si. Suposem que també s'han disposat δ, δ', δ'', de manera que $(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \mathfrak{k}$ resulti o bé $= +1$ o bé $= -1$, i que la forma f es transforma, per la substitució

$$\begin{array}{ccc} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'', \end{array}$$

en $\left(\begin{array}{ccc} \mathfrak{a}, & \mathfrak{a}', & \mathfrak{a}'' \\ \mathfrak{b}, & \mathfrak{b}', & \mathfrak{b}'' \end{array}\right) = \mathfrak{g}$, l'adjunta de la qual és

$$\left(\begin{array}{ccc} \mathfrak{A}, & \mathfrak{A}', & \mathfrak{A}'' \\ \mathfrak{B}, & \mathfrak{B}', & \mathfrak{B}'' \end{array}\right) = \mathfrak{G}.$$

Llavors, g, $\mathfrak{g}$, seran equivalents, de manera que també G i $\mathfrak{G}$, i per aplicació dels preceptes transmesos en els articles 269, 270,* es troba que, si s'estableix $(\beta'\gamma'' - \beta''\gamma')\delta + (\beta''\gamma - \beta\gamma'')\delta' + (\beta\gamma' - \beta'\gamma)\delta'' = \zeta$, $(\gamma'\alpha'' - \gamma''\alpha')\delta + (\gamma''\alpha - \gamma\alpha'')\delta' + (\gamma\alpha' - \gamma'\alpha)\delta'' = \eta$, la forma $\mathfrak{G}$ es transforma en G per la substitució

$$\begin{array}{lll} k, & 0, & 0 \\ 0, & k, & 0 \\ \zeta, & \eta, & \mathfrak{k}. \end{array}$$

D'aquí serà $B = \eta\mathfrak{k}D + \mathfrak{k}k\mathfrak{B}$, $B' = \zeta\mathfrak{k}D + \mathfrak{k}k\mathfrak{B}'$, de manera que, a causa que $\mathfrak{k}k = \pm 1$, o bé $B \equiv \mathfrak{B}$, $B' \equiv \mathfrak{B}'$, o bé $B \equiv -\mathfrak{B}$, $B' \equiv -\mathfrak{B}'$ (mòd. D). En el primer cas, anomenem els valors (B, B'), $(\mathfrak{B}, \mathfrak{B}')$, equivalents; en el darrer, oposats; i direm, però, que la representació de la forma ϕ *pertany* a qualsevol valor de l'expressió $\sqrt{\Delta(p, -q, r)}$ (mòd. D) que es pot deduir d'ella pel mètode de I. D'aquí, tots els valors a què pertany la mateixa representació seran o bé equivalents o bé oposats.

III. Però, recíprocament, si, com abans en I, la representació $x = \alpha t + \beta u$, etc., de la forma ϕ per f pertany al valor (B, B'), la que es dedueix d'això amb l'ajut de la transformació

$$\begin{array}{lll} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'', \end{array}$$

també pertanyerà a qualsevol altre valor $(\mathfrak{B}, \mathfrak{B}')$ que és o bé equivalent o bé oposat a aquell; és a dir, en lloc de

* Deduint, de la transformació de la forma f en g, la transformació de la forma g en f; d'aquesta i de la transformació de la forma f en $\mathfrak{g}$, la transformació de la forma g en $\mathfrak{g}$; finalment, d'aquesta, per transposició, la transformació de la forma $\mathfrak{G}$ en G.

γ, γ', γ'', serà lícit agafar altres enters δ, δ', δ'', per als quals tingui lloc l'equació (Ω) $(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \pm 1$, i que siguin preparats de manera que el coeficient 4 i 5 en la seva forma adjunta, en la qual es transforma f per la substitució (S)

$$\begin{array}{ccc} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'', \end{array}$$

siguin, respectivament, $= \mathfrak{B}$, $\mathfrak{B}'$. En efecte, si s'estableix $\pm B = \mathfrak{B} + \eta D$, $\pm B' = \mathfrak{B}' + \zeta D$ (agafant aquí i posteriorment el signe superior o bé l'inferior segons que els valors (B, B'), $(\mathfrak{B}, \mathfrak{B}')$, siguin equivalents o bé oposats), d'on ζ, η, seran enters, i g es transforma per la substitució

$$\begin{array}{ccc} 1, & 0, & \zeta \\ 0, & 1, & \eta \\ 0, & 0, & \pm 1 \end{array}$$

en la forma $\mathfrak{g}$, el determinant de la qual és Δ, es copsarà fàcilment, però, que els coeficients 4 i 5 en la forma adjunta resulten $\mathfrak{B}$, $\mathfrak{B}'$, respectivament. Però, fent $\alpha\zeta + \beta\eta \pm \gamma = \delta$, $\alpha'\zeta + \beta'\eta \pm \gamma' = \delta'$, $\alpha''\zeta + \beta''\eta \pm \gamma'' = \delta''$, serà clar sense cap dificultat que f es transforma en $\mathfrak{g}$ per la substitució (S) i que s'ha satisfet l'equació (Ω). *Q. E. D.*

283. D'aquests principis es dedueix el mètode següent per a trobar totes les representacions pròpies de la forma binària $\phi = ptt + 2qtu + ruu$ de determinant D per una ternària f de determinant Δ.

I. Es descobreixen tots els valors diferents (és a dir, no equivalents) de l'expressió $\sqrt{\Delta(p, -q, r)}$ (mòd. D).

Aquest problema, per al cas en què ϕ és una forma primitiva i Δ és primer amb D, ha estat resolt més amunt (article 233), i els casos restants es redueixen molt fàcilment a aquest, però la brevetat no permet explicar aquí aquesta qüestió més extensament. Observem, només, que sempre que Δ sigui primer amb D, l'expressió $\Delta(p, -q, r)$ no pot ser residu quadràtic de D, llevat que ϕ sigui una forma primitiva. En efecte, suposant que $\Delta p = BB - DA'$, $-\Delta q = BB' - DB''$, $\Delta r = B'B' - DA$, resulta $(DB'' - \Delta q)^2 = (DA' + \Delta p)(DA + \Delta r)$; d'aquí, per desenvolupament, i substituint D per $qq - pr$, resulta $(qq - pr)(B''B'' - AA') - \Delta(Ap + 2B''q + A'r) + \Delta\Delta = 0$, d'on es conclou fàcilment que si p, q, r, tinguessin un divisor comú, aquest dividiria també $\Delta\Delta$; però, llavors, Δ no podria ser primer amb D. Per tant p, q, r, no poden tenir cap divisor comú, o sigui, ϕ serà una forma primitiva.

II. Designem per m la quantitat d'aquests valors, i suposem que entre ells es troben n valors que són oposats a si mateixos (establint $n = 0$ quan no apareixen tals). Llavors, és evident que dels $m-n$ valors restants, sempre seran oposats a parelles (ja que se suposa que es tenen la totalitat dels valors); de qualsevol parella de valors oposats se'n rebutja un a voluntat, i restaran en total $\frac{1}{2}(m + n)$ valors. Així, per exemple, dels vuit valors de l'expressió $\sqrt{-1(19, -3, 41)}$ (mòd. 770), (39, 237), (171, −27), (269, −83), (291, −127), (−39, −237), (−171, 27), (−269, 83), (−291, 127), els quatre darrers s'han de rebutjar com a oposats als quatre primers. D'altra banda, es copsa que si (B, B') és un valor oposat a si mateix, $2B$, $2B'$ i, en conseqüència, també $2\Delta p$, $2\Delta q$, $2\Delta r$, seran divisibles per D; així, si Δ, D són primers

entre si, també $2p$, $2q$, $2r$, seran divisibles per D, i, com que, per I, en aquest cas, tampoc p, q, r, no poden tenir cap divisor comú, també 2 haurà de ser divisible per D, cosa que no pot ser llevat que D, o bé $= \pm 1$, o bé $= \pm 2$. Per la qual cosa, per a tots els valors de D més grans que 2 sempre serà $n = 0$, si Δ és primer amb D.

III. Fet això així, és evident que qualsevol representació pròpia de la forma ϕ per f, necessàriament ha de pertànyer a alguns dels valors restants, i certament només a un. Per tant, aquests valors s'han de recórrer successivament, i cal investigar les representacions que corresponen a cadascun d'ells. Per a trobar les representacions que pertanyen a un valor *donat* (B, B'), s'ha de determinar, primer, la forma ternària

$$g = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

el determinant de la qual és $= \Delta$ i en la qual $a = p$, $b'' = q$, $a' = r$, $ab - b'b'' = B$, $a'b' - bb'' = B'$; els valors de a'', b, b', que es troben d'aquí amb l'ajut de les equacions de l'article 276, II, de les quals es copsa fàcilment que, en el cas en què Δ, D, siguin primers entre si, b, b', a'', resulten necessàriament enters (ja que aquests tres nombres, multiplicats tant per D com per Δ, produeixen enters). Ara, si o bé algun dels coeficients b, b', b'', és una fracció, o bé les formes f, g, no són equivalents, no es pot donar cap representació de la forma ϕ per f que pertanyi a (B, B'); però si b, b', b'', són enters, i les formes f, g, equivalents, qualsevol transformació d'aquella en aquesta, com

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'', \end{matrix}$$

proporciona una tal representació, posem $x = \alpha t + \beta u$, $x' = \alpha' t + \beta' u$, $x'' = \alpha'' t + \beta'' u$; i, evidentment, no podrà existir cap representació d'aquest tipus que no es pugui deduir d'alguna transformació. Així, d'aquesta manera, aquesta part del segon problema, que investiga les representacions *pròpies*, ja s'ha reduït al tercer problema.

IV. D'altra banda, transformacions diferents de la forma f en g sempre produeixen representacions diferents, exceptuant-ne l'únic cas en què el valor $(B,\ B')$ és oposat a si mateix, en el qual un parell de transformacions sempre proporcionen una única representació. En efecte, suposant que f també es transforma en g per la substitució

$$\begin{matrix} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{matrix}$$

(que proporciona la mateixa representació que la transformació precedent), i denotant per k, $\mathfrak{k}$, ζ, η, els mateixos nombres que en II de l'article precedent, serà $B = k\mathfrak{k}B + \eta\mathfrak{k}D$, $B' = k\mathfrak{k}B' + \zeta\mathfrak{k}D$; així, si se suposa que o bé ambdós k, $\mathfrak{k}$, són $= +1$, o bé ambdós $= -1$, serà (ja que hem exclòs el cas $D = 0$) $\zeta = 0$, $\eta = 0$, d'on se segueix fàcilment $\delta = \gamma$, $\delta' = \gamma'$, $\delta'' = \gamma''$; per tant, aquelles dues transformacions poden ser diferents en l'únic cas en què un dels nombres k, $\mathfrak{k}$, és $= +1$, l'altre $= -1$; llavors, serà $B \equiv -B$, $B' \equiv -B'$ (mòd. D), o sigui, el valor $(B,\ B')$ oposat a si mateix.

V. Del que hem transmès més amunt (article 271) dels criteris de formes definides i indefinides se segueix fàcilment que si Δ és positiu, D, negatiu, i ϕ, una forma negativa, g resulta una forma definida negativa; però si Δ és positiu i, o bé D positiu, o bé D negatiu i ϕ una

forma positiva, g surt una forma indefinida. Ara, com que f, g, no poden ser, certament, equivalents llevat que siguin similars respecte a aquesta qualitat, és evident que no es poden representar pròpiament ni formes binàries de determinant positiu ni tampoc positives per una ternària negativa, ni formes binàries negatives per una ternària indefinida de determinant positiu; sinó que per una forma ternària del primer o bé del darrer tipus, únicament binàries del darrer o bé del primer tipus, respectivament. Es conclou de manera similar que per una forma de determinant negatiu, ternària, definida (és a dir, positiva), únicament es representen binàries positives, i per una indefinida, únicament negatives i formes de determinant positiu.

284. Com que les representacions *impròpies* d'una forma binària ϕ de determinant D per una ternària f a la qual és adjunta F, són aquelles de les quals se segueixen les representacions impròpies del nombre D per la forma F, evidentment ϕ no es pot representar impròpiament per f llevat que D impliqui factors quadrats. Posem que tots els quadrats que divideixen D (excepte 1) són ee, $e'e'$, $e''e''$, etc. (la quantitat dels quals serà finita, ja que hem suposat que D no és $= 0$), i qualsevol representació impròpia de la forma ϕ per f proporcionarà una representació del nombre D per F en la qual els valors de les indeterminades tindran algun dels nombres e, e', e'', etc., com a màxim comú divisor; respecte d'això, per abreujar, direm que qualsevol representació impròpia de la forma ϕ *pertany* al divisor quadrat ee, o bé $e'e'$, o bé $e''e''$, etc. Ara, totes les representacions de la forma ϕ que pertanyen al mateix divisor quadrat *donat* ee (del qual suposem l'arrel e presa positivament) es troben per les regles següents, de la demostració sin-

tètica de les quals, que cal preferir aquí per brevetat, es podrà restituir fàcilment l'anàlisi mitjançant la qual s'han desenvolupat.

Primer, es descobreixen totes les formes binàries de determinant $\frac{D}{ee}$ que es transformen en la forma ϕ per una substitució pròpia tal com $T = \kappa t + \lambda u$, $U = \mu u$, on T, U, designen les indeterminades de la tal forma; t, u, les indeterminades de la forma ϕ; κ, μ, enters positius (el producte dels quals, així, és $= e$); λ, un enter positiu menor que μ (o també zero). Aquestes formes, amb les transformacions corresponents, es troben així.

S'iguala κ successivament a cadascun dels divisors de e presos positivament (incloent-hi també 1 i e) i resulti $\mu = \frac{e}{\kappa}$; per a cadascun dels valors determinats de κ, μ, s'atribueixen a λ tots els valors enters des de 0 fins a $\mu - 1$, amb la qual cosa es tindran, certament, totes les transformacions. Ara, es troba la forma que es transforma en ϕ per qualsevol substitució $T = \kappa t + \lambda u$, $U = \mu u$, investigant la forma en què es transforma ϕ per la $t = \frac{1}{\kappa}T - \frac{\lambda}{e}U$, $u = \frac{1}{\mu}U$; així s'obtindran les formes que corresponen a cadascuna de les transformacions; però de totes aquestes formes només s'han de retenir aquelles en les quals tots tres coeficients han sortit enters.*

* Si aquí es pogués tractar més profundament d'aquest problema, podríem reduir considerablement la solució. Immediatament és obvi que no és necessari agafar per a κ altres divisors de e llevat que aquells el quadrat dels quals divideixi el primer coeficient de la forma ϕ. D'altra banda, ens reservem per a una altra ocasió idònia reprendre aquest problema, del qual també es poden deduir solucions més simples dels problemes dels articles 213, 214.

Segon, posem que Φ és alguna d'aquestes formes que es pot transformar en ϕ per la substitució $T = \kappa t + \lambda u$, $U = \mu u$; s'investiguen totes les representacions *pròpies* de la forma Φ per f (si aquestes es donen), i s'expressen formalment per $x = \mathfrak{A}T + \mathfrak{B}U$, $x' = \mathfrak{A}'T + \mathfrak{B}'U$, $x'' = \mathfrak{A}''T + \mathfrak{B}''U \cdots$ $(\mathfrak{R})$; finalment, de cadascuna de $(\mathfrak{R})$ es dedueix la representació $(\rho) \cdots$ $x = \alpha t + \beta u$, $x' = \alpha' t + \beta' u$, $x'' = \alpha'' t + \beta'' u$, per les equacions $(R) \cdots \alpha = \kappa\mathfrak{A}$, $\alpha' = \kappa\mathfrak{A}'$, $\alpha'' = \kappa\mathfrak{A}''$, $\beta = \lambda\mathfrak{A} + \mu\mathfrak{B}$, $\beta' = \lambda\mathfrak{A}' + \mu\mathfrak{B}'$, $\beta'' = \lambda\mathfrak{A}'' + \mu\mathfrak{B}''$. Les formes restants trobades per la primera regla (si n'hi ha més d'una) es tracten completament de la mateixa manera que la forma Φ, de manera que es derivin les altres representacions d'una qualsevol de les representacions pròpies; i afirmo que d'aquesta manera es produeixen totes les representacions de la forma ϕ que pertanyen al divisor ee, i qualsevol, certament, només una vegada.

Dem. I. Que la forma ternària f es transforma realment en ϕ per qualsevol substitució (ρ) és tan obvi que no és necessària una explicació més àmplia; però que qualsevol representació (ρ) és impròpia i pertany al divisor ee, resulta del fet que els nombres $\alpha'\beta'' - \alpha''\beta'$, $\alpha''\beta - \alpha\beta''$, $\alpha\beta' - \alpha'\beta$, resulten, respectivament, $= e(\mathfrak{A}'\mathfrak{B}'' - \mathfrak{A}''\mathfrak{B}')$, $e(\mathfrak{A}''\mathfrak{B} - \mathfrak{A}\mathfrak{B}'')$, $e(\mathfrak{A}\mathfrak{B}' - \mathfrak{A}'\mathfrak{B})$, d'on el seu màxim comú divisor serà, evidentment, e (ja que $(\mathfrak{R})$ és una representació pròpia).

II. Mostrem que de qualsevol representació donada (ρ) de la forma ϕ es pot trobar una representació pròpia de la forma de determinant $\dfrac{D}{ee}$ continguda entre les formes trobades per la primera regla, o sigui, que dels valors donats de α, α', α'', β, β', β'', es poden

deduir valors enters de κ, λ, μ, que satisfacin les condicions prescrites, i els valors de $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$, $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$, les condicions (R); i, certament, només d'una única manera. Primer, de les tres primeres equacions de (R), és clar immediatament que per a κ s'ha d'agafar el màxim comú divisor de α, α', α'', amb signe positiu (en efecte, com que $\mathfrak{A}'\mathfrak{B}''-\mathfrak{A}''\mathfrak{B}'$, $\mathfrak{A}''\mathfrak{B}-\mathfrak{A}\mathfrak{B}''$, $\mathfrak{A}\mathfrak{B}'-\mathfrak{A}'\mathfrak{B}$, no han de tenir divisor comú, tampoc $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$, no poden tenir divisor comú); d'aquí, també estaran determinats $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$, i també $\mu = \dfrac{e}{\kappa}$ (que es copsa fàcilment que necessàriament resulta enter). Posem que s'han agafat tres enters $\mathfrak{a}$, $\mathfrak{a}'$, $\mathfrak{a}''$, de manera que resulti $\mathfrak{a}\mathfrak{A}+\mathfrak{a}'\mathfrak{A}'+\mathfrak{a}''\mathfrak{A}'' = 1$, i escrivim, per abreujar, k per $\mathfrak{a}\mathfrak{B} + \mathfrak{a}'\mathfrak{B}' + \mathfrak{a}''\mathfrak{B}''$. Llavors, de les tres últimes equacions de (R), se segueix que ha de ser $\mathfrak{a}\beta+\mathfrak{a}'\beta'+\mathfrak{a}''\beta'' = \lambda+\mu k$, d'on és clar immediatament que per a λ només es dóna un únic valor situat entre els límits 0 i $\mu - 1$. Fet això, com que $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$, també obtenen valors determinats, només resta que demostrem que, d'aquí, aquests sempre surten enters. Resultarà, però, $\mathfrak{B} = \dfrac{1}{\mu}(\beta-\lambda\mathfrak{A}) = \dfrac{1}{\mu}(\beta(1-\mathfrak{a}\mathfrak{A})-\mathfrak{A}(\mathfrak{a}'\beta'+\mathfrak{a}''\beta'')) + \mathfrak{A}k = \dfrac{1}{\mu}(\mathfrak{a}''(\mathfrak{A}''\beta-\mathfrak{A}\beta'') - \mathfrak{a}'(\mathfrak{A}\beta'-\mathfrak{A}'\beta)) + \mathfrak{A}k = \dfrac{1}{e}(\mathfrak{a}''(\alpha''\beta-\alpha\beta'') - \mathfrak{a}'(\alpha\beta'-\alpha'\beta)) + \mathfrak{A}k$, i, així, serà evidentment enter; i, similarment, es confirma fàcilment que $\mathfrak{B}'$, $\mathfrak{B}''$, també obtenen valors enters. D'aquests raonaments es conclou que no pot existir cap representació impròpia de la forma ϕ per f pertanyent al divisor ee que, pel mètode transmès, o bé no s'obtingui, o bé [s'obtingui] moltes vegades.

Ara, si es tracten de la mateixa manera els restants divisors quadrats de D i es descobreixen les representa-

cions que pertanyen a cadascun d'ells, es tindran totes les representacions impròpies de la forma ϕ per f.

D'altra banda, d'aquesta solució es dedueix fàcilment que el teorema transmès al final de l'article precedent per a les representacions pròpies també s'estén per a les impròpies; això és, que, en general, cap forma binària positiva de determinant negatiu no es pot representar per una ternària negativa, etc.; en efecte, és clar que si ϕ és una tal forma binària que, per causa d'aquell teorema, no es pot representar pròpiament per f, tampoc totes les formes de determinants $\frac{D}{ee}$, $\frac{D}{e'e'}$, etc., que impliquen ϕ no es podran representar pròpiament per f, ja que totes aquestes formes tenen el determinant afectat del mateix signe que ϕ, i quan aquests determinants són negatius, totes surten formes, o bé positives, o bé negatives, segons que ϕ pertanyi a aquelles, o bé a aquestes.

285. De les qüestions que constitueixen el tercer problema proposat per nosaltres (al qual s'han reduït els dos primers en el que precedeix), això és, proposades dues formes ternàries del mateix determinant decidir si són equivalents o no i, en el primer cas, trobar totes les transformacions de l'una en l'altra, en aquest lloc només podem inserir poc, ja que la solució completa que hem transmès per a problemes anàlegs en formes binàries, aquí és sotmès a dificultats encara més grans. Per la qual cosa, limitarem la nostra disquisició a certs casos particulars, pels quals s'ha emprès principalment aquesta digressió.

I. S'ha mostrat més amunt que per al determinant +1 totes les formes ternàries es distribueixen en dues classes, de les quals una conté totes les formes indefinides, l'altra, totes les definides (negatives). D'aquí es conclou immediatament que dues formes ternàries qualssevol de determinant 1 són equivalents si, o bé totes dues són definides, o bé totes dues indefinides; però, si una és definida i l'altra indefinida, l'equivalència no té lloc (evidentment, la darrera part de la proposició val, en general, per a formes de determinant qualsevol). De manera similar, dues formes qualssevol de determinant −1 equivaldran certament si, o bé totes dues són definides, o bé totes dues indefinides. Dues formes definides de determinant 2 sempre equivaldran; dues indefinides no equivaldran si en una els tres primers coeficients són tots parells però en l'altra no tots són parells; en els casos restants (si, o bé totes dues, o bé cap, tenen els tres primers coeficients simultàniament parells), equivaldran. D'aquesta manera, encara podríem aplicar moltes proposicions especials si, més amunt (article 277), s'haguessin desenvolupat més exemples.

II. Per a tots aquests casos també es podrà, designant f, f', formes ternàries equivalents, trobar una transformació de l'una en l'altra. Efectivament, més amunt s'ha assignat, per a tots els casos, en qualsevol classe de formes ternàries, una quantitat bastant petita de formes a alguna de les quals es pot reduir per mètodes uniformes qualsevol forma d'aquesta classe; i allà mateix hem ensenyat a reduir totes aquestes a una sola. Sigui F aquesta forma en la classe en què hi ha f, f', i, pels preceptes transmesos més amunt, es podran trobar transformacions de les formes f, f', en F i també de la

forma F en f, f'. D'aquí, per l'article 270, es podran deduir transformacions de la forma f en f' i de la forma f' en f.

III. Així, només restaria mostrar com d'una transformació d'una forma ternària f en una altra f' es poden derivar totes les transformacions possibles. Aquest problema depèn d'un altre més simple, això és, trobar totes les transformacions d'una forma ternària f en si mateixa. En efecte, si f es transforma en si mateixa per moltes substitucions (τ), (τ'), (τ''), etc., i en f' per la substitució (t), és clar que si, segons la norma de l'article 270, es combina la transformació (t) amb (τ), (τ'), (τ''), etc., es produiran transformacions per totes les quals f es transformarà en f'; a part d'això, es prova fàcilment per càlcul que qualsevol transformació de la forma f en f' es pot deduir d'aquesta manera de la combinació de la transformació donada (t) de la forma f en f' amb alguna (i, certament, *única*) transformació de la forma f en si mateixa, de manera que de la combinació d'una transformació donada de la forma f en f' amb *totes* les transformacions de la forma f en si mateixa s'originen *totes* les transformacions de la forma f en f', i, certament, cadascuna d'elles només una vegada.

Restringim aquí la investigació de totes les transformacions de la forma f en si mateixa al cas en què f és una forma definida els coeficients 4, 5, 6, de la qual són tots $= 0$.* Així, sigui $f = \begin{pmatrix} a, & a', & a'' \\ 0, & 0, & 0 \end{pmatrix}$,

* Els casos restants en què f és una forma definida es poden reduir a aquest; però si f és una forma indefinida, cal aplicar un mètode completament diferent, i la quantitat de transformacions serà infinita.

i s'expressen formalment totes les substitucions per les quals f es transforma en si mateixa per

$$\begin{array}{ccc} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'', \end{array}$$

de manera que s'han de satisfer les equacions (Ω) $\cdots$ $a\alpha\alpha+a'\alpha'\alpha'+a''\alpha''\alpha''=a$, $a\beta\beta+a'\beta'\beta'+a''\beta''\beta''=a'$, $a\gamma\gamma+a'\gamma'\gamma'+a''\gamma''\gamma''=a''$, $a\alpha\beta+a'\alpha'\beta'+a''\alpha''\beta''=0$, $a\alpha\gamma+a'\alpha'\gamma'+a''\alpha''\gamma''=0$, $a\beta\gamma+a'\beta'\gamma'+a''\beta''\gamma''=0$. Ara s'han de distingir tres casos.

I. Quan a, a', a'' (que tindran el mateix signe), són tots diferents, suposem que $a<a'$, $a'<a''$ (si es presenta un altre ordre per a les quantitats, es descobriran les mateixes conclusions de manera completament similar). Llavors, la primera equació de Ω requereix, evidentment, que sigui $\alpha'=\alpha''=0$, de manera que $\alpha=\pm1$; d'aquí, per les equacions 4, 5, serà $\beta=0$, $\gamma=0$; similarment, de l'equació 2, serà $\beta''=0$ i, en conseqüència, $\beta'=\pm1$, d'aquí resulta, per l'equació 6, $\gamma'=0$ i, per 3, $\gamma''=\pm1$, de manera que (per l'ambigüitat independent dels signes) es tenen en total 8 transformacions diferents.

II. Quan dos dels nombres a, a', a'', són iguals, *per exemple*, $a'=a''$, i el tercer diferent, suposem, *primer*, $a<a'$. Llavors, de la mateixa manera que en el cas precedent, serà $\alpha'=0$, $\alpha''=0$, $\alpha=\pm1$, $\beta=0$, $\gamma=0$; però, de les equacions 2, 3, 6, es dedueix fàcilment que ha de ser o bé $\beta'=\pm1$, $\gamma'=0$, $\beta''=0$, $\gamma''=\pm1$, o bé $\beta'=0$, $\gamma'=\pm1$, $\beta''=\pm1$, $\gamma''=0$. Però si, *segon*, $a>a'$, s'obtenen les mateixes conclusions així: de les

equacions 2, 3, serà, necessàriament, $\beta = 0$, $\gamma = 0$ i, o bé $\beta' = \pm 1$, $\gamma' = 0$, $\beta'' = 0$, $\gamma'' = \pm 1$, o bé $\beta' = 0$, $\gamma' = \pm 1$, $\beta'' = \pm 1$, $\gamma'' = 0$; per a cadascun dels supòsits, de les equacions 4, 5, serà $\alpha' = 0$, $\alpha'' = 0$, i, de 1, $\alpha = \pm 1$. Així, es tenen 16 transformacions diferents per a cada cas. Els dos casos restants, en què o bé $a = a''$ o bé $a = a'$, s'acaben de manera completament similar si els caràcters α, α', α'', es commuten, en el primer cas, amb β, β', β'', en el darrer, amb γ, γ', γ'', respectivament.

III. Quan tots els a, a', a'', són iguals, les equacions 1, 2, 3 requereixen que dels tres nombres α, α', α'', i també dels β, β', β'', i també dels γ, γ', γ'', dos siguin $= 0$, el tercer, $= \pm 1$. De les equacions 4, 5, 6, però, s'entén fàcilment que dels tres nombres α, β, γ, només un pot ser $= \pm 1$, i similarment per a α', β', γ', i també α'', β'', γ''. Per la qual cosa, només es donen sis combinacions:

$$\begin{array}{c|c|c|c|c|c|l} \alpha & \alpha & \alpha' & \alpha' & \alpha'' & \alpha'' & = \pm 1 \\ \beta' & \beta'' & \beta & \beta'' & \beta & \beta' & = \pm 1 \\ \gamma'' & \gamma' & \gamma'' & \gamma & \gamma' & \gamma & = \pm 1; \end{array}$$

els sis coeficients restants, $= 0$, de manera que, per l'ambigüitat dels signes, es tenen en total 48 transformacions. La mateixa figura també comprèn els casos precedents, però de les sis columnes primeres només s'ha d'agafar la primera quan a, a', a'', són tots diferents; la primera columna i la segona, quan $a' = a''$; la primera i la tercera, quan $a = a'$; la primera i la sisena, quan $a = a''$.

D'aquí es conclou que si la forma $f = axx + a'x'x' + a''x''x''$ es transforma en una altra equivalent f' per la substitució $x = \delta y + \varepsilon y' + \zeta y''$, $x' = \delta' y + \varepsilon' y' + \zeta' y''$,

$x'' = \delta''y + \varepsilon''y' + \zeta''y''$, totes les transformacions de la forma f en f' es contenen en l'esquema següent:

$$\begin{array}{cccccc|l} x & x & x' & x' & x'' & x'' & = \pm(\delta y + \epsilon y' + \zeta y'') \\ x' & x'' & x & x'' & x & x' & = \pm(\delta' y + \epsilon' y' + \zeta' y'') \\ x'' & x' & x'' & x & x' & x & = \pm(\delta'' y + \epsilon'' y' + \zeta'' y''), \end{array}$$

amb la discriminació que s'han d'aplicar totes sis primeres columnes quan $a = a' = a''$; les columnes 1 i 2 quan a', a'', iguals, a diferent; 1 i 3 quan $a = a'$; 1 i 6 quan $a = a''$; i, finalment, només la primera columna quan a, a', a'', tots diferents. En el primer cas, la quantitat de transformacions serà 48; en els segon, tercer i quart, 16; i, en el cinquè, 8.

* * *

Després d'aquesta breu exposició dels primers elements de la teoria de les formes ternàries, passem a algunes aplicacions especials, entre les quals mereix el primer lloc el següent

286. Problema. *Proposada una forma binària $F = (A, B, C)$ de determinant D que pertany al gènere principal, trobar una forma binària f per duplicació de la qual s'origina aquella.*

Solució. I. Se cerca una representació pròpia de la forma $F' = ATT - 2BTU + CUU$ oposada a F per la forma ternària $xx - 2yz$; sigui aquesta $x = \alpha T + \beta U$, $y = \alpha' T + \beta' U$, $z = \alpha'' T + \beta'' U$, cosa que es conclou fàcilment que es pot fer de la teoria precedent de les

formes ternàries. En efecte, com que, per hipòtesi, F és del gènere principal, es donarà un valor de l'expressió $\sqrt{(A, B, C)}$ (mòd. D), d'on es podrà trobar una forma ternària ϕ de determinant 1, en la qual $(A,\ -B,\ C)$ intervé com una part, i que es copsarà sense cap dificultat que tots els coeficients d'aquesta forma seran enters. S'entén de manera igualment fàcil que ϕ serà una forma indefinida (ja que, per hipòtesi, F no és, certament, una forma negativa); d'on, necessàriament, serà equivalent a la forma $xx - 2yz$. Així, es podrà assignar una transformació d'aquesta en aquella que proporcionarà una representació pròpia de la forma F' per $xx - 2yz$. Llavors, doncs, serà $A = \alpha\alpha - 2\alpha'\alpha''$, $-B = \alpha\beta - \alpha'\beta'' - \alpha''\beta'$, $C = \beta\beta - 2\beta'\beta''$; a més a més, designats els nombres $\alpha\beta' - \alpha'\beta$, $\alpha'\beta'' - \alpha''\beta'$, $\alpha''\beta - \alpha\beta''$, per a, b, c, respectivament, aquests no tindran cap divisor comú i serà $D = bb - 2ac$.

II. D'aquí es conclou fàcilment, amb l'ajut de l'última observació de l'article 235, que F es transforma en el producte de la forma $(2a,\ -b,\ c)$ per si mateixa per la substitució $2\beta'$, β, β, β''; $2\alpha'$, α, α, α'', i també en el producte de la forma $(a,\ -b,\ 2c)$ per si mateixa per la substitució β', β, β, $2\beta''$; α', α, α, $2\alpha''$. Ara, el màxim comú divisor dels nombres $2a$, $2b$, $2c$, és 2; així, si c és imparell, $2a$, $2b$, c, no tindran cap divisor comú, o sigui, $(2a,\ -b,\ c)$ serà una forma pròpiament primitiva; similarment, si a és imparell, $(a,\ -b,\ 2c)$ serà una forma pròpiament primitiva; en el primer cas, F s'origina de la duplicació de la forma $(2a,\ -b,\ c)$; en el darrer, de la duplicació de la forma $(a,\ -b,\ 2c)$ (vegeu la conclusió 4 de l'article 235); certament, però, sempre tindrà lloc un d'aquests casos. En efecte, si ambdós a, c, fossin

parells, b seria necessàriament imparell; ara, es confirma fàcilment que és $\beta''a+\beta b+\beta' c=0$, $\alpha''a+\alpha b+\alpha' c=0$, d'on se seguiria que βb, αb, de manera que també α, β, són parells. D'aquí, però, A i C serien parells, cosa que seria contrària a la hipòtesi segons la qual F és una forma del gènere principal, de manera que d'un ordre pròpiament primitiu. D'altra banda, també pot resultar que tant a com c siguin imparells, i així, en aquest cas, es tindran immediatament dues formes de la duplicació de les quals s'origina F.

Exemple. Sigui proposada la forma $F=(5,\,2,\,31)$, de determinant -151. El valor de l'expressió $\sqrt{(5,2,31)}$, aquí es troba $(55,\,22)$; d'aquí, la forma ternària

$$\phi=\begin{pmatrix} 5, & 31, & 4 \\ 11, & 0, & -2 \end{pmatrix};$$

pels preceptes de l'article 272, es troba equivalent a aquesta la forma $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$, que es transforma en ϕ per la substitució

$$\begin{matrix} 2, & 2, & 1 \\ 1, & -6, & -2 \\ 0, & 3, & 1. \end{matrix}$$

D'aquí, amb l'ajut de les transformacions transmeses en l'article 277, es troba que $\begin{pmatrix} 1, & 0, & 0 \\ -1, & 0, & 0 \end{pmatrix}$ es transforma en ϕ per la substitució

$$\begin{matrix} 3, & -7, & -2 \\ 2, & -1, & 0 \\ 1, & -9, & -3. \end{matrix}$$

Així, resulta $a = 11$, $b = -17$, $c = 20$; per tant, com que a és imparell, F s'origina de la duplicació de la forma (11, 17, 40) i es transforma en el producte d'aquesta forma per si mateixa per la substitució -1, -7, -7, -18; 2, 3, 3, 2.

287. Pel que fa al problema resolt a l'article precedent, encara hi afegim les observacions següents.

I. Si la forma F es transforma en el producte de les dues formes (h, i, k), (h', i', k') (com sempre, suposem les dues agafades pròpiament) per la substitució $p, p', p'', p'''; q, q', q'', q'''$, es tindran les equacions que cal deduir fàcilment de la conclusió 3 de l'article 235: $p''hn' - p'h'n - p(in' - i'n) = 0$, $(p'' - p')(in' + i'n) - p(kn' - k'n) + p'''(hn' - h'n) = 0$, $p'kn' - p''k'n - p'''(in' - i'n) = 0$, i unes altres tres que s'originen d'aquestes per la commutació dels nombres p, p', p'', p''', amb q, q', q'', q'''; n, n', són les arrels quadrades positives dels quocients que es produeixen si es divideixen els determinants de les formes (h, i, k), (h', i', k') pel determinant de la forma F. Així, si aquestes formes són idèntiques, o sigui, $n = n'$, $h = h'$, $i = i'$, $k = k'$, aquelles equacions es transformen en les $(p'' - p')hn = 0$, $(p'' - p')in = 0$, $(p'' - p')kn = 0$, d'on serà, *necessàriament*, $p' = p''$, i, de manera completament similar, $q' = q''$. Així, atribuint a les formes (h, i, k), (h', i', k'), *les mateixes* indeterminades t, u, i designant les indeterminades de la forma F per T, U, per la substitució $T = ptt + 2p'tu + p'''uu$, $U = qtt + 2q'tu + q'''uu$, F es transformarà en $(htt + 2itu + kuu)^2$.

II. Si la forma F s'origina de la duplicació de la forma f, també s'originarà de la duplicació de qualsevol altra forma continguda en la mateixa classe que f, o sigui, la classe de la forma F, de la duplicació de la classe de la forma f (vegeu l'article 238). Així, en l'exemple de l'article precedent, (5, 2, 31) també s'originarà de la duplicació de la forma (11, −5, 16), pròpiament equivalent a (11, 17, 40). D'una classe per la duplicació de la qual s'origina la classe de la forma F, es troben *totes* (si se'n donen més) amb l'ajut del problema 260; en el nostre exemple, no es donarà cap altra classe positiva d'aquest tipus, ja que només existeix una classe ambigua pròpiament primitiva positiva de determinant −151 (posem, la principal); com que, de la composició de l'única classe ambigua negativa (−1, 0, −151) amb la classe (11, −5, 16), s'origina la classe (−11, −5, −16), aquesta serà l'única negativa per duplicació de la qual s'origina la classe (5, 2, 31).

III. Com que, per la mateixa resolució del problema de l'article precedent, s'ha obtingut que qualsevol classe pròpiament primitiva (positiva) de formes binàries que pertany al gènere principal es pot originar per duplicació d'alguna classe pròpiament primitiva del mateix determinant, el teorema de l'article 261, pel qual estàvem segurs que *com a mínim* la meitat de tots els caràcters assignables per a un determinant no quadrat donat D no poden correspondre a gèneres pròpiament primitius (positius), ara s'amplia de manera que *precisament* la meitat de tots aquests caràcters corresponen realment a un tal gènere i l'altra meitat no poden correspondre a cap (vegeu la demostració d'aquell teorema). Per tant, com que en l'article 264 tots aquells caràcters

assignables s'han distribuït equitativament en dues espècies P, Q, dels quals s'havia provat que els posteriors, Q, no poden correspondre a formes pròpiament primitives (positives), però dels restants, P, es mantenia la incertesa de si a cadascun sempre corresponien realment gèneres, ara s'ha suprimit completament aquest dubte i tenim la certesa que en tot el complex de caràcters P no n'hi ha cap al qual no correspongui cap gènere. D'aquí també es dedueix fàcilment que, per a un determinant negatiu, en un ordre pròpiament primitiu *negatiu*, en el qual s'ha mostrat a l'article 264, I, que tots els P són impossibles i *només* els Q possibles, realment *tots* els Q són possibles. En efecte, si K designa un caràcter qualsevol de Q, f una forma arbitrària de l'ordre pròpiament primitiu negatiu de formes de determinant D, i K' el seu caràcter, aquest serà de Q; d'on es copsa fàcilment que el caràcter compost de K, K' (per la norma de l'article 246), pertany a P, de manera que existeixen formes pròpiament primitives positives de determinant D que li corresponen; de la composició d'una tal forma amb f s'originarà, evidentment, una forma pròpiament primitiva negativa de determinant D, el caràcter de la qual serà K. Es prova, per una raó completament similar, que en un ordre impròpiament primitiu, aquests caràcters, que pels preceptes de l'article 264, II, III, es van trobar els *únics* possibles, *tots* són possibles, tant si són P com Q. Aquests teoremes, si no errem terriblement, s'han de considerar entre els més bonics de la teoria de les formes binàries, això més, perquè malgrat que gaudeixen d'una gran simplicitat, no obstant això són tan inaccessibles que no podria construir-se'n una demostració rigorosa sense l'ajut de moltes altres disquisicions.

Passem ara a una altra aplicació de la digressió precedent, a la descomposició tant de nombres com de formes binàries en tres quadrats, per a la qual enunciem el següent

288. Problema. *Si M designa un nombre positiu, trobar condicions sota les quals es puguin donar formes binàries primitives negatives de determinant $-M$ que siguin residus quadràtics de M, o sigui, per a les quals* 1 *sigui un nombre característic.*

Solució. Designem per Ω el complex de tots els caràcters particulars que donen les relacions del nombre 1 tant per a cadascun dels divisors primers (imparells) de M com per al nombre 8 o bé 4 quan divideixen M; evidentment, aquests caràcters seran Rp, Rp', Rp'', etc., on p, p', p'', etc., designen aquells divisors primers; i 1, 4, quan 4 [divideix M]; 1, 8, quan 8 divideix M. A part d'això, usarem les lletres P, Q, amb el mateix significat que en un article precedent, o sigui, com en 264. Distingim, ara, els casos següents.

I. Quan M és divisible per 4, Ω serà un caràcter íntegre, i és clar de l'article 233, V, que 1 només pot ser nombre característic de formes tals que el seu caràcter sigui Ω. Però és evident que Ω serà un caràcter de la forma principal $(1, 0, M)$, de manera que pertany a P i, en conseqüència, no pot coincidir amb una forma pròpiament primitiva negativa; per tant, com que no es donen formes impròpiament primitives per a tal determinant, en aquest cas no es dóna cap forma primitiva negativa en absolut que sigui residu de M.

II. Quan $M \equiv 3\,(\text{mòd. } 4)$, valen completament els mateixos raonaments amb la sola excepció que existirà, en aquest cas, un ordre *impròpiament* primitiu negatiu en el qual els caràcters P seran o bé possibles o bé impossibles segons que $M \equiv 3$ o bé $\equiv 7\,(\text{mòd. } 8)$, vegeu l'article 264, III. Així, doncs, en el primer cas, en aquest ordre es donarà un gènere el caràcter del qual sigui Ω, d'on 1 serà un nombre característic de totes les formes contingudes en ell; en el darrer cas, no es podrà donar cap forma negativa en absolut amb la propietat predita.

III. Quan $M \equiv 1\,(\text{mòd. } 4)$, Ω no és encara un caràcter íntegre, sinó que, a sobre, se li ha d'afegir la relació amb el nombre 4; però és clar que Ω ha d'intervenir necessàriament en el caràcter d'una forma el nombre característic de la qual sigui 1; i recíprocament, que qualsevol forma el caràcter de la qual sigui o bé Ω; 1, 4, o bé Ω; 3, 4, té nombre característic 1. Ara, Ω; 1, 4, és, evidentment, el caràcter del gènere principal que pertany a P, de manera que és impossible en un ordre pròpiament primitiu negatiu; per la mateixa raó, Ω; 3, 4, pertanyerà a Q (article 263), d'on li correspondrà un gènere en l'ordre pròpiament primitiu negatiu, totes les formes del qual tindran nombre característic 1. En aquest cas, com en el següent, no es dóna cap ordre impròpiament primitiu.

IV. Quan $M \equiv 2\,(\text{mòd. } 4)$, s'ha d'afegir a Ω la relació amb 8 perquè resulti un caràcter íntegre, posem, o bé 1 *i* 3, 8, o bé 5 *i* 7, 8, quan $M \equiv 2\,(\text{mòd. } 8)$; i o bé 1 *i* 7, 8, o bé 3 *i* 5, 8, quan $M \equiv 6\,(\text{mòd. } 8)$. Per al primer cas, el caràcter Ω; 1 *i* 3, 8, pertany evidentment a P, de manera que Ω; 5 *i* 7, 8, a Q, d'on li correspondrà un gènere pròpiament primitiu negatiu; i per una raó

similar, per al darrer, es donarà un gènere en un ordre pròpiament primitiu negatiu les formes del qual estiguin proveïdes de la propietat prescrita, posem que el seu caràcter és Ω; 3 *i* 5, 8.

D'aquí es conclou que es donen formes primitives negatives de determinant $-M$ el nombre característic de les quals és 1, quan M és congru a un dels nombres 1, 2, 3, 5, 6, segons el mòdul 8 i, certament, sempre en un únic gènere, que serà impropi quan $M \equiv 3$; no es donen en absolut tals formes quan $M \equiv 0$, 4, o bé 7 (mòd. 8). D'altra banda, és evident que si $(-a, -b, -c)$ és una forma primitiva negativa, el nombre característic de la qual és $+1$, (a, b, c) és una forma primitiva positiva el nombre característic de la qual és -1; d'aquí, és evident que en els cinc casos primers (quan $M \equiv 1, 2, 3, 5, 6$) es dóna un gènere primitiu positiu les formes del qual tenen nombre característic -1, i, certament, *impropi* per a $M \equiv 3$; però en els tres restants (quan $M \equiv 0, 4, 7$) tals formes positives no es poden donar en absolut.

289. Sobre les representacions pròpies de les formes binàries per la ternària $xx + yy + zz = f$, de la teoria general transmesa en l'article 282, es conclouen aquestes [proposicions]:

I. La forma binària ϕ no es pot representar pròpiament per f, llevat que sigui una forma primitiva positiva i -1 (és a dir, el determinant de la forma f) el seu nombre característic. Per tant, no es donen formes binàries representables pròpiament per f per a un determinant positiu, i tampoc per a un negatiu $-M$ quan M, o bé és divisible per 4, o bé de la forma $8n + 7$.

II. Però si $\phi = (p,\ q,\ r)$ és una forma primitiva positiva de determinant $-M$ i -1 un nombre característic de la forma ϕ, de manera que també de la seva oposada $(p,\ -q,\ r)$, es donaran representacions pròpies de la forma ϕ per f que pertanyen a qualsevol valor donat de l'expressió $\sqrt{-(p,-q,r)}$. Això és, tots els coeficients de la forma ternària g de determinant -1 (article 283) resultaran necessàriament enters, però g una forma definida, de manera que, certament, equivalent a f (article 285, I).

III. La quantitat de totes les representacions que pertanyen al mateix valor de l'expressió $\sqrt{-(p,-q,r)}$ en tots els casos, excepte $M = 1$ i $M = 2$, per l'article 283, III, és igual de gran com la quantitat de transformacions de la forma f en g, de manera que, per l'article 285, $= 48$; d'aquí i d'això, és clar que si es té una representació que pertany a un valor donat, les 47 restants es deriven d'això tant permutant entre si els valors de x, y, z, de totes les maneres que es pot fer, com afectant-los de signes oposats; per tant, totes 48 representacions produeixen una *única* descomposició de la forma ϕ en tres quadrats si només es tenen en compte els quadrats però no el seu ordre ni els signes de les arrels.

IV. Posada $= \mu$ la quantitat de tots els nombres primers imparells diferents que divideixen M, es conclou no difícilment de l'article 233 que la quantitat dels valors diferents de l'expressió $\sqrt{-(p,-q,r)}\,(\text{mòd.}\,M)$ serà $= 2^{\mu}$, dels quals, per l'article 283, convé considerar-ne només la meitat (quan $M > 2$). Per tant, la quantitat de totes les representacions pròpies de la forma ϕ per f serà $= 48 \cdot 2^{\mu-1} = 3 \cdot 2^{\mu+3}$; però la quantitat de les diferents descomposicions en tres quadrats $= 2^{\mu-1}$.

Exemple. Sigui $\phi = 19tt + 6tu + 41uu$, de manera que $M = 770$; aquí convé considerar (article 283) els quatre valors següents de l'expressió $\sqrt{-(19,-3,41)}$ (mòd. 770): (39, 237), (171, −27), (269, −83), (291, −127). Per a trobar les representacions que pertanyen al valor (39, 237), primer es descobreix la forma ternària $\begin{pmatrix} 19, & 41, & 2 \\ 3, & 6, & 3 \end{pmatrix} = g$, en la qual, pels preceptes dels articles 272, 275, es troba que f es transforma per la substitució

$$\begin{matrix} 1, & -6, & -0 \\ -3, & -2, & -1 \\ -3, & -1, & -1, \end{matrix}$$

d'on es té la representació de la forma ϕ per f, $x = t-6u$, $y = -3t - 2u$, $z = -3t - u$; no escrivim, per abreujar, les 47 representacions restants que pertanyen al mateix valor, que s'originen per permutació d'aquests valors i per canvi de signes. Però totes 48 representacions produeixen la mateixa descomposició de la forma ϕ en tres quadrats, $tt-12tu+36uu$, $9tt+12tu+4uu$, $9tt+6tu+uu$.

De manera completament similar, el valor (171, −27) procura la descomposició en els quadrats $(3t+5u)^2$, $(3t-4u)^2$, tt; el valor (269, −83) la $(t+6u)^2+(3t+u)^2+(3t-2u)^2$, i, finalment, el valor (291, −127), la $(t+3u)^2+(3t+4u)^2+(3t-4u)^2$; cadascuna d'aquestes descomposicions és equivalent a 48 representacions. Però excepte aquestes 192 representacions, o sigui, quatre descomposicions, no se'n donen altres, ja que 770 no és divisible per cap quadrat, de manera que no poden existir representacions impròpies.

290. Tractarem breument de manera separada de les formes de determinant −1 i −2, les quals eren

sotmeses a algunes excepcions. Enunciem l'observació general que si ϕ, ϕ', són formes binàries equivalents qualssevol, (Θ) una transformació donada d'aquella en aquesta, de la combinació de qualsevol representació de la forma ϕ per alguna ternària f amb la substitució (Θ) es produeix una representació de la forma ϕ' per f; a més a més, de representacions pròpies de ϕ s'originen, d'aquesta manera, representacions pròpies de ϕ', de diferents, diferents; i, finalment, de totes, totes. Tot això es comprova facilíssimament per càlcul. Per tant, una de les formes ϕ, ϕ', es podrà representar per f de tantes maneres com l'altra.

I. Primer, sigui $\phi = tt + uu$ i ϕ' una altra forma binària positiva qualsevol de determinant -1, a la qual, així, ϕ equivaldrà; es transforma ϕ en ϕ' per la substitució $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$. La forma ϕ es representa per la ternària $f = xx + yy + zz$ posant $x = t$, $y = u$, $z = 0$; permutant x, y, z, d'aquí surten *sis* representacions, i novament, canviant els signes de t, u, quatre de cada una, de manera que es tenen en total 24 representacions diferents a les quals equival una única descomposició en tres quadrats i es copsa fàcilment que no se'n poden donar altres excepte aquestes. D'aquí es conclou que també la forma ϕ' es pot descompondre només d'una única manera en tres quadrats, posem en $(\alpha t' + \beta u')^2$, $(\gamma t' + \delta u')^2$ i 0; aquesta descomposició equival a 24 representacions.

II. Sigui $\phi = tt + 2uu$, ϕ' qualsevol altra forma binària positiva de determinant -2 en la qual ϕ es transforma per la substitució $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$. Llavors, de manera similar com en el cas precedent, es conclou que ϕ i, en conseqüència, també ϕ', només es

pot descompondre d'una única manera en tres quadrats, posem ϕ en $tt + uu + uu$ i ϕ' en $(\alpha t' + \beta u')^2 + (\gamma t' + \delta u')^2 + (\gamma t' + \delta u')^2$; es pot copsar fàcilment que una tal descomposició equival a 24 representacions.

D'aquí es conclou que les formes binàries de determinants -1 i -2, respecte de la quantitat de representacions per la ternària $xx + yy + zz$, concorden completament amb les altres formes binàries; en efecte, com que en ambdós casos resulta $\mu = 0$, la fórmula transmesa en l'article precedent, IV, produeix certament 24 representacions. La raó d'aquest fet és que les dues excepcions, a les quals estaven sotmeses tals formes, es compensen mútuament.

Sobreseiem, per abreujar, aplicar a la forma $xx + yy + zz$ la teoria general de representacions impròpies explicada a l'article 284.

291. La qüestió de trobar totes les representacions pròpies d'un *nombre* positiu donat M per la forma $xx + yy + zz$ es redueix, primer, per l'article 281, a la investigació de les representacions pròpies del nombre $-M$ per la forma $-xx - yy - zz = f$; aquestes, però, pels preceptes de l'article 280, es descobreixen així.

I. Es desenvolupen totes les classes de formes binàries de determinant $-M$, les formes de les quals es poden representar pròpiament per $XX + YY + ZZ = F$ (la forma ternària adjunta a la qual és f). Quan $M \equiv 0$, 4, o bé 7 (mòd. 8), per l'article 288, no es donen tals classes, de manera que M no es pot descompondre en tres quadrats que no tinguin divisor comú.* Però quan

* Aquesta impossibilitat també és evident del fet que la

$M \equiv 1, 2, 5$, o bé 6, es donarà un gènere pròpiament primitiu positiu, i quan $M \equiv 3$, impròpiament primitiu, que comprèn totes aquelles classes; designem per k la quantitat d'aquestes classes.

II. Ara, s'elegeixen a voluntat k formes d'aquestes classes, de cadascuna, una; siguin aquestes, ϕ, ϕ', ϕ'', etc.; s'investiguen totes les representacions pròpies de totes per F, la quantitat de les quals serà, així, $3 \cdot 2^{\mu+3}k = K$, on μ designa la quantitat de factors primers (imparells) de M; finalment, de qualsevol representació d'aquest tipus, tal com $X = mt + nu$, $Y = m't + n'u$, $Z = m''t + n''u$, es derivarà una representació de M per $xx + yy + zz$, la $x = m'n'' - m''n'$, $y = m''n - mn''$, $z = mn' - m'n$. En el complex d'aquestes K representacions, que designarem per Ω, hi estaran contingudes necessàriament totes les representacions de M.

III. Així, només resta que ens preguntem si, en Ω, poden ocórrer representacions *idèntiques*; i, com que ja se sap, per l'article 280, III, que les representacions de Ω que han estat derivades de formes diferents, *per exemple*, ϕ i ϕ', són necessàriament diferents, només resta la disquisició de si representacions diferents de la mateixa forma, *per exemple*, de ϕ, per F, podrien produir representacions idèntiques del nombre M per $xx + yy + zz$. Ara, és evident immediatament que, si entre les representacions de ϕ s'hi troba la $(r) \cdots X = mt + nu$, $Y = m't + n'u$, $Z = m''t + n''u$, entre aquestes hi

---

suma de tres quadrats imparells resulta, necessàriament, $\equiv 3$ (mòd. 8); la suma de dos imparells amb un parell, o bé $\equiv 2$ o bé $\equiv 6$; la suma d'un imparell amb dos parells, o bé $\equiv 1$ o bé $\equiv 5$; finalment, la suma de tres parells, o bé $\equiv 0$ o bé $\equiv 4$; però, en el darrer cas, la representació és, evidentment, impròpia.

haurà la $(r')\ \cdots\ X = -mt - nu$, $Y = -m't - n'u$, $Z = -m''t - n''u$, i d'ambdues es deriva la mateixa representació de M, que es designarà per (R); així, examinem si (R) es pot seguir encara d'altres representacions de la forma ϕ. De l'article 280, III, es dedueix fàcilment, establint allà $\chi = \phi$, que si totes les transformacions pròpies de la forma ϕ en si mateixa s'expressen per $t = \alpha t + \beta u$, $u = \gamma t + \delta u$, totes les representacions de la forma ϕ de les quals se segueix R s'expressaran per $x = (\alpha m+\gamma n)t+(\beta m+\delta n)u$, $y = (\alpha m'+\gamma n')t+(\beta m'+\delta n')u$, $z = (\alpha m'' + \gamma n'')t + (\beta m'' + \delta n'')u$. Però, de la teoria de les transformacions de les formes binàries de determinant negatiu explicada a l'article 179, se segueix que en tots els casos, excepte $M = 1$ i $M = 3$, només es donen dues transformacions pròpies de la forma ϕ en si mateixa, posem α, β, γ, $\delta = 1, 0, 0, 1$, i $= -1, 0, 0, -1$, respectivament (en efecte, com que ϕ és una forma primitiva, el que a l'article 179 es designava per m serà o bé 1 o bé 2 i, en conseqüència, tret dels casos exceptuats, aquí tindrà lloc (1), certament). Per tant, (R) podrà provenir només de r, r', de manera que qualsevol representació pròpia del nombre M es trobarà dues vegades i no més en Ω, i la quantitat de totes les representacions pròpies diferents de M serà $\frac{1}{2}K = 3 \cdot 2^{\mu+2}k$.

Pel que fa als casos exceptuats, la quantitat de transformacions pròpies de la forma ϕ en si mateixa, per l'article 179, serà 4 per a $M = 1$, i 6 per a $M = 3$; i, realment, es confirma fàcilment que la quantitat de representacions pròpies dels nombres 1, 3 és $\frac{1}{4}K$ i $\frac{1}{6}K$, respectivament; això és, cadascun dels nombres es pot descompondre en tres quadrats només d'una única manera: 1 en $1 + 0 + 0$, 3 en $1 + 1 + 1$; la descomposició de

1 proporciona sis representacions diferents, la descomposició de 3, vuit; K però, resulta $= 24$ per a $M = 1$ (on $\mu = 0$, $k = 1$), i $= 48$ per a $M = 3$ (on $\mu = 1$, $k = 1$).

D'altra banda, observem que si h designés la quantitat de classes en el gènere principal, a la qual, per l'article 252, és igual la quantitat de classes en qualsevol gènere pròpiament primitiu, serà $k = h$ per a $M \equiv 1$, 2, 5, o bé $6\,(\text{mòd.}\,8)$, però $k = \frac{1}{3}h$ per a $M \equiv 3\,(\text{mòd.}\,8)$, exceptuat l'únic cas $M = 3$, en què $k = h = 1$. Així, per als nombres de la forma $8n + 3$, la quantitat de representacions és, *en general*, $= 2^{\mu+2}h$, ja que en el nombre 3 les dues excepcions es compensen.

292. Distingim les descomposicions dels nombres (com de les formes binàries més amunt) en tres quadrats de les representacions per la forma $xx+yy+zz$ de manera que en aquelles només tenim en compte la magnitud dels quadrats, però en aquestes, a sobre, el seu ordre i el signe de les arrels, de manera que tindrem com a diferents les representacions $x = a$, $y = b$, $z = c$, i $x = a'$, $y = b'$, $z = c'$, llevat que, simultàniament, $a = a'$, $b = b'$, $c = c'$; però les descomposicions en $aa + bb + cc$ i $a'a' + b'b' + c'c'$ per una sola si aquests quadrats són iguals a aquells i no es té cap respecte a l'ordre. D'aquí és clar que

I. La descomposició del nombre M en quadrats $aa + bb + cc$ equival a 48 representacions si cap no és $= 0$ i tots són diferents; però a 24 si, *o bé* un és $= 0$ i els restants diferents, *o bé* cap $= 0$ i dos iguals entre si. Però, si en la descomposició d'un nombre donat en tres quadrats, dos d'ells són $= 0$, *o bé* un $= 0$ i els

restants iguals, *o bé* tots iguals, serà equivalent a 6, *o bé* 12, *o bé* 8 representacions; però aquestes només poden esdevenir en els casos particulars en què $M = 1$, o bé 2, o bé 3, respectivament, suposat que les representacions han de ser pròpies. Exclosos aquests, suposem que la quantitat de totes les descomposicions del nombre M en tres quadrats (privats de divisor comú) és E, i entre elles se'n troben e en què un quadrat és 0 i e' en què dos quadrats són iguals; aquelles també es poden mirar com a descomposicions en dos quadrats, i aquestes com a descomposicions en un quadrat i el doble d'un quadrat. Llavors, la quantitat de totes les representacions pròpies del nombre M per $xx + yy + zz$ serà $= 24(e + e') + 48(E - e - e') = 48E - 24(e + e')$. Però de la teoria de les formes binàries es dedueix fàcilment que e serà o bé $= 0$ o bé $= 2^{\mu-1}$, segons que -1 sigui no-residu o bé residu quadràtic de M, i també $e' = 0$ o bé $= 2^{\mu-1}$, segons que -2 sigui no-residu o bé residu de M, on μ denota la quantitat de factors primers (imparells) de M (vegeu l'article 182; suprimim aquí una exposició més extensa). D'aquí es conclou fàcilment que serà $E = 2^{\mu-2}k$, si tant -1 com -2 són no-residus de M, $E = 2^{\mu-2}(k + 2)$, si cada un dels dos nombres és residu; i, finalment, $E = 2^{\mu-2}(k+1)$, si l'un és residu, l'altre, no-residu. En els casos exclosos, $M = 1$ i $M = 2$, aquesta fórmula proporcionaria $E = \frac{3}{4}$, mentre que ha de ser $E = 1$; per a $M = 3$, però, apareix rectament $E = 1$, perquè les excepcions es compensen mútuament.

Així, si M és un nombre primer, resulta $\mu = 1$, de manera que $E = \frac{1}{2}(k + 2)$ quan $M \equiv 1 \,(\text{mòd. } 8)$, $E = \frac{1}{2}(k + 1)$ quan $M \equiv 3$ o bé $\equiv 5$. Aquests teoremes

especials foren deduïts per l'il·lm. Le Gendre per inducció i presentats en l'egregi comentari ja citat sovint, *Hist. de l'Ac. de Paris* 1785 *p.* 530 *s.*, però d'una manera bastant diferent, la raó de la qual cosa recau principalment en què no va distingir l'equivalència pròpia de la impròpia i, en conseqüència, va barrejar les classes oposades.

II. Per a la trobada de totes les descomposicions d'un nombre M en tres quadrats (sense divisor comú) no és necessari descobrir totes les representacions pròpies de totes les formes ϕ, ϕ', ϕ''. En efecte, primer, es confirma fàcilment que totes (48) representacions de la forma ϕ que pertanyen al mateix valor de l'expressió $\sqrt{-(p,-q,r)}$ (establint $\phi = (p,\ q,\ r)$) proporcionen la mateixa descomposició del nombre M, de manera que és suficient si se'n té una, o sigui, el que rendeix el mateix, si només s'han escrit totes les descomposicions diferents* de la forma ϕ en tres quadrats, i igualment per a les restants ϕ', ϕ'', etc. Tot seguit, si ϕ és d'una classe no ambigua, es podrà ometre completament la forma que s'ha elegit de la classe oposada, o sigui, de dues classes oposades és suficient considerar-ne una. En efecte, com que és completament arbitrari quina forma s'elegeix de cada classe, suposem que de la classe oposada a aquella en què hi ha ϕ s'elegeix la forma oposada a ϕ; sigui aquesta $= \phi'$. Llavors, es copsa sense cap dificultat que si les descomposicions pròpies de la forma ϕ es representen formalment per $(gt+hu)^2+(g't+h'u)^2+(g''t+h''u)^2$, totes les descomposicions de la forma ϕ' s'expressaran per $(gt-hu)^2+(g't-h'u)^2+(g''t-h''u)^2$, i d'aquestes es deriven les mateixes descomposicions del nombre M

* Sempre cal sobreentendre *pròpies* si es vol transferir aquesta expressió de les representacions a les descomposicions.

que d'aquelles. Finalment, per al cas en què ϕ és una forma d'una classe ambigua, però ni de la classe principal ni equivalent a la forma $(2,\ 0,\ \frac{1}{2}M)$ o bé a la $(2,\ 1,\ \frac{1}{2}(M+1))$ (segons que M sigui parell o bé imparell), es pot suprimir la meitat dels valors de l'expressió $\sqrt{-(p,-q,r)}$; però, per abreujar, no expliquem aquí més extensament aquesta simplificació. D'altra banda, també podem utilitzar les mateixes simplificacions quan es desitgen totes les representacions pròpies de M per $xx+yy+zz$, ja que aquestes surten facilíssimament de les descomposicions.

Com a exemple, investigarem totes les descomposicions del nombre 770 en tres quadrats, on $\mu = 3$, $e = e' = 0$, de manera que $E = 2k$. Per la classificació de les formes binàries positives de determinant -770, la qual, per abreujar, no escrivim, ja que pot ser construïda fàcilment per qualsevol per la norma de d'article 231, es troba la quantitat de classes positives $= 32$, totes les quals són pròpiament primitives, i es distribueixen entre 8 gèneres, de manera que és $k = 4$ i, en conseqüència, $E = 8$. El gènere, un nombre característic del qual és -1, ha de tenir, evidentment, els caràcters particulars $R5$, $N7$, $N11$, respecte dels nombres 5, 7, 11; d'on, per l'article 263, es conclou fàcilment que el seu caràcter respecte del nombre 8 ha de ser 1 *i* 3, 8. Ara, en el gènere el caràcter del qual és 1 *i* 3, 8; $R5$; $N7$; $N11$, es troben quatre classes, per a les quals elegim com a representants les formes (6, 2, 129), (6, -2, 129), (19, 3, 41), (19, -3, 41); però rebutgem les classes segona i quarta, com a oposades de la primera i la tercera. Ja en l'article 289 vàrem transme-

tre les quatre descomposicions de la forma (19, 3, 41), de les quals se segueixen les descomposicions del nombre 770 en $9+361+400$, $16+25+729$, $81+400+289$, $576+169+25$. Per una raó similar, es troben les quatre descomposicions de la forma $6tt+4tu+129uu$ en $(t-8u)^2+(2t+u)^2+(t+8u)^2$, $(t-10u)^2+(2t+5u)^2+(t+2u)^2$, $(2t-5u)^2+(t+10u)^2+(t+2u)^2$, $(2t+7u)^2+(t-8u)^2+(t-4u)^2$, originades, respectivament, dels valors (48, 369), (62, −149), (92, −159), (202, 61) de l'expressió $\sqrt{-(6,-2,129)}$; d'on surten les descomposicions del nombre 770 en $225+256+289$, $1+144+625$, $64+81+625$, $16+225+529$. Excepte aquestes vuit descomposicions, no se'n donen altres.

Les [proposicions] que atenyen a les descomposicions de nombres en tres quadrats que tenen divisors comuns, se segueixen tan fàcilment de la teoria general de l'article 281 que no és necessari insistir en aquesta qüestió.

293. Les disquisicions precedents també proporcionen una demostració del famós teorema que *tot nombre enter positiu es pot descompondre en tres nombres triangulars*, que fa temps va ser descobert per Fermat, però una demostració rigorosa del qual fins ara es desitjava. És evident que qualsevol descomposició del nombre M en triangulars $\frac{1}{2}x(x+1)+\frac{1}{2}y(y+1)+\frac{1}{2}z(z+1)$ produeix una descomposició del nombre $8M+3$ en tres quadrats imparells $(2x+1)^2+(2y+1)^2+(2z+1)^2$, i recíprocament. Però, per la teoria precedent, qualsevol nombre enter positiu $8M+3$ és descomponible en tres quadrats, que seran, necessàriament, imparells (vegeu la nota de l'article 291); i la quantitat de descomposicions

depèn tant de la quantitat de factors primers de $8M+3$ com de la quantitat de classes en què es distribueixen les formes binàries de determinant $-(8M+3)$. Es donarà la mateixa quantitat de descomposicions del nombre M en ternes triangulars. Però hem suposat que, per a qualsevol valor enter de x, $\frac{1}{2}x(x+1)$ es considera com a triangular; si plagués més excloure el zero, convindria modificar el teorema així: Qualsevol enter positiu, o bé és ell mateix triangular, o bé és descomponible en dos o bé tres triangulars. S'hauria de fer una modificació similar en el teorema següent, si plagués excloure el zero dels quadrats.

Dels mateixos principis es demostra l'altre teorema de Fermat, *qualsevol nombre enter positiu es pot descompondre en quatre quadrats.* Restant, d'un nombre de la forma $4n+2$, un quadrat arbitrari (més petit que aquell nombre), d'un nombre de la forma $4n+1$, un quadrat parell, i d'un nombre de la forma $4n+3$, un quadrat imparell, en tots aquests casos el residu serà descomponible en tres quadrats, de manera que el nombre proposat, en quatre. Finalment, un nombre de la forma $4n$ es pot expressar per $4^{\mu}N$ de manera que N pertanyi a alguna de les tres formes precedents; però, descompost N en quatre quadrats, $4^{\mu}N$ també serà descompost. D'un nombre de la forma $8n+3$ també es pot extreure un quadrat d'arrel parellament parella, d'un nombre de la forma $8n+1$, un d'arrel imparellament parella, i d'un nombre de la forma $8n+4$ un quadrat imparell, i el residu serà descomponible en tres quadrats. D'altra banda, aquest teorema ja havia estat demostrat per l'il·lm. La Grange en *Nouv. Mem. de l'Ac. de Berlin* 1770 *p.* 123, demostració (completament diferent de la

nostra) que va explicar més extensament l'il·lm. Euler en *Actis Ac. Petr. Vol. II. p.* 48. Altres teoremes de Fermat que constitueixen quasi una continuació dels precedents, que qualsevol nombre enter és descomponible en cinc nombres pentagonals, sis hexagonals, set heptagonals, etc., fins ara estan mancats de demostració i semblen requerir alguns altres principis.

294. Teorema. *Si a, b, c, designen nombres primers entre si dels quals cap no és $= 0$ ni divisible per un quadrat, l'equació $axx + byy + czz = 0 \cdots \Omega$ no admetrà cap solució en enters excepte la $x = y = z = 0$, que no considerem, llevat que $-bc$, $-ac$, $-ab$, siguin residus quadràtics de a, b, c, respectivament, i que aquests nombres siguin afectats de signes diferents; però, si aquestes quatre condicions tenen lloc,* (Ω) *serà resoluble en enters.*

Dem. Si (Ω) és efectivament resoluble per enters, també es podrà resoldre per valors de x, y, z, tals que no tenen divisor comú; efectivament, qualssevol valors que satisfacin l'equació (Ω) encara la satisfaran si es divideixen pel màxim comú divisor. Ara, suposant que $app + bqq + crr = 0$, i p, q, r, lliures de divisor comú, també seran primers entre si; en efecte, si q, r, tinguessin un divisor comú μ, aquest seria primer amb p, però $\mu\mu$ dividiria app, de manera que també a, contra la hipòtesi; i, igualment, p, r; i p, q, seran primers entre si. Així, $-app$ es representa per la forma binària $byy + czz$ atribuint a y, z, valors q, r, primers entre si; d'on el seu determinant $-bc$ serà residu quadràtic de app, de manera que també de a (article 154); de la mateixa manera, serà $-acRb$, $-abRc$. Però que (Ω) no pot admetre cap

solució si a, b, c, tenen el mateix signe, és tan obvi que no exigeix explicació.

Acabarem la demostració de la proposició inversa, que constitueix la segona part del teorema, de manera que, *primer*, ensenyem a trobar una forma ternària equivalent a $\begin{pmatrix} a, & b, & c \\ 0, & 0, & 0 \end{pmatrix} \cdots f$, els coeficients 2, 3, 4, de la qual siguin divisibles per abc, d'on, *segon*, deduirem una solució de l'equació (Ω).

I. S'investiguen tres enters A, B, C, lliures de divisor comú i establerts de manera que A sigui primer amb b i c; B, amb a i c; C, amb a i b; però $aAA + bBB + cCC$, divisible per abc, cosa que s'efectuarà de la manera següent. Siguin $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, respectivament, valors de les expressions $\sqrt{-bc}\,(\text{mòd.}\,a)$, $\sqrt{-ac}\,(\text{mòd.}\,b)$, $\sqrt{-ab}\,(\text{mòd.}\,c)$, que, necessàriament, seran primers amb a, b, c, respectivament. S'agafen tres enters $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, completament a voluntat, de manera que siguin primers, respectivament, amb a, b, c (per exemple, tots $= 1$), i es determinen A, B, C, de manera que sigui $A \equiv \mathfrak{b}c\,(\text{mòd.}\,b)$ i $\equiv c\mathfrak{C}\,(\text{mòd.}\,c)$, $B \equiv \mathfrak{c}a\,(\text{mòd.}\,c)$ i $\equiv a\mathfrak{A}$ $(\text{mòd.}\,a)$, $C \equiv \mathfrak{a}b\,(\text{mòd.}\,a)$ i $\equiv b\mathfrak{B}\,(\text{mòd.}\,b)$. Llavors, resultarà $aAA+bBB+cCC \equiv \mathfrak{a}\mathfrak{a}(b\mathfrak{A}\mathfrak{A}+cbb) \equiv \mathfrak{a}\mathfrak{a}(b\mathfrak{A}\mathfrak{A}-\mathfrak{A}\mathfrak{A}b) \equiv 0\,(\text{mòd.}\,a)$, o sigui, divisible per a, i igualment per a b, c, de manera que també serà divisible per abc. A part d'això, és clar que A resulta, necessàriament, primer amb b i c; B, amb a i c; C, amb a i b. Però si aquests valors de A, B, C, impliquen un (màxim) divisor comú μ, aquest, evidentment, serà primer amb a, b, c, de manera que amb abc; per tant, dividint aquells valors per μ, n'obtindrem de nous que no tindran divisor comú que produiran un valor de $aAA+bBB+cCC$

encara divisible per abc, de manera que satisfaran totes les condicions.

II. Determinats els nombres A, B, C, d'aquesta manera, tampoc Aa, Bb, Cc, no tindran cap divisor comú. En efecte, si tinguessin un divisor comú μ, aquest seria necessàriament primer amb a (ja que aquest és primer tant amb Bb com amb Cc) i similarment per a b i c; per tant, μ també hauria de dividir A, B, C, contràriament a la hipòtesi. Així, es podran trobar enters α, β, γ, tals que sigui $\alpha Aa + \beta Bb + \gamma Cc = 1$; a sobre, se cerquen sis enters α', β', γ', α'', β'', γ'', tals que sigui $\beta'\gamma'' - \gamma'\beta'' = Aa$, $\gamma'\alpha'' - \alpha'\gamma'' = Bb$, $\alpha'\beta'' - \beta'\alpha'' = Cc$. Ara, es transforma f per la substitució

$$\begin{array}{ccc} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'', \end{array}$$

en $\left(\begin{array}{ccc} m, & m', & m'' \\ n, & n', & n'' \end{array} \right) = g$ (que serà equivalent a f), i afirmo que m', m'', n, seran divisibles per abc. En efecte, es posa $\beta''\gamma - \gamma''\beta = A'$, $\gamma''\alpha - \alpha''\gamma = B'$, $\alpha''\beta - \beta''\alpha = C'$, $\beta\gamma' - \gamma\beta' = A''$, $\gamma\alpha' - \alpha\gamma' = B''$, $\alpha\beta' - \beta\alpha' = C''$, i serà $\alpha' = B''Cc - C''Bb$, $\beta' = C''Aa - A''Cc$, $\gamma' = A''Bb - B''Aa$, $\alpha'' = C'Bb - B'Cc$, $\beta'' = A'Cc - C'Aa$, $\gamma'' = B'Aa - A'Bb$. Substituïts aquests valors en les equacions $m' = a\alpha'\alpha' + b\beta'\beta' + c\gamma'\gamma'$, $m'' = a\alpha''\alpha'' + b\beta''\beta'' + c\gamma''\gamma''$, $n = a\alpha'\alpha'' + b\beta'\beta'' + c\gamma'\gamma''$, resulta que, segons el mòdul a, $m' \equiv bcA''A''(BBb + CCc) \equiv 0$, $m'' \equiv bcA'A'(BBb + CCc) \equiv 0$, $n \equiv bcA'A''(BBb + CCc) \equiv 0$, és a dir, m', m'' i n seran divisibles per a; de manera similar els mateixos nombres es troben divisibles per b, c, de manera que també per abc. *Q. E. P.*

III. Posem $= d$, per raó de concisió, el determinant de les formes f, g; és a dir, el nombre $-abc$, $md = M$, $m' = M'd$, $m'' = M''d$, $n = Nd$, $n' = N'$, $n'' = N''$, i és clar que f es transforma, per la substitució (S)

$$\begin{array}{lll} \alpha d, & \alpha', & \alpha'' \\ \beta d, & \beta', & \beta'' \\ \gamma d, & \gamma', & \gamma'', \end{array}$$

en la forma ternària $\left(\begin{array}{lll} Md, & M'd, & M''d \\ Nd, & N'd, & N''d \end{array} \right) = g'$ de determinant d^3, la qual, així, estarà continguda en f. Ara, afirmo que a aquesta forma g' equival, necessàriament, la $\left(\begin{array}{lll} d, & 0, & 0 \\ d, & 0, & 0 \end{array} \right) = g''$. En efecte, és clar que

$$\left(\begin{array}{lll} M, & M', & M'' \\ N, & N', & N'' \end{array} \right) = g'''$$

serà una forma ternària de determinant 1; a més a més, com que, per hipòtesi, a, b, c, no tenen els mateixos signes, f serà una forma indefinida, d'on es conclou fàcilment que g i g'' també han de ser indefinides; per tant, g''' equivaldrà a la forma $\left(\begin{array}{lll} 1, & 0, & 0 \\ 1, & 0, & 0 \end{array} \right)$ (article 277), i es podrà trobar una transformació (S') d'aquella en aquesta; evidentment, però, la forma g' es transformarà en g'' per (S'). D'aquí, també g'' estarà continguda en f, i, de la combinació de les substitucions (S), (S') es dedueix una transformació de la forma f en g''. Si aquesta fos

$$\begin{array}{lll} \delta, & \delta', & \delta'' \\ \varepsilon, & \varepsilon', & \varepsilon'' \\ \zeta, & \zeta', & \zeta'', \end{array}$$

és evident que es té una doble solució de l'equació (Ω), posem $x = \delta'$, $y = \varepsilon'$, $z = \zeta'$ i $x = \delta''$, $y = \varepsilon''$, $z = \zeta''$; és clar que aquests valors no poden sortir simultàniament $= 0$, ja que, necessàriament, resulta $\delta\varepsilon'\zeta'' + \delta'\varepsilon''\zeta + \delta''\varepsilon\zeta' - \delta\varepsilon''\zeta' - \delta'\varepsilon\zeta'' - \delta''\varepsilon'\zeta = d$. *Q. E. S.*

Exemple. Sigui $7xx - 15yy + 23zz = 0$ l'equació proposada, que és resoluble ja que $345R7$, $-161R15$, $105R23$. Aquí, els valors de $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, es tenen 3, 7, 6; i, fent $\mathfrak{a} = \mathfrak{b} = \mathfrak{c} = 1$, es troba $A = 98$, $B = -39$, $C = -8$. D'aquí surt la substitució

$$\begin{array}{rrr} 3, & 5, & 22 \\ -1, & 2, & -28 \\ 8, & 25, & -7, \end{array}$$

per la qual f es transforma en

$$\left(\begin{array}{rrr} 1520, & 14490, & -7245 \\ -2415, & -1246, & 4735 \end{array} \right) = g.$$

D'aquí, resulta

$$(S) = \left\{ \begin{array}{rrr} 7245, & 5, & 22 \\ -2415, & 2, & -28 \\ 19320, & 25, & -7 \end{array} \right.$$

$$g''' = \left(\begin{array}{rrr} 3670800, & 6, & -3 \\ -1, & -1246, & 4735 \end{array} \right).$$

Es troba que la forma g''' es transforma en

$$\left(\begin{array}{rrr} 1, & 0, & 0 \\ 1, & 0, & 0 \end{array} \right)$$

per la substitució

$$\left.\begin{array}{rrr} 3, & 5, & 1 \\ -2440, & -4066, & -813 \\ -433, & -722, & -144 \end{array}\right\} \qquad (S')$$

que, combinada amb (S), produeix la

$$\begin{array}{rrr} 9, & 11, & 12 \\ -1, & 9, & -9 \\ -9, & 4, & 3, \end{array}$$

per la qual f es transforma en g''. Així, tenim la doble solució de l'equació proposada, $x = 11$, $y = 9$, $z = 4$ i $x = 12$, $y = -9$, $z = 3$; la darrera es torna més simple dividint els seus valors pel divisor comú 3, d'on $x = 4$, $y = -3$, $z = 1$.

295. La darrera part del teorema de l'article precedent també es pot acabar de la manera següent. Se cerca un enter h tal que sigui $ah \equiv \mathfrak{C}\,(\text{mòd.}\,c)$ (agafem els caràcters $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, amb el mateix significat que en l'article precedent), i resulti $ahh + b = ci$. Llavors, es copsa fàcilment que i resulta enter i que el nombre $-ab$ és el determinant de la forma binària $(ac,\ ah,\ i)\ \cdots\ \phi$. Aquesta forma, certament, no serà positiva (en efecte, com que, per hipòtesi, a, b, c, no tenen el mateix signe, ab i ac no poden ser simultàniament positius); a més a més, tindrà nombre característic -1, la qual cosa demostrem sintèticament així. Es determinen enters e, e', de manera que sigui $e \equiv 0\,(\text{mòd.}\,a)$ i $\equiv \mathfrak{B}\,(\text{mòd.}\,b)$; $ce' \equiv \mathfrak{A}\,(\text{mòd.}\,a)$ i $\equiv h\mathfrak{B}\,(\text{mòd.}\,b)$; i $(e,\ e')$ serà un valor de l'expressió $\sqrt{-(ac, ah, i)}\,(\text{mòd.}\,-ab)$. Efectivament, segons el mòdul a, serà $ee \equiv 0 \equiv -ac$, $ee' \equiv 0 \equiv -ah$, $cce'e' \equiv \mathfrak{A}\mathfrak{A} \equiv -bc \equiv -cci$, de manera que $e'e' \equiv -i$; però, segons el mòdul b, serà $ee \equiv$

$\mathfrak{BB} \equiv -ac$, $cee' \equiv h\mathfrak{BB} \equiv -ach$, de manera que $ee' \equiv -ah$, $cce'e' \equiv hh\mathfrak{BB} \equiv -achh \equiv -cci$, de manera que $e'e' \equiv -i$; però les mateixes tres congruències que tenen lloc segons ambdós mòduls a, b, també valdran segons el mòdul ab. D'aquí es conclou fàcilment, per la teoria de les formes ternàries, que ϕ és representable per la forma $\begin{pmatrix} -1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$; així, sigui $actt + 2ahtu + iuu = -(\alpha t+\beta u)^2+2(\gamma t+\delta u)(\varepsilon t+\zeta u)$, i, multiplicant per c, serà $a(ct+hu)^2+buu = -c(\alpha t+\beta u)^2+2c(\gamma t+\delta u)(\varepsilon t+\zeta u)$. D'aquí, és clar que si s'atribueixen a t, u, valors determinats tals que o bé $\gamma t+\delta u$ o bé $\varepsilon t+\zeta u$ resulti $= 0$, es té una solució de l'equació (Ω), la qual se satisfarà, doncs, tant per $x = \delta c - \gamma h$, $y = \gamma$, $z = \alpha\delta - \beta\gamma$ com per $x = \zeta c - \varepsilon h$, $y = \varepsilon$, $z = \alpha\zeta - \beta\varepsilon$; simultàniament, és evident que ni aquells valors ni aquests no poden resultar simultàniament $= 0$; en efecte, si $\delta c - \gamma h = 0$, $\gamma = 0$, també resultaria $\delta = 0$ i $\phi = -(\alpha t + \beta u)^2$, d'on $ab = 0$, contràriament a la hipòtesi, i igualment per als altres. En el nostre exemple, trobem la forma ϕ, $(161, -63, 24)$, el valor de l'expressió $\sqrt{-\phi}$ (mòd. 105), $= (7, -51)$, i la representació de la forma ϕ per $\begin{pmatrix} -1, & 0, & 0 \\ 1, & 0, & 0, \end{pmatrix}$ la $\phi = -(13t - 4u)^2 + 2(11t - 4u)(15t - 5u)$; d'aquí, es produeixen les solucions $x = 7$, $y = 11$, $z = -8$; $x = 20$, $y = 15$, $z = -5$, o sigui, dividint per 5 i negligint el signe de z, $x = 4$, $y = 3$, $z = 1$.

D'aquests dos mètodes per a resoldre l'equació Ω, el darrer es distingeix perquè, sovint, s'acaba per nombres menors; però el primer, que es pot abreujar per diversos artificis que aquí cal passar en silenci, sembla més elegant, principalment per la raó que els nombres a, b, c, es tracten completament de la mateixa mane-

ra i el càlcul no canvia gens per qualsevol permutació d'aquests. Això es té diferentment en el segon mètode, on el càlcul es presenta sovint molt còmode si s'agafa per a a el mínim i per a c el màxim dels tres nombres donats, com hem fet en el nostre exemple.

296. El teorema elegant explicat en els articles precedents va ser trobat primer per l'il·lm. Le Gendre, *Hist. de l'Ac. de Paris* 1785*, p.* 507, i proveït d'una demostració bonica (completament diferent de les dues nostres). Però, simultàniament, aquest geòmetra egregi, en aquest lloc, es lliurà a la tasca de derivar d'això una demostració de proposicions que tenen relació amb el teorema fonamental de la secció precedent; aquesta, ja hem declarat més amunt, en l'article 151, que no ens sembla idònia per a aquest fi. Així, serà aquest el lloc per a exposar breument aquesta demostració (força elegant per si mateixa) i afegir les raons del nostre judici. Es comença amb l'observació següent. *Si tots els nombres* a*,* b*,* c*, són* $\equiv 1 \,(\text{mòd. } 4)$*, l'equació* $axx + byy + czz = 0$ $\cdots$ (Ω) *no pot tenir solució.* En efecte, es copsa facilíssimament que el valor de $axx + byy + czz$, en aquest cas, resulta necessàriament o bé $\equiv 1$, o bé $\equiv 2$, o bé $\equiv 3 \,(\text{mòd. } 4)$, llevat que tots els x, y, z, s'agafin simultàniament parells; així, si Ω fos resoluble, això no podria resultar altrament que per valors parells de x, y, z, *Q. E. A.*, ja que qualssevol valors que satisfacin l'equació (Ω), també la satisfan si es divideixen pel màxim comú divisor, d'on, necessàriament, n'ha d'aparèixer com a mínim un d'imparell. Ara, els diferents casos del teorema per a demostrar se sotmeten a les consideracions següents.

I. Si p, q, designen nombres primers de la forma $4n + 3$ (positius diferents), no pot ser simultàniament pRq, qRp. En efecte, si fos possible, és evident que establint $1 = a$, $-p = b$, $-q = c$, serien complertes totes les condicions per a la resolubilitat de l'equació $axx + byy + czz = 0$ (article 294); però, per l'observació precedent, aquesta no admet solució; per tant, la suposició no pot ser consistent. D'aquí se segueix directament la proposició 7 de l'article 131.

II. Si p és un nombre primer de la forma $4n+1$ i q un nombre primer de la forma $4n+3$, no pot ser simultàniament qRp, pNq. En efecte, altrament seria $-pRq$ i l'equació $xx + pyy - qzz = 0$, resoluble; aquesta, per l'observació precedent, refusa la resolubilitat. D'aquí es deriven els casos 4 i 5 de l'article 131.

III. Si p, q, són nombres primers de la forma $4n+1$, no pot ser simultàniament pRq, qNp. S'agafa algun nombre primer r de la forma $4n + 3$ que sigui residu de q i del qual p sigui no-residu. Llavors, pels casos demostrats fa un moment (II), serà qRr, rNp. Així, si fos pRq, qNp, seria $qrRp$, $prRq$, $pqNr$, i, en conseqüència, $-pqRr$. D'aquí, l'equació $pxx+qyy-rzz = 0$ seria resoluble, contràriament a l'observació precedent; per tant, la suposició no pot ser consistent. D'aquí se segueixen els casos 1 i 2 de l'article 131.

Aquest cas es tracta de la manera més elegant següent. Designi r un nombre primer de la forma $4n+3$ del qual p sigui no-residu. Llavors, també serà rNp, de manera que (suposant pRq, qNp) $qrRp$; a més a més, $-pRq$, $-pRr$ i, en conseqüència, també $-pRqr$; per tant, l'equació $xx + pyy - qrzz = 0$ seria resoluble, contràriament a l'observació precedent. D'aquí, etc.

IV. Si p és un nombre primer de la forma $4n+1$, q un primer de la forma $4n+3$, no pot ser simultàniament pRq, qNp. S'agafa un nombre primer auxiliar r de la forma $4n+1$ que sigui no-residu d'ambdós p, q. Llavors, (per II) serà qNr i (per III) pNr; d'aquí, $pqRr$; així, si fos pRq, qNp, també es tindria $prNq$, $-prRq$, $qrRp$; per tant, l'equació $pxx - qyy + rzz = 0$ seria resoluble, *Q. E. A.* D'aquí es deriven els casos 3 i 6 de l'article 131.

V. Si p, q, designen nombres primers de la forma $4n+3$, no pot ser simultàniament pNq, qNp. En efecte, suposant que pot resultar, i agafant un nombre primer auxiliar r de la forma $4n+1$ que sigui no-residu d'ambdós p, q, serà $qrRp$, $prRq$; a més a més, (per II) pNr, qNr, d'on $pqRr$ i $-pqRr$; d'aquí, l'equació $-pxx-qyy+rzz = 0$ possible, contra l'observació precedent. D'aquí es dedueix el cas 8 de l'article 131.

297. Contemplant més pròpiament la demostració precedent, qualsevol entendrà fàcilment que els casos I i II són absoluts, de manera que no s'hi pot objectar res. Però les demostracions dels casos restants es basen en l'existència de nombres auxiliars, la qual no s'ha demostrat encara, i, evidentment, el mètode perd tota la força. Aquestes suposicions, encara que siguin tan atractives que, si s'està poc atent, podria semblar que no tenen, de fet, necessitat de demostració, i, certament, eleven al màxim grau de *probabilitat* el teorema que cal demostrar, no obstant això, si es desitja un rigor geomètric, no s'han d'admetre gratuïtament de cap manera. Pel que fa, certament, a la suposició en IV i V, que existeixi un nombre primer r de la forma $4n + 1$ que sigui no-residu de dos altres primers donats p, q, es

conclou fàcilment de la secció IV que tots els nombres menors que $4pq$ i primers amb ell (la quantitat dels quals és $2(p-1)(q-1)$) es distribueixen per igual en quatre classes, de les quals una conté els no-residus d'ambdós p, q, i les tres restants els residus de p i no-residus de q, els no-residus de p i residus de q, i els residus d'ambdós p, q; i a cada classe la meitat seran nombres de la forma $4n+1$, l'altra meitat de la forma $4n+3$. Així, entre ells es tindran $\frac{1}{4}(p-1)(q-1)$ no-residus d'ambdós p, q, de la forma $4n+1$; siguin aquests g, g', g'', etc.; els $\frac{7}{4}(p-1)(q-1)$ nombres restants siguin h, h', h'', etc. Evidentment, tots els nombres continguts en les formes $4pqt+g$, $4pqt+g'$, $4pqt+g''$, etc. (G), també seran no-residus de p, q, de la forma $4n+1$. Ara, és clar que per a establir la suposició només s'ha de demostrar que en les formes (G) es contenen, certament, *nombres primers*, cosa que ara sembla raonablement molt plausible en si, ja que aquestes formes, unides amb les $4pqt+h$, $4pqt+h'$, etc. (H), comprenen tots els nombres primers amb $4pq$, de manera que també tots els nombres absolutament primers (excepte 2, p, q), i no hi ha cap raó per la qual la sèrie dels nombres primers no estigui distribuïda per igual entre aquelles formes, de manera que l'octava part es consignin en (G), els restants en (H). No obstant això, es copsa que un tal raonament dista molt del rigor geomètric. L'il·lm. Le Gendre mateix confessa que la demostració del teorema que en una tal forma $kt+l$, on k, l, designen nombres donats primers entre si, t indefinit, certament, conté nombres primers, sembla bastant difícil, i afegeix de passada un mètode que potser podria conduir a ella; però ens semblen necessàries moltes disquisicions preliminars, abans de poder arribar, certament, per aquesta via a una demostració rigorosa. Però,

sobre l'altra suposició (III, segon mètode), que es dóna un nombre primer r de la forma $4n+3$ del qual un altre nombre primer donat p de la forma $4n+1$ sigui no-residu, l'il·lm. Le Gendre no hi va afegir res en absolut. Hem demostrat més amunt (article 129) que, certament, es donen nombres primers dels quals p és no-residu, però el nostre mètode no sembla idoni per a mostrar l'existència de tals nombres primers *que siguin simultàniament de la forma* $4n+3$ (com es requereix aquí, però no en la nostra primera demostració). D'altra banda, certament podem provar fàcilment la veritat d'aquesta suposició així. Per l'article 287, es donarà un gènere positiu de formes binàries de determinant $-p$ el caràcter del qual és 3, 4; Np; sigui (a, b, c) una tal forma i a imparell (cosa que es pot suposar). Llavors, a serà de la forma $4n+3$ i, o bé primer, o bé implicarà, almenys, un factor primer de la forma $4n+3$. Però serà $-pRa$, de manera que també $-pRr$, d'on pNr. Cal notar perfectament, però, que les proposicions dels articles 263, 287 es recolzen en el teorema fonamental, de manera que serà un cercle viciós si una part d'aquesta es basa en aquelles. Finalment, la suposició en el primer mètode de II encara és molt més gratuïta, de manera que no és necessari afegir aquí res més d'ella.

Es podria afegir una observació sobre el cas V, que, certament, pel mètode precedent no es prova suficientment; no obstant això, s'acaba còmodament pel que segueix. Si allà fos simultàniament pNq, qNp, seria $-pRq$, $-qRp$, d'on es deriva fàcilment que -1 és nombre característic de la forma $(p, 0, q)$, la qual, conseqüentment (segons la teoria de les formes ternàries), es podrà representar per la forma $xx+yy+zz$. Sigui $ptt+quu = (\alpha t+\beta u)^2+(\alpha' t+\beta' u)^2+(\alpha'' t+\beta'' u)^2$,

o sigui, $\alpha\alpha + \alpha'\alpha' + \alpha''\alpha'' = p$, $\beta\beta + \beta'\beta' + \beta''\beta'' = q$, $\alpha\beta + \alpha'\beta' + \alpha''\beta'' = 0$, i, de les equacions 1 i 2, tots els α, α', α'', β, β', β'', seran imparells; però, llavors, evidentment, la tercera equació no pot ser consistent. També es pot acabar el cas II de manera no diferent.

298. PROBLEMA. *Si a, b, c, designen nombres qualssevol, però cap dels quals $= 0$, trobar condicions per a la resolubilitat de l'equació $axx + byy + czz = 0$ $\cdots$ (ω).*

Solució. Siguin $\alpha\alpha$, $\beta\beta$, $\gamma\gamma$, els quadrats màxims que divideixen bc, ac, ab, respectivament, i resulti $\alpha a = \beta\gamma A$, $\beta b = \alpha\gamma B$, $\gamma c = \alpha\beta C$. Llavors, A, B, C, seran enters primers entre si; l'equació (ω), però, serà resoluble o bé no ho serà segons que la $AXX + BYY + CZZ = 0$ $\ldots$ (Ω) admeti solució o bé no n'admeti, cosa que es podrà decidir per l'article 294.

Dem. Es posa $bc = \mathfrak{A}\alpha\alpha$, $ac = \mathfrak{B}\beta\beta$, $ab = \mathfrak{C}\gamma\gamma$, i $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, seran enters lliures de factors quadrats i $\mathfrak{A} = BC$, $\mathfrak{B} = AC$, $\mathfrak{C} = AB$; d'aquí, $\mathfrak{ABC} = (ABC)^2$, de manera que $ABC = A\mathfrak{A} = B\mathfrak{B} = C\mathfrak{C}$ necessàriament enter. Sigui m el màxim comú divisor dels nombres $\mathfrak{A}$, $A\mathfrak{A}$, i $\mathfrak{A} = gm$, $A\mathfrak{A} = hm$, i g serà primer amb h, i també (ja que $\mathfrak{A}$ és lliure de factors quadrats) amb m. Ara, resulta $hhm = gAA\mathfrak{A} = g\mathfrak{BC}$, d'on g dividirà hhm que, evidentment, és impossible llevat que $g = \pm 1$. D'aquí, $\mathfrak{A} = \pm m$, $A = \pm h$, i, en conseqüència, enter; i, igualment, B, C, seran enters. *Q. E. P.* Quan $\mathfrak{A} = BC$ no impliqui factors quadrats, necessàriament B, C, hauran de ser primers entre si; i similarment A serà primer amb C i amb B. *Q. E. S.* Finalment, és clar que si $X = P$, $Y = Q$, $Z = R$, satisfà l'equació (Ω),

l'equació (ω) es resoldrà per $x = \alpha P$, $y = \beta Q$, $z = \gamma R$; i, recíprocament, si a aquesta se la satisfà per a $x = p$, $y = q$, $z = r$, aquella se satisfarà per a $X = \beta\gamma p$, $Y = \alpha\gamma q$, $Z = \alpha\beta r$; d'on, o bé totes dues són resolubles, o bé [no ho és] cap. *Q. E. T.*

299. Problema. *Proposada una forma ternària* $f = axx + a'x'x' + a''x''x'' + 2bx'x'' + 2b'xx'' + 2b''xx'$, *trobar si el zero es pot representar per ella (per valors de les indeterminades que no siguin simultàniament* $= 0$*).*

Solució. I. Quan $a = 0$, es poden prendre a voluntat els valors de x', x'', i és clar de l'equació $a'x'x' + 2bx'x'' + a''x''x'' = -2x(b'x'' + b''x')$ que x obté d'això un valor racional determinat; quan, d'aquesta manera, per a x apareix una fracció, només convé multiplicar els valors de x, x', x'', pel denominador de la fracció i es tindran enters. Únicament s'han d'excloure els valors de x', x'', tals que tornen $b'x'' + b''x' = 0$, llevat que facin simultàniament $a'x'x' + 2bx'x'' + a''x''x'' = 0$, cas en què x es podrà agafar a voluntat. Simultàniament, és clar que totes les solucions possibles es poden obtenir d'aquesta manera. D'altra banda, el cas en què b' i $b'' = 0$ no pertany a aquest; en efecte, llavors x no intervé en f, o sigui, f és una forma binària, i la representabilitat de zero per f s'ha de decidir per la teoria de tals formes.

II. Però quan no és $a = 0$, a l'equació $f = 0$ equivaldrà la $(ax+b''x'+b'x'')^2 - A''x'x'+2Bx'x''-A'x''x'' = 0$, posant $b''b''-aa' = A''$, $ab-b'b'' = B$, $b'b'-aa'' = A'$. Ara, quan aquí $A'' = 0$ però B no és $= 0$, és evident que si $ax + b''x' + b'x''$ i x'' es prenen a voluntat, x i x' es determinen racionalment d'això, i quan no resultin en-

ters un multiplicador idoni els produirà enters. Per a un únic valor de x'' el valor de $ax + b''x' + b'x''$ no és arbitrari sinó que també s'ha de posar $= 0$; llavors, però, es podrà prendre a voluntat x' i es produirà un valor racional de x. Però quan, simultàniament, A'' i $B = 0$, és clar que si A' és un quadrat $= kk$, l'equació $f = 0$ es redueix a les dues lineals (de les quals *o bé* l'una *o bé* l'altra ha de tenir lloc) $ax + b''x' + (b' + k)x'' = 0$, $ax+b''x'+(b'-k)x'' = 0$; però si (en les mateixes hipòtesis) A' és no quadrat, la solució de l'equació proposada depèn, evidentment, de les $x'' = 0$ i $ax + b''x' = 0$ (que han de tenir lloc *simultàniament*).

D'altra banda, gairebé no serà necessari observar que el mètode de I també es pot aplicar quan a' o bé $a'' = 0$, i el mètode de II quan $A' = 0$.

III. Però quan ni a ni $A'' = 0$, a l'equació $f = 0$ equival la $A''(ax + b''x' + b'x'')^2 - (A''x' - Bx'')^2 + Dax''x'' = 0$, designant per D el determinant de la forma f, o sigui, per Da el nombre $BB - A'A''$. Quan $D = 0$, la solució es tindrà de manera similar que en el final del cas precedent; això és, si A'' és un quadrat $= kk$, l'equació proposada es redueix a les $kax+(kb''-A'')x'+(kb'+B)x'' = 0$, $kax+(kb''+A'')x'+(kb''-B)x'' = 0$; però si A'' és no quadrat, ha de resultar $ax+b''x'+b'x'' = 0$, $A''x' - Bx'' = 0$. Però quan D no és $= 0$ ens hem reduït a l'equació $A''tt - uu + Davv = 0$, la possibilitat de la qual es pot decidir per l'article precedent. Si aquesta no es pot resoldre altrament que per $t = 0$, $u = 0$, $v = 0$, tampoc la proposada, evidentment, no admetrà cap altra solució que la $x = 0$, $x' = 0$, $x'' = 0$; però si aquella és resoluble altrament, de qualssevol valors enters de t, u, v, es derivaran, per les equacions $ax+b''x'+b'x'' = t$,

$A''x' - Bx'' = u$, $x'' = v$, almenys valors racionals de x, x', x''; per als quals, si inclouen fraccions, es podran obtenir enters per un multiplicador idoni.

Però tan aviat com s'ha trobat *una* solució en enters de l'equació $f = 0$, el problema es redueix al cas I, i igualment com allà es podran expressar totes les solucions de la manera següent. Satisfacin l'equació $f = 0$ els valors α, α', α'', de x, x', x'', els quals se suposen lliures de factors comuns; s'agafen (pels articles 40 i 279) enters β, β', β'', γ, γ', γ'', tals que sigui $\alpha(\beta'\gamma'' - \beta''\gamma') + \alpha'(\beta''\gamma - \beta\gamma'') + \alpha''(\beta\gamma' - \beta'\gamma) = 1$, i es transforma f en $g = cyy + c'y'y' + c''y''y'' + 2dy'y'' + 2d'yy'' + 2d''yy'$ per la substitució (S) $x = \alpha y + \beta y' + \gamma y''$, $x' = \alpha' y + \beta' y' + \gamma' y''$, $x'' = \alpha'' y + \beta'' y' + \gamma'' y''$. Llavors, evidentment, serà $c = 0$ i g equivalent a f, d'on es conclou fàcilment que de totes les solucions de l'equació $g = 0$ es deriven (per (S)) totes les solucions en enters de l'equació $f = 0$. Ara, se segueix de I que totes les solucions de l'equació $g = 0$ es contenen en les fórmules $y = -z(c'pp + 2dpq + c''qq)$, $y' = 2z(d''pp + d'pq)$, $y'' = 2z(d''pq + d'qq)$, on p, q, designen enters indefinits, z un nombre indefinit per al qual també es poden agafar fraccions, però de manera que y, y', y'', es mantinguin enters. Substituïts aquests valors de y, y', y'', en (S), es tindran totes les solucions en enters de l'equació $f = 0$. Així, *per exemple*, si $f = xx + x'x' + x''x'' - 4x'x'' + 2xx'' + 8xx'$, i es té una solució de l'equació $f = 0$, $x = 1$, $x' = -2$, $x'' = 1$, fent β, β', β'', γ, γ', $\gamma'' = 0$, 1, 0, 0, 0, 1, surt $g = y'y' + y''y'' - 4y'y'' + 12yy''$. D'aquí, totes les solucions en enters de l'equació $g = 0$ estaran contingudes en la fórmula $y = -z(pp - 4pq + qq)$, $y' = 12zpq$, $y'' = 12zqq$, i, en conseqüència, totes les solucions de l'equació $f = 0$

en la $x = -z(pp - 4pq + qq)$, $x' = 2z(pp + 2pq + qq)$, $x'' = -z(pp - 4pq - 11qq)$.

300. Del problema de l'article precedent sorgeix espontàniament una solució de l'equació indeterminada $axx + 2bxy + cyy + 2dx + 2ey + f = 0$ si només es desitgen valors racionals, que ja hem acabat més amunt (articles 216 i següents) si aquests es demanen enters. Efectivament, tots els valors racionals de x, y, es poden expressar per $\frac{t}{v}$, $\frac{u}{v}$, de manera que t, u, v, siguin enters; d'on és clar que la solució d'aquella equació per nombres racionals és idèntica a la solució de l'equació $att + 2btu + cuu + 2dtv + 2euv + fvv = 0$ per nombres enters; aquesta, però, coincideix amb l'equació tractada en l'article precedent. Només s'han d'excloure les solucions en què $v = 0$; però tals no poden presentar-se quan $bb - ac$ és un nombre no quadrat. Així, per exemple, totes les solucions per nombres racionals de l'equació $xx + 8xy + yy + 2x - 4y + 1 = 0$ (resolta en general per enters en l'article 221) estaran contingudes en la fórmula

$$x = \frac{pp - 4pq + qq}{pp - 4pq - 11qq}, \quad y = -\frac{2pp + 4pq + 2qq}{pp - 4pq - 11qq},$$

on p, q, designen nombres enters qualssevol. D'altra banda, aquí només hem tractat breument sobre aquests dos problemes connectats per un nexe molt fort, i hem suprimit moltes observacions pertinents, tant per no resultar massa prolixos com perquè tenim una altra solució del problema de l'article precedent basada en principis més generals, l'exposició de la qual ens hem de reservar per una altra ocasió ja que demana una disquisició més profunda de les formes ternàries.

301. Tornem a les formes binàries, de les quals encara convé revisar moltes propietats singulars. I, primer, afegirem algunes observacions sobre la quantitat de gèneres i classes en un ordre pròpiament primitiu (positiu per a un determinant negatiu), al qual restringim, per abreujar, la disquisició.

La *quantitat de gèneres* en què es distribueixen totes les formes (pròpiament primitives positives) de determinant donat positiu o bé negatiu $\pm D$ sempre és 1, 2, 4, o bé una potència més alta del nombre 2, l'exponent de la qual depèn dels factors de D, i que es pot trobar completament a priori per les disquisicions precedents. Ara, com que, a la sèrie dels nombres, els nombres naturals primers estan barrejats amb més i menys compostos, succeeix que, per a molts determinants successius $\pm D$, $\pm(D+1)$, $\pm(D+2)$, etc., la quantitat de gèneres ara creix ara decreix, i sembla que en aquesta sèrie pertorbada no es presenta cap ordre. No obstant això, si se sumen les quantitats de gèneres que corresponen a molts determinants successius $\pm D$, $\pm(D+1)$, $\ldots$, $\pm(D+m)$, i es divideix la suma per la quantitat de determinants, apareix una *quantitat mitjana de gèneres*, que es podrà considerar que té lloc prop del determinant del mig $\pm\left(D+\frac{1}{2}m\right)$ i constitueix una progressió molt regular. Suposem, però, que no només m és bastant gran, sinó també que D és tant més gran que la raó dels determinants extrems D i $D+m$ no difereixi gaire de la raó d'igualtat. S'haurà d'entendre així la regularitat d'aquella progressió: si D' és un nombre molt més gran que D, la quantitat mitjana de gèneres prop del determinant $\pm D'$ serà sensiblement més gran que prop de D; però, si D, D' no difereixen gaire, les quantitats mit-

janes dels gèneres prop de D i D' seran gairebé iguals. D'altra banda, la quantitat mitjana de gèneres prop d'un determinant positiu $+D$ sempre es troba gairebé igual a la quantitat mitjana prop del negatiu, i com més gran és D, més exactament, mentre que per a un valor petit, la primera surt una mica més gran que la darrera. Aquestes observacions s'il·lustraran més pels exemples següents, extrets d'una taula de classificació de formes binàries que comprèn més de 4000 determinants. Entre els cent determinants des de 801 fins a 900 se'n troben 7 als quals correspon un sol gènere; 32, 52, 8, 1, als quals corresponen 2, 4, 8, 16, gèneres, respectivament; d'aquí surten, en total, 359 gèneres, d'on la quantitat mitjana $= 3,59$. Els cent determinants negatius des de -801 fins a -900 produeixen 360 gèneres. Tots els exemples següents s'han elegit per a determinants negatius. En el 16 centenar (des de -1501 fins a -1600) la quantitat mitjana de gèneres es troba $3,89$; en el 25 centenar és $4,03$; en el centenar 51, apareix $4,24$; dels siscents determinants $-9401 \cdots -10000$ es calcula $4,59$. D'aquests exemples és clar que la quantitat mitjana de gèneres creix molt més lentament que els mateixos determinants; però se cerca quina és la llei d'aquesta progressió? Per una disquisició teòrica bastant difícil, que seria massa llarg explicar aquí, s'ha descobert que la quantitat mitjana de gèneres prop del determinant $+D$ o bé $-D$ s'expressa al més aproximadament possible per la fórmula $\alpha \log D + \beta$, on α, β, són quantitats constants, i certament $\alpha = \dfrac{4}{\pi\pi} = 0,4052847346$ (on π designa la semiperifèria d'un cercle el radi del qual és 1), $\beta = 2\alpha g + 3\alpha\alpha h - \dfrac{1}{6}\alpha \log 2 = 0,8830460462$, on g és

la suma de la sèrie $1 - \log(1+1) + \frac{1}{2} - \log\left(1+\frac{1}{2}\right)$ $+\frac{1}{3} - \log\left(1+\frac{1}{3}\right) + etc. = 0,5772156649$ (vegeu Euler, Inst. Cal. Diff. p. 444); però h la suma de la sèrie $\frac{1}{4}\log 2 + \frac{1}{9}\log 3 + \frac{1}{16}\log 4 + etc.$ que s'ha descobert per aproximació que és $= 0,9375482543$. D'aquesta fórmula és clar que la quantitat mitjana de gèneres creix en progressió aritmètica si els determinants augmenten en geomètrica. Els valors d'aquesta fórmula per a $D = 850\frac{1}{2}$, $1550\frac{1}{2}$, $2450\frac{1}{2}$, $5050\frac{1}{2}$, $9700\frac{1}{2}$, es troben $3,617$; $3,86$; $4,046$; $4,339$; $4,604$, que difereixen poc de les quantitats mitjanes donades més amunt. Com més gran sigui el determinant mitjà i també com més quantitats mitjanes de determinants es calculin, tant menys diferirà el valor de la fórmula. Amb l'ajut d'aquesta fórmula també es pot descobrir al més aproximadament possible la suma de les quantitats de gèneres que corresponen a determinants successius $\pm D$, $\pm(D+1)$, $\cdots$, $\pm(D+m)$, si es calculen i es recullen en una suma les quantitats mitjanes que corresponen a cadascun, per més diferents que siguin els extrems D, $D+m$. Aquesta suma serà $= \alpha(\log D + \log(D+1) + etc. + \log(D+m)) + \beta(m+1)$, o sigui, bastant exactament $= \alpha((D+m)\log(D+m) - (D-1)\log(D-1)) + (\beta-\alpha)(m+1)$. D'aquesta manera, la suma de les quantitats de gèneres per als determinants des de -1 fins a -100, es troba $= 234,4$, mentre que realment és 233; similarment, des de -1 fins a -2000, $= 7116,6$, mentre que és 7112; des de -9001 fins a -10000, on és 4595, la fórmula proporciona $4594,9$, consens que a penes s'hauria pogut esperar.

302. Respecte de la *quantitat de classes* (que cal entendre sempre pròpiament primitives positives) els determinants positius es comporten de manera completament altra que els negatius; per la qual cosa, considerarem ambdós separadament. Els uns amb els altres concorden en què, per a un determinant donat, en cada un dels gèneres es contenen igual quantitat de classes, de manera que la quantitat de totes les classes és igual al producte de la quantitat de gèneres per la quantitat de classes contingudes en cada gènere.

Primer, pel que fa respecte a determinants negatius, la quantitat de classes corresponents a molts determinants successius $-D$, $-(D+1)$, $-(D+2)$, etc., constitueix una progressió igualment pertorbada com la quantitat de gèneres. Però la quantitat mitjana de classes (que no tindrà necessitat de definició) creix molt regularment, com serà evident dels exemples següents. Els cent determinants des de -500 fins a -600 proporcionen 1729 classes, d'on la quantitat mitjana $= 17,29$. Similarment, en el 15 centenar la quantitat mitjana de classes es troba $28,26$; en els dos centenars 24 i 25 es calcula $36,28$; en els tres 61, 62 i 63 surt $58,50$; i en els cinc $91 \cdots 95$, resulta $71,56$; finalment, dels cinc $96 \cdots 100$, resulta $73,54$. Aquests exemples mostren que la quantitat mitjana de classes creix, certament, més lentament que els determinants, però molt més de pressa que la quantitat mitjana de gèneres; amb una lleu atenció, però, es reconeixerà que aquella creix, bastant exactament, amb la raó de les arrels quadrades dels determinants del mig. Realment, per una disquisició teòrica, trobem que la quantitat mitjana de classes prop del determinant $-D$ s'expressa aproximadament per $\gamma\sqrt{D} - \delta$, on $\gamma = 0,7467183115 = \dfrac{2\pi}{7e}$, on e denota

la suma de la sèrie $1 + \frac{1}{8} + \frac{1}{27} + \frac{1}{64} + \frac{1}{125} etc.$; $\delta = 0,2026423673 = \frac{2}{\pi\pi}$; els valors mitjans calculats segons aquesta fórmula difereixen poc dels que havíem transcrit més amunt de la taula de classificació. Amb l'ajut d'aquesta fórmula també es pot assignar tan aproximadament com és possible la suma de les quantitats de totes les classes (pròpiament primitives positives) que corresponen als determinants successius $-D$, $-(D+1)$, $-(D+2)$, $\ldots$, $-(D+m-1)$, per més diferents que siguin els extrems, sumant les quantitats mitjanes corresponents a aquells determinants segons la fórmula, d'on serà $= \gamma(\sqrt{D} + \sqrt{D+1} + etc. + \sqrt{D+m-1}) - \delta m$, o sigui, tan aproximadament com és possible, $= \frac{2}{3}\gamma\left(\left(D+m+\frac{1}{2}\right)^{\frac{3}{2}} - \left(D-\frac{1}{2}\right)^{\frac{3}{2}}\right) - \delta m$. Així, per exemple, per als cent determinants $-1 \cdots -100$, aquella suma es calcula per la fórmula $= 481,1$ mentre que, realment, és $= 477$; els mil determinants $-1 \cdots -1000$ proporcionen, segons la taula, 15533 classes, la fórmula en dóna $15551,4$; el segon miler fixa, segons la taula, 28595 classes, mentre que la fórmula en dóna $28585,7$; similarment, el tercer miler procura realment 37092 classes, la fórmula en dóna $37074,3$; el desè miler en dóna 72549 per la taula, la fórmula, 72572.

303. Una taula de determinants negatius, ordenada segons la diversitat de classificacions que els corresponen, ofereix moltes altres observacions singulars. Per als determinants de la forma $-(8n+3)$, la quantitat de classes (tant de les que estan contingudes en tots, com de les que ho estan en cada gènere pròpiament primitiu) sempre és divisible per 3, exceptuat l'únic determinant

−3, la raó de la qual cosa se segueix espontàniament per l'article 256, VI. Per als determinants les formes dels quals esgoten un sol gènere, la quantitat de classes sempre és imparella; en efecte, com que per un tal determinant només es donarà una única classe ambigua, posem la principal, la quantitat de les classes restants, dues de les quals sempre seran oposades, serà necessàriament parella, de manera que la quantitat de totes, imparella; d'altra banda, aquesta darrera propietat també val per a determinants positius. A més a més, la sèrie de determinants als quals correspon la mateixa classificació donada (és a dir, la quantitat donada tant de gèneres com de classes) sembla que sempre es trenca, observació bastant notable que il·lustrem amb alguns exemples. (El primer nombre, romà, indica la quantitat de gèneres pròpiament primitius positius; el següent, la quantitat de classes contingudes en cada gènere; després, se segueix la sèrie de determinants a què correspon aquella classificació i dels quals s'omet, per abreujar, el signe negatiu.)

I. 1 . . . , 1, 2, 3, 4, 7.

I. 3 . . . , 11, 19, 23, 27, 31, 43, 67, 163.

I. 5 . . . , 47, 79, 103, 127.

I. 7 . . . , 71, 151, 223, 343, 463, 487.

II. 1 . . . , 5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58.

II. 2 . . . , 14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193.

IV. 1 . . . , 21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253.

VIII. 1 . . . , 105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760.

XVI. 1 . . . , 840, 1320, 1365, 1848.

Similarment, es troben 20 determinants (el màxim = −1423) als quals correspon la classificació I. 9; 4 (el màxim = −1303) als quals correspon la classificació I. 11, etc.; les classificacions II. 3; II. 4; II. 5; IV. 2 corresponen a no més de 48, 31, 44, 69, determinants respectivament, dels quals els màxims són −652, −862, −1318, −1012. Com que la taula de la qual hem extret aquests exemples s'ha produït més enllà dels determinants màxims que ocorren aquí,* i no n'apareixen més que pertanyin a aquelles classificacions, sembla que no hi ha cap dubte que les sèries transcrites s'han trencat realment, i, per analogia, es podrà estendre la mateixa conclusió a qualssevol altres classificacions. Per exemple, com que en tot el desè miler de determinants no se n'ha presentat cap al qual correspongui una quantitat de classes inferior a 24, és molt versemblant que les classificacions I. 23; I, 21, etc.; II. 11; II. 10, etc.; IV. 5; IV. 4; IV. 3; VIII. 2, ja s'hagin acabat abans de −9000, o bé, almenys, que corresponguin a molt pocs determinants més enllà de −10000. Però les demostracions *rigoroses* d'aquestes observacions semblen molt difícils. No és menys digne d'admiració que tots els determinants les formes dels quals es distribueixen en 32 o bé més gèneres tinguin com a mínim dues classes a cada gènere, de manera que les classificacions XXXII. 1, LXIV. 1, etc., desapareguin

* Mentrestant s'imprimia aquesta, n'hem *estesa una* fins a −3000, també per a tot el desè miler i moltes altres centenes disperses, a les quals s'afegeixen molts determinants singulars elegits curosament.

completament (al mínim determinant d'aquest tipus, -9240, li correspon XXXII. 2); i sembla bastant probable que en créixer contínuament la quantitat de gèneres desapareixen més classificacions. Respecte d'això, els 65 determinants transmesos més amunt, als quals corresponen les classificacions I. 1; II. 1; IV. 1; VIII. 1; XVI. 1, són molt notables, i es copsa fàcilment que tots i només ells gaudeixen d'aquestes dues propietats insignes: que totes les classes de formes que pertanyen a ells són ambigües, i que formes qualssevol contingudes en el mateix gènere equivalen necessàriament tant pròpiament com impròpiament. D'altra banda, tots aquests 65 nombres (en un aspecte una mica diferent, al qual es farà menció més avall, i amb un criteri fàcil de demostrar) ja van ser transmesos per l'il·lm. Euler en *Nouv. Mem. de l'Ac. de Berlin* 1776 *p.* 338.

304. La quantitat de classes pròpiament primitives que constitueixen les formes binàries de determinant positiu *quadrat* kk es pot assignar completament *a priori*, i és igual a la quantitat de nombres primers amb $2k$ i menors que ell; d'on, per uns raonaments no difícils, però que cal suprimir aquí, es dedueix que la quantitat mitjana de classes que pertanyen a tals determinants prop de kk s'expressa aproximadament per $\frac{8k}{\pi\pi}$. Respecte d'això, però, els determinants positius no quadrats ofereixen fenòmens completament singulars. Això és, mentre que una quantitat petita de classes, per exemple, en la classificació I. 1, o bé I. 3, o bé II. 1, etc., només té lloc per a determinants negatius i quadrats petits, i aviat desapareixen del tot, per contra, per a determinants positius no quadrats, almenys per als no molt grans, la major part d'ells presenten classificacions

tals que en qualsevol gènere es conté una única classe, de manera que les I. 3; I. 5; II. 2; II. 3; IV. 2, etc., són raríssimes. Així, per exemple, entre els 90 determinants no quadrats per sota de 100 se'n troben 11, 48, 27, als quals corresponen les classificacions I. 1; II. 1; IV. 1, respectivament; només un únic (37) té I. 3; dos (34 i 82) tenen II. 2; un (79), II. 3. No obstant això, en créixer els determinants, resulten més freqüents quantitats de classes gradualment més grans; així, entre els 96 determinants no quadrats des de 101 fins a 200, dos (101, 197) tenen I. 3; quatre (145, 146, 178, 194), II. 2; tres (141, 148, 189), II. 3. Entre els 197 determinants des de 801 fins a 1000, tres tenen I. 3; quatre, II. 2; catorze, II. 3; dos, II. 5; dos, II. 6; quinze, IV. 2; sis, IV. 3; dos, IV. 4; quatre, VIII. 2; els restants 145, una classe en qualsevol gènere. Seria curiosa la qüestió, no indigna de la sagacitat dels geòmetres, d'investigar la llei segons la qual els determinants que tenen una classe en qualsevol gènere resulten contínuament més rars; fins ara, ni podem decidir per teoria, ni conjecturar per l'observació amb suficient certesa, si finalment es trenquen completament (cosa, però, que sembla poc probable), o bé, almenys, surten *infinitament espaiats*, o bé si la seva freqüència s'acosta contínuament més a un límit fix. La quantitat mitjana de classes creix amb una raó poc més gran que la quantitat de gèneres, i molt més lentament que les arrels quadrades dels determinants; entre 800 i 1000, aquella es troba $= 5,01$. Valgui afegir a aquestes observacions una altra, que restitueix d'alguna manera l'analogia entre determinants positius i negatius. Això és, trobem que per a un determinant positiu D no tant la mateixa quantitat de classes com millor aquesta quantitat multiplicada pel logaritme de la quantitat $t+u\sqrt{D}$ (on t, u, designen els nombres mínims, excepte 1, 0, que

satisfan l'equació $tt - Duu = 1$), per moltes raons que aquí no cal explicar extensament, és anàloga a la quantitat de classes per a determinant negatiu, i que el valor mitjà d'aquell producte s'expressa de manera igualment exacta per la tal fórmula $m\sqrt{D} - n$; però els valors de les quantitats constants m, n, no s'han pogut determinar per teoria fins ara; sembla que m difereix poc de $2\frac{1}{3}$, si és permès concloure això, comparats entre si alguns centenars de determinants. D'altra banda, ens reservem per a una altra ocasió tractar més extensament dels principis de les disquisicions precedents sobre els valors mitjans de quantitats que no progressen per una llei analítica sinó que contínuament s'aproximen més asimptòticament a una tal llei. Passem ara a una altra disquisició, per la qual es compararan entre si diferents classes pròpiament primitives del mateix determinant, i es posarà fi a aquesta llarga secció.

305. Teorema. *Si K designa la classe principal de formes de determinant donat D, C, una altra classe qualsevol del gènere principal de formes del mateix determinant, $2C$, $3C$, $4C$, etc., les classes produïdes (com a l'article 249) respectivament de la duplicació, triplicació, quadruplicació, etc., de la classe C, en la progressió C, $2C$, $3C$, etc., suficientment continuada, s'arriba finalment a una classe idèntica a K; i, suposant que mC és la primera idèntica a K, i que la quantitat de totes les classes en el gènere principal és $= n$, o bé serà $m = n$, o bé m una part alíquota de n.*

Dem. I. Com que totes les classes K, C, $2C$, $3C$, etc., pertanyen, necessàriament, al gènere principal (ar-

ticle 247), les $n+1$ primeres classes d'aquesta sèrie, K, C, $2C$, $3C$, ..., nC, no poden ser, evidentment, totes diferents. Així, o bé K serà idèntica a alguna de les classes C, $2C$, $3C$, ..., nC, o bé almenys dues d'aquestes classes idèntiques entre si. Sigui $rC = sC$ i $r > s$, i també serà $(r-1)C = (s-1)C$, $(r-2)C = (s-2)C$, etc., i $(r+1-s)C = C$, d'on $(r-s)C = K$. *Q. E. P.*

II. D'aquí també se segueix directament que és o bé $m = n$ o bé $m < n$, i només resta que demostrem que, en el darrer cas, m és una part alíquota de n. Com que les classes K, C, $2C$, ..., $(m-1)C$, el complex de les quals designarem per $\mathfrak{C}$, encara no exhaureixen en aquest cas tot el gènere principal, sigui C' alguna classe d'aquest gènere no continguda en $\mathfrak{C}$, i es designarà per $\mathfrak{C}'$ el complex de les classes que s'originen de la composició de C' amb cadascuna de les classes de $\mathfrak{C}$, posem C', $C'+C$, $C'+2C$, ..., $C'+(m-1)C$. Es copsa fàcilment que totes les classes de $\mathfrak{C}'$ són diferents tant entre si com de totes les de $\mathfrak{C}$, i que pertanyen al gènere principal; així, si $\mathfrak{C}$ i $\mathfrak{C}'$ exhaureixen completament aquest gènere, tindrem $n = 2m$; si no, serà $2m < n$. En el darrer cas, sigui C'' alguna classe del gènere principal no continguda ni en $\mathfrak{C}$ ni en $\mathfrak{C}'$, i es designarà per $\mathfrak{C}''$ el complex de les classes produïdes per la composició de C'' amb cadascuna de les classes de C, és a dir, de les C'', $C''+C$, $C''+2C$, ..., $C''+(m-1)C$; i és clar fàcilment que totes aquestes són diferents entre si i de totes les de $\mathfrak{C}$ i $\mathfrak{C}'$, i que pertanyen al gènere principal. Per tant, si $\mathfrak{C}$, $\mathfrak{C}'$, $\mathfrak{C}''$, exhaureixen aquest gènere, serà $n = 3m$; si no, $n > 3m$, cas en què una altra classe C''', continguda en el gènere principal però no en $\mathfrak{C}$, $\mathfrak{C}'$ o bé $\mathfrak{C}''$, tractada de manera similar, ensenyarà que és, o bé $n = 4m$, o bé $n > 4m$, i així successivament. Ara, com que n i m són nombres finits,

necessàriament el gènere principal s'exhaurirà finalment, i n serà un múltiple de m, o sigui, m una part alíquota de n. *Q. E. S.*

Exemple. Sigui $D = -356$, $C = (5, 2, 72)$,* i es trobarà que $2C = (20, 8, 21)$, $3C = (4, 0, 89)$, $4C = (20, -8, 21)$, $5C = (5, -2, 72)$, $6C = (1, 0, 356)$. Així, aquí és $m = 6$; però n, per a aquest determinant, és 12. Agafant la classe $(8, 2, 45)$ per a C', les cinc classes restants de $\mathfrak{C}'$ seran $(9, -2, 40)$, $(9, 2, 40)$, $(8, -2, 45)$, $(17, 1, 21)$, $(17, -1, 21)$.

306. La demostració del teorema precedent es troba completament anàloga a les demostracions dels articles 45, 49, i, realment, la teoria de la multiplicació de classes té una gran afinitat en tots sentits amb l'argument tractat a la Secció III. Però els límits d'aquesta obra no permeten prosseguir aquí aquella teoria amb el profit de què és digna; conseqüentment, aquí només afegirem algunes observacions, també suprimirem les demostracions que requereixin una preparació més extensa, i ens reservarem una disquisició més àmplia per a una altra ocasió.

I. Si la sèrie K, C, $2C$, $3C$, etc., es condueix més enllà de $(m-1)C$, compareixen de nou les mateixes classes, $mC = K$, $(m+1)C = C$, $(m+2)C = 2C$, etc.; i, en general (mirant, per causa de concisió, K com $= 0C$), les classes gC, $g'C$, seran idèntiques o bé diferents segons que g i g' siguin congrus o bé incongrus segons el mòdul m. Així, la classe nC sempre és idèntica a la classe principal K.

* Aquí les classes sempre s'expressen per les *formes* (més simples) contingudes en elles.

II. Anomenarem *període* de la classe C el complex de les classes K, C, $2C$, $\ldots$, $(m-1)C$, que hem designat més amunt per $\mathfrak{C}$, expressió que no s'ha de confondre amb els *períodes de les formes* reduïdes de determinant positiu no quadrat tractats en l'article 186 i següents. Així, és clar que de la composició de classes qualssevol contingudes en el mateix període s'origina una classe també continguda en aquest període, $gC + g'C + g''C + etc. = (g + g' + g'' + etc.)C$.

III. Com que $C + (m-1)C = K$, les classes C i $(m-1)C$ seran oposades, i, igualment, $2C$ i $(m-2)C$, $3C$ i $(m-3)C$, etc. Així, si m és parell, la classe $\frac{1}{2}mC$ serà oposada a si mateixa, de manera que *ambigua*; recíprocament, si en $\mathfrak{C}$, a part de K, encara ocorre una altra classe ambigua, posem gC, serà $gC = (m-g)C$, de manera que $g = (m-g) = \frac{1}{2}m$. D'aquí se segueix que no hi pot haver cap altra classe ambigua continguda en $\mathfrak{C}$ excepte les dues K i $\frac{1}{2}mC$, si m és parell, però excepte l'única K, si m és imparell.

IV. Si se suposa que el període d'alguna classe hC continguda en $\mathfrak{C}$ és K, hC, $2hC$, $3hC$, $\ldots$, $(m'-1)hC$, és evident que $m'h$ és el mínim múltiple de h divisible per m. Així, si m i h són primers entre si, serà $m' = m$, i els dos períodes contindran les mateixes classes però disposades en ordre diferent; en general, però, si μ designa el màxim comú divisor de m, h, serà $m' = \frac{m}{\mu}$. D'aquí és clar que la quantitat de classes contingudes en el període de qualsevol classe de $\mathfrak{C}$ és o bé m o bé una part alíquota de m; i, certament, tantes classes de

$\mathfrak{C}$ tindran períodes de m termes, com nombres dels 0, 1, 2, ..., $m-1$, són primers amb m, o sigui, utilitzant el símbol de l'article 39, $\phi(m)$; però, en general, tantes classes de $\mathfrak{C}$ tindran períodes de $\frac{m}{\mu}$ termes com nombres dels 0, 1, 2, ..., $m-1$, tenen màxim comú divisor μ amb m, la quantitat dels quals es copsa fàcilment que és $\phi\left(\frac{m}{\mu}\right)$. Així, si $m = n$, o sigui, *tot* el gènere principal està contingut en $\mathfrak{C}$, en aquest gènere es donaran en total $\phi(n)$ classes els períodes de les quals inclouen tot el mateix gènere, i $\phi(e)$ classes els períodes de les quals consten de e termes, on e denota un divisor qualsevol de n. Aquesta conclusió val en general quan en el gènere principal es dóna alguna classe el període de la qual consta de n termes.

V. Sota la mateixa suposició, no es pot disposar un sistema de classes del gènere principal de millor manera que prenent per *base* alguna classe que tingui un període de n termes, i col·locant les classes del gènere principal en el mateix ordre en què apareixen en aquell període. Llavors, si s'adscriu l'*índex* 0 a la classe principal, l'índex 1 a la classe que s'ha pres per base, i així successivament, es podrà trobar, per la sola addició dels índexs, quina classe s'origina de la composició de classes qualssevol del gènere principal. Heus aquí un exemple per al determinant -356, on hem agafat per base la classe (9, 2, 40).

0	$(1, 0, 356)$	4	$(20, 8, 21)$	8	$(20, -8, 21)$
1	$(9, 2, 40)$	5	$(17, 1, 21)$	9	$(8, 2, 45)$
2	$(5, 2, 72)$	6	$(4, 0, 89)$	10	$(5, -2, 72)$
3	$(8, -2, 45)$	7	$(17, -1, 21)$	11	$(9, -2, 40)$

VI. Però, encara que tant l'analogia amb la Secció III com un indici instituït sobre més de 200 determinants negatius i encara molts més determinants positius no quadrats, semblen al·legar la màxima probabilitat que aquella suposició té lloc per a *tots* els determinants, no obstant això, una tal conclusió seria falsa i es refutaria per la continuació de la taula de classificació. Per abreujar, sigui permès anomenar *regulars* aquells determinants per als quals tot el gènere principal pot ser inclòs en un únic període, però *irregulars* els restants, per als quals això no pot resultar. Aquí podem il·lustrar aquest argument, que pertany als misteris més recòndits de l'aritmètica superior, i que sembla que deixa lloc a disquisicions més difícils, només amb algunes observacions, de les quals avancem la següent més general.

VII. Si en el gènere principal ocorren classes C, C', els períodes de les quals consten de m, m', classes, i si M és el nombre mínim divisible per m i m', en el mateix gènere també es donaran classes els períodes de les quals contindran M termes. Es descompon M en dos factors r, r', primers entre si, dels quals un (r) divideixi m i l'altre (r'), m' (vegeu l'article 73), i la classe $\frac{m}{r}C + \frac{m'}{r'}C' = C''$ tindrà la propietat prescrita. En efecte, suposem que el període de la classe C'' consta de g termes, i serà $K = grC'' = gmC + \frac{grm'}{r'}C' = K + \frac{grm'}{r'}C' = \frac{grm'}{r'}C'$, d'on $\frac{grm'}{r'}$ haurà de ser divisible per m', o sigui, gr per r', de manera que també g per r'. De manera completament similar, es troba g divisible per r, d'on també serà divisible per $rr' = M$. Però, com que, evidentment, és $MC'' = K$, també M serà divisible per g; per tant, necessàriament, $M = g$.

D'aquí se segueix sense cap dificultat que la quantitat *màxima* de classes contingudes en algun període (per a un determinant donat) és divisible per la quantitat de classes en qualsevol altre període (d'una classe del mateix gènere principal). D'aquí mateix es pot derivar simultàniament un mètode per a descobrir la tal classe el període de la qual sigui el més gran possible (de manera que, per a un determinant regular, comprengui tot el gènere principal); mètode completament anàleg al dels articles 73, 74; però a la pràctica es pot reduir la feina per molts artificis. El quocient de la divisió del nombre n per la quantitat de classes en el període màxim, que per als determinants regulars és 1, per als irregulars sempre resulta un enter més gran que 1, i per això, principalment, és còmode per a expressar diferents espècies d'irregularitats; per la qual cosa, es pot anomenar *exponent d'irregularitat*.

VIII. Fins ara no es té una regla general per la qual es puguin distingir *a priori* els determinants regulars dels irregulars, principalment, perquè entre els darrers apareixen tant nombres primers com compostos; així, sigui suficient aquí adjuntar algunes observacions particulars. Quan en el gènere principal es contenen més de dues classes ambigües, el determinant és, certament, irregular, i l'exponent d'irregularitat, parell; però quan en aquell gènere només n'hi ha una o bé dues, el determinant serà o bé regular o bé, almenys, l'exponent d'irregularitat, imparell. Tots els determinants negatius de la forma $-(216k + 27)$, exceptuat únicament -27, són irregulars i l'exponent d'irregularitat divisible per 3; el mateix val per a determinants negatius de la forma $-(1000k + 75)$ i $-(1000k + 675)$, exceptuant-ne únicament -75, i per a altres infinits. Si l'exponent d'irregu-

laritat és un nombre primer p, o bé, almenys, divisible per p, n serà divisible per pp, d'on se segueix que, si n no implica cap divisor quadrat, el determinant és, certament, regular. Només per a determinants *quadrats* positius *ee* es pot discernir sempre *a priori* si són regulars o irregulars; això és, s'esdevindrà allò quan e és 1, o bé 2, o bé un nombre primer imparell, o bé una potència d'un nombre primer imparell; això, en tots els casos restants. Per a determinants negatius, els irregulars surten cada vegada més freqüents, com més grans resulten els determinants; per exemple, en tot el primer miler se'n troben 13 d'irregulars, (omès el signe negatiu) 576, 580, 820, 884, 900, l'exponent d'irregularitat dels quals és 2, i 243, 307, 339, 459, 675, 755, 891, 974, l'exponent d'irregularitat dels quals és 3; en el segon miler se'n troben 13 l'exponent d'irregularitat dels quals és 2, i 15 l'exponent d'irregularitat dels quals és 3; en el desè miler, 31 amb exponent d'irregularitat 2, i 32 amb exponent d'irregularitat 3. Encara no es pot decidir si hi ha determinants per sota de -10000 amb exponent d'irregularitat més gran que 3; més enllà d'aquest límit podrien aparèixer exponents donats qualssevol. És molt probable que, en créixer els determinants, la freqüència dels determinants negatius irregulars s'aproximi més contínuament a la freqüència dels regulars amb una raó constant, la determinació de la qual seria molt digna de la sagacitat dels geòmetres. Per a determinants positius no quadrats, els irregulars són molt més rars; es donen tals, certament infinits, dels quals l'exponent d'irregularitat és parell (per exemple, 3026, per al qual és 2); i sembla també fora de dubte que n'existeixen tals l'exponent d'irregularitat dels quals és imparell, encara que convindria confessar que, fins ara, no se'ns n'ha presentat cap.

IX. A causa de la brevetat, no es pot tractar aquí de la disposició més còmoda del sistema de classes contingudes en el gènere principal per a un determinant irregular; observem, només, que, com que aquí no és suficient una única base, s'han d'agafar dues o bé, fins i tot, encara més classes de la multiplicació i composició de les quals es produeixin totes. D'aquí, sortiran *índexs dobles o bé múltiples*, que prestaran gairebé el mateix servei que els simples per als regulars. Però tractarem aquesta qüestió més extensament en una altra ocasió.

X. Finalment, observem que com que totes les propietats considerades en aquest article i en el precedent depenen principalment del nombre n, que és similar a com és $p-1$ en la secció III, aquest nombre és digne de molta atenció; per la qual cosa, el que caldria desitjar més és que es descobrís el nexe general entre aquest i el determinant al qual pertany. Considerem que no cal desesperar d'aquesta cosa importantíssima perquè ja hem aconseguit sotmetre (article 302) el valor mitjà del producte de n per la quantitat de gèneres (els quals es poden assignar *a priori*) a una fórmula analítica, almenys, per a determinants negatius.

307. Les disquisicions dels articles precedents comprenen només les classes del gènere principal, de manera que són suficients tant per a determinants positius en què es dóna un únic gènere, com per a negatius en què es presenta un únic gènere positiu, si no volem tenir en compte el gènere negatiu. Resta que també afegim quelcom dels gèneres restants (pròpiament primitius).

I. Quan en un gènere G' diferent del principal G (del mateix determinant) es dóna alguna classe ambigua,

se'n presentaran tantes en ell com en G. Siguin L, M, N, etc., les classes ambigües de G (entre les quals també hi haurà la classe principal K), però L', M', N', etc., les de G'; i es designa per A el complex d'aquelles, per A' el complex d'aquestes. Com que, evidentment, totes les classes $L + L'$, $M + L'$, $N + L'$, etc., són ambigües i diferents i pertanyen a G', de manera que han d'estar contingudes en A', la quantitat de classes de A' no pot ser, certament, menor que la de A; similarment, com que les classes $L' + L'$, $M' + L'$, $N' + L'$, etc., són diferents i ambigües i pertanyen a G, de manera que es contenen en A, la quantitat de classes de A no pot ser menor que la de A'; per tant, les quantitats de classes de A i A' seran, necessàriament, iguals.

II. Com que la quantitat de totes les classes ambigües és igual a la quantitat de gèneres (articles 261, 287, III), és evident que si en G es donés només una classe ambigua, en *qualsevol* gènere hi hauria d'haver continguda una classe ambigua; si, en G, n'existeixen dues d'ambigües, en la meitat de tots els gèneres se'n donaran dues, i en els restants, cap; finalment, si en G es contenen més ambigües, posem a,* la a-èsima part de tots els gèneres conté a classes ambigües, les restants, cap.

III. En el cas en què G conté dues classes ambigües, siguin G, G', G'', etc., els gèneres que en contenen dues, i H, H', H'', etc., els que [no en contenen] cap, i es designa el complex d'aquelles per $\mathfrak{G}$, el complex d'aquestes per $\mathfrak{H}$. Com que de la composició de dues classes ambigües sempre prové una classe ambigua (article 249),

* Això només pot succeir per a determinants irregulars, i a serà sempre una potència de 2.

es copsarà sense cap dificultat que de la composició de dos gèneres de $\mathfrak{G}$ sempre es produeix un gènere de $\mathfrak{G}$. A més a més, d'aquí se segueix que de la composició d'un gènere de $\mathfrak{G}$ amb un gènere de $\mathfrak{H}$ es produeix un gènere de $\mathfrak{H}$; en efecte, si, per exemple, $G' + H$ no pertanyés a $\mathfrak{H}$ sinó a $\mathfrak{G}$, també s'hauria de dur $G' + H + G'$ a $\mathfrak{G}$, *Q. E. A.*, ja que $G' + G' = G$, de manera que $G' + H + G' = H$. Finalment, s'entén facilíssimament que els gèneres $G + H$, $G' + H$, $G'' + H$, etc., junt amb els $H + H$, $H' + H$, $H'' + H$, etc., seran tots diferents, de manera que, presos simultàniament, idèntics als $\mathfrak{G}$ i $\mathfrak{H}$; però, pel que s'ha demostrat fa un instant, tots els gèneres $G + H$, $G' + H$, $G'' + H$, etc., pertanyen a $\mathfrak{H}$, de manera que exhaureixen aquest complex; per tant, els restants, $H + H$, $H' + H$, $H'' + H$, etc., pertanyeran tots necessàriament a $\mathfrak{G}$; *és a dir*, de la composició de dos gèneres de $\mathfrak{H}$ sempre s'origina un gènere de $\mathfrak{G}$.

IV. Si E és una classe d'un gènere V diferent del principal G, és clar que $2E$, $4E$, $6E$, etc., pertanyen totes a G; però les $3E$, $5E$, $7E$, etc., a V. Així, si el període de la classe $2E$ consta de m termes, en la sèrie E, $2E$, $3E$, etc., la classe $2mE$, i no cap altra anterior, serà, evidentment, idèntica a K, o sigui, el període de la classe E constarà de $2m$ termes. D'aquí, la quantitat de termes en el període d'una classe qualsevol, d'un altre gènere que el principal, serà o bé $2n$ o bé una part alíquota de $2n$, on n designa la quantitat de classes de cadascun dels gèneres.

V. Sigui C una classe donada del gènere principal G; E una classe del gènere V de la duplicació de la qual s'origina C (que sempre es donarà, article 286); i

K, K', K'', etc., totes les classes ambigües (pròpiament primitives del mateix determinant); i *totes* les classes de la duplicació de les quals s'origina C seran les E $(= E + K)$, $E + K'$, $E + K''$, etc., el complex de les quals s'expressarà per Ω; la quantitat d'aquestes classes serà igual a la quantitat de classes ambigües, o sigui, a la quantitat de gèneres. És evident que de les classes de Ω en pertanyen tantes al gènere V com ambigües es donin en G; així, si es designa per a la quantitat d'aquestes, és clar que en qualsevol gènere es donen o bé a classes de Ω o bé cap. D'aquí es conclou fàcilment que, quan sigui $a = 1$, en qualsevol gènere es conté una classe de Ω; quan $a = 2$, la meitat de tots els gèneres conté dues classes de Ω, els restants, cap, i que, certament, o bé la primera meitat coincideix tota amb $\mathfrak{G}$ (en el mateix significat com més amunt, III) i la posterior amb $\mathfrak{H}$, o bé aquesta amb $\mathfrak{G}$ i aquella amb $\mathfrak{H}$. Quan a és encara més gran, les a-èsimes parts de tots els gèneres sempre inclouran classes de Ω (cadascuna a classes).

VI. Suposem, ara, que C és una classe tal, el període de la qual consti de n termes; es copsarà fàcilment, en el cas en què $a = 2$, de manera que n parell, que no pot pertànyer a G cap de Ω (en efecte, llavors una tal classe estaria continguda en el període de la classe C; així, si fos $= rC$, o sigui, $2rC = C$, seria $2r \equiv 1 \,(\text{mòd.}\, n)$, *Q. E. A.*); per la qual cosa, com que G pertany a $\mathfrak{G}$, necessàriament totes les classes de Ω estaran distribuïdes entre els gèneres $\mathfrak{H}$. D'aquí es conclou que, com que (per a un determinant regular) en G es donen en total $\phi(n)$ classes que tenen períodes de n termes, per al cas en què $a = 2$ en qualsevol gènere $\mathfrak{H}$ es troben en total $2\phi(n)$ classes els períodes de les quals són de $2n$ termes,

de manera que comprenen tant el seu gènere com el principal; però quan $a = 1$, en qualsevol gènere diferent del principal es donaran $\phi(n)$ classes d'aquest tipus.

VII. Edifiquem sobre aquestes observacions el mètode següent per a construir tan apropiadament com sigui possible el sistema de *totes* les classes pròpiament primitives per a qualsevol determinant regular donat (en efecte, hem separat completament els irregulars). S'elegeix a voluntat una classe E, el període de la qual, de $2n$ termes, de manera que comprèn tant el seu gènere, que sigui V, com el principal, G; les classes d'aquests dos gèneres es disposen de la manera com se succeeixen en aquell període. D'aquesta manera, la qüestió ja estarà acabada quan no es presentin en total més gèneres que aquests dos, o sigui, no sembli necessari afegir els restants (per exemple, per a un tal determinant negatiu en què només es donen dos gèneres positius). Però quan s'han de construir quatre o bé més gèneres, els restants es tractaran d'aquesta manera. Sigui V' algun dels restants i $V + V' = V''$, i en V' i V'' es donaran dues classes ambigües (posem, o bé una a cadascun, o bé dues en un i cap a l'altre); s'elegeix una d'aquestes a voluntat, A, i és clar fàcilment que si A es compon amb cadascuna de les classes de G i V, es produeixen $2n$ classes diferents pertanyents a V' i V'', de manera que exhaureixen completament aquests gèneres; així, aquests gèneres també es podran ordenar. Si, a part d'aquests quatre gèneres, encara en resten altres, sigui V''' un dels restants, i V^{IV}, V^{V}, V^{VI}, els gèneres que surten de la composició del gènere V''' amb V, V' i V''. Aquests quatre gèneres V''', ..., V^{VI}, contindran quatre classes ambigües, i és clar que si se n'elegeix una d'aquestes, A', i es compon amb cadascuna de les classes

de G, V, V', V'', surten totes les classes de V''', ..., V^{VI}. Si encara resten més gèneres, es continuarà de manera similar fins que s'hagin exhaurit tots. És clar que si la quantitat de tots els gèneres que cal construir és 2^μ, seran necessàries en total $\mu - 1$ classes ambigües, i que qualsevol classe d'aquests gèneres es pot produir, o bé per multiplicació de la classe E, o bé per composició d'una classe sorgida d'una tal composició amb una o més d'ambigües. Heus aquí dos exemples pels quals s'il·lustraran aquests preceptes; aquí no es pot afegir res més de l'ús de tals construccions o bé dels artificis pels quals es pot disminuir la feina.

I. Determinant -161

Quatre gèneres positius; quatre classes a cadascun

G	V
$1, 4;\ R7; R23$	$3, 4;\ N7; R23$
$(1, 0, 161) = K$	$(3, 1, 54) = E$
$(9, 1, 18) = 2E$	$(6, -1, 27) = 3E$
$(2, 1, 81) = 4E$	$(6, 1, 27) = 5E$
$(9, -1, 18) = 6E$	$(3, -1, 54) = 7E$

V'	V''
$3, 4;\ R7; N23$	$1, 4;\ N7; N23$
$(7, 0, 23) = A$	$(10, 3, 17) = A + E$
$(11, -2, 15) = A + 2E$	$(5, 2, 33) = A + 3E$
$(14, 7, 15) = A + 4E$	$(5, -2, 33) = A + 5E$
$(11, 2, 15) = A + 6E$	$(10, -3, 17) = A + 7E$

II. Determinant −546
Vuit gèneres positius; tres classes a cadascun

G	V
$1\,i\,3,8;\ R3;R7;\ R13$	$5\,i\,7,8;\ N3;N7;\ N13$
$(1,0,546) = K$	$(5,2,110) = E$
$(22,-2,25) = 2E$	$(21,0,26) = 3E$
$(22,2,25) = 4E$	$(10,-2,110) = 5E$

V'	V''
$1\,i\,3,8;\ N3;R7;\ N13$	$5\,i\,7,8;\ R3;N7;\ R13$
$(2,0,273) = A$	$(10,2,55) = A+E$
$(11,-2,50) = A+2E$	$(13,0,42) = A+3E$
$(11,2,50) = A+4E$	$(10,-2,55) = A+5E$

V'''	V^{IV}
$1\,i\,3,8;\ N3;N7;\ R13$	$5\,i\,7,8;\ R3;R7;\ N13$
$(3,0,182) = A'$	$(15,-3,37) = A'+E$
$(17,7,35) = A'+2E$	$(7,0,78) = A'+3E$
$(17,-7,35) = A'+4E$	$(15,3,37) = A'+5E$

V^{V}	V^{VI}
$1\,i\,3,8;\ R3;N7;\ N13$	$5\,i\,7,8;\ N3;R7;\ R13$
$(6,0,91) = A+A'$	$(23,11,29) = A+A'+E$
$(19,9,33) = A+A'+2E$	$(14,0,39) = A+A'+3E$
$(19,-9,33) = A+A'+4E$	$(-23,11,29) = A+A'+5E$

Secció Sisena

APLICACIONS DIVERSES
DE LES DISQUISICIONS PRECEDENTS

308. Ja hem indicat de passada en molts llocs com és de fèrtil l'aritmètica superior per a veritats que també presten el seu ús en altres branques de la matemàtica; però hem valorat no inútil tractar separadament algunes aplicacions, que es mereixen una exposició més àmplia, no tant per a exhaurir aquest argument, que podria omplir fàcilment molts volums, sinó perquè més aviat s'il·lustrarà amb alguns models. Certament, en aquesta secció tractarem, primer, de la descomposició de fraccions en més simples; de seguida, de la conversió de fraccions comunes en decimals; després, explicarem un nou mètode d'exclusió que servirà per a la resolució d'equacions indeterminades de segon grau; finalment, transmetrem nous mètodes ràpids per a distingir nombres primers de compostos i per a explorar els factors d'aquests. A la secció següent, però, establirem fins a quin punt la teoria general d'un gènere peculiar de

funcions, amplíssimament patent per tota l'anàlisi, està connectada estretíssimament amb l'aritmètica superior, i estudiarem principalment engrandir amb nous increments la teoria de les seccions del cercle, de la qual fins ara només s'han donat a conèixer els primers elements.

309. PROBLEMA. *Descompondre la fracció* $\frac{m}{n}$*, el denominador de la qual,* n*, és el producte de dos nombres primers entre si* a*,* b*, en dues altres els denominadors de les quals siguin* a*,* b*.*

Solució. Siguin $\frac{x}{a}$, $\frac{y}{b}$, les fraccions cercades, i haurà de resultar $bx + ay = m$; d'aquí, x serà una arrel de la congruència $bx \equiv m \,(\text{mòd.}\, a)$, que es podrà trobar per la secció II; y, però, resultarà $= \frac{m - bx}{a}$.

D'altra banda, se sap que la congruència $bx \equiv m$ té infinites arrels, encara que còngrues segons a, però se'n donarà només una única de positiva i menor que a; també pot resultar, en canvi, que y surti negativa. A penes serà necessari recordar que y també es pot trobar per la congruència $ay \equiv m \,(\text{mòd.}\, b)$, i x per l'equació $x = \frac{m - ay}{b}$. Per exemple, proposada la fracció $\frac{58}{77}$, el valor de l'expressió $\frac{58}{11} \,(\text{mòd.}\, 7)$ serà 4, d'on $\frac{58}{77}$ es descompon en $\frac{4}{7} + \frac{2}{11}$.

310. Si es proposa una fracció $\frac{m}{n}$, el denominador de la qual, n, és el producte de factors qualssevol primers entre si a, b, c, d, etc., primer, per l'article precedent, es pot descompondre en dues els denominadors de les quals

siguin a, $bcd\,etc.$; la segona, de nou, en dues de denominadors b, $cd\,etc.$; la darrera, novament, en dues, i així successivament, d'on, finalment, la fracció proposada es reduirà a la forma $\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + etc.$ Evidentment, els numeradors α, β, γ, δ, etc., es podran agafar positius i menors que els seus denominadors, excepte l'últim, el qual, determinats els restants, ja no és arbitrari i també pot resultar negatiu o bé més gran que el denominador (sempre que no suposem $m < n$). Llavors, sovint serà convenient reduir-lo a la forma $\frac{\varepsilon}{e} \mp k$, de manera que ε sigui positiu i menor que e, però k enter. Finalment, és clar que a, b, c, etc., es poden agafar de manera que siguin o bé nombres primers o bé potències de nombres primers.

Exemple. La fracció $\frac{391}{924}$, el denominador de la qual és $= 4\cdot 3\cdot 7\cdot 11$, es descompon, d'aquesta manera, en $\frac{1}{4} + \frac{40}{231}$; $\frac{40}{231}$ en $\frac{2}{3} - \frac{38}{77}$; $-\frac{38}{77}$ en $\frac{1}{7} - \frac{7}{11}$; d'on, escrivint $\frac{4}{11} - 1$ per $-\frac{7}{11}$, resulta $\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1$.

311. La fracció $\frac{m}{n}$ es pot reduir a la forma $\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + etc. \mp k$ *només d'una única manera*, de manera que α, β, etc., siguin positius i menors que a, b, etc.; això és, suposant que $\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + etc. \mp k = \frac{\alpha'}{a} + \frac{\beta'}{b} + \frac{\gamma'}{c} + etc. \mp k'$, i també α', β', etc., positius i menors que a, b, etc., serà, necessàriament, $\alpha = \alpha'$, $\beta = \beta'$, $\gamma = \gamma'$, etc., $k = k'$. En efecte, multiplicant per $n = abc\,etc.$, és clar que resulta $m \equiv \alpha bcd\,etc. \equiv \alpha' bcd\,etc.$ (mòd. a),

d'on, com que *bcd etc.* és primer amb a, necessàriament $\alpha \equiv \alpha'$, de manera que $\alpha = \alpha'$, i igualment $\beta = \beta'$, etc., d'on, també, espontàniament $k = k'$. Ara, com que és completament arbitrari de quin denominador es calculi primer el numerador, és evident que *tots* els numeradors es poden investigar així, com α a l'article precedent; posem β per la congruència $\beta acd\,etc. \equiv m\,(\text{mòd. } b)$, γ per la $\gamma abd\,etc. \equiv m\,(\text{mòd. } c)$, etc.; la suma de totes les fraccions trobades així, o bé serà igual a la proposada $\frac{m}{n}$, o bé, la diferència, un nombre enter $= k$; via per la qual, simultàniament, obtenim la confirmació del càlcul. Així, en l'exemple de l'article precedent, els valors de les expressions $\frac{391}{231}\,(\text{mòd. } 4)$, $\frac{391}{308}\,(\text{mòd. } 3)$, $\frac{391}{132}\,(\text{mòd. } 7)$, $\frac{391}{84}\,(\text{mòd. } 11)$, proporcionen immediatament els numeradors 1, 2, 1, 4, corresponents als denominadors 4, 3, 7, 11, i es troba que la suma d'aquestes fraccions supera en una unitat la proposada.

312. Definició. Si una fracció comuna es converteix a decimal, anomenem *mantissa* de la fracció la sèrie de xifres decimals* (excloent-ne el nombre enter si aquest es presenta), ja sigui finita, ja es prolongui a l'infinit, agafant l'expressió, altrament només usada en logaritmes, en un significat més ampli. Així, per exemple, la mantissa de la fracció $\frac{1}{8}$ és 125; la mantissa de la fracció $\frac{35}{16}$, 1875; la mantissa de la fracció $\frac{2}{37}$, 054054 . . . a l'infinit.

* Per abreujar, restringim la disquisició següent al sistema decimal vulgar, encara que *es podria* estendre fàcilment a qualsevol altre.

D'aquesta definició és clar a l'instant que fraccions del mateix denominador $\frac{l}{n}$, $\frac{m}{n}$, tenen les mateixes mantisses o bé diferents, segons que els numeradors l, m, siguin congrus o bé incongrus segons n. Una mantissa finita no canvia si s'afegeix a la dreta qualsevol nombre de zeros. La mantissa de la fracció $\frac{10m}{n}$ s'obté separant la primera xifra de la mantissa de la fracció $\frac{m}{n}$, i, en general, la mantissa de la fracció $\frac{10^\nu m}{n}$ es troba separant les ν xifres primeres de la mantissa de $\frac{m}{n}$. La mantissa de la fracció $\frac{1}{n}$ comença immediatament per una xifra significativa (és a dir, diferent de zero) si $n < 10$; però si $n = 10$ o bé > 10, i la quantitat de xifres de què consta és k, les $k-1$ primeres xifres de la mantissa de $\frac{1}{n}$ seran zeros, i precisament la següent, la k-èsima, serà significativa. D'aquí es dedueix fàcilment que si $\frac{l}{n}$, $\frac{m}{n}$, tenen mantisses diferents (és a dir, si l, m, són incongrus segons n), aquestes no poden coincidir, certament, en les k primeres xifres, sinó que, almenys, han de diferir en la k-èsima.

313. Problema. *Donat el denominador d'una fracció* $\frac{m}{n}$ *i les* k *primeres xifres de la seva mantissa, trobar el numerador* m*, que suposem menor que* n.

Solució. Es consideren aquelles k xifres com un nombre enter, que es multiplicarà per n, i el producte es divideix per 10^k (o sigui, se suprimeixen les k últimes xifres). Si el quocient és enter (o sigui, les xifres suprimides, zeros), aquest serà, evidentment, el nume-

rador cercat i la mantissa donada és completa; si no, el numerador cercat serà l'enter més gran més pròxim, o sigui, aquell quocient augmentat en una unitat després que s'han rebutjat les xifres decimals següents. La raó d'aquesta regla es reconeix tan fàcilment del que hem observat al final de l'article precedent, que no té necessitat d'una explicació més extensa.

Exemple. Si se sap que les dues primeres xifres de la mantissa d'una fracció, el denominador de la qual és 23, són 69, tenim el producte $23 \cdot 69 = 1587$; llençant d'aquest les dues últimes xifres i sumant la unitat, el numerador cercat surt = 16.

314. Comencem amb la consideració de les tals fraccions els denominadors de les quals són nombres primers o bé potències de nombres primers, i després d'això mostrarem com reduir les restants a aquestes. I, primer, observem immediatament que la mantissa de la fracció $\frac{a}{p^\mu}$ (el numerador de la qual, a, sempre suposem que no és divisible pel nombre primer p) és finita i consta de μ xifres, si $p = 2$ o bé $p = 5$; en el primer cas, aquesta mantissa, considerada com a nombre enter, serà $= 5^\mu a$, en el darrer, $= 2^\mu a$. Això és tan obvi que no exigeix explicació.

Però si p és un altre nombre primer, $10^r a$, per gran que s'agafi r, mai no serà divisible per p^μ, d'on se segueix espontàniament que la mantissa de la fracció $F = \frac{a}{p^\mu}$ arriba necessàriament a l'infinit. Suposem que 10^e és la potència més petita del nombre 10 que resulta còngrua a la unitat segons el mòdul p^μ (confronteu la secció III, on hem mostrat que e és, o bé igual al nombre $(p-1)p^{\mu-1}$,

o bé una part alíquota d'aquest), i es copsarà fàcilment que $10^e a$ també serà el primer nombre de la sèrie $10a$, $100a$, $1000a$, etc., que és congru a a segons el mateix mòdul. Ara, com que, per l'article 312, les mantisses de les fraccions $\frac{10a}{p^\mu}$, $\frac{100a}{p^\mu}$, ..., $\frac{10^e a}{p^\mu}$, s'originen traient de la mantissa de la fracció F la primera xifra, les dues, ..., les e primeres xifres, respectivament, és evident que en aquesta mantissa, després de les e primeres xifres, i no abans, es repetiran de nou aquestes mateixes. Podem anomenar *període* d'aquesta mantissa, o sigui, de la fracció F, aquestes e primeres xifres, de les quals, repetides infinitament, és formada la mantissa; i és clar que la magnitud del període, és a dir, la quantitat de xifres de què consta, què és $= e$, és completament independent del numerador a i es determina només pel denominador. Així, per exemple, el període de la fracció $\frac{1}{11}$ és 09; el període de la fracció $\frac{3}{7}$, 428571.*

315. Així, doncs, simultàniament que es té el període d'alguna fracció, es podrà prolongar la mantissa a tantes xifres com es vulgui. A més a més, és clar que, si fos $b \equiv 10^\lambda a \,(\text{mòd.}\, p^\mu)$, s'origina el període de la fracció $\frac{b}{p^\mu}$ si les λ primeres xifres del període de la fracció F (suposant $\lambda < e$, que és lícit) s'escriuen després de les $e - \lambda$ restants, de manera que, simultàniament amb el període de la fracció F, es tenen els períodes de totes les fraccions, els numeradors de les quals són congrus a

* El cèlebre Robertson (*Theory of circulating fractions, Philos. Trans.* 1764) indica l'inici i el final del període amb dos punts escrits sobre la primera i l'última xifres, cosa que aquí no considerem necessària.

$10a$, $100a$, $1000a$, etc., segons el denominador p^μ. Així, *per exemple*, com que $6 \equiv 3 \cdot 10^2$ (mòd. 7), el període de la fracció $\frac{6}{7}$, immediatament del període de la fracció $\frac{3}{7}$, resulta 857142.

Així, quan el nombre 10 és una arrel primitiva per al mòdul p^μ (articles 57, 89), del període de la fracció $\frac{1}{p^\mu}$ es podrà deduir directament el període de qualsevol altra fracció $\frac{m}{p^\mu}$ (el numerador de la qual, m, no és divisible per p) suprimint a l'esquerra i restituint a la dreta d'aquella tantes xifres com unitats té l'índex de m, si s'ha agafat per base el nombre 10. D'aquí, és evident per què, en aquest cas, sempre s'ha agafat per base el nombre 10 en la taula I (vegeu l'article 72).

Però quan 10 no és una arrel primitiva, del període de la fracció $\frac{1}{p^\mu}$ només es poden escindir els períodes de les fraccions els numeradors de les quals són congrus a alguna potència de 10 segons p^μ. Sigui 10^e la potència més petita de 10 còngrua a la unitat segons p^μ, $(p-1)p^{\mu-1} = ef$ i presa per base una arrel primitiva r tal que l'índex del nombre 10 resulti f (article 71). Així, en aquest sistema, els numeradors de les fraccions els períodes de les quals es poden escindir del període de la fracció $\frac{1}{p^\mu}$ tindran els índexs f, $2f$, $3f$, $\ldots$, $ef - f$; de manera similar, del període de la fracció $\frac{r}{p^\mu}$ es poden deduir els períodes de les fraccions els numeradors de les quals, $10r$, $100r$, $1000r$, etc., corresponen als índexs $f+1$, $2f+1$, $3f+1$, etc.; del període de la fracció de numerador rr (l'índex del qual és 2) es dedueixen els

períodes de les fraccions de numeradors els índexs dels quals són $f+2$, $2f+2$, $3f+2$, etc.; i, en general, del període de la fracció de numerador r^i es podran derivar els períodes de les fraccions de numeradors els índexs dels quals són $f+i$, $2f+i$, $3f+i$, etc. D'aquí es conclou fàcilment que, si només es tenen els períodes de les fraccions de numeradors $1, r, rr, r^3, \ldots, r^{f-1}$, d'això es poden deduir tots els restants per la sola transposició i l'ajut de la regla següent. Sigui $= i$ l'índex del numerador m de la fracció proposada $\frac{m}{p^\mu}$ en un sistema en el qual s'ha pres r per base (que suposem menor que $(p-1)p^{\mu-1}$); resulti (dividint per f) $i = \alpha f + \beta$ de manera que α, β, siguin enters positius (o també 0) i $\beta < f$; fet això, el període de la fracció $\frac{m}{p^\mu}$ s'originarà del període de la fracció el numerador de la qual és r^β (de manera que 1 quan $\beta = 0$) col·locant les primeres α xifres d'aquest després de les restants (de manera que retenint aquest mateix període quan $\alpha = 0$). Això mostrarà suficientment per què, en construir la taula I, hem seguit la norma explicada en l'article 72.

316. Segons aquests principis, hem construït una taula dels períodes necessaris per a tots els denominadors de la forma p^μ per sota de 1000 que, donada l'ocasió, donarem a judici públic íntegra o bé continuada més enllà. En aquest lloc, sigui suficient com a mostra la taula III, produïda només fins a 100, que a penes tindrà necessitat d'explicació. Per als denominadors on 10 és arrel primitiva, mostra els períodes de les fraccions amb numerador 1 (posem per a 7, 17, 19, 23, 29, 47, 59, 61, 97); per als restants, els f períodes corresponents als numeradors $1, r, rr, \ldots, r^{f-1}$, que es distingeixen pels nombres adscrits (0), (1), (2), etc.; per a la base

r sempre s'ha pres la mateixa arrel primitiva que en la taula I. D'aquí, doncs, el període de qualsevol fracció el denominador de la qual es contingui en aquesta taula es podrà trobar, després que s'ha calculat l'índex del numerador per la taula I, amb l'ajut dels preceptes de l'article precedent. D'altra banda, per a denominadors tan petits, podrem acabar la feina de manera igualment fàcil sense la taula I si calculem per una vulgar divisió tantes xifres inicials de la mantissa cercada com són necessàries per l'article 313, fins que es pugui distingir de totes les altres del mateix denominador (per a la taula III, no més de 2), i examinem tots els períodes corresponents al denominador donat fins que arribem a aquelles xifres inicials, les quals indicaran, sens dubte, l'inici del període; no obstant això, convé recordar que aquelles xifres també poden estar separades, de manera que la primera (o moltes) constitueixen el final d'algun període, la restant o bé les restants, el seu inici.

Exemple. Se cerca el període de la fracció $\frac{12}{19}$. Aquí, per al mòdul 19, per la taula I, es té $\operatorname{Ind} 12 = 2\operatorname{Ind} 2 + \operatorname{Ind} 3 = 39 \equiv 3\,(\text{mòd. } 18)$, (article 57); per tant, com que, per a aquest cas, només es té un únic període corresponent al numerador 1, convé canviar de lloc les seves tres primeres xifres al final, d'on resulta el període cercat 631578947368421052. S'hauria trobat de manera igualment fàcil l'inici del període de les dues primeres xifres 63.

Si es desitja el període de la fracció $\frac{45}{53}$, per al mòdul 53 resulta $\operatorname{Ind} 45 = 2\operatorname{Ind} 3 + \operatorname{Ind} 5 = 49$; aquí, la quantitat de períodes és $4 = f$, i $49 = 12f + 1$, per tant, del període indicat amb (1), les 12 primeres xifres

s'hauran de posposar a l'última, i el període cercat resulta 8490566037735. En aquest cas, les xifres inicials 84 estan separades en la taula.

Encara observarem que, amb l'ajut de la taula III, també es pot trobar un nombre que, per a un mòdul donat (contingut en aquesta amb el títol de denominador), correspongui a un índex donat, tal com hem promès en l'article 59. En efecte, del que precedeix, és clar que es pot trobar el període d'una fracció al numerador de la qual (encara que sigui desconegut) correspongui un índex donat; però és suficient extreure tantes xifres inicials d'aquest període com xifres té el denominador; d'aquestes, per l'article 313, es trobarà el numerador, o sigui, el nombre cercat corresponent a l'índex donat.

317. Pel que precedeix, la mantissa de qualsevol fracció, el denominador de la qual és un nombre primer o bé una potència d'un nombre primer dins dels límits de la taula, es pot trobar sense càlcul fins a un nombre qualsevol de xifres; però amb l'ajut de les disquisicions de l'inici d'aquesta secció, l'àmbit de la taula s'estén molt més enllà i comprèn totes les fraccions els denominadors de les quals són productes de nombres primers o bé de potències de primers dins del seu límit. En efecte, com que una tal fracció es pot descompondre en altres els denominadors de les quals siguin aquests factors, i es pot convertir aquestes en fraccions decimals fins a qualsevol nombre de xifres, només resta que aquestes es reuneixin en una suma. D'altra banda, a penes serà necessari recordar que l'última xifra de la suma produïda així pot sortir legítimament menor; però, evidentment, el defecte no pot ascendir a tantes unitats com fraccions particulars se sumen, d'on convindrà calcular aquestes

fins a algunes xifres més enllà que les que es desitja per a la fracció justa proposada. Com a exemple, considerarem la fracció $\frac{6099380351}{1271808720} = F$,* el denominador de la qual és el producte dels nombres 16, 9, 5, 49, 13, 47, 59. Pels preceptes donats més amunt, es troba $F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59}$, les fraccions particulars de la qual es converteixen en decimals així com segueix:

$$
\begin{array}{rlll}
1 &= 1 & & \\
\frac{11}{16} &= 0,6875 & & \\
\frac{4}{5} &= 0,8 & & \\
\frac{4}{9} &= 0,4444444444 & 4444444444 & 44 \\
\frac{22}{49} &= 0,4489795918 & 3673469387 & 75 \\
\frac{5}{13} &= 0,3846153846 & 1538461538 & 46 \\
\frac{7}{47} &= 0,1489361702 & 1276595744 & 68 \\
\frac{52}{59} &= 0,8813559322 & 0338983050 & 84 \\
\hline
F &= 4,7958315233 & 1271954166 & 17.
\end{array}
$$

El defecte d'aquesta suma al [valor] just és, certament, menor que cinc unitats en l'última xifra vigèsima

* Aquesta fracció és una de les que aproximen millor l'arrel quadrada de 23 i, certament, l'excés és menor que set unitats en el lloc de la vigèsima xifra decimal.

segona, per tant, les vint primeres d'aquí no es poden canviar. Portant el càlcul a més xifres, per a les dues últimes xifres, 17, surt 1893936... D'altra banda, qualsevol veurà, sense que ho advertim, que aquest mètode de convertir fraccions comunes en decimals s'acomoda particularment al cas en què es desitgen moltes xifres decimals; en efecte, quan poques són suficients, sovint es podran aplicar de manera igualment ràpida la divisió vulgar o bé els logaritmes.

318. Així, com que la descomposició de les tals fraccions, els denominadors de les quals estan compostos de molts nombres primers diferents, ja s'ha reduït al cas en què el denominador és primer o bé potència d'un primer, només afegirem poc de les seves mantisses. Si el denominador no conté els factors 2 i 5, aquí la mantissa també constarà de períodes, ja que, també per a aquest cas, en la sèrie 10, 100, 1000, etc., s'arribarà finalment a un terme congru a la unitat segons el denominador, i simultàniament l'exponent d'aquest terme, que per l'article 92 es podrà determinar fàcilment, indicarà la magnitud del període, independentment del numerador, sempre que aquest sigui primer amb el denominador. Però si el denominador és de la forma $2^\alpha 5^\beta N$, on N designa un nombre primer amb 10, α i β nombres dels quals almenys un no és 0, la mantissa de la fracció començarà a constar de períodes després de les primeres α o bé β xifres (segons que α o bé β sigui el més gran), i concordaran, respecte de la longitud, amb els períodes de les fraccions de denominador N; això es deriva facilíssimament del fet que aquella fracció és descomponible en unes altres dues de denominadors $2^\alpha 5^\beta$ i N, la primera de les quals es trencarà després de les primeres α o bé β xifres. D'altra banda, podríem afegir

moltes altres observacions d'aquest argument, sobretot sobre artificis per a construir moltíssim millor una taula tal com la III, que, per abreujar, suprimim amb molt de gust en aquest lloc, ja que molt del que pertany a això ja ha estat tractat tant pel cèlebre Robertson, al lloc citat, com pel cèlebre Bernoulli (*Nouv. Mem. de l'Ac. de Berlin* 1771).

319. De la congruència $xx \equiv A\,(\text{mòd.}\,m)$, que coincideix amb l'equació indeterminada $xx = A + my$, n'hem tractat *la possibilitat* a la secció IV (article 146) de manera que sembla que no es pot desitjar res més; però, respecte a la investigació de la seva incògnita, ja hem observat més amunt (article 152) que són preferibles en gran manera els mètodes indirectes als directes. Si m és un nombre primer (cas al qual es redueixen fàcilment els restants), podem utilitzar per a aquest fi la taula d'índexs I (combinada amb la III segons l'observació de l'article 316), com hem mostrat més generalment en l'article 60, però aquest mètode quedaria restringit dins dels límits de la taula. A causa d'aquestes raons, esperem que el mètode general següent i més ràpid no serà ingrat als amants de l'aritmètica.

Abans que tot, observem que és suficient si només es tenen els valors de x que són positius i no més grans que $\frac{1}{2}m$, ja que qualsevol altre és congru segons el mòdul m a algun d'ells pres o bé ell mateix o bé negativament; però, per a un tal valor de x, el de y estarà contingut necessàriament entre els límits $-\frac{A}{m}$ i $\frac{1}{4}m - \frac{A}{m}$. Així, el mètode que s'ofereix tot seguit consisteix en què per a cada un dels valors de y contingut entre aquests límits, el complex dels quals expressarem per Ω, es calcularà

el valor de $A + my$, que denotarem per V, i només es retindran aquells per als quals V resulta un quadrat. Quan m és un nombre petit (per exemple, per sota 40) aquesta temptativa és tan breu que a penes té necessitat de contracció; però quan m és gran, es podrà abreujar la feina tant com es vulgui pel *mètode d'exclusió* següent.

320. Sigui E un nombre enter arbitrari primer amb m i més gran que 2; a, b, c, etc., tots els seus no-residus quadràtics diferents (és a dir, incongrus segons E); finalment, α, β, γ, etc., les arrels de les congruències $A + my \equiv a$, $A + my \equiv b$, $A + my \equiv c$, etc., segons el mòdul E, que totes es podran agafar positives i menors que E. Així, si s'atribueix a y un valor congru a algun dels nombres α, β, γ, etc., segons E, el valor de $V = A + my$ originat d'això serà congru a algun dels a, b, c, etc., i, en conseqüència, no-residu de E, i, així, no podrà ser quadrat. D'aquí, és clar que es poden excloure immediatament de Ω com a inútils tots els nombres que estiguin continguts en les formes $Et+\alpha$, $Et+\beta$, $Et+\gamma$, etc., i serà suficient fer la temptativa per als restants, el complex dels quals sigui Ω'. En aquella operació es pot atribuir al nombre E el nom d'*excloent*.

Agafant per excloent, però, un altre nombre idoni E', es trobaran de manera completament similar tants nombres α', β', γ', etc., com no-residus quadràtics diferents té, als quals y no pot ser congru segons el mòdul E'. Per tant, es podran rebutjar de nou de Ω' tots els nombres continguts en les formes $E't + \alpha'$, $E't + \beta'$, $E't + \gamma'$, etc. Es podrà continuar d'aquesta manera, utilitzant sempre més i més excloents, fins que la quantitat de nombres de Ω hagi disminuït tant que no

sembli més difícil sotmetre realment a la temptativa tots els sobrevivents que fer noves exclusions.

Exemple. Proposada l'equació $xx = 22 + 97y$, els límits dels valors de y seran $-\frac{22}{97}$ i $24\frac{1}{4} - \frac{22}{97}$, d'on (com que la inutilitat del valor 0 és òbvia en si) Ω comprendrà els nombres 1, 2, 3, ..., 24. Per a $E = 3$ es té l'únic no-residu $a = 2$, d'on resulta $\alpha = 1$; així, s'han d'excloure de Ω tots els nombres de la forma $3t + 1$; la quantitat dels romanents en Ω' serà 16. De manera similar, per a $E = 4$ es té $a = 2$, $b = 3$, d'on $\alpha = 0$, $\beta = 1$; per tant, s'han de rebutjar els nombres de la forma $4t$ i $4t + 1$, i resten els vuit 2, 3, 6, 11, 14, 15, 18, 23. Igualment, per a $E = 5$ es troben rebutjables els nombres de les formes $5t$ i $5t+3$; i romanen els 2, 6, 11, 14. L'excloent 6 trauria els nombres de les formes $6t + 1$, $6t + 4$, però aquests (que coincideixen amb nombres de la forma $3t+1$) ja no hi són. L'excloent 7 rebutja els nombres de les formes $7t + 2$, $7t + 3$, $7t + 5$, i deixa els 6, 11, 14. Substituïts aquests per y, produeixen, respectivament, $V = 604$, 1089, 1380, dels quals només el segon valor és quadrat, d'on $x = \pm 33$.

321. Com que l'operació feta amb l'excloent E dels valors de V corresponents a valors de y de Ω relega tots els que són no-residus quadràtics de E, però no toca els residus del mateix nombre, s'entén fàcilment que l'ús dels excloents E i $2E$ no difereix en res, si E és imparell, ja que, en aquest cas, E i $2E$ tenen els mateixos residus i no-residus. D'aquí és clar que si s'apliquen com a excloents els successius nombres 3, 4, 5, etc., els nombres imparellament parells 6, 10, 14, etc., productes de 2 s'han d'ometre com a superflus. A més a més,

és evident que la doble operació feta amb excloents E, E' suprimeix els valors de V que són no-residus o bé d'ambdós E, E', o bé d'un, i romanen els que són residus de tots dos. Ara, com que, en el cas en què E i E' no tenen divisor comú, tots els nombres rebutjats són no-residus del producte EE', i els sobrevivents, residus, és evident que l'ús de l'excloent EE', en aquest cas, farà exactament el mateix que l'ús dels dos E, E'; de manera que aquells, després aquest, resulta superflu. Per tant, també es podran ometre tots els excloents que es poden descompondre en dos factors primers entre si, i serà suficient l'ús d'aquells que són, o bé nombres primers (no-divisors de m), o bé potències de primers. Finalment, és evident que després de l'ús de l'excloent p^μ, que és potència d'un nombre primer p, l'excloent p, o bé p^ν quan $\nu < \mu$, resulta superflu; en efecte, com que p^μ, entre els valors de V, deixa només els seus residus, amb més raó no es presentaran més no-residus de p o bé de qualsevol potència inferior p^ν. Però, si p o bé p^ν ja s'ha aplicat abans que p^μ, aquest, evidentment, només podrà rebutjar valors de V tals que, simultàniament, són residus de p (o de p^ν) i no-residus de p^μ; per tant, serà suficient agafar per a a, b, c, etc., només no-residus de p^μ d'aquest tipus.

322. El càlcul dels nombres α, β, γ, etc., corresponents a qualsevol excloent donat E es redueix per les observacions següents. Siguin $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., les arrels de les congruències $my \equiv a$, $my \equiv b$, $my \equiv c$, etc. (mòd. E) i k una arrel de $my \equiv -A$, i és clar que resulta $\alpha \equiv \mathfrak{A} + k$, $\beta \equiv \mathfrak{B} + k$, $\gamma \equiv \mathfrak{C} + k$, etc. Ara, si convingués trobar $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., realment per resolució d'aquelles congruències, aquesta via per a trobar els α, β, γ, etc., no seria gens més breu que aquella que hem

mostrat més amunt; però allò no és necessari de cap manera. En efecte, si, primer, E és un nombre primer i m un residu quadràtic de E, és clar per l'article 98 que els $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., que són valors de les expressions $\frac{a}{m}$, $\frac{b}{m}$, $\frac{c}{m}$, etc., (mòd. E), resulten no-residus diferents de E, de manera que coincideixen completament amb els α, β, γ, etc., fent abstracció del seu ordre, que aquí no comporta res; però si, amb la mateixa suposició, m és no-residu de E, els nombres $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., coincidiran amb tots els residus quadràtics, deixat de banda 0. Si E és el quadrat d'un nombre primer (imparell), $= pp$, i p ja s'ha aplicat com a excloent, és suficient, per l'article precedent, prendre per a a, b, c, etc., aquells no-residus de pp que són residus de p, és a dir, els nombres p, $2p$, $3p$, $\ldots$, $pp - p$ (això és, tots els nombres per sota de pp, excepte 0, que són divisibles per p); però, d'aquí, es copsa fàcilment que, per a $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., han d'aparèixer completament els mateixos nombres només disposats altrament. Similarment, si després de l'aplicació dels excloents p i pp es posa $E = p^3$, serà suficient d'agafar per a a, b, c, etc., els productes de cadascun dels no-residus de p per pp, d'on, per a $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., apareixeran o bé els mateixos nombres, o bé els productes de pp per cadascun dels residus de p excepte 0, segons si m és residu o no-residu de p. En general, agafant per a E qualsevol potència d'un nombre primer, posem p^μ, ja aplicades totes les inferiors, per a $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., apareixeran els productes de $p^{\mu-1}$, o bé per tots els nombres més petits que p, sempre exceptuat 0, quan μ és parell, o bé per tots els no-residus de p menors que p quan μ és imparell i mRp, o bé per tots els residus quan mNp. Si $E = 4$, de manera que $a = 2$, $b = 3$, per a $\mathfrak{A}$, $\mathfrak{B}$, tenim o bé 2 i 3 o bé 2 i 1 segons que $m \equiv 1$ o bé $\equiv 3$ (mòd. 4). Si

després de l'ús de l'excloent 4 s'estableix $E = 8$, tenim $\alpha = 5$, d'on $\mathfrak{A}$ resulta 5, 7, 1, 3, segons que $m \equiv 1, 3, 5, 7 \pmod 8$. En general, però, si E és qualsevol potència més alta de 2, posem 2^μ, ja aplicades les inferiors, s'ha de posar $a = 2^{\mu-1}$, $b = 3 \cdot 2^{\mu-2}$, quan μ és parell, d'on resulta $\mathfrak{A} = 2^{\mu-1}$, $\mathfrak{B} = 3 \cdot 2^{\mu-2}$ o bé $= 2^{\mu-2}$, segons que $m \equiv 1$ o bé $\equiv 3$; però quan μ és imparell, cal posar $a = 5 \cdot 2^{\mu-3}$, d'on $\mathfrak{A}$ resulta igual al producte del nombre $2^{\mu-3}$ per 5, 7, 1, o bé 3 segons que $m \equiv 1, 3, 5$, o bé $7 \pmod 8$.

D'altra banda, els experts s'imaginaran fàcilment un aparell pel qual es puguin rebutjar *mecànicament* de Ω els valors inútils de y, després que s'hagin calculat els nombres α, β, γ, etc., per a tants excloents com sembli necessari; però no es pot tractar aquí d'això ni d'altres artificis per a reduir la feina.

323. A la secció V, hem ensenyat a trobar amb un mètode general, la brevetat del qual també sembla que no deixa res a desitjar, totes les representacions d'un nombre donat A per una forma binària $mxx + nyy$, o sigui, les solucions de l'equació indeterminada $mxx + nyy = A$, si ja es tenen tots els valors de l'expressió $\sqrt{-mn}$ segons el mòdul A mateix, i dividit pels seus factors quadrats; però aquí, per al cas en què mn és positiu, explicarem una solució, molt més ràpida que la directa, si abans convé calcular aquells valors per a aquesta. Suposarem que els nombres m, n i A són positius i primers entre si, ja que els casos restants es poden reduir fàcilment a aquest. Evidentment, també és suficient trobar els valors positius de x, y, ja que els restants es deduiran d'aquests pel sol canvi de signes.

És evident que x s'ha de disposar de manera que $\frac{A-mxx}{n}$, per al qual escriurem V, surti positiu, enter i quadrat. La primera condició requereix que x no sigui més gran que $\sqrt{\frac{A}{m}}$; la segona ja té lloc en si quan $n = 1$, altrament, requereix que el valor de l'expressió $\frac{A}{m}$ (mòd. n) sigui un residu quadràtic de n, i designant tots els valors diferents de l'expressió $\sqrt{\frac{A}{m}}$ (mòd. n) per $\pm r$, $\pm r'$, etc., x haurà d'estar contingut en alguna de les formes $nt+r$, $nt-r$, $nt+r'$, etc. Així, el més senzill seria substituir x per tots els nombres d'aquestes formes per sota del límit $\sqrt{\frac{A}{m}}$, el complex dels quals expressarem per Ω, i retenir només aquells per als quals V resulta un quadrat. En l'article següent ensenyarem a reduir aquesta temptativa tant com es vulgui.

324. El mètode d'exclusions, pel qual fem això, consisteix, igualment com en la disquisició precedent, en què agafem a voluntat molts nombres, que també cal anomenar aquí *excloents*, investiguem per a quins valors de x el valor de V resulta no-residu quadràtic d'aquests excloents, i traiem de Ω els tals x. Per raonaments completament anàlegs al que hem exposat en l'article 321, és evident que només s'han d'utilitzar excloents tals que siguin nombres primers o bé potències de nombres primers, i que, per a un excloent del gènere posterior, només s'han de rebutjar dels valors de V els seus no-residus que siguin residus de totes les potències inferiors del mateix nombre primer, sempre que ja s'hagi fet l'exclusió amb aquests.

Així, sigui l'excloent $E = p^\mu$ (incloent-hi també el cas en què $\mu = 1$), on p és un nombre primer que no divideix m, i suposem que* p^ν és la potència més gran d'aquest nombre primer per la qual n és divisible. Siguin a, b, c, etc., no-residus quadràtics de E (tots, quan $\mu = 1$, els necessaris, o sigui, els que són residus de potències inferiors, quan $\mu > 1$). Es calculen les arrels de les congruències $mz \equiv A - na$, $mz \equiv A - nb$, $mz \equiv A - nc$, etc. (mòd. $Ep^\nu = p^{\mu+\nu}$); siguin aquestes α, β, γ, etc., i és clar fàcilment que si per a algun valor de x resulta $xx \equiv \alpha$ (mòd. Ep^ν), el valor corresponent de V resultarà $\equiv a$ (mòd. E), o sigui, no-residu de E, i similarment per als nombres restants β, γ, etc.; recíprocament, es copsa de manera igualment fàcil que si algun valor de x produeix $V \equiv a$ (mòd. E), per a aquest mateix resultarà $xx \equiv \alpha$ (mòd. Ep^ν), de manera que tots els valors de x per als quals xx no és congru a cap dels nombres α, β, γ, etc., segons el mòdul Ep^ν, produeixen valors de V tals que no són congrus a cap dels nombres a, b, c, etc., segons el mòdul E. Ara, dels nombres α, β, γ, etc., s'elegeixen tots els residus quadràtics de Ep^ν; siguin aquests g, g', g'', etc., es calculen els valors de les expressions $\sqrt{g}$, $\sqrt{g'}$, $\sqrt{g''}$, etc. (mòd. Ep^ν), i suposem que d'aquí apareixen $\pm h$, $\pm h'$, $\pm h''$, etc. Fet això així, és evident que tots els nombres de les formes $Ep^\nu t \pm h$, $Ep^\nu t \pm h'$, $Ep^\nu t \pm h''$, etc., es poden treure de Ω sense perill, i cap dels valors de x que romanen a Ω després d'aquesta exclusió no pot correspondre a un valor de V contingut en les formes $Eu + a$, $Eu + b$, $Eu + c$, etc. D'altra banda, és evident en si que tals valors de V ja no poden sortir de cap valor de x, quan entre els nombres

* Per abreujar, apleguem simultàniament els dos casos en què n és divisible per p, o no divisible; en el darrer, convé posar $\nu = 0$.

α, β, γ, etc., no es troba cap residu quadràtic de Ep^ν, de manera que, en aquest cas, el nombre E no es pot aplicar com a excloent. Es poden aplicar tants excloents d'aquest tipus com plagui i, així, disminuir a voluntat els nombres en Ω.

Vegem, ara, si també es poden aplicar o no com a excloents nombres primers que divideixin m, o bé potències de tals nombres. Sigui B el valor de l'expressió $\frac{A}{n}$ (mòd. m), i és clar que V sempre resultarà congru a B segons el mòdul m, qualsevol valor que s'agafi per a x, de manera que per a la possibilitat de l'equació proposada es requereix necessàriament que B sigui residu quadràtic de m. Així, si p designa qualsevol divisor primer imparell de m que, per hipòtesi, no divideix n ni A, de manera que tampoc B, per a qualsevol valor de x V serà residu de p, de manera que també de qualsevol potència de p; per la qual cosa, p i les seves potències no poden tenir lloc com a excloents. Per una raó completament similar, quan m és divisible per 8, per a la possibilitat de l'equació proposada es requereix necessàriament que sigui $B \equiv 1$ (mòd. 8), d'on també V per a qualsevol valor de x resultarà $\equiv 1$ (mòd. 8) i, en conseqüència, les potències binàries no són idònies per a l'exclusió. Però quan m és divisible per 4 però no per 8, per una raó similar, haurà de ser $B \equiv 1$ (mòd. 4), de manera que el valor de l'expressió $\frac{A}{n}$ (mòd. 8), o bé 1 o bé 5, es designarà per C. Es copsarà sense cap dificultat que per a un valor parell de x aquí resulta $V \equiv C$; per a un imparell, $V \equiv C+4$ (mòd. 8); d'on és clar que s'han de rebutjar els valors parells quan $C = 5$, els imparells quan $C = 1$. Finalment, quan m és divisible per 2 però no per 4, sigui,

com abans, C el valor de l'expressió $\frac{A}{n}$ (mòd. 8), que serà 1, 3, 5, o bé 7; i D el valor de la $\frac{\frac{1}{2}m}{n}$ (mòd. 4), que serà 1 o bé 3. Ara, com que, evidentment, el valor de V sempre resulta $\equiv C - 2Dxx$ (mòd. 8), de manera que per a x parell, $\equiv C$, per a imparell, $\equiv C - 2D$, d'aquí es conclou fàcilment que s'han de rebutjar tots els valors imparells de x quan $C = 1$, tots els parells quan $C = 3$ i $D = 1$ o bé $C = 7$ i $D = 3$; i tots els valors romanents produeixen $V \equiv 1$ (mòd. 8), o sigui, residu de qualsevol potència binària; en els casos restants, però, posem quan $C = 5$, o bé $C = 3$ i $D = 3$, o bé $C = 7$ i $D = 1$, resultarà $V \equiv 3$, 5, o bé 7 (mòd. 8), tant si s'agafa x parell com imparell, d'on és clar que, en aquests casos, l'equació proposada no admet cap solució en absolut.

D'altra banda, com que, també, canviat el que cal canviar, podríem elegir el valor de y de manera completament similar a com aquí hem ensenyat a trobar el valor de x per exclusions, el mètode d'exclusió es podrà aplicar per a la solució del problema proposat sempre de dues maneres (llevat que $m = n = 1$, on coincideixen), de les quals sovint s'ha de preferir aquella per a la qual Ω conté una quantitat menor de termes, cosa que es podrà estimar fàcilment *a priori*. Finalment, a penes serà necessari observar que, si després d'algunes exclusions, *tots* els nombres han desaparegut de Ω, s'ha de considerar això com un indici cert de la impossibilitat de l'equació proposada.

325. *Exemple.* Sigui proposada l'equació $3xx + 455yy = 10857362$, que resoldrem de dues maneres, primer, investigant els valors de x, després, els valors

de y. En aquest cas, el límit d'aquells és $\sqrt{3619120\frac{2}{3}}$, que cau entre 1902 i 1903; el valor de l'expressió $\frac{A}{3}$ (mòd. 455) és 354, i ± 82, ± 152, ± 173, ± 212, els valors de l'expressió $\sqrt{354}$ (mòd. 455). D'aquí, Ω consta dels 33 nombres següents: 82, 152, 173, 212, 243, 282, 303, 373, 537, 607, 628, 667, 698, 737, 758, 828, 992, 1062, 1083, 1122, 1153, 1192, 1213, 1283, 1447, 1517, 1538, 1577, 1608, 1647, 1668, 1738, 1902. En aquest cas, el nombre 3 no es pot utilitzar per a l'exclusió, ja que divideix m. Per a l'excloent 4 tenim $a = 2$, $b = 3$, d'on $\alpha = 0$, $\beta = 3$; $g = 0$, i els valors de l'expressió $\sqrt{g}$ (mòd. 4), els 0 i 2; d'aquí se segueix que tots els nombres de les formes $4t$ i $4t + 2$, és a dir, tots els parells, s'han de suprimir de Ω; es designen els (setze) restants per Ω'. Per a $E = 5$, que també divideix n, tenim les arrels de les congruències $mz \equiv A - 2n$ i $mz \equiv A - 3n$ (mòd. 25), 9 i 24, que ambdós són residus de 25, i els valors de les expressions $\sqrt{9}$, $\sqrt{24}$ (mòd. 25) resulten ± 3, ± 7; suprimits de Ω' tots els nombres de les formes $25t \pm 3$, $25t \pm 7$ queden aquests deu (Ω''): 173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577. Per a $E = 7$ de les congruències $mz \equiv A - 3n$, $mz \equiv A - 5n$, $mz \equiv A - 6n$ (mòd. 49) tenim les arrels 32, 39, 18, totes les quals són residus de 49, i els valors de les expressions $\sqrt{32}$, $\sqrt{39}$, $\sqrt{18}$ (mòd. 49), els ± 9, ± 23, ± 19; suprimits de Ω'' els nombres de les formes $49t \pm 9$, $49t \pm 19$, $49t \pm 23$, romanen aquests cinc (Ω'''): 537, 737, 1083, 1213, 1517. Per a $E = 8$ tenim $a = 5$, d'on $\alpha = 5$, que és no-residu de 8; per tant, l'excloent 8 no es pot utilitzar. El nombre 9 s'ha de desestimar per la mateixa raó que el 3. Per a $E = 11$, els nombres a, b, etc., resulten 2, 6, 7, 8, 10; $\nu = 0$; d'on els nombres α, β, etc. = 8, 10, 5, 0, 1, dels quals tres són residus de 11,

posem 0, 1, 5; d'aquí es dedueix que s'han de rebutjar de Ω''' els nombres de les formes $11t$, $11t \pm 1$, $11t \pm 4$; fet això, romanen 537, 1083, 1213. Provant aquests, surten per a V els valors 21961, 16129, 14161, respectivament, dels quals només són quadrats el segon i el tercer. Per tant, l'equació proposada admet dues solucions per valors positius de x, y, $x = 1083$, $y = 127$, i $x = 1213$, $y = 119$.

II. Si plau indagar per exclusions l'altra incògnita de la mateixa equació, es posa aquesta en la forma $455xx + 3yy = 10857362$, commutant x amb y, perquè es puguin retenir tots els signes dels articles 323, 324. Aquí, el límit dels valors de x cau entre 154 i 155; el valor de l'expressió $\frac{A}{m}\,(\text{mòd.}\, n)$ és 1; els valors de la $\sqrt{1}\,(\text{mòd.}\, 3)$ són $+1$ i -1. Per tant, Ω conté tots els nombres de les formes $3t + 1$, $3t - 1$, és a dir, tots els no divisibles per 3 fins al 154, inclusivament, la quantitat dels quals és 103; aplicant, però, els preceptes donats més amunt, es troba que

per a l'excloent	s'han de rebutjar els nombres de les formes
3	$9t \pm 4$
4	$4t, 4t + 2$ o sigui, tots els parells
9	$27t \pm 1, 27t \pm 10$
11	$11t, 11t \pm 1, 11t \pm 3$
17	$17t \pm 3, 17t \pm 4, 17t \pm 5, 17t \pm 7$
19	$19t \pm 2, 19t \pm 3, 19t \pm 8, 19t \pm 9$
23	$23t, 23t \pm 5, 23t \pm 7, 23t \pm 9, 23t \pm 10$.

Esborrats aquests, es troben els sobrevivents 119, 127, 137, dels quals només els dos primers proporcionen a V un valor quadrat, i suggereixen les mateixes solucions a les quals hem arribat més amunt.

326. El mètode precedent ja és tan ràpid en si que a penes queda quelcom per desitjar; no obstant això, encara es pot reduir en gran manera per multitud d'artificis, dels quals aquí només se'n poden considerar pocs. Així, restringirem la disquisició al cas en què l'excloent és un nombre primer imparell que no divideix A, o bé una potència d'un tal primer, sobretot, perquè els casos restants es poden o bé reduir a aquest o bé tractar per un mètode anàleg. Suposant, *primer*, que l'excloent $E = p$ és un nombre primer que no divideix m, n, i els valors de les expressions $\frac{A}{m}$, $-\frac{na}{m}$, $-\frac{nb}{m}$, $-\frac{nc}{m}$, etc. (mòd. p), respectivament, k, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., els nombres α, β, γ, etc., es troben per les congruències $\alpha \equiv k + \mathfrak{A}$, $\beta \equiv k + \mathfrak{B}$, $\gamma \equiv k + \mathfrak{C}$, etc. (mòd. p). Però els nombres $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. es poden descobrir sense el càlcul de les congruències per un artifici completament similar al que hem utilitzat en l'article 322, i coincidiran o bé amb tots els no-residus o bé amb tots els residus de p (excepte 0), segons si el valor de l'expressió $-\frac{m}{n}$ (mòd. p), o sigui (el que aquí rendeix el mateix), el nombre $-mn$, és residu o bé no-residu de p. Així, en l'exemple II de l'article precedent, per a $E = 17$ resulta $k = 7$; $-mn = -1365 \equiv 12$ és no-residu de 17; d'aquí, els nombres $\mathfrak{A}$, $\mathfrak{B}$, etc., seran 1, 2, 4, 8, 9, 13, 15, 16, de manera que els nombres α, β, etc., 8, 9, 11, 15, 16, 3, 5, 6; d'aquests, 8, 9, 15, 16, són residus, d'on $\pm h$, h', etc., resulten ± 5, 3, 7, 4. Per als que tenen molt sovint l'ocasió de resoldre problemes d'aquest tipus, miraran més per la seva comoditat si calculen per a molts nombres primers p els valors de h, h', etc., corresponents a cadascun dels valors de k (1, 2, 3, ..., $p - 1$) amb la doble suposició (posem, on $-mn$ és residu i on

no-residu de p). D'altra banda, encara observem que la quantitat de nombres h, $-h$, h', etc., sempre és $\frac{1}{2}(p-1)$ quan cada un dels nombres k i $-mn$ és residu o bé cada un no-residu de p; $\frac{1}{2}(p-3)$ quan el primer, residu, el darrer, no-residu; $\frac{1}{2}(p+1)$ quan el primer, no-residu, el darrer, residu; però hem de suprimir la demostració d'aquest teorema perquè no resultem massa prolixos.

Però, *segon*, pel que fa als casos en què E és un nombre primer que divideix n, o bé una potència d'un nombre primer (imparell) que divideix o bé no divideix n, aquests encara es poden tractar més ràpidament. Aplegarem simultàniament tots aquests casos i, retinguts els signes de l'article 324, posarem $n = n'p^\nu$, de manera que n' no sigui divisible per p. Els nombres a, b, c, etc., seran els productes del nombre $p^{\mu-1}$ o bé per tots els nombres menors que p (excepte 0) o bé per tots els no-residus de p per sota de p, segons si μ és parell o bé imparell; s'expressaran formalment per $up^{\mu-1}$. Sigui k el valor de l'expressió $\frac{A}{m}\,(\text{mòd.}\,p^{\mu+\nu})$, i serà no divisible per p, ja que se suposa la mateixa propietat per a A; a més a més, és clar que tots els α, β, γ, etc., resultaran congrus a k segons el mòdul p, de manera que p^μ no exclou res de Ω si kNp; però si kRp, de manera que també $kRp^{\mu+\nu}$, sigui r un valor de l'expressió $\sqrt{k}\,(\text{mòd.}\,p^{\mu+\nu})$, que no serà divisible per p, i e el valor de la $-\frac{n'}{2mr}\,(\text{mòd.}\,p)$, i serà $\alpha \equiv rr + 2erap^\nu\,(\text{mòd.}\,p^{\mu+\nu})$, d'on es conclou fàcilment que α és residu de $p^{\mu+\nu}$, i els valors de l'expressió $\sqrt{\alpha}\,(\text{mòd.}\,p^{\mu+\nu})$ resultaran $\pm(r + eap^\nu)$; d'aquí, tots els h, h', h'', etc.,

s'expressaran per $r + uep^{\mu+\nu-1}$. Finalment, d'aquí es conclou sense cap dificultat que els nombres h, h', h'', etc., s'originen de la suma del nombre r amb els productes del nombre $p^{\mu+\nu-1}$, *o bé* per tots els nombres per sota de p (excepte 0), quan μ és parell, *o bé* per tots els no-residus de p per sota d'aquest límit, quan μ és imparell i eRp, o sigui, el que aquí rendeix el mateix, quan $-2mrn'Rp$; *o bé* per tots els residus (excepte 0) quan μ és imparell i $-2mrn'Np$.

D'altra banda, al mateix temps que s'han descobert els nombres h, h', etc., per a cadascun dels excloents que plau aplicar, també es podrà fer la mateixa exclusió per operacions mecàniques, les quals cada expert en aquestes coses podrà desenvolupar fàcilment amb el seu propi esforç si li sembla que val la pena.

Finalment, hem d'observar que qualsevol equació $axx + 2bxy + cyy = M$, en la qual $bb - ac$ és negatiu $= -D$, es pot reduir fàcilment a la forma que hem considerat en els [articles] precedents. En efecte, designant per m el màxim comú divisor dels nombres a, b i posant $a = ma'$, $b = mb'$, $\dfrac{D}{m} = a'c - mb'b' = n$, $a'x + b'y = x'$, aquella equació equival evidentment a la $mx'x' + nyy = a'M$, que es podrà resoldre pels preceptes transmesos més amunt. Però de les seves solucions només s'hauran de retenir aquelles en què $x' - b'y$ resulta divisible per a', o sigui, on x obté valors enters.

327. De la mateixa manera que la solució directa de l'equació $axx+2bxy+cyy = M$ continguda en la secció V suposa coneguts els valors de l'expressió $\sqrt{bb - ac}$ (mòd. M), així, recíprocament, en el cas en què $bb -$

ac és negatiu, la solució indirecta exposada en el que precedeix subministra un mètode rapidíssim per a trobar aquells valors, el qual, sobretot per a un valor molt gran de M, s'ha de preferir, de bon tros, al mètode de l'article 322 i següents. Suposem, però, que M és un nombre primer, o almenys, si fos compost, els seus factors encara desconeguts; en efecte, si se sabés que un nombre primer p divideix M, i si és $M = p^\mu M'$, de manera que M' no implica més el factor p, seria molt més còmode explorar els valors de l'expressió $\sqrt{bb - ac}$ per als mòduls p^μ i M' separadament (els primers, dels valors segons el mòdul p, article 101), i deduir els valors segons el mòdul M de la combinació d'aquests (article 105).

Així, siguin els que s'han de cercar tots els valors de l'expressió $\sqrt{-D}\,(\text{mòd.}\,M)$, on D i M se suposen positius, i M contingut en una forma dels divisors de $xx + D$ (article 147 i següents); en efecte, altrament, se sabria *a priori* que cap nombre no pot satisfer l'expressió proposada. Siguin els valors buscats, els quals sempre seran oposats a parelles, $\pm r$, $\pm r'$, $\pm r''$, etc., i $D + rr = Mh$, $D + r'r' = Mh'$, $D + r''r'' = Mh''$, etc.; a més a més, es designen per $\mathfrak{C}$, $-\mathfrak{C}$, $\mathfrak{C}'$, $-\mathfrak{C}'$, $\mathfrak{C}''$, $-\mathfrak{C}''$, etc., respectivament, les classes a què pertanyen les formes (M, r, h), $(M, -r, h)$, (M, r', h'), $(M, -r', h')$, (M, r'', h''), $(M, -r'', h'')$, etc., i el seu complex per $\mathfrak{G}$. Parlant en general, aquestes classes s'han de mirar, certament, com a incògnites; no obstant això, és evident, *primer*, que totes són positives i pròpiament primitives; *segon*, que totes pertanyen al mateix gènere, el *caràcter* del qual es podria conèixer fàcilment de l'índole del nombre M, és a dir, de les seves relacions amb cadascun dels divisors primers de D (i, a sobre, amb 4 i 8 quan aquestes són necessàries) (article 230). Com que s'ha

suposat que M es conté en una forma dels divisors de $xx + D$, podem estar segurs *a priori* que a aquest caràcter correspon necessàriament un gènere positiu pròpiament primitiu de formes de determinant $-D$, encara que potser pot no satisfer l'expressió $\sqrt{-D}\,(\text{mòd. } M)$; així, com que aquest gènere és conegut, es podran trobar totes les classes contingudes en ell; siguin aquestes C, C', C'', etc., i el seu complex G. Així, doncs, és clar que cadascuna de les classes $\mathfrak{C}$, $-\mathfrak{C}$, etc., ha de ser idèntica a alguna classe de G; també pot resultar que moltes classes de $\mathfrak{G}$ siguin idèntiques entre elles, de manera que a la mateixa de G, i quan G conté una única classe, certament totes les de $\mathfrak{G}$ coincidiran amb aquesta. Per tant, si de les classes C, C', C'', etc., s'elegeixen les formes (més simples) f, f', f'', etc. (una de cadascuna), de cada una de les classes de $\mathfrak{G}$ es trobarà una forma entre aquestes. Ara, si $axx + 2bxy + cyy$ és una forma continguda en la classe $\mathfrak{C}$, es donaran dues representacions del nombre M per ella pertanyents al valor r, i si una és $x = m$, $y = n$, l'altra serà $x = -m$, $y = -n$; s'ha d'exceptuar un únic cas, on $D = 1$, en el qual es donaran quatre representacions (vegeu l'article 180).

D'aquí es conclou que si s'investiguen totes les representacions del nombre M per cadascuna de les formes f, f', f'', etc. (pel mètode indirecte transmès en el que precedeix), i es dedueixen d'aquí els valors de l'expressió $\sqrt{-D}\,(\text{mòd. } M)$ a què pertany cadascuna (article 154 i següents), d'això s'obtenen *tots* els valors d'aquesta expressió, i, certament, cadascun d'ells dues vegades, o bé quatre, si $D = 1$. *Q. E. F.* Si es troben algunes formes entre les f, f', etc., per les quals no es pot representar M, això és un indici que aquestes no pertanyen a cap classe de $\mathfrak{G}$, de manera que han de ser negligides; però

si M no es pot representar per cap d'aquelles formes, $-D$ haurà de ser, necessàriament, no-residu quadràtic de M. Sobre aquestes operacions es tenen encara les observacions següents.

I. Les representacions del nombre M per les formes f, f', etc., que aquí apliquem, s'entén que són les tals en què els valors de les indeterminades són primers entre si; si se'n presenten algunes altres en què aquests valors tenen un divisor comú μ (cosa que, llavors, només pot succeir si $\mu\mu$ divideix M, i succeirà certament quan $-DR\frac{M}{\mu\mu}$), per al propòsit present s'han de negligir completament, encara que respecte a un altre puguin ser útils.

II. Amb les altres [hipòtesis] iguals, la feina serà evidentment més fàcil com menor sigui la quantitat de classes f, f', etc., de manera que tan breu com [sigui] possible quan D és un dels 65 nombres transmesos en l'article 303, per als quals només es dóna una única classe en cada gènere.

III. Com que dues representacions del tipus $x = m$, $y = n$; $x = -m$, $y = -n$ sempre pertanyen al mateix valor, és evident que és suficient si només es consideren les representacions en les quals y és positiu. Així, *les tals* representacions diferents sempre corresponen a valors diferents de l'expressió $\sqrt{-D}\,(\text{mòd.}\,M)$, d'on la quantitat de tots els valors diferents serà igual a la quantitat que apareix de totes les tals representacions (exceptuant sempre el cas $D = 1$, en què aquella serà la meitat d'aquesta).

IV. Com que al mateix temps que és conegut un dels dos valors oposats $+r$, $-r$, es distingeix espontàniament l'altre, les operacions encara es poden abreujar bastant. Si el valor de r s'obté d'una representació del nombre M per una forma continguda en la classe C, és a dir, si $\mathfrak{C} = C$, el valor oposat $-r$ sorgirà, evidentment, d'una representació per una forma continguda en la classe oposada a C, que serà diferent de la classe C, llevat que aquesta sigui ambigua. D'aquí se segueix que, quan no totes les classes de G siguin ambigües, només convé considerar la meitat de les restants, posem una de cada parella d'oposades, negligint l'altra, de la qual ara es pot preveure sense càlcul que els seus valors resulten oposats als que ha proporcionat la primera. Però quan C és ambigua, ambdós valors r i $-r$ sorgiran simultàniament d'això; posem, si s'ha elegit de C la forma ambigua $axx + 2bxy + cyy$ i de la representació $x = m$, $y = n$ ha sortit el valor r, el valor $-r$ sortirà de la $x = -m - \dfrac{2bn}{a}$, $y = n$.

V. Per al cas en què $D = 1$, només es dóna en total una classe, de la qual es podrà suposar que s'ha elegit la forma $xx + yy$. Si de la representació $x = m$, $y = n$, apareix el valor r, aquest mateix apareixerà de les $x = -m$, $y = -n$; $x = n$, $y = -m$; $x = -n$, $y = m$, i l'oposat, $-r$, de les $x = m$, $y = -n$; $x = -m$, $y = n$; $x = n$, $y = m$; $x = -n$, $y = -m$; per tant, d'aquestes vuit representacions, que constitueixen una única descomposició, és suficient una, sempre que al valor resultant d'aquí li associem l'oposat.

VI. El valor de l'expressió $\sqrt{-D}\,(\text{mòd.}\, M)$ a què pertany la representació $M = amm + 2bmn + cnn$ és,

per l'article 155, $\mu(mb + nc) - \nu(ma + nb)$, o sigui, qualsevol nombre congru a ell segons M, agafats μ, ν, de manera que resulti $\mu m + \nu n = 1$. Així, designant el tal valor per v, serà $mv \equiv \mu m(mb + nc) - \nu(M - mnb - nnc) \equiv (\mu m + \nu n)(mb + nc) \equiv mb + nc$ (mòd. 4). D'aquí és clar que v és el valor de l'expressió $\frac{mb+nc}{m}$ (mòd. M); i de manera similar es troba que v és el valor de l'expressió $-\frac{ma+nb}{n}$ (mòd. M). Aquestes fórmules s'han de preferir molt sovint a aquella de la qual han estat deduïdes.

328. *Exemples.* I. Se cerquen tots els valors de l'expressió $\sqrt{-1365}$ (mòd. $5428681 = M$); el nombre M aquí és $\equiv 1, 1, 1, 6, 11$ (mòd. $4, 3, 5, 7, 13$), de manera que contingut en una forma dels divisors de $xx + 1$, $xx + 3$, $xx - 5$, i en una forma dels no-divisors de $xx + 7$, $xx - 13$, i, en conseqüència, en una forma de divisors de $xx + 1365$; i el caràcter del gènere en què es trobaran les classes de $\mathfrak{G}$ serà 1, 4; $R3$; $R5$; $N7$; $N13$. En aquest gènere es conté una única classe, de la qual elegim la forma $6xx + 6xy + 229yy$; perquè es trobin totes les representacions del nombre M per aquesta, posarem $2x + y = x'$, d'on haurà de resultar $3x'x' + 455yy = 2M$. Aquesta equació admet quatre solucions en les quals y és positiu, posem $y = 127$, $x' = \pm 1083$, $y = 119$, $x' = \pm 1213$. D'aquí surten quatre solucions de l'equació $6xx + 6xy + 229yy = M$, en les quals y és positiu,

x	478	-605	547	-666
y	127	127	119	119.

La primera solució dóna per a v el valor de l'expressió $\frac{30517}{478}$, o sigui, $-\frac{3249}{127}$ (mòd. M), d'on es troba 2350978;

la segona produeix el valor oposat -2350978; la tercera, el 2600262; la quarta, l'oposat -2600262.

II. Si s'han de cercar tots els valors de l'expressió $\sqrt{-286}$ (mòd. $4272943 = M$), el caràcter del gènere en què estan contingudes les classes $\mathfrak{G}$ es troba 1 *i* 7, 8; $R11$; $R13$; per tant, serà el gènere principal, en què es contenen tres classes, representades per les formes (1, 0, 286), (14, 6, 23), (14, -6, 23); la tercera d'aquestes, com a oposada a la segona, es pot negligir. Es troben dues representacions del nombre M per la forma $xx + 286yy$ en les quals y és positiu, posem $y = 103$, $x = \pm 1113$, d'on els valors de l'expressió proposada surten 1493445, -1493445. Però M es troba no representable per la forma (14, 6, 23), d'on es conclou que, excepte aquests dos valors trobats, no se'n donen altres.

III. Proposada l'expressió $\sqrt{-70}$ (mòd. 997331), les classes de $\mathfrak{G}$ hauran d'estar contingudes en el gènere el caràcter del qual és 3 *i* 5, 8; $R5$; $N7$; en aquest apareix una única classe, la forma representant de la qual és la (5, 0, 14). Fet el càlcul, es troba que el nombre 997331 no és representable per la forma (5, 0, 14), per la qual cosa, -70 serà, necessàriament, no-residu quadràtic d'aquell nombre.

329. El problema de distingir nombres primers de compostos i descompondre aquests en els seus factors primers, que pertany als més importants i més útils de tota l'aritmètica, i que ha ocupat la diligència i la sagacitat dels geòmetres, tant els antics com els més moderns, és tan conegut que seria superflu parlar abundantment d'això. Malgrat tot, convé reconèixer que tots els mètodes presentats fins ara són, o bé restringits a casos

molt especials, o bé tan laboriosos i prolixos que, ja per a nombres tals que no excedeixen els límits de les taules construïdes per homes prestigiosos, és a dir, per als quals els mètodes artificials són innecessaris, també fatiguen la paciència del calculador expert; sovint, però, a penes es poden aplicar a [nombres] més grans. Però, encara que aquelles taules, que estan en totes les mans i que es pot esperar que encara seran continuades de seguida més enllà, siguin suficients per a la major part dels casos que ocorren vulgarment, no obstant això, es presenta no rarament l'ocasió al calculador expert de treure grans profits de la descomposició en factors de nombres grans que compensen llargament una despesa de temps regular; i, a part d'això, la dignitat de la ciència sembla requerir que es perfeccionin curosament tots els recursos per a la resolució d'un problema tan elegant i tan cèlebre. A causa d'aquestes raons, no dubtem que els dos mètodes següents, l'eficàcia i la brevetat dels quals podem confirmar per una llarga experiència, no han de ser ingrats als amants de l'aritmètica. D'altra banda, està fonamentat en la naturalesa del problema que *qualssevol* mètodes sortiran contínuament més prolixos com més grans són els nombres als quals s'apliquin; no obstant això, per als mètodes següents les dificultats creixen més lentament, i han estat tractats feliçment sempre amb èxit, sobretot pel segon, nombres que consten de set, vuit o bé encara més xifres, i amb tota la rapidesa que és esperable per a nombres tan grans que per tots els mètodes coneguts fins ara requerien un esforç també insuportable a un calculador infatigable.

Abans que els mètodes següents siguin invocats, sempre és utilíssim intentar la divisió de qualsevol nombre proposat per alguns nombres primers molt petits,

posem per 2, 3, 5, 7, etc., fins a 19 o encara més enllà, no només perquè no disgusti haver descobert, per mètodes subtils i artificiosos, un nombre, quan és divisor, tal que s'hauria pogut trobar molt més fàcilment solament per divisió,* sinó també perquè, llavors, on cap divisió no té èxit, per a l'aplicació del segon mètode s'usa amb gran profit dels *residus* obtinguts d'aquelles divisions. Així, per exemple, si el nombre 314159265 s'ha de descompondre en els seus factors, la divisió per 3 té èxit dues vegades, i després també les divisions per 5 i 7, d'on es té $314159265 = 9 \cdot 5 \cdot 7 \cdot 997331$, i és suficient sotmetre a un examen més subtil el nombre 997331, que no es troba divisible per 11, 13, 17, 19. Similarment, proposat el nombre 43429448, traurem el factor 8, i aplicarem mètodes més artificials al quocient 5428681.

330. El fonament del PRIMER MÈTODE és el teorema que *qualsevol nombre positiu o negatiu que sigui residu quadràtic d'un altre nombre M, també és residu de qualsevol divisor de M.* Vulgarment és conegut que si M no és divisible per cap nombre primer per sota de $\sqrt{M}$, M és, certament, primer; però si tots els nombres primers per sota d'aquest límit que divideixen M són p, q, etc., el nombre M, o bé està compost d'aquests *sols* (o bé potències d'ells), o bé només pot implicar *un* altre factor primer més gran que $\sqrt{M}$, que es troba dividint M per p, q, etc., tantes vegades com es pugui. Així, designant per Ω el complex de tots els nombres primers per sota de $\sqrt{M}$ (excloent-ne aquells per als quals s'ha intentat en va la divisió), és suficient, evidentment, si

* Encara més, perquè, parlant en general, entre sis nombres a penes se'n troba *un* no divisible per cap dels nombres 2, 3, 5, . . . , 19.

es tenen tots els divisors primers de M continguts en Ω. Ara, si se sap d'alguna manera que algun nombre r (no quadrat) és residu quadràtic de M, certament cap nombre primer del qual r és NR no podrà ser divisor de M; per tant, es podran treure de Ω tots els nombres primers d'aquest tipus (que, sovint, gairebé faran la meitat de tots). A sobre, si d'un altre nombre no quadrat r' se sap que és residu de M, dels nombres primers de Ω que queden després de la primera exclusió podrem excloure de nou aquells dels quals r' és NR, que novament faran quasi la meitat d'aquells sempre que els residus r i r' siguin independents (*és a dir*, llevat que un sigui necessàriament residu de tots els nombres dels quals l'altre és residu, cosa que succeiria quan rr' fos un quadrat). Si encara són coneguts altres residus r'', r''', etc., de M, que tots són independents dels restants,* es poden fer exclusions similars amb cada un per les quals es disminuirà rapidíssimament la quantitat de nombres de Ω, de manera que aviat, o bé s'han esborrat tots, cas en què M serà, certament, un nombre primer, o bé en resten tan pocs (entre els quals, evidentment, es trobaran tots els divisors primers de M, si en té cap) que la divisió per ells es pot intentar sense cap dificultat. Per a un nombre que no superi gaire el milió, sovint seran suficients sis o bé set exclusions; per a un nombre que consti de vuit o nou xifres, nou o deu exclusions. Dues són, ara, les coses de què convindrà tractar; *primer*, de quina manera es poden trobar residus idonis

* Si el producte de qualssevol nombres r, r', r'', etc., és un quadrat, cadascun d'ells, per exemple r, serà residu de qualsevol nombre primer (que no divideixi cap d'ells) que és residu dels restants r', r'', etc. Així, doncs, perquè residus qualssevol es puguin considerar com a independents, convé que no sigui quadrat cap producte ni de parelles, ni de ternes, etc.

de M i en quantitat suficient, *després*, fet això, com es pot fer comodíssimament aquesta exclusió. Però invertirem l'ordre d'aquestes qüestions, principalment perquè la segona ensenyarà el més important, quins residus són còmodes per a aquesta finalitat.

331. Hem ensenyat abundantment en la secció IV a distingir nombres primers dels quals un nombre donat r és residu (que es pot suposar no divisible per cap quadrat) d'aquells dels quals és no-residu, o sigui, els divisors de l'expressió $xx - r$ dels no-divisors; que tots els primers estan continguts en certes fórmules del tipus $rz + a$, $rz + b$, etc., o bé en tals $4rz + a$, $4rz + b$, etc., i els darrers en altres de similars. Quan r és un nombre molt petit, es poden fer exclusions molt còmodament amb l'ajut d'aquestes fórmules; per exemple, s'hauran d'excloure tots els nombres de la forma $4z + 3$, quan $r = -1$; tots els nombres de les formes $8z + 3$ i $8z + 5$, quan $r = 2$; etc. Però, com que no sempre s'és en poder de trobar residus d'aquest tipus del nombre proposat M, ni l'aplicació de les fórmules no és prou còmoda per a un valor gran de r, és de gran profit, i la feina d'exclusió disminueix meravellosament, si ja es té construïda una *taula* per a una quantitat prou gran de nombres (r), tant positius com negatius, no divisibles per quadrats, en la qual els nombres primers dels quals cadascun d'aquells (r) són residus es distingeixen dels que en són no-residus. Es podrà disposar una taula igual que la mostra afegida al final d'aquesta obra, i ja descrita més amunt; però, perquè presti una utilitat prou àmplia per al propòsit present, els nombres primers posats al marge (mòduls) s'han de continuar molt més enllà, posem almenys fins a 1000 o bé 10000; i, a part d'això, s'augmentarà molt

la comoditat si a la capçalera també es reben nombres compostos i negatius, encara que això no sigui absolutament necessari, com és evident de la secció IV. Però l'ús d'una tal taula s'elevarà al nivell més alt de comoditat si es talla cadascuna de les columnes verticals de què consta i s'enganxa en làmines de metall o bé (com les neperianes) en bastons, de manera que les que són necessàries en cada cas, és a dir, les que corresponen als nombres r, r', r'', etc., residus del nombre donat que cal descompondre en factors, es puguin examinar separadament. Posats aquests *degudament* al costat de la primera columna de la taula (que mostra els mòduls), és a dir, de manera que els llocs de cada un dels bastons que corresponen al mateix nombre primer de la primera columna siguin en perpendicular amb aquest, o sigui, estiguin situats en la mateixa línia horitzontal, evidentment, els nombres primers que romanen de Ω després de les exclusions amb els residus r, r', r'', es podran reconèixer immediatament per la sola inspecció; en efecte, aquests coincidiran amb els de la primera columna als quals corresponen les ratlletes en *tots* els bastons adjacents, i s'han de rebutjar tots els que són adjacents a un forat buit en *algun* bastó. S'il·lustrarà això suficientment per un exemple. Si se sap d'alguna manera que els nombres -6, $+13$, -14, $+17$, $+37$, -53, són residus de 997331, s'hauran de concordar la primera columna (que en aquest cas s'ha de continuar fins a 997, és a dir, fins al nombre primer més pròxim menor que $\sqrt{997331}$) i les làmines en la capçalera de les quals hi ha escrits els nombres -6, $+13$, etc. Heus aquí una part de l'esquema que surt d'aquesta manera:

	−6	+13	−14	+17	+37	−53
3	–	–	–		–	–
5	–		–			
7	–		–		–	
11	–				–	
13		–	–	–		–
17		–		–		–
19			–	–		–
23		–	–			–
			etc.			
113		–	–			–
127	–	–	–	–	–	–
131	–	–	–			
			etc.			

De la mateixa manera que aquí es reconeix, per la sola inspecció, que dels nombres primers *que es contenen en aquesta part de l'esquema*, després de les exclusions amb els residus −6, 13, etc., només queda en Ω el 127, així l'esquema íntegre estès fins a 997 mostra que de Ω no en resta *cap altre* en absolut; però, intentada la divisió, 997331 es troba realment divisible per 127. Així, d'aquesta manera, es tindrà aquell nombre descompost en factors primers 127×7853.*

* L'autor donaria de bona gana a judici públic un aparell bastant ampli de la taula descrita aquí, que s'ha preocupat de construir per al seu ús, si l'escassetat d'aquells als quals pot ser útil fos suficient per a sustentar les despeses d'una tal empresa. Si, mentrestant, algun amant de l'aritmètica, interioritzats perfectament els principis, opta per construir amb el seu propi esforç una tal taula, l'autor tindrà una gran satisfacció de comunicar-li

D'altra banda, d'aquesta exposició es conclou suficientment que són especialment útils els residus no massa grans, o almenys descomponibles en factors primers no massa grans, ja que l'ús immediat de la taula auxiliar no s'estén més enllà dels nombres posats a la capçalera i l'ús mediat només aplega els tals que es poden descompondre en factors continguts en la taula.

332. Per a trobar els residus d'un nombre donat M, transmetrem tres mètodes diferents a l'exposició dels quals avancem dues observacions amb l'ajuda de les quals es poden derivar de residus menys idonis els més simples. *Primer*, si un nombre akk divisible pel quadrat kk (que se suposa que és primer amb M) és residu de M, també a en serà residu; a causa d'aquesta raó, els residus divisibles per quadrats grans són igualment útils que els petits; i suposem alliberats immediatament dels seus factors quadrats tots els residus procurats pels mètodes següents. *Segon*, si dos o més nombres són residus, el seu producte també serà residu. Combinant aquesta observació amb la precedent, de molts residus, que no tots són suficientment simples, molt sovint se'n pot deduir un altre molt simple, sempre que aquells impliquen molts factors comuns. Per aquesta causa també són oportuns els residus tals que estan compostos de molts factors no massa grans, i convindrà descompondre'ls tots immediatament en els seus factors. La força d'aquestes observacions es copsarà millor per exemples i ús freqüent que per preceptes.

I. Per a aquells que per una pràctica freqüent ja han adquirit alguna destresa, el mètode més simple i

---

per carta tots els avantatges d'això i els artificis.

més còmode consisteix en què M, o més generalment, un múltiple qualsevol de M, es descompon de qualsevol manera en dues parts $kM = a+b$ (bé ambdues siguin positives, bé una positiva i l'altra negativa), el producte de les quals amb signe canviat serà residu de M, en efecte, serà $-ab \equiv aa \equiv bb\,(\text{mòd. } M)$, de manera que $-abRM$. Els nombres a, b, s'han d'agafar de manera que el producte surti divisible per un quadrat gran i el quocient o bé petit o almenys descomponible en factors no massa grans, cosa que sempre es podrà fer no difícilment. S'ha de recomanar principalment que per a a s'agafi o bé un quadrat, o bé el doble d'un quadrat, o bé el triple, etc., que difereixi del nombre M en un nombre o bé petit o bé descomponible en factors còmodes. Així, per exemple, es troba $997331 = 999^2 - 2\cdot 5\cdot 67 = 994^2 + 5\cdot 11\cdot 13^2 = 2\cdot 706^2 + 3\cdot 17\cdot 3^2 = 575^2 + 11\cdot 31\cdot 4^2 = 3\cdot 577^2 - 7\cdot 13\cdot 4^2 = 3\cdot 578^2 - 7\cdot 19\cdot 37 = 11\cdot 299^2 + 2\cdot 3\cdot 5\cdot 29\cdot 4^2 = 11\cdot 301^2 + 5\cdot 12^2$, etc. D'aquí, es tenen els residus següents: $2\cdot 5\cdot 67$, $-5\cdot 11$, $-2\cdot 3\cdot 17$, $-3\cdot 11\cdot 31$, $3\cdot 7\cdot 13$, $3\cdot 7\cdot 19\cdot 37$, $-2\cdot 3\cdot 5\cdot 11\cdot 29$; l'última descomposició proporciona el residu $-5\cdot 11$, que ja tenim. Per als residus $-3\cdot 11\cdot 31$, $-2\cdot 3\cdot 5\cdot 11\cdot 29$, podem adoptar $3\cdot 5\cdot 31$, $2\cdot 3\cdot 29$, originats de la combinació d'aquells amb $-5\cdot 11$.

II. El segon i el tercer mètodes s'obtenen del fet que si dues formes binàries (A, B, C), (A', B', C'), del mateix determinant M, o bé $-M$, o bé, més generalment, $\pm kM$, pertanyen al mateix gènere, els nombres AA', AC', $A'C$, són residus de kM; això es copsa sense cap dificultat del fet que qualsevol nombre característic d'una forma, posem m, també és un nombre característic de l'altra, de manera que mA, mC, mA', mC', són tots residus de kM. Així, si (a, b, a') és una forma reduïda de determinant positiu M, o bé, més generalment, kM, i

(a', b', a''), (a'', b'', a'''), etc., formes del seu període, de manera que equivalents a ella i, encara més, contingudes en el mateix gènere, els nombres aa', aa'', aa''', etc., seran tots residus de M. El càlcul d'una gran quantitat de formes d'un tal període es fa molt fàcilment amb l'ajut de l'algoritme de l'article 187; sovint, els residus més simples surten establint $a = 1$; s'hauran de suprimir els que impliquen factors massa grans. Heus aquí els inicis dels períodes de les formes (1, 998, −1327), (1, 1412, −918), els determinants de les quals són 997331, 1994662:

$(1, 998, -1327)$	$(1, 1412, -918)$
$(-1327, 329, 670)$	$(-918, 1342, 211)$
$(670, 341, -1315)$	$(211, 1401, -151)$
$(-1315, 974, 37)$	$(-151, 1317, 1723)$
$(37, 987, -626)$	$(1723, 406, -1062)$
$(-626, 891, 325)$	$(-1062, 656, 1473)$
$(325, 734, -1411)$	$(1473, 817, -901)$
$(-1411, 677, 382)$	$(-901, 985, 1137)$
$(382, 851, -715)$	etc.

Així, són residus del nombre 997331 tots els nombres −1327, 670, etc.; però, negligint aquells que impliquen factors massa grans, tenim els $2 \cdot 5 \cdot 67$, 37, 13, $-17 \cdot 83$, $-5 \cdot 11 \cdot 13$, $-2 \cdot 3 \cdot 17$, $-2 \cdot 59$, $-17 \cdot 53$; ja havíem trobat més amunt el residu $2 \cdot 5 \cdot 67$ i també el $-5 \cdot 11$, que es fa sortir de la combinació del tercer amb el cinquè.

III. Si C és una classe qualsevol, diferent de la principal, de formes de determinant negatiu $-M$ o més generalment $-kM$, i el seu període $2C$, $3C$, etc. (article 307), les classes $2C$, $4C$, etc., pertanyeran al gènere principal; però les $3C$, $5C$, etc., al mateix gènere que C. Així, si (a, b, c) és una forma (la més simple) de C, i $(a',$

b', c') una forma d'alguna classe d'aquell període, posem de nC, o bé a' o bé aa' serà residu de M, segons que n sigui parell o bé imparell (en el primer cas, evidentment, també c'; en el darrer, ac', ca', i cc'). El desenvolupament del període, és a dir, de les formes més simples en les seves classes, es fa amb sorprenent facilitat quan a és molt petit, especialment quan és $= 3$, cosa que es pot fer sempre quan $kM \equiv 2 \,(\text{mòd. } 3)$. Heus aquí l'inici del període de la classe en què hi ha la forma (3, 1, 332444):

C	$(3, 1, 332444)$	$6C$	$(729, -209, 1428)$
$2C$	$(9, -2, 110815)$	$7C$	$(476, 209, 2187)$
$3C$	$(27, 7, 36940)$	$8C$	$(1027, 342, 1085)$
$4C$	$(81, 34, 12327)$	$9C$	$(932, -437, 1275)$
$5C$	$(243, 34, 4109)$	$10C$	$(425, 12, 2347)$.

D'aquí provenen els residus (rebutjats els inútils) $3 \cdot 476$, 1027, 1085, 425, o sigui (suprimint els factors quadrats), $3 \cdot 7 \cdot 17$, $13 \cdot 79$, $5 \cdot 7 \cdot 31$, 17, i de la seva adequada combinació amb els vuit residus trobats en II surten fàcilment els dotze següents: $-2 \cdot 3$, 13, $-2 \cdot 7$, 17, 37, -53, $-5 \cdot 11$, 79, -83, $-2 \cdot 59$, $-2 \cdot 5 \cdot 31$, $2 \cdot 5 \cdot 67$; els sis primers són els mateixos que hem usat en l'article 331. Es podrien afegir, si també els volguéssim invocar, els residus 19 i -29, que s'han trobat en I; els restants descoberts allà ja són dependents dels que hem desenvolupat aquí.

333. El SEGON MÈTODE per a descompondre en factors un nombre donat M s'obté de la consideració dels valors d'una expressió tal com $\sqrt{-D} \,(\text{mòd. } M)$, i es recolza en les observacions següents.

I. Quan M és un nombre primer o bé una potència d'un nombre primer (imparell i que no divideix D), $-D$ serà residu o no-residu de M, segons que M es contingui

o bé en una forma de divisors o bé en una forma de no-divisors de $xx + D$, i, en el primer cas, l'expressió $\sqrt{-D}\,(\text{mòd. } M)$ només tindrà dos valors diferents, que seran oposats.

II. Però quan M és compost, posem $= pp'p''\,etc.$, on p p', p'', etc., designen nombres primers (diferents, imparells, que no divideixen D) o bé potències de tals nombres, llavors $-D$ només serà residu de M quan és residu de cadascun dels p, p', p'', etc., és a dir, quan tots aquests nombres es contenen en formes de divisors de $xx + D$. Però, designant els valors de l'expressió $\sqrt{-D}$ segons els mòduls p, p', p'', etc., per $\pm r$, $\pm r'$, $\pm r''$, etc., respectivament, s'originaran tots els valors de la mateixa expressió segons el mòdul M descobrint nombres que siguin o bé $\equiv r$ o bé $\equiv -r$, segons p; o bé $\equiv r'$ o bé $\equiv -r'$, segons p'; etc.; en conseqüència, la quantitat d'aquests resultarà $= 2^\mu$, on μ designa la quantitat de nombres p, p', p'', etc. Així, si aquests valors són R, $-R$, R', $-R'$, R'', etc., serà espontàniament $R \equiv R$ segons tots els p, p', p'', etc., però $R \equiv -R$ segons cap d'ells, d'on el màxim comú divisor del nombre M amb $R - R$ serà M, i 1 el màxim comú divisor de M amb $R+R$; però dos valors ni idèntics ni oposats, com R i R', seran congrus necessàriament segons un o bé més dels nombres p, p', p'', etc., però no segons tots, i segons els restants $R \equiv -R'$; d'aquí, el producte d'aquells serà el màxim comú divisor dels nombres M i $R - R'$, i el producte d'aquests, el màxim comú divisor dels M i $R+R'$. D'aquí se segueix fàcilment que si es calculen tots els màxims comuns divisors de M amb les diferències entre cada un dels valors de l'expressió $\sqrt{-D}\,(\text{mòd. } M)$ i algun valor donat, el complex d'aquests conté els nombres 1, p, p', p'', etc., i tots els productes de parelles, ternes, etc.,

d'aquests nombres. *Així, dels valors d'aquella expressió, es podran descobrir d'aquesta manera els nombres* p, p', p'', *etc.*

D'altra banda, com que el mètode de l'article 327 redueix cadascun d'aquests valors a valors d'expressions de la forma $\frac{m}{n}$ (mòd. M) de manera que el denominador n és primer amb M, no és, certament, necessari per al propòsit present calcular-les. Efectivament, el màxim comú divisor del nombre M amb la diferència entre R i R', que coincideixen amb $\frac{m}{n}$ i $\frac{m'}{n'}$, també serà, evidentment, el màxim comú divisor dels M i $nn'(R - R')$, o sigui, dels M i $mn' - m'n$, ja que $nn'(R - R')$ és congru a aquest segons el mòdul M.

334. L'aplicació de les observacions precedents al problema que tractem es pot fer de dues maneres: la primera no solament decidirà si el nombre proposat M és primer o bé compost, sinó que, en aquest cas, també proporciona els seus factors; la darrera, però, es presta fins al punt que sovint permet un càlcul més ràpid, però a vegades no revela els factors dels nombres compostos, que també distingeix directament dels primers, llevat que es repeteixi moltes vegades.

I. S'investiga un nombre negatiu $-D$ que sigui residu quadràtic de M, fi per al qual es podran aplicar els mètodes transmesos en I i II de l'article 332. Certament, és arbitrari en si quin residu s'elegeixi, i aquí, com en el mètode precedent, no és necessari que D sigui un nombre petit; però el càlcul serà tant més breu com menor sigui la quantitat de classes de formes binàries

contingudes en cada gènere pròpiament primitiu de determinant $-D$; per la qual cosa, seran oportuns principalment els residus tals que es contenen entre els 65 nombres de l'article 303, si aquests es presenten. Així, per a $M = 997331$, de tots els residus negatius descoberts més amunt, el més idoni seria el -102. Es descobreixen tots els valors diferents de l'expressió $\sqrt{-D}$ (mòd. M); si només n'apareixen dos (oposats), M serà, certament, o bé un nombre primer o bé una potència d'un nombre primer; si més, posem 2^μ, M serà compost de μ nombres primers o bé potències de primers, diferents, factors que es podran descobrir pel mètode de l'article precedent. Però, d'una banda, serà facilíssim en si distingir si aquests factors són nombres primers o bé potències de primers; de l'altra, la via per la qual es troben els valors de l'expressió $\sqrt{-D}$ també indica espontàniament tots els nombres primers alguna potència dels quals divideix M; això és, si M és divisible pel quadrat d'un nombre primer π, aquell càlcul, certament, també ens produirà una o més representacions del nombre M, tals com $M = amm + 2bmn + cnn$, en les quals el màxim comú divisor dels nombres m, n, és π (i així, certament, que, en aquest cas, $-D$ també és residu de $\frac{M}{\pi\pi}$). Però quan no apareix cap representació en la qual m i n tenen divisor comú, això és un indici cert que M no és divisible per cap quadrat, de manera que tots els p, p', p'', etc., són nombres primers.

Exemple. Per a l'expressió $\sqrt{-408}$ (mòd. 997331), pel mètode transmès més amunt, es troben quatre valors, que coincideixen amb els valors $\pm\frac{1664}{113}$, $\pm\frac{2824}{3}$; els màxims comuns divisors de 997331 amb $3 \cdot 1664 - 113 \cdot$

2824 i $3 \cdot 1664 + 113 \cdot 2824$, o sigui, amb 314120 i 324104, es descobreixen els 7853 i 127, d'on $997331 = 127 \cdot 7853$ com més amunt.

II. S'agafa algun nombre negatiu $-D$ tal que M estigui contingut en una forma de divisors de $xx + D$; és arbitrari en si quin nombre d'aquest tipus s'elegeixi, però per comoditat s'ha de veure principalment que la quantitat de classes en els gèneres de determinant $-D$ sigui tan petita com sigui possible. D'altra banda, la recerca d'un tal nombre no està sotmesa a cap dificultat, si es fa temptejant; efectivament, sovint, entre una quantitat considerable de nombres temptejats, M es conté gairebé tantes vegades en la forma de divisors com en la forma de no-divisors. Per tant, serà molt adequat començar el tempteig pels 65 nombres de l'article 303 (i, certament, pels més grans), i si succeís que no n'hi hagués cap d'idoni (cosa, però, que, parlant en general, ocorrerà només una sola vegada entre 16384 casos), passar a altres en què es contenen dues classes en cada gènere. Llavors, s'investiguen els valors de l'expressió $\sqrt{-D}\,(\text{mòd. } M)$, i, si se'n troba algun, es dedueixen d'aquí els factors de M completament de la mateixa manera que més amunt; però si no apareix cap valor, de manera que $-D$ és no-residu de M, M no podrà ser, certament, ni un nombre primer ni una potència d'un nombre primer. Si, en aquest cas, es desitgen els factors, o bé convé repetir la mateixa operació agafant altres valors per a D, o bé recórrer a un altre mètode.

Així, per exemple, fet el tempteig, 997331 es troba contingut en una forma de no-divisors de $xx + 1848$, $xx + 1365$, $xx + 1320$, però en la forma de divisors de $xx + 840$; per valors de l'expressió $\sqrt{-840}\,(\text{mòd. } 997331)$,

apareixen les expressions $\pm\frac{1272}{163}$, $\pm\frac{3288}{125}$, d'on es dedueixen els mateixos factors que abans. Si algú desitja més exemples, que consulti l'article 328, on el primer ensenya que és $5428681 = 307 \cdot 17683$; el segon, que 4272943 és un nombre primer; el tercer, que 997331 és compost, certament, de molts primers.

* * *

D'altra banda, els límits d'aquesta obra només han permès incloure aquí els aspectes principals d'un i altre mètode per a investigar factors; reservem per a una altra ocasió una disquisició més extensa juntament amb més taules auxiliars i altres recursos.

Secció Setena

de les

EQUACIONS QUE DEFINEIXEN

les seccions del cercle

335. Entre els desenvolupaments més esplèndids afegits a la matemàtica pels treballs dels [autors] més recents, la teoria de les funcions que depenen del cercle ocupa sense cap dubte un lloc principalment distingit. A aquest admirable gènere de quantitats, al qual som portats en disquisicions molt sovint molt heterogènies i de l'ajuda del qual no pot estar mancada cap part de la matemàtica universal, els grans geòmetres més recents li han dedicat la seva activitat i sagacitat tan assíduament i n'han format una disciplina tan vasta que poc s'hauria pogut esperar que cap part d'aquesta teoria, i encara menys l'elemental i situada quasi en el límit, fos capaç encara de desenvolupaments importants. Parlo de la teoria de les funcions trigonomètriques corresponents a arcs commensurables amb la perifèria, o sigui, de la teoria dels polígons regulars, de la qual fins aquí ha estat aclarida una petita part, que obrirà la secció present.

Els lectors es poden sorprendre que hagi emprès tal disquisició sobretot en aquesta obra dedicada especialment a una disciplina a primera vista molt heterogènia; però el mateix tractament mostrarà suficientment que entre aquesta qüestió i l'aritmètica superior hi ha inherent un nexe íntim.

D'altra banda, els principis de la teoria que anem a exposar s'estenen molt més amplament que aquí s'expliquen. Efectivament, no només es poden aplicar a les funcions circulars, sinó, amb èxit semblant, a moltes altres funcions transcendents, per exemple, a les que depenen de la integral $\int \frac{dx}{\sqrt{1-x^4}}$, i, a part d'això, també a diversos gèneres de congruències; però, com que preparem una àmplia obra peculiar d'aquelles funcions transcendents, mentre que de congruències se'n tractarà copiosament a continuació de les disquisicions aritmètiques, s'ha volgut considerar en aquest lloc només les funcions circulars. I de fet, també reduirem al cas més simple aquestes, que es podrien abraçar amb molta generalitat pels recursos que cal exposar en l'article següent, mirant tant per la brevetat com perquè els principis clarament nous d'aquesta teoria s'entenguin més fàcilment.

336. Designant la perifèria del cercle, o sigui, quatre angles rectes, per P, i suposant que m, n, són enters i n el producte de factors primers entre si a, b, c, etc., l'angle $A = \frac{mP}{n}$, per l'article 310, es pot reduir a la forma $A = (\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + etc.)P$, i les funcions trigonomètriques corresponents a ell es deduiran per mètodes coneguts de les funcions pertanyents a les parts

$\frac{\alpha P}{a}$, $\frac{\beta P}{b}$, etc. Així, com que per a a, b, c, etc., es poden agafar nombres primers o bé potències de nombres primers, evidentment és suficient considerar la secció del cercle en parts, la quantitat de les quals és un nombre primer o bé potència d'un primer, i es tindrà directament un polígon de n costats de polígons de a, b, c, etc., costats. No obstant això, en aquest lloc restringirem la disquisició al cas en què el cercle s'ha de dividir en parts, la quantitat de les quals és un nombre primer (imparell), conduïts sobretot per la raó següent. Se sap que les funcions circulars corresponents a l'angle $\frac{mP}{pp}$ es deriven de les funcions que pertanyen a $\frac{mP}{p}$ per la solució d'una equació de p-èsim grau, i igualment d'aquelles, per una equació igualment alta, les funcions que pertanyen a $\frac{mP}{p^3}$, etc., de manera que si ja es té un polígon de p costats, per la determinació d'un polígon de p^λ costats es requeriria necessàriament la solució de $\lambda - 1$ equacions de p-èsim grau. Però, encara que la teoria següent també es podria estendre a aquest cas, no obstant això, per aquesta via, també cauríem a la mateixa quantitat d'equacions de p-èsim grau, les quals, si p és un nombre primer, no es poden rebaixar de cap manera a inferiors. Així, per exemple, més avall es mostrarà que un polígon de 17 costats es pot construir geomètricament; però per a la determinació d'un polígon de 289 costats no es pot evitar de cap manera una equació de 17-èsim grau.

337. Se sap suficientment que les funcions trigonomètriques de tots els angles $\frac{kP}{n}$, denotant formalment per k tots els nombres 0, 1, 2, $\ldots$, $n-1$, s'expressen per

les arrels d'equacions de n-èsim grau, posem el *sinus* per les arrels de la (I)

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \text{etc.} \pm \frac{1}{2^{n-1}}nx = 0;$$

el *cosinus* per les arrels de la (II)

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \text{etc.} \pm \frac{1}{2^{n-1}}nx - \frac{1}{2^{n-1}} = 0;$$

finalment, la *tangent* per les arrels de la (III)

$$x^n - \frac{n(n-1)}{1\cdot 2}x^{n-2} + \frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4}x^{n-4} - \text{etc.} \pm nx = 0.$$

Aquestes equacions (que valen en general per a qualsevol valor imparell de n, II, però, també, per als parells) es rebaixen fàcilment al m-èsim grau posant $n = 2m + 1$; això és, I i III, dividint la part de l'esquerra per x i substituint xx per y. Però l'equació II, evidentment, implica l'arrel $x = 1$ $(= \cos 0)$ i les restants sempre són iguals a parelles ($\cos\frac{P}{n} = \cos\frac{(n-1)P}{n}$, $\cos\frac{2P}{n} = \cos\frac{(n-2)P}{n}$, etc.); per tant, la seva part esquerra és divisible per $x-1$, i el quocient serà un quadrat, extraient l'arrel quadrada del qual l'equació II es redueix a la

$$x^m + \frac{1}{2}x^{m-1} - \frac{1}{4}(m-1)x^{m-2} - \frac{1}{8}(m-2)x^{m-3} + \frac{1}{16}\frac{(m-2)(m-3)}{1\cdot 2}x^{m-4} + \frac{1}{32}\frac{(m-3)(m-4)}{1\cdot 2}x^{m-5} - etc. = 0,$$

les arrels de la qual seran els cosinus dels angles $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$, …, $\frac{mP}{n}$. Fins ara no es tenien ulteriors reduccions d'aquestes equacions ni tan sols per al cas en què n és un nombre primer.

No obstant això, cap d'aquestes equacions no és tan tractable i tan idònia per al nostre propòsit com la $x^n - 1 = 0$, les arrels de la qual se sap que estan connectades estretíssimament amb les arrels d'aquelles. Això és, escrivint, per abreujar, i per a la quantitat imaginària $\sqrt{-1}$, les arrels de l'equació $x^n - 1 = 0$ s'expressen per $\cos\frac{kP}{n} + i\sin\frac{kP}{n} = r$, on per a k s'han d'agafar tots els nombres 0, 1, 2, …, $n-1$. En conseqüència, com que és $\frac{1}{r} = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$, les arrels de l'equació I s'expressaran per $\frac{1}{2i}(r - \frac{1}{r})$, o sigui, per $\frac{i(1-rr)}{2r}$; les arrels de l'equació II, per $\frac{1}{2}(r + \frac{1}{r}) = \frac{1+rr}{2r}$; finalment, per $\frac{i(1-rr)}{1+rr}$, les arrels de l'equació III. Per aquesta causa, construirem la disquisició de la consideració de l'equació $x^n - 1 = 0$, suposant que n és un nombre primer imparell. Però perquè no convingui interrompre l'ordre de la investigació, enunciem aquí el lema següent.

338. Problema. *Donada l'equació* (W) … $z^m + Az^{m-1} + etc. = 0$, *trobar una equació* (W') *les arrels de la qual siguin les potències* λ*-èsimes de les arrels de l'equació* (W), *on* λ *designa un exponent enter positiu donat.*

Solució. Designades per a, b, c, etc., les arrels de l'equació W, les arrels de l'equació W' hauran de ser a^λ, b^λ, c^λ, etc. Pel conegut teorema de Newton, dels coeficients de l'equació W es pot trobar la suma de qualssevol potències de les arrels a, b, c, etc. Així, se cerquen les sumes $a^\lambda+b^\lambda+c^\lambda+etc.$, $a^{2\lambda}+b^{2\lambda}+c^{2\lambda}+etc.$, etc., fins a $a^{m\lambda}+b^{m\lambda}+c^{m\lambda}+etc.$, d'on, per la via inversa, pel mateix teorema, es podran deduir els coeficients de l'equació W'. *Q. E. F.* Simultàniament, d'aquí és clar que si tots els coeficients de W són racionals, també surten racionals tots els de W'. Certament, es pot provar per una altra via que si tots aquells són enters, tots aquests també resultaran enters; però no ens entretenim aquí en aquest teorema no especialment necessari per al nostre propòsit.

339. L'equació $x^n - 1 = 0$ (en la suposició, que cal sobreentendre sempre aquí, que n és un nombre primer imparell) implica una única arrel real, $x = 1$; les $n - 1$ restants, que aplega l'equació $x^{n-1} + x^{n-2} + etc. + x + 1 = 0$, totes són imaginàries; denotarem per Ω el complex d'aquestes i per X la funció $x^{n-1} + x^{n-2} + etc. + x + 1$. Així, si r és una arrel qualsevol de Ω, serà $1 = r^n = r^{2n}$ etc., i, en general, $r^{en} = 1$, per a qualsevol valor enter de e, positiu o bé negatiu; d'aquí és evident que si λ, μ, són enters congrus segons n, serà $r^\lambda = r^\mu$. Però si λ, μ, són incongrus segons el mòdul n, r^λ i r^μ seran diferents; en efecte, en aquest cas, es pot agafar un enter ν de manera que resulti $(\lambda - \mu)\nu \equiv 1 \,(\text{mòd.}\, n)$, d'on $r^{(\lambda-\mu)\nu} = r$, de manera que $r^{\lambda-\mu}$, certament, no $= 1$. A més a més, és clar que qualsevol potència de r també és arrel de l'equació $x^n - 1 = 0$; en conseqüència, com que les quantitats $1\ (= r^0)$, r, rr, $\ldots$, r^{n-1}, totes són diferents, aquestes expressaran totes les arrels de

l'equació $x^n - 1 = 0$, i, en conseqüència, les r, rr, r^3, ..., r^{n-1}, coincideixen amb Ω. D'aquí es conclou fàcilment més generalment que Ω coincideix amb r^e, r^{2e}, r^{3e}, ..., $r^{(n-1)e}$, si e és un enter qualsevol no divisible per n, positiu o bé negatiu. Així, serà $X = (x-r^e)(x-r^{2e})(x-r^{3e})\cdots(x-r^{(n-1)e})$, d'on $r^e + r^{2e} + r^{3e} + \cdots + r^{(n-1)e} = -1$ i $1 + r^e + r^{2e} + \cdots + r^{(n-1)e} = 0$. Anomenarem *recíproques* dues arrels tals com r i $\frac{1}{r}$ $(= r^{n-1})$, o bé, més generalment, r^e i r^{-e}; és evident que el producte dels dos factors simples $x - r$ i $x - \frac{1}{r}$ resulta real $= xx - 2x\cos\omega + 1$, de manera que l'angle ω o bé és igual a l'angle $\frac{P}{n}$ o bé a algun múltiple d'ell.

340. Així, com que, expressada per r una arrel de Ω, totes les arrels de l'equació $x^n - 1 = 0$ s'expressen per potències de r, el producte, format de qualsevol manera de moltes arrels d'aquesta equació, es podrà expressar per r^λ, de manera que λ és o bé 0 o bé positiu i $< n$. Així, designant per $\phi(t, u, v, \ldots)$ una funció algebraica racional entera de les indeterminades t, u, v, etc., la qual es pot expressar per una suma de parts tals com $ht^\alpha u^\beta v^\gamma \cdots$, és evident que si se substitueixen t, u, v, etc. per algunes de les arrels de l'equació $x^n - 1 = 0$, posem $t = a$, $u = b$, $v = c$, etc., $\phi(a, b, c, \ldots)$ es pot reduir a la forma $A + A'r + A''rr + A'''r^3 + \cdots + A^n r^{n-1}$, de manera que els coeficients A, A', etc. (alguns dels quals també poden faltar, de manera que ser $= 0$) són quantitats determinades i, a sobre, tots aquests coeficients resulten enters si tots els coeficients determinats de $\phi(t, u, v, \ldots)$, és a dir, tots els h, són enters. Però, si, posteriorment, se substitueixen t, u, v, ..., per aa, bb, cc, etc., respectivament, qualsevol part com

$ht^\alpha u^\beta v^\gamma \cdots$, que abans es reduïa a r^σ, ara resultarà $r^{2\sigma}$, d'on es conclou fàcilment que resulta $\phi(aa, bb, cc, \dots) = A + A'rr + A''r^4 + A'''r^6 + \cdots + A^\nu r^{2n-2}$. Igualment, en general, per a un valor enter qualsevol de λ, serà $\phi(a^\lambda, b^\lambda, c^\lambda, \dots) = A + A'r^\lambda + A''r^{2\lambda} + \cdots + A^\nu r^{(n-1)\lambda}$, proposició que és de màxima importància i constitueix el fonament de les disquisicions següents. D'aquí també se segueix que $\phi(1, 1, 1, \dots) = \phi(a^n, b^n, c^n, \dots) = A + A' + A'' + \cdots + A^\nu$; i també $\phi(a, b, c, \dots) + \phi(aa, bb, cc, \dots) + \phi(a^3, b^3, c^3, \dots) \cdots + \phi(a^n, b^n, c^n, \dots) = nA$; així, aquesta suma sempre resulta un enter divisible per n quan tots els coeficients determinats en $\phi(t, u, v, \dots)$ són enters.

341. Teorema. *Si la funció X és divisible per una funció de grau inferior $P = x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \cdots + Kx + L$, tots els coeficients $A, B, \dots, L$, no poden ser enters.*

Dem. Sigui $X = PQ$, i $\mathfrak{P}$ el complex de les arrels de l'equació $P = 0$, $\mathfrak{Q}$ el complex de les arrels de l'equació $Q = 0$ de manera que Ω consta de $\mathfrak{P}$ i $\mathfrak{Q}$ presos simultàniament. A més a més, sigui $\mathfrak{R}$ el complex de les arrels recíproques de $\mathfrak{P}$, $\mathfrak{S}$ el complex de les arrels recíproques de $\mathfrak{Q}$, i siguin les arrels que es contenen en $\mathfrak{R}$ les arrels de l'equació $R = 0$ (que es copsa fàcilment que resultarà $x^\lambda + \frac{K}{L}x^{\lambda-1} + etc. + \frac{A}{L}x + \frac{1}{L} = 0$), i les que es contenen en $\mathfrak{S}$, arrels de l'equació $S = 0$. Evidentment, les arrels $\mathfrak{R}$ i $\mathfrak{S}$ juntes també faran el complex Ω, i serà $RS = X$. Ara distingim quatre casos.

I. Quan $\mathfrak{P}$ coincideix amb $\mathfrak{R}$, de manera que $P = R$. En aquest cas, evidentment, les arrels de $\mathfrak{P}$ sempre seran recíproques a parelles, de manera que P el pro-

ducte de $\frac{1}{2}\lambda$ factors dobles tals com $xx - 2x\cos\omega + 1$; com que un tal factor és $= (x - \cos\omega)^2 + \sin^2\omega$, es copsarà fàcilment que P, per a qualsevol valor real de x, obté necessàriament un valor real. Siguin les equacions les arrels de les quals són els quadrats, els cubs, els biquadrats, ..., les potències $(n-1)$-èsimes de les arrels de $\mathfrak{P}$, respectivament $P' = 0$, $P'' = 0$, $P''' = 0$, ..., $P^\nu = 0$, i siguin p, p', p'', ..., p^ν, respectivament, els valors de les funcions P, P', P'', ..., P^ν, que s'obtenen establint $x = 1$; llavors, pel que s'ha dit abans, p serà una quantitat positiva, i per una raó completament similar p', p'', etc., també seran positives. Així, com que p és el valor de la funció $(1-t)(1-u)(1-v)etc.$ que s'obté posant per a t, u, v, etc., les arrels de $\mathfrak{P}$; p' el valor d'aquesta mateixa establint per a t, u, v, etc., els quadrats d'aquelles arrels, etc., i, a sobre, el valor per a $t = 1$, $u = 1$, $v = 1$, etc., resulta, evidentment, $= 0$, la suma $p + p' + p'' + \cdots + p^\nu$ serà un enter divisible per n. A part d'això, es copsarà fàcilment que el producte $PP'P''\cdots$ resulta $= X^\lambda$, de manera que $pp'p''\cdots = n^\lambda$.

Ara, si tots els coeficients de P fossin racionals, també tots els de P', P'', etc., per l'article 338, sortirien racionals; però, per l'article 42, aquests coeficients junts serien necessàriament enters. D'aquí, també p, p', p'', etc., serien tots enters; com que el seu producte és n^λ, però la quantitat $n-1 > \lambda$, necessàriament alguns d'ells (almenys $n-1-\lambda$) hauran de ser $= 1$, però els restants iguals a n o bé a una potència de n. Així, si g d'ells són $= 1$, la suma $p+p'+etc.$ serà, evidentment, $\equiv g$ (mòd. n), de manera que, certament, no divisible per n. Per tant, la suposició no pot ser consistent.

II. Certament, quan $\mathfrak{P}$ i $\mathfrak{R}$ no coincideixen, no obstant això contenen algunes arrels comunes, sigui $\mathfrak{T}$ el complex d'aquestes i $T = 0$ l'equació de la qual són arrels. Llavors, T serà el màxim comú divisor de les funcions P, R (com se sap de la teoria d'equacions). Però, evidentment, les arrels de $\mathfrak{T}$ sempre seran recíproques per parelles, d'on, pel que s'ha demostrat abans, tots els coeficients de T no poden ser racionals. Però això succeiria, certament, si tots els de P, de manera que, també, tots els de R, fossin racionals, com se segueix espontàniament de la naturalesa de l'operació d'investigar el màxim comú divisor. Per tant, la suposició és absurda.

III. Quan $\mathfrak{Q}$ i $\mathfrak{S}$, o bé coincideixen, o almenys impliquen arrels comunes, completament de la mateixa manera, tots els coeficients de Q no poden ser racionals; però resultarien racionals si tots els de P fossin racionals; així, això és impossible.

IV. Però si $\mathfrak{P}$ no té cap arrel comuna amb $\mathfrak{R}$, ni $\mathfrak{Q}$ amb $\mathfrak{S}$, necessàriament totes les arrels de $\mathfrak{P}$ es trobaran en $\mathfrak{S}$ i totes les de $\mathfrak{Q}$ en $\mathfrak{R}$, d'on serà $P = S$ i $Q = R$. Per la qual cosa, $X = PQ$ serà el producte de P per R, és a dir, de $x^\lambda + Ax^{\lambda-1} + \cdots + Kx + L$ per $x^\lambda + \dfrac{K}{L}x^{\lambda-1} + \cdots + \dfrac{A}{L}x + \dfrac{1}{L}$, d'on, establint $x = 1$, resulta $nL = (1 + A \cdots + K + L)^2$. Ara, si tots els coeficients de P fossin racionals, de manera que, per l'article 42, també enters, L, que ha de dividir l'últim coeficient de X, és a dir, la unitat, serà necessàriament $= \pm 1$, d'on $\pm n$ seria un nombre quadrat. Com que això s'oposa a la hipòtesi, la suposició no pot ser consistent.

Així, d'aquest teorema és clar que, de qualsevol manera que X es descompongui en factors, almenys part dels seus coeficients resulten irracionals, de manera que no es poden determinar altrament que per una equació elevada.

342. El propòsit de les disquisicions següents, que no serà inútil que s'hagi anunciat en poques paraules, tendeix a descompondre GRADUALMENT i contínuament X en més factors, i, certament, de manera que els seus coeficients es determinin per equacions d'ordre tan petit com sigui possible, fins que d'aquesta manera s'arribi a factors simples, o sigui, a les arrels Ω. Això és, mostrarem que, de qualsevol manera que el nombre $n-1$ es descompongui en factors enters α, β, γ, etc. (per a cadascun dels quals es poden agafar nombres primers), X es pot descompondre en α factors de $\frac{n-1}{\alpha}$ dimensions, els coeficients dels quals es determinen per una equació de α-èsim grau; cadascun d'aquests factors, de nou, en altres β de $\frac{n-1}{\alpha\beta}$ dimensions, amb l'ajut d'una equació de β-èsim grau, etc., de manera que si ν designa la quantitat de factors α, β, γ, etc., la trobada de les arrels Ω es redueixi a la resolució de ν equacions de graus α-èsim, β-èsim, γ-èsim, etc. Per exemple, per a $n = 17$, on $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$, convindrà resoldre quatre equacions quadràtiques; per a $n = 73$, tres de quadràtiques i dues de cúbiques.

Com que en el que segueix molt sovint s'han de considerar tals potències de l'arrel r, els exponents de les quals són a la vegada potències, però expressions d'aquest tipus es copien a la impremta no sense molèstia, per a facilitar la impressió utilitzarem, d'aquí endavant,

l'abreviatura següent. Per a r, rr, r^3, etc., escriurem [1], [2], [3], etc., i, en general, per a r^λ, on λ denota un enter qualsevol, $[\lambda]$. Així, tals expressions encara no són absolutament determinades, però ho resulten sempre que per a r, o sigui, [1], s'agafi una arrel determinada de Ω. Així, en general, $[\lambda]$, $[\mu]$, seran iguals o bé diferents segons si λ, μ, són congrus o bé incongrus segons el mòdul n; a més a més, $[0] = 1$; $[\lambda]\cdot[\mu] = [\lambda+\mu]$; $[\lambda]^\nu = [\lambda\nu]$; la suma $[0] + [\lambda] + [2\lambda] + \cdots + [(n-1)\lambda]$ o bé 0 o bé n, segons si λ és no divisible per n o bé divisible.

343. Si per al mòdul n, g és un nombre tal com els que a la secció III hem anomenat arrel primitiva, els $n-1$ nombres 1, g, gg, …, g^{n-2}, seran congrus als 1, 2, 3, …, $n-1$, segons el mòdul n, encara que en un altre ordre; és a dir, qualsevol nombre d'una sèrie en tindrà un de congru a l'altra. D'aquí se segueix espontàniament que les arrels [1], $[g]$, $[gg]$, …, $[g^{n-2}]$, coincideixen amb Ω; i, de manera completament similar, més generalment, $[\lambda]$, $[\lambda g]$, $[\lambda gg]$, …, $[\lambda g^{n-2}]$, coincideixen amb Ω, on λ designa un enter qualsevol no divisible per n. A més a més, com que és $g^{n-1} \equiv 1\,(\text{mòd.}\,n)$, es copsarà sense cap dificultat que dues arrels $[\lambda g^\mu]$, $[\lambda g^\nu]$, són idèntiques o bé diferents segons que μ, ν, siguin congrus o bé incongrus segons el mòdul $n-1$.

Així, si G és una altra arrel primitiva, les arrels [1], $[g]$, …, $[g^{n-2}]$, també coincideixen amb les [1], $[G]$, …, $[G^{n-2}]$, si no es considera l'ordre. Però, a part d'això, es prova fàcilment que si e és un divisor de $n-1$, i es posa $n-1 = ef$, $g^e = h$, $G^e = H$, els f nombres 1, h, hh, …, h^{f-1}, també són congrus amb els 1, H, H^2, …, H^{f-1}, segons n (sense respecte a l'ordre). En efecte, suposem que $G \equiv g^\omega\,(\text{mòd.}\,n)$ i sigui μ un

nombre arbitrari, positiu, i $< f$, i ν el residu mínim de $\mu\omega \,(\text{mòd.}\, f)$. Llavors, serà $\nu e \equiv \mu\omega e \,(\text{mòd.}\, n-1)$, d'aquí, $g^{\nu e} \equiv g^{\mu\omega e} \equiv G^{\mu e} \,(\text{mòd.}\, n)$, o sigui, $H^{\mu} \equiv h^{\nu}$; és a dir, qualsevol nombre de la darrera sèrie 1, H, H^2, etc., en tindrà un de congru en la sèrie 1, h, hh, ..., i igualment, a la inversa. D'aquí és evident que les f arrels [1], [h], [hh], ..., [h^{f-1}], són idèntiques a les [1], [H], [H^2], ..., [H^{f-1}], i, més generalment, es copsarà fàcilment de la mateixa manera que [λ], [λh], [λhh], ..., [λh^{f-1}], coincideixen amb [λ], [λH], [λH^2], ..., [λH^{f-1}]. Designarem per (f, λ) la *suma* de les tals f arrels, [λ]+[λh]+*etc.*+[λh^{f-1}], que s'ha de considerar independent de g, ja que no canvia agafant per a g una altra arrel primitiva; i anomenarem *període* de (f, λ) el *complex* de les seves arrels, on no es considera l'ordre de les arrels.* En exhibir un tal període, serà convenient reduir cada arrel de què consta a la seva expressió més simple, posem, substituir els nombres λ, λh, λhh, etc., pels seus residus mínims segons el mòdul n; i, si plau, també es podran ordenar les parts del període segons les seves magnituds.

Exemple. Per a $n = 19$, on 2 és arrel primitiva, el període (6, 1) consta de les arrels [1], [8], [64], [512], [4096], [32768], o sigui, [1], [7], [8], [11], [12], [18]. Similarment, el període (6, 2) consta de [2], [3], [5], [14], [16], [17]. El període (6, 3) es troba idèntic al precedent. El període (6, 4) conté [4], [6], [9], [10], [13], [15].

344. Sobre els períodes d'aquest tipus es presenten immediatament les observacions següents.

* En el que segueix, la suma es podrà anomenar també valor numèric del període, o més simplement període, quan no s'ha de témer ambigüitat.

I. Com que $\lambda h^f \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h$, etc. (mòd. n), és evident que de les mateixes arrels de què consta (f, λ) també consten $(f, \lambda h)$, $(f, \lambda hh)$, etc.; així, en general, si $[\lambda']$ designa qualsevol arrel de (f, λ), aquest període serà completament idèntic a (f, λ'). Així, si dos períodes que consten del mateix nombre d'arrels (els quals anomenarem *semblants*) tenen alguna arrel comuna, evidentment seran idèntics. Per tant, no pot resultar que dues arrels es continguin simultàniament en algun període, però en un altre similar només se'n trobi una d'elles; a més a més, és clar que si dues arrels $[\lambda]$, $[\lambda']$ pertanyen al mateix període de f termes, el valor de l'expressió $\dfrac{\lambda'}{\lambda}$ (mòd. n) és congru a alguna potència de h, o sigui, es pot suposar que $\lambda' \equiv \lambda g^{\nu e}$ (mòd. n).

II. Si $f = n-1$, $e = 1$, el període $(f, 1)$ coincideix, evidentment, amb Ω; però en els casos restants Ω estarà compost dels e períodes $(f, 1)$, (f, g), (f, gg), …, (f, g^{e-1}). Així, aquests períodes seran completament diferents entre si i és clar que qualsevol altre període similar (f, λ) coincideix amb algun d'aquests si $[\lambda]$ pertany a Ω, és a dir, si λ no és divisible per n. Però el període $(f, 0)$, o bé (f, kn), està compost, evidentment, de f unitats. De manera igualment fàcil es copsa que si λ és un nombre qualsevol no divisible per n, el complex dels e períodes (f, λ), $(f, \lambda g)$, $(f, \lambda gg)$, …, $(f, \lambda g^{e-1})$, també coincideix amb Ω. Així, per exemple, per a $n = 19$, $f = 6$, Ω consta dels tres períodes (6, 1), (6, 2), (6, 4), a algun dels quals es redueix qualsevol altre similar, excepte el (6, 0).

III. Si $n-1$ és el producte de tres nombres positius a, b, c, és evident que qualsevol període de bc termes és

compost de b períodes de c termes, posem $(bc,\ \lambda)$ de $(c,\ \lambda)$, $(c,\ \lambda g^a)$, $(c,\ \lambda g^{2a})$, $\ldots$, $(c,\ \lambda g^{ab-a})$, d'on aquests s'anomenaran continguts en aquell. Així, per a $n = 19$, el període $(6,\ 1)$ consta dels tres $(2,\ 1)$, $(2,\ 8)$, $(2,\ 7)$, el primer dels quals conté les arrels r, r^{18}; el segon, r^8, r^{11}; el tercer, r^7, r^{12}.

345. Teorema. *Siguin* $(f,\ \lambda)$, $(f,\ \mu)$, *dos períodes similars, idèntics o diferents, i consti* $(f,\ \lambda)$ *de les arrels* $[\lambda]$, $[\lambda']$, $[\lambda'']$, *etc. Llavors, el producte de* $(f,\ \lambda)$ *per* $(f,\ \mu)$ *serà la suma de* f *períodes similars, posem* $= (f,\ \lambda+\mu) + (f,\ \lambda'+\mu) + (f,\ \lambda''+\mu) + etc. = W$.

Dem. Sigui, com més amunt, $n - 1 = ef$; g una arrel primitiva per al mòdul n, i $h = g^e$, d'on, pel que precedeix, serà $(f,\ \lambda) = (f,\ \lambda h) = (f,\ \lambda hh)$ etc. D'aquí, el producte cercat serà $= [\mu]\cdot(f,\ \lambda) + [\mu h]\cdot(f,\ \lambda h) + [\mu hh]\cdot(f,\ \lambda hh) + etc.$, de manera que

$$
\begin{aligned}
&= [\lambda+\mu] + [\lambda h+\mu] + \cdots + [\lambda h^{f-1}+\mu] \\
&+[\lambda h+\mu h] + [\lambda hh+\mu h] + \cdots + [\lambda h^{f}+\mu h] \\
&+[\lambda hh+\mu hh] + [\lambda h^3+\mu hh] + \cdots + [\lambda h^{f+1}+\mu hh] \\
&\qquad \text{etc.},
\end{aligned}
$$

expressió que conté en total ff arrels. Si aquí cada una de les columnes verticals es recull separadament en una suma, apareix, evidentment, $(f,\ \lambda+\mu) + (f,\ \lambda h+\mu) + \cdots + (f,\ \lambda h^{f-1}+\mu)$, expressió que es copsa sense cap dificultat que coincideix amb W, ja que els nombres λ, λ', λ'', etc., han de ser, per hipòtesi, congrus als λ, λh, λhh, $\ldots$, λh^{f-1}, segons el mòdul n (on l'ordre aquí no interessa gens), de manera que també $\lambda+\mu$, $\lambda'+\mu$, $\lambda''+\mu$, etc., als $\lambda+\mu$, $\lambda h+\mu$, $\lambda hh+\mu$, $\ldots$, $\lambda h^{f-1}+\mu$. *Q. E. D.*

Afegim a aquest teorema els corol·laris següents.

I. Si k designa un enter qualsevol, el producte de $(f,\ k\lambda)$ per $(f,\ k\mu)$ serà $= (f,\ k(\lambda+\mu)) + (f,\ k(\lambda'+\mu)) + (f,\ k(\lambda''+\mu)) + etc.$

II. Com que cadascuna de les parts de què consta W, coincideix, o bé amb la suma $(f,\ 0)$, que és $= f$, o bé amb alguna de les $(f,\ 1)$, $(f,\ g)$, $(f,\ gg)$, $\ldots$, $(f,\ g^{e-1})$, W es podrà reduir a la forma següent: $W = af + b(f,\ 1) + b'(f,\ g) + b''(f,\ gg) + \cdots + b^{\varepsilon}(f,\ g^{e-1})$, on els coeficients a, b, b', etc., seran enters positius (o també algun $= 0$); a més a més, és clar que el producte de $(f,\ k\lambda)$ per $(f,\ k\mu)$ resulta llavors $= af + b(f,\ k) + b'(f,\ kg) + \cdots + b^{\varepsilon}(f,\ kg^{e-1})$. Així, per exemple, per a $n = 19$, el producte de la suma $(6,\ 1)$ per si mateixa, o sigui, el quadrat d'aquesta suma, resulta $= (6,2) + (6,8) + (6,9) + (6,12) + (6,13) + (6,19) = 6 + 2(6,1) + (6,2) + 2(6,4)$.

III. Com que el producte de cadascuna de les parts de W per un període similar $(f,\ \nu)$ es pot reduir a una forma anàloga, és evident que el producte de tres períodes $(f,\ \lambda)\cdot(f,\ \mu)\cdot(f,\ \nu)$ també es pot expressar per $cf + d(f,\ 1) + \cdots + d^{\varepsilon}(f,\ g^{e-1})$, i els coeficients c, d, etc., surten enters i positius (o bé $= 0$) i, a sobre, per a qualsevol valor enter de k resulta $(f,\ k\lambda)\cdot(f,\ k\mu)\cdot(f,\ k\nu) = cf + d(f,\ k) + d'(f,\ kg) + etc.$ Igualment, aquest teorema s'estén als productes de períodes similars qualssevol, i no importa gens si aquests períodes són tots diferents, o si en part o bé tots idèntics.

IV. D'aquí es conclou que si en qualsevol funció algebraica racional entera $F = \phi(t,\ u,\ v,\ \ldots)$ se substitueixen les indeterminades t, u, v, etc., pels períodes

similars $(f,\ \lambda)$, $(f,\ \mu)$, $(f,\ \nu)$, etc., respectivament, el seu valor és reductible a la forma $A + B(f,\ 1) + B'(f,\ g) + B''(f,\ gg) + \cdots + B^{\varepsilon}(f,\ g^{e-1})$ i els coeficients A, B, B', etc., resulten tots enters, si tots els coeficients determinats en F són enters; però, si posteriorment se substitueixen t, u, v, etc., per $(f,\ k\lambda)$, $(f,\ k\mu)$, $(f,\ k\nu)$, etc., respectivament, el valor de F es redueix a $A + B(f,\ k) + B'(f,\ kg) + etc.$

346. Teorema. *Suposant que λ és un nombre no divisible per n, i escrivint, per abreujar, p per $(f,\ \lambda)$, qualsevol altre període similar $(f,\ \mu)$, on també se suposa μ no divisible per n, es podrà reduir a una tal forma $\alpha + \beta p + \gamma pp + \cdots + \theta p^{e-1}$ de manera que els coeficients α, β, etc., siguin quantitats racionals determinades.*

Dem. Es designen, per abreujar, els períodes $(f,\ \lambda g)$, $(f,\ \lambda gg)$, $(f,\ \lambda g^3)$, etc., fins a $(f,\ \lambda g^{e-1})$, la quantitat dels quals és $e-1$, i amb algun dels quals coincideix necessàriament $(f,\ \mu)$, per p', p'', p''', etc. Així, es té immediatament l'equació $0 = 1 + p + p' + p'' + p''' + etc. \ldots$ (I); però, desenvolupant, segons els preceptes de l'article precedent, els valors de les potències de p fins a la $(e-1)$-èsima, en sorgiran $e-2$ altres tals com

$$0 = pp + A + ap + a'p' + a''p'' + a'''p''' + etc. \qquad \text{(II)}$$
$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + etc. \qquad \text{(III)}$$
$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + etc. \qquad \text{(IV)}$$
$$\text{etc.,}$$

on tots els coeficients A, a, a', etc., B, b, b', etc., seran enters i, cosa que cal notar molt bé, completament independents de λ, com se segueix espontàniament de l'article precedent; és a dir, les mateixes equacions també valdran qualsevol que sigui l'altre valor que s'atribuei-

xi a λ; aquesta observació, evidentment, també s'estén a l'equació (I), sempre que s'agafi λ no divisible per n. Suposem que $(f,\ \mu) = p'$; en efecte, es copsarà molt fàcilment que si $(f,\ \mu)$ coincideix amb un altre període dels p'', p''', etc., es poden aplicar uns raonaments completament anàlegs als següents. Com que la quantitat d'equacions I, II, III, etc., és $e-1$, les quantitats p'', p''', etc., la quantitat de les quals és $= e-2$, es poden eliminar d'allà per mètodes coneguts, de manera que surti una equació (Z) lliure d'elles, $0 = \mathfrak{A} + \mathfrak{B}p + \mathfrak{C}pp + etc. + \mathfrak{M}p^{e-1} + \mathfrak{N}p'$, que això es podrà fer de manera que tots els coeficients $\mathfrak{A}$, $\mathfrak{B}$, $\ldots$, $\mathfrak{N}$, siguin enters i, certament, no tots $= 0$. Ara, si aquí no és $\mathfrak{N} = 0$, és clar directament que p' es determina d'aquí de la manera que s'ha enunciat en el teorema. Així, resta que demostrem que no pot resultar $\mathfrak{N} = 0$.

Suposant que és $\mathfrak{N} = 0$, l'equació Z resulta $\mathfrak{M}p^{e-1} + etc. + \mathfrak{B}p + \mathfrak{A} = 0$, a la qual, com que certament no ascendeix més enllà del grau $(e-1)$-èsim, no poden satisfer més de $e-1$ valors diferents de p. Però com que les equacions de les quals fou deduïda Z són independents de λ, és clar que tampoc Z no depèn de λ, o sigui, que té lloc qualsevol que sigui l'enter no divisible per n que s'agafi per λ. Per tant, l'equació Z se satisfà si s'estableix p igual a qualsevol de les e sumes $(f,\ 1)$, $(f,\ g)$, $(f,\ gg)$, $\ldots$, $(f,\ g^{e-1})$, d'on se segueix espontàniament que totes aquestes sumes no poden ser diferents, sinó que com a mínim dues han de ser iguals entre si. Contingui una de dues tals sumes iguals les arrels $[\zeta]$, $[\zeta']$, $[\zeta'']$, etc., i l'altra, les $[\eta]$, $[\eta']$, $[\eta'']$, etc., i suposem (cosa que és lícita) que tots els nombres ζ, ζ', ζ'', etc., η, η', η'', etc., són positius i $< n$; evidentment, també tots seran diferents i cap $= 0$. Es designa per Y la funció

$x^{\zeta} + x^{\zeta'} + x^{\zeta''} + etc. - x^{\eta} - x^{\eta'} - x^{\eta''} - etc.$, el terme més gran de la qual no ascendeix més enllà de x^{n-1}, i és clar que resulta $Y = 0$ si s'estableix $x = [1]$; d'aquí, Y implicarà el factor $x - [1]$, el qual tindrà *comú* amb la funció denotada per X en el que precedeix; això, però, es podrà demostrar fàcilment que és absurd. En efecte, si Y tingués algun factor comú amb X, el *màxim* comú divisor de les funcions X, Y (que ja és clar d'aquí que, certament, no pot ascendir a $n - 1$ dimensions perquè Y és divisible per x), tindria tots els seus coeficients racionals, com se segueix espontàniament de la natura de les operacions per a investigar el màxim comú divisor de dues tals funcions, els coeficients de les quals són tots racionals. Però en l'article 341 hem mostrat que X no pot implicar un factor més petit que de $n-1$ dimensions els coeficients del qual siguin tots racionals; per la qual cosa, la suposició de ser $\mathfrak{N} = 0$ no pot ser consistent.

Exemple. Per a $n = 19$, $f = 6$, resulta $pp = 6 + 2p + p' + 2p''$, d'on, i de $0 = 1 + p + p' + p''$, es dedueix $p' = 4 - pp$, $p'' = -5 - p + pp$. Per tant, $(6,2) = 4-(6,1)^2$, $(6,4) = -5-(6,1)+(6,1)^2$; $(6,4) = 4-(6,2)^2$, $(6,1) = -5-(6,2)+(6,2)^2$; $(6,1) = 4-(6,4)^2$, $(6,2) = -5-(6,4)+(6,4)^2$.

347. Teorema. *Si $F = \phi(t, u, v, \ldots)$ és una funció invariable,* algebraica, racional, entera, de les f indeterminades t, u, v, etc., i substituint aquestes per*

* Se sap que s'anomenen funcions invariables aquelles en les quals totes les indeterminades entren de la mateixa manera, o sigui, més clarament, aquelles que no canvien qualsevol que sigui la manera com es permutin les indeterminades entre si; d'aquest tipus són, per exemple, la suma de totes, el producte de totes, la suma dels productes de les parelles, etc.

les f arrels contingudes en el període $(f,\ \lambda)$, el valor de F, pels preceptes de l'article 340*, es redueix a la forma $A + A'[1] + A''[2] + etc. = W$; les arrels que en aquesta expressió pertanyen a un mateix període qualsevol de f termes tindran els coeficients iguals.*

Dem. Siguin $[p]$, $[q]$, dues arrels pertanyents a un mateix període, i se suposen p, q, positius i menors que n, de manera que convé demostrar que $[p]$ i $[q]$ tenen el mateix coeficient en W. Sigui $q \equiv pg^{\nu e}$ (mòd. n); siguin, a més a més, $[\lambda]$, $[\lambda']$, $[\lambda'']$, etc., les arrels contingudes en $(f,\ \lambda)$, on suposem els nombres λ, λ', λ'', etc., positius i menors que n; finalment, siguin μ, μ', μ'', etc., els residus mínims positius dels nombres $\lambda g^{\nu e}$, $\lambda' g^{\nu e}$, $\lambda'' g^{\nu e}$, etc., segons el mòdul n, que, evidentment, seran idèntics als nombres λ, λ', λ'', etc., encara que amb l'ordre transposat. Ara, de l'article 340, és clar que $\phi([\lambda g^{\nu e}], [\lambda' g^{\nu e}], [\lambda'' g^{\nu e}], \ldots)$ =(I) es redueix a $A + A'[g^{\nu e}] + A''[2g^{\nu e}] + etc.$ o bé a $A + A'[\theta] + A''[\theta'] + etc. = (W')$, designant per θ, θ', etc., els residus mínims dels nombres $g^{\nu e}$, $2g^{\nu e}$, etc., segons el mòdul n, d'on és evident que $[q]$ té el mateix coeficient en (W') que $[p]$ té en (W). Però es copsa sense cap dificultat que, del desenvolupament de l'expressió (I), apareix el mateix que del desenvolupament de la $\phi([\mu], [\mu'], [\mu''], etc.)$, ja que $\mu \equiv \lambda g^{\nu e}$, $\mu' \equiv \lambda' g^{\nu e}$, etc. (mòd. n); aquesta expressió, però, produeix el mateix que la $\phi([\lambda], [\lambda'], [\lambda''], etc.)$, ja que els nombres μ, μ', μ'', etc., només difereixen de λ, λ', λ'', etc., en l'ordre, el qual no interessa gens en una funció invariable. D'aquí es conclou que W' serà completament idèntica a W; per la qual cosa, l'arrel $[q]$ tindrà el mateix coeficient en W que $[p]$. *Q. E. D.*

D'aquí és evident que W es pot reduir a la forma $A + a(f, 1) + a'(f, g) + a''(f, gg) + \cdots + a^{\varepsilon}(f, g^{e-1})$, de manera que els coeficients A, a, $\ldots$, a^{ε}, són quantitats determinades que, a sobre, seran enters si tots els coeficients racionals de F són enters. Així, per exemple, si $n = 19$, $f = 6$, $\lambda = 1$, i la funció ϕ designa la suma dels productes de les parelles d'indeterminades, el seu valor es redueix a $3 + (6, 1) + (6, 4)$.

A més a més, es copsarà fàcilment que si després se substitueixen t, u, v, etc., per les arrels d'un altre període $(f, k\lambda)$, el valor de F resulta $A + a(f, k) + a'(f, kg) + a''(f, kgg) + etc.$

348. Com que en una equació qualsevol $x^f - \alpha x^{f-1} + \beta x^{f-2} - \gamma x^{f-3} + \cdots = 0$ els coeficients α, β, γ, etc., són funcions invariables de les arrels, posem α la suma de totes, β la suma dels productes de les parelles, γ la suma dels productes de les ternes, etc., en l'equació les arrels de la qual són les arrels contingudes en el període (f, λ), el primer coeficient serà $= (f, \lambda)$, però cadascun dels restants es podrà reduir a una forma tal com $A + a(f, 1) + a'(f, g) + \cdots + a^{\varepsilon}(f, g^{e-1})$, on tots els A, a, a', etc., seran enters; i, a part d'això, és clar que l'equació les arrels de la qual són les arrels contingudes en qualsevol altre període $(f, k\lambda)$ es deriva d'aquella si se substitueix en cadascun dels coeficients $(f, 1)$ per (f, k); (f, g) per (f, kg) i, en general, (f, p) per (f, kp). Així, d'aquesta manera, es podran assignar e equacions $z = 0$, $z' = 0$, $z'' = 0$, etc., les arrels de les quals són les arrels contingudes en $(f, 1)$, en (f, g), (f, gg), etc., quan abans es coneixen les e sumes $(f, 1)$, (f, g), (f, gg), etc., o bé, millor, quan abans s'ha trobat *una* qualsevol d'aquestes, ja que, per l'article precedent,

d'una es poden deduir racionalment totes les restants. Fet això, es té simultàniament descomposta la funció X en e factors de f dimensions; en efecte, el producte de les funcions z, z', z'', etc., serà, evidentment, $= X$.

Exemple. Per a $n = 19$, la suma de totes les arrels del període $(6, 1)$ és $= (6, 1) = \alpha$; la suma dels productes de les parelles resulta $= 3 + (6, 1) + (6, 4) = \beta$; similarment, la suma dels productes de les ternes es troba $= 2 + 2(6, 1) + (6, 2) = \gamma$; la suma dels productes de les quaternes, $= 3 + (6, 1) + (6, 4) = \delta$; la suma dels productes de les quinternes, $= (6, 1) = \varepsilon$; el producte de totes $= 1$; per tant, l'equació $z = x^6 - \alpha x^5 + \beta x^4 - \gamma x^3 + \delta xx - \varepsilon x + 1 = 0$ aplega totes les arrels contingudes en $(6, 1)$. Si, en els coeficients α, β, γ, etc., se substitueixen $(6, 1)$, $(6, 2)$, $(6, 4)$, respectivament, per $(6, 2)$, $(6, 4)$, $(6, 1)$, apareixerà l'equació $z' = 0$, que aplegarà les arrels de $(6, 2)$; i, si, aquí, novament, s'aplica la mateixa commutació, es tindrà l'equació $z'' = 0$, que aplega les arrels de $(6, 4)$, i el producte $zz'z''$ serà $= X$.

349. Sovint és més còmode, sobretot quan f és un nombre gran, deduir els coeficients β, γ, etc., del teorema de Newton sobre les sumes de les potències de les arrels. Això és, espontàniament és clar que la suma dels quadrats de les arrels contingudes en (f, λ) és $= (f, 2\lambda)$, la suma dels cubs, $= (f, 3\lambda)$, etc. Així, escrivint, per abreujar, q, q', q'', etc., per (f, λ), $(f, 2\lambda)$, $(f, 3\lambda)$, etc., serà $\alpha = q$, $2\beta = \alpha q - q'$, $3\gamma = \beta q - \alpha q' + q''$, etc., on, per l'article 345, els productes de dos períodes s'hauran de convertir immediatament en sumes de períodes. Així, en el nostre exemple, escrivint p, p', p'', per $(6, 1)$, $(6, 2)$, $(6, 4)$, respectivament, q, q', q'', q''', q^{IV}, q^V, resulten, respectivament, $= p$, p', p', p'', p', p''; d'aquí, $\alpha = p$,

$2\beta = pp - pp' = 6+2p+2p''$; $3\gamma = (3+p+p'')p - pp' + p' = 6+6p+3p'$; $4\delta = (2+2p+p')p - (3+p+p'')p' + pp' - p'' = 12+4p+4p''$, etc. D'altra banda, d'aquesta manera, és suficient calcular només la meitat dels coeficients; efectivament, no és difícil provar que els últims són, o bé iguals als primers en ordre invers, posem, l'últim = 1, el penúltim = α, l'avantpenúltim = β, etc., o bé es dedueixen respectivament d'aquests mateixos si se substitueixen $(f, 1)$, (f, g), etc., per $(f, -1)$, $(f, -g)$, etc., o sigui, $(f, n-g)$, $(f, n-1)$, etc. El primer cas té lloc quan f és parell; el darrer, quan f és imparell; però l'últim coeficient sempre resulta = 1. El fonament d'això es troba en el teorema de l'article 79; però, per abreujar, no ens entretenim en aquest argument.

350. Teorema. *Sigui $n-1$ el producte de tres enters positius α, β, γ; consti el període $(\beta\gamma, \lambda)$, que és de $\beta\gamma$ termes, dels β períodes menors, de γ termes, (γ, λ), (γ, λ'), (γ, λ''), etc., i suposem que si en una funció de β indeterminades, disposada similarment com en l'article precedent, és a dir, en $F = \phi(t, u, v, \ldots)$, les indeterminades t, u, v, etc., se substitueixen per les sumes (γ, λ), (γ, λ'), (γ, λ''), etc., respectivament, el seu valor es redueix, pels preceptes de l'article precedent, a $A + a(\gamma, 1) + a'(\gamma, g) + \cdots + a^{\zeta}(\gamma, g^{\alpha\beta-\alpha}) + \cdots + a^{\theta}(\gamma, g^{\alpha\beta-1}) = W$. Llavors, afirmo que, si F és una funció invariable, els períodes de W que estan continguts en el mateix període de $\beta\gamma$ termes, és a dir, en general, tals com (γ, g^{μ}) i $(\gamma, g^{\alpha\nu+\mu})$, on ν designa un enter qualsevol, hauran de tenir els mateixos coeficients.*

Dem. Com que el període $(\beta\gamma, \lambda g^{\alpha})$ és idèntic al $(\beta\gamma, \lambda)$, els menors $(\gamma, \lambda g^{\alpha})$, $(\gamma, \lambda' g^{\alpha})$, $(\gamma, \lambda'' g^{\alpha})$, etc., dels quals se sap, evidentment, el primer, coincidiran

necessàriament amb aquells dels quals se sap el darrer, encara que en un altre ordre. Així, si se suposa que F es transforma en W' substituïts t, u, v, etc., respectivament, per aquells, W' coincidirà amb W. Però, per l'article 347, serà $W' = A+a(\gamma, g^{\alpha})+a'(\gamma, g^{\alpha+1})+\cdots+a^{\zeta}(\gamma, g^{\alpha\beta})+\cdots+a^{\theta}(\gamma, g^{\alpha\beta+\alpha-1}) = A+a(\gamma, g^{\alpha})+a'(\gamma, g^{\alpha+1})+\cdots+a^{\zeta}(\gamma, 1)+\cdots+a^{\theta}(\gamma, g^{\alpha-1})$; per tant, com que aquesta expressió ha de coincidir amb W, el coeficient primer, segon, tercer, etc., de W (començant per a) coincidirà necessàriament amb el $(\alpha+1)$-èsim, el $(\alpha+2)$-èsim, el $(\alpha+3)$-èsim, etc., d'on es conclou sense cap dificultat que, en general, els coeficients dels períodes (γ, g^{μ}), $(\gamma, g^{\alpha+\mu})$, $(\gamma, g^{2\alpha+\mu})$, $\ldots$, $(\gamma, g^{\nu\alpha+\mu})$, que són els $(\mu+1)$-èsim, $(\alpha+\mu+1)$-èsim, $(2\alpha+\mu+1)$-èsim, $\ldots$, $(\nu\alpha+\mu+1)$-èsim, han de coincidir entre si. *Q. E. D.*

D'aquí, és evident que W es pot reduir a la forma $A+a(\beta\gamma, 1)+a'(\beta\gamma, g)+\cdots+a^{\varepsilon}(\beta\gamma, g^{\alpha-1})$, on tots els coeficients A, a, etc., seran enters si tots els coeficients determinats de F són enters. A més a més, es copsarà fàcilment que si, després, per les indeterminades de F se substitueixen β períodes de γ termes continguts en un altre període de $\beta\gamma$ termes, posem en $(\beta\gamma, \lambda k)$, que, evidentment, seran $(\gamma, \lambda k)$, $(\gamma, \lambda' k)$, $(\gamma, \lambda'' k)$, etc., el valor que surt d'aquí serà $A+a(\beta\gamma, k)+a'(\beta\gamma, gk)+\cdots+a^{\varepsilon}(\beta\gamma, g^{\alpha-1}k)$.

D'altra banda, és clar que el teorema també es pot estendre al cas en què $\alpha = 1$, o sigui, $\beta\gamma = n-1$; això és, aquí *tots* els coeficients de W seran iguals, d'on W es reduirà a la forma $A+a(\beta\gamma, 1)$.

351. Així, retinguts tots els signes de l'article precedent, és evident que cadascun dels coeficients de l'equació les arrels de la qual són β sumes $(\gamma,\ \lambda)$, $(\gamma,\ \lambda')$, $(\gamma,\ \lambda'')$, etc., es pot reduir a una forma tal com $A + a(\beta\gamma,\ 1) + a'(\beta\gamma,\ g) + \cdots + a^{\varepsilon}(\beta\gamma,\ g^{\alpha-1})$ i tots els nombres A, a, etc., resulten enters; però, l'equació les arrels de la qual són β períodes de γ termes continguts en algun període $(\beta\gamma,\ k\lambda)$ es deriva d'aquella, si, a tot arreu, en els coeficients, se substitueix qualsevol període $(\beta\gamma,\ \mu)$ pel període $(\beta\gamma,\ k\mu)$. Així, doncs, si $\alpha = 1$, tots els β períodes de γ termes es determinaran per una equació de β-èsim grau, cadascun dels coeficients de la qual es redueix a la forma $A + a(\beta\gamma,\ 1)$, *de manera que són quantitats conegudes*, ja que $(\beta\gamma,\ 1) = (n-1,\ 1) = -1$. Però, si $\alpha > 1$, els coeficients de l'equació les arrels de la qual són tots els períodes de γ termes continguts en algun període donat de $\beta\gamma$ termes, seran quantitats conegudes sempre que se sàpiguen els valors numèrics de tots els α períodes de $\beta\gamma$ termes. D'altra banda, el càlcul dels coeficients d'aquestes equacions es fa sovint més còmodament, sobretot quan β no és molt petit, si, primer, es descobreixen les sumes de les potències de les arrels i, després, es dedueixen d'aquestes, pel teorema de Newton, els coeficients, de manera similar com més amunt en l'article 349.

Exemple. I. Se cerca, per a $n = 19$, l'equació les arrels de la qual són les sumes $(6,\ 1)$, $(6,\ 2)$, $(6,\ 4)$. Designant aquestes arrels per p, p', p'', respectivament, i l'equació cercada per $x^3 - Axx + Bx - C = 0$, resulta $A = p+p'+p''$, $B = pp'+pp''+p'p''$, $C = pp'p''$. D'aquí $A = (18,\ 1) = -1$; a més a més, es té $pp' = p+2p'+3p''$, $pp'' = 2p+3p'+p''$, $p'p'' = 3p+p'+2p''$, d'on $B = 6(p+p'+p'') = 6(18,\ 1) = -6$; finalment, resulta $C = (p+$

$2p'+3p'')p'' = 3(6,0)+11(p+p'+p'') = 18-11 = 7$; per tant, l'equació cercada, $x^3+xx-6x-7=0$. Utilitzant l'altre mètode, tenim $p+p'+p'' = -1$; $pp = 6+2p+p'+2p''$, $p'p' = 6+2p'+p''+2p$, $p''p'' = 6+2p''+p+2p'$, d'on $pp+p'p'+p''p'' = 18+5(p+p'+p'') = 13$; i, similarment, $p^3+p'^3+p''^3 = 36+34(p+p'+p'') = 2$; d'aquí, pel teorema de Newton, es deriva la mateixa equació que més amunt.

II. Se cerca, per a $n = 19$, l'equació les arrels de la qual són les sumes (2, 1), (2, 7), (2, 8). Designades aquestes per q, q', q'', respectivament, es troba $q+q'+q'' = (6,1)$, $qq'+qq''+q'q'' = (6,1)+(6,4)$, $qq'q'' = 2+(6,2)$, d'on, retinguts els símbols de l'exemple precedent, l'equació cercada serà $x^3-pxx+(p+p'')x-2-p' = 0$. L'equació les arrels de la qual són les sumes (2, 2), (2, 3), (2, 5), contingudes en (6, 2), es dedueix de la precedent substituint per a p, p', p'', respectivament p', p'', p, i, feta de nou la mateixa substitució, apareix l'equació les arrels de la qual són les sumes (2, 4), (2, 6), (2, 9), contingudes en (6, 4).

352. Els teoremes precedents, amb les conclusions annexes, contenen les parts principals de tota la teoria, i la manera de trobar els valors de les arrels Ω es podrà tractar ara en poques paraules.

Abans de tot, s'ha d'agafar un nombre g que sigui una arrel primitiva per al mòdul n i descobrir els residus mínims de les potències de g fins a g^{n-2} segons el mòdul n. Es descompon $n-1$ en factors, i, certament, en factors primers, si el problema es vol reduir a equacions de grau tan petit com sigui possible; siguin aquests (en ordre completament arbitrari) α, β, γ, $\ldots$, ζ, i es posa

$\frac{n-1}{\alpha} = \beta\gamma\cdots\zeta = a$, $\frac{n-1}{\alpha\beta} = \gamma\cdots\zeta = b$, etc. Es distribueixen totes les arrels Ω en α períodes de a termes; cadascun d'aquests, a la vegada, en β períodes de b termes; cadascun d'aquests, de nou, en γ períodes; etc. Se cerca, per l'article 350, una equació (A) de α-èsim grau les arrels de la qual siguin aquelles α sumes de a termes, així, els seus valors es coneixeran per la resolució d'aquesta equació.

Aquí s'origina una dificultat, perquè sembla incert a quina arrel de l'equació (A) s'ha d'establir igual cada suma, posem quina arrel s'ha de denotar per $(a,\ 1)$, quina per $(a,\ g)$, etc.; a això es podrà posar remei de la manera següent. Es pot designar per $(a,\ 1)$ qualsevol arrel de l'equació (A); en efecte, com que qualsevol arrel d'aquesta equació és la suma de a arrels de Ω, i és completament arbitrari quina arrel de Ω es denoti per [1], evidentment es podrà suposar que per [1] s'expressa alguna d'aquestes arrels de les quals consta qualsevol arrel donada de l'equació (A), d'on aquella arrel de l'equació A resultarà $(a,\ 1)$; però, d'aquí, l'arrel [1] encara no es determina absolutament, sinó que encara resta completament arbitrari o indefinit quina arrel de les que constitueixen $(a,\ 1)$ volem adoptar per a [1]. Però simultàniament que s'ha determinat $(a,\ 1)$ totes les sumes restants de a termes també es podran deduir racionalment d'aquí (article 346). D'aquí és clar, simultàniament, que només convé trobar una única arrel per a la resolució d'aquesta. També es pot aplicar el mètode següent, menys directe, per a aquesta finalitat. S'agafa per a [1] una arrel determinada, és a dir, es posa $[1] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$, amb l'enter k elegit a voluntat, però de manera que no sigui divisible per n; fet això, també [2], [3], etc., indicaran

arrels determinades, d'on les sumes $(a, 1)$, (a, g), etc., també designaran quantitats determinades. Calculades aquestes a partir de taules de sinus amb una ploma tan fina, posem per cas, amb una precisió tal que pugui decidir quines són més grans, quines més petites, no podrà quedar cap dubte per quins signes s'ha de distingir cadascuna de les arrels de l'equació (A).

Quan s'han trobat d'aquesta manera totes les α sumes de a termes, s'investiga per l'article 350 l'equació (B) de β-èsim grau les arrels de la qual són les β sumes de b termes contingudes en $(a, 1)$; els coeficients d'aquesta equació seran tots quantitats conegudes. Com que encara és arbitrari quina de les $a = \beta b$ arrels contingudes en $(a, 1)$ es denota per [1], qualsevol arrel donada de l'equació (B) es podrà expressar per $(b, 1)$, ja que, evidentment, es pot suposar que alguna de les b arrels de les quals està compost es denota per [1]. Així, s'investiga una arrel qualsevol de l'equació (B) per la seva resolució, s'estableix $= (b, 1)$, i es deriven d'aquí, per l'article 346, totes les sumes restants de b termes. D'aquesta manera obtenim simultàniament una confirmació del càlcul, ja que sempre aquestes sumes de b termes que pertanyen als mateixos períodes de a termes han de procurar sumes conegudes. En alguns casos pot ser igualment ràpid descobrir unes altres $\alpha - 1$ equacions de β-èsim grau les arrels de les quals siguin, respectivament, cadascuna de les β sumes de b termes contingudes en els períodes restants de a termes (a, g), (a, gg), etc., i investigar *totes* les arrels per a la resolució tant d'aquestes equacions com de l'equació (B); llavors, però, de manera similar com més amunt, amb l'ajut d'una taula de sinus, convindrà decidir a quins períodes de b termes s'han d'establir iguals cadascuna de les ar-

rels produïdes d'aquesta manera. D'altra banda, per a aquest judici, es poden aplicar altres artificis diversos, que en aquest lloc no es poden explicar completament; però un, per al cas en què $\beta = 2$, que és particularment útil, i que es podrà aclarir més breument per exemples que per preceptes, es podrà conèixer en els exemples següents.

Després que s'han descobert d'aquesta manera els valors de totes les $\alpha\beta$ sumes de b termes, de manera completament similar, es podran determinar d'aquí totes les $\alpha\beta\gamma$ sumes de c termes per una equació de grau γ-èsim. Això és, convindrà trobar: *o bé una* equació de γ-èsim grau les arrels de la qual, per l'article 350, siguin les γ sumes de c termes contingudes en $(b,\ 1)$, per la seva resolució, elegir una arrel qualsevol, establir-la $= (c,\ 1)$, i, finalment, per l'article 346, deduir totes les sumes similars restants; *o bé*, de manera similar, desenvolupar completament les $\alpha\beta$ equacions de γ-èsim grau les arrels de les quals són, respectivament, les γ sumes de c termes contingudes en cadascun dels períodes de b termes, extreure els valors de totes les arrels per resolució de totes aquestes equacions i, finalment, determinar l'ordre d'aquestes arrels igualment com més amunt amb l'ajut d'una taula de sinus, o bé, per a $\gamma = 2$, per l'artifici que es mostrarà més avall en els exemples.

Evidentment, en prosseguir d'aquesta manera, es tindran finalment totes les $\dfrac{n-1}{\zeta}$ sumes de ζ termes; així, desenvolupant per l'article 348 l'equació de ζ-èsim grau les arrels de la qual són les ζ arrels de Ω contingudes en $(\zeta,\ 1)$, tots els seus coeficients seran quantitats conegudes; si s'elegeix una arrel qualsevol d'aquesta per

resolució, aquesta es podrà establir = [1] i es tindran totes les arrels restants de Ω per les seves potències. Si plau més, descobrir també per resolució *totes* les arrels d'aquella equació i, a part d'això, per resolució de les altres $\frac{n-1}{\zeta} - 1$ equacions de ζ-èsim grau, les quals, respectivament, mostren totes les ζ arrels contingudes en cadascun dels períodes restants de ζ termes, es podran trobar totes les arrels restants de Ω.

D'altra banda, és clar que al mateix temps que s'ha resolt la primera equació (A), o sigui, al mateix temps que es tenen els valors de totes les α sumes de a termes, també es té espontàniament la descomposició de la funció X en α factors de a dimensions per l'article 348; i, a més a més, després de la resolució de l'equació (B), o sigui, després que s'han trobat els valors de totes les $\alpha\beta$ sumes de b termes, cadascun d'aquells factors s'ha descompost novament en β factors, o sigui, X en $\alpha\beta$ de b dimensions, etc.

353. *Exemple primer, per a* $n = 19$. Com que aquí resulta $n - 1 = 3 \cdot 3 \cdot 2$, la trobada de les arrels Ω s'ha de reduir a la resolució de dues equacions cúbiques i una de quadràtica. Aquest exemple s'entendrà més fàcilment, perquè la major part de les operacions necessàries ja estan contingudes en el que precedeix. Agafant per arrel primitiva g el nombre 2, els residus mínims de les seves potències surten (els exponents de les potències s'han escrit sobre els residus, a la primera sèrie):

0	1	2	3	4	5	6	7	8	9
1	2	4	8	16	13	7	14	9	18

10	11	12	13	14	15	16	17
17	15	11	3	6	12	5	10.

D'aquí, pels articles 344, 345, es dedueix fàcilment la distribució següent de totes les arrels de Ω en tres períodes de sis, i cadascun d'aquests, en terns de parelles de termes:

$$\Omega = (18,1)\begin{cases} (6,1)\begin{cases} (2,1)\ldots & [1],[18] \\ (2,8)\ldots & [8],[11] \\ (2,7)\ldots & [7],[12] \end{cases} \\ (6,2)\begin{cases} (2,2)\ldots & [2],[17] \\ (2,16)\ldots & [3],[16] \\ (2,14)\ldots & [5],[14] \end{cases} \\ (6,4)\begin{cases} (2,4)\ldots & [4],[15] \\ (2,13)\ldots & [6],[13] \\ (2,9)\ldots & [9],[10] \end{cases} \end{cases}$$

L'equació (A), les arrels de la qual són les sumes (6, 1), (6, 2), (6, 4), es troba $x^3 + xx - 6x - 7 = 0$, una de les arrels de la qual surt $= -1,2218761623$. Expressant aquesta per (6, 1), resulta (6, 2) $= 4 -$ (6, 1)$^2 = 2,5070186441$, (6, 4) $= -5 -$ (6, 1) + (6, 1)$^2 = -2,2851424818$. D'aquí, X serà descomposta en tres factors de 6 dimensions, si se substitueixen aquests valors en l'article 348.

L'equació (B), les arrels de la qual són les sumes (2, 1), (2, 7), (2, 8), surt la $x^3 - (6,1)xx + ((6,1) + (6,4))x - 2 - (6,2) = 0$, o sigui, $x^3 + 1,2218761623xx - 3,5070186441x - 4,5070186441 = 0$, una arrel de la qual s'elegeix $-1,3545631433$, que expressarem per (2, 1).

Però, pel mètode de l'article 346, es troben les equacions següents on, per abreujar, s'escriu q per (2, 1): (2, 2) $= qq - 2$, (2, 3) $= q^3 - 3q$, (2, 4) $= q^4 - 4qq + 2$, (2, 5) $= q^5 - 5q^3 + 5q$, (2, 6) $= q^6 - 6q^4 + 9qq - 2$, (2, 7) $= q^7 - 7q^5 + 14q^3 - 7q$, (2, 8) $= q^8 - 8q^6 + 20q^4 - 16qq + 2$, (2, 9) $= q^9 - 9q^7 + 27q^5 - 30q^3 + 9q$. En el cas present, aquestes equacions es poden treure més còmodament per les reflexions següents que pels preceptes de l'article 346. Suposant $[1] = \cos\frac{kP}{19} + i\sin\frac{kP}{19}$, resulta $[18] = \cos\frac{18kP}{19} + i\sin\frac{18kP}{19} = \cos\frac{kP}{19} - i\sin\frac{kP}{19}$ de manera que $(2,\ 1) = 2\cos\frac{kP}{19}$; i també, en general, $[\lambda] = \cos\frac{\lambda kP}{19} + i\sin\frac{\lambda kP}{19}$, de manera que $(2,\ \lambda) = [\lambda] + [18\lambda] = [\lambda] + [-\lambda] = 2\cos\frac{\lambda kP}{19}$. Per tant, si $\frac{1}{2}q = \cos\omega$, serà $(2,\ 2) = 2\cos 2\omega$, $(2,\ 3) = 2\cos 3\omega$, etc., d'on per les conegudes equacions per als cosinus dels múltiples dels angles es deriven les mateixes fórmules que més amunt. Ara, d'aquestes fórmules s'obtenen els valors numèrics següents:

$(2,2) = -0,1651586909$ $\quad$ $(2,6) = \ 0,4909709743$
$(2,3) = \ 1,5782810188$ $\quad$ $(2,7) = -1,7589475024$
$(2,4) = -1,9727226068$ $\quad$ $(2,8) = \ 1,8916344834$
$(2,5) = \ 1,0938963162$ $\quad$ $(2,9) = -0,8033908493.$

Els valors de (2, 7), (2, 8), també es poden obtenir de l'equació (B), de la qual són les dues arrels restants, i el dubte de *quina* d'aquestes arrels resulta (2, 7) i quina (2, 8) es resoldrà o bé per un càlcul aproximat segons les fórmules precedents, o bé per les taules dels sinus, que amb una consulta només de passada mostren

que resulta $(2,\ 1) = 2\cos\omega$ posant $\omega = \frac{7}{19}P$, d'on convé fer $(2,\ 7) = 2\cos\frac{49}{19}P = 2\cos\frac{8}{19}P$, i $(2,\ 8) = 2\cos\frac{56}{19}P = 2\cos\frac{1}{19}P$. Similarment, també es poden trobar les sumes $(2,\ 2)$, $(2,\ 3)$, $(2,\ 5)$ per l'equació $x^3-(6,\ 2)xx+((6,\ 1)+(6,\ 2))x-2-(6,\ 4)=0$, de la qual són arrels, i la incertesa de quines arrels s'han d'establir iguals *respectivament* a aquelles sumes es resoldrà absolutament de la mateixa manera com més amunt; i igualment també es podran trobar les sumes $(2,\ 4)$, $(2,\ 6)$, $(2,\ 9)$, per l'equació $x^3-(6,\ 4)xx+((6,\ 2)+(6,\ 4))x-2-(6,\ 1)=0$.

Finalment, [1] i [18] són arrels de l'equació $xx-(2,\ 1)x+1=0$; una d'elles resulta

$$= \frac{1}{2}(2,1)+i\sqrt{1-\frac{1}{4}(2,1)^2} = \frac{1}{2}(2,1)+i\sqrt{\frac{1}{2}-\frac{1}{4}(2,2)},$$

l'altra, $= \frac{1}{2}(2,1)-i\sqrt{\frac{1}{2}-\frac{1}{4}(2,2)}$, d'aquí, els valors numèrics $= -0,6772815716 \pm 0,7357239107i$. Les setze arrels restants es poden deduir, o bé del desenvolupament de les potències de cadascuna d'aquestes arrels, o bé de la resolució d'unes altres vuit equacions similars, on, en el darrer mètode, s'haurà de decidir, o bé per taules de sinus, o bé per un artifici que s'explicarà en l'exemple següent, per a quina arrel s'ha de prefixar el signe positiu a la part imaginària i per a quina el negatiu. D'aquesta manera s'han trobat els valors següents, on se suposa que el signe superior correspon a la primera arrel, l'inferior a la darrera.

[1] i [18] $= -0,6772815716 \pm 0,7357239107i$
[2] i [17] $= -0,0825793455 \mp 0,9965844930i$
[3] i [16] $= 0,7891405094 \pm 0,6142127127i$
[4] i [15] $= -0,9863613034 \pm 0,1645945903i$
[5] i [14] $= 0,5469481581 \mp 0,8371664783i$
[6] i [13] $= 0,2454854871 \pm 0,9694002659i$
[7] i [12] $= -0,8794737512 \mp 0,4759473930i$
[8] i [11] $= 0,9458172417 \mp 0,3246994692i$
[9] i [10] $= -0,4016954247 \pm 0,9157733267i$

354. *Exemple segon, per a* $n = 17$. Aquí es té $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$, per la qual cosa, el càlcul de les arrels de Ω s'haurà de reduir a quatre equacions quadràtiques. Aquí agafarem per arrel primitiva el nombre 3, les potències del qual proporcionen els residus mínims següents segons el mòdul 17:

$$\begin{array}{cccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 3 & 9 & 10 & 13 & 5 & 15 & 11 & 16 & 14 & 8 & 7 & 4 & 12 & 2 & 6. \end{array}$$

D'aquí sorgeixen les distribucions següents del complex Ω en dos períodes d'octerns, quatre de quaterns, vuit de parells de termes:

$$\Omega = (16,1)\begin{cases} (8,1)\begin{cases} (4,1)\begin{cases} (2,1)\ldots & [1],[16] \\ (2,13)\ldots & [4],[13] \end{cases} \\ (4,9)\begin{cases} (2,9)\ldots & [8],[9] \\ (2,15)\ldots & [2],[15] \end{cases} \end{cases} \\ (8,3)\begin{cases} (4,3)\begin{cases} (2,3)\ldots & [3],[14] \\ (2,5)\ldots & [5],[12] \end{cases} \\ (4,10)\begin{cases} (2,10)\ldots & [7],[10] \\ (2,11)\ldots & [6],[11]. \end{cases} \end{cases} \end{cases}$$

L'equació (A) les arrels de la qual són les sumes (8, 1), (8, 3), pels preceptes de l'article 351, es troba la $xx + x - 4 = 0$; es calculen les seves arrels $-\frac{1}{2} + \frac{1}{2}\sqrt{17} = 1,5615528128$, i $-\frac{1}{2} - \frac{1}{2}\sqrt{17} = -2,5615528128$; establirem la primera = (8, 1), d'on, necessàriament, la darrera s'haurà de posar = (8, 3).

A més a més, l'equació les arrels de la qual són les sumes (4, 1) i (4, 9) es descobreix la (B) $xx - (8,1)x - 1 = 0$; les arrels d'aquesta són $\frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{4 + (8,1)^2}$ = $\frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{12 + 3(8,1) + 4(8,3)}$; establirem = (4, 1) aquella en què s'atribueix signe positiu a la quantitat radical, i el valor numèric de la qual és $2,0494811777$; d'on, espontàniament, l'altra, on la quantitat radical s'ha pres negativament i el valor de la qual és

-0,4879283649,

s'haurà d'expressar per (4, 9). Les sumes restants de quatre termes, però, posem (4, 3) i (4, 10), es poden esbrinar de dues maneres. Això és, *primer*, pel mètode de l'article 346, que proporciona les fórmules següents on, per abreujar, s'escriu p per (4, 1):

$$(4,3) = -\frac{3}{2} + 3p - \frac{1}{2}p^3 = 0,3441507314$$
$$(4,10) = \frac{3}{2} + 2p - pp - \frac{1}{2}p^3 = -2,9057035442.$$

El mateix mètode també proporciona la fórmula $(4, 9) = -1 - 6p + pp + p^3$, d'on s'obté el mateix valor que hem transmès abans. *Segon*, però, les sumes (4, 3), (4, 10), també es poden determinar per resolució

de l'equació de la qual són arrels, equació que resulta $xx - (8,3)x - 1 = 0$, d'on les seves arrels són $\frac{1}{2}(8,3) \pm \frac{1}{2}\sqrt{4 + (8,3)^2}$, o sigui,

$$\frac{1}{2}(8,3) + \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)}$$

i

$$\frac{1}{2}(8,3) - \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)};$$

el dubte, però, de *quina* arrel convé expressar per (4, 3), i quina per (4, 10), s'aixecarà per l'artifici següent, del qual hem fet menció en l'article 352. Es desenvolupa el producte de (4, 1)−(4, 9) per (4, 3)−(4, 10), d'on es trobarà que sorgeix 2(8, 1)−2(8, 3);* ara, el valor d'aquesta expressió és, evidentment, positiu, posem $= +2\sqrt{17}$ i, a part d'això, el primer factor del producte (4, 1) − (4, 9) també és positiu, posem $= +\sqrt{12 + 3(8,1) + 4(8,3)}$; per tant, l'altre factor (4, 3)−(4, 10) també haurà de ser, necessàriament, positiu, i, en conseqüència, [s'haurà] d'establir (4, 3) igual a la *primera* arrel en què s'ha prefixat el signe positiu al radical, i (4, 10) a la darrera. D'altra banda, d'aquí es deriven els mateixos valors numèrics que més amunt.

Trobades totes les sumes de quatre termes, passem a les sumes de dos termes. L'equació (C), les arrels de la qual són (2, 1), (2, 13), contingudes en (4, 1),

* L'índole vertadera d'aquest artifici consisteix en el fet que es podia preveure *a priori* que, desenvolupat aquest producte, no conté sumes de quatre termes, sinó que només es pot expressar per sumes de vuit termes; els experts descobriran facilíssimament la raó d'això, que s'ha d'ometre aquí per abreujar.

s'ha trobat la $xx - (4,\ 1)x + (4,\ 3) = 0$; les seves arrels són $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{-4(4,3) + (4,1)^2}$, o sigui, $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{4 + (4,9) - 2(4,3)}$; establim $= (2,\ 1)$ aquesta en què la quantitat radical es pren positivament i el valor de la qual es troba $= 1,8649444588$, d'on (2, 13) resultarà igual a l'altra, el valor de la qual és $= 0,1845367189$. Si plau investigar les sumes restants de dos termes pel mètode de l'article 346, es podran utilitzar per a (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (2, 7), (2, 8), les mateixes fórmules que hem transmès en l'exemple precedent per a les quantitats designades similarment, posem (2, 2) (o bé (2, 15)) $= (2,\ 1)^2 - 2$, etc. Però si agrada més calcular-les a parelles per resolució d'equacions quadràtiques, per a (2, 9), (2, 15), es troba l'equació $xx - (4,\ 9)x + (4,\ 10) = 0$, les arrels de la qual s'han tret $\frac{1}{2}(4,9) \pm \frac{1}{2}\sqrt{4 + (4,13) - 2(4,3)}$; fet això, però, aquí convindria definir el signe ambigu, i es decidirà de manera similar com més amunt. Això és, pel desenvolupament del producte $(2,\ 1) - (2,\ 13)$ per $(2,\ 9) - (2,\ 15)$ es produeix $-(4,\ 1) + (4,\ 9) - (4,\ 3) + (4,\ 10)$; que, com que, evidentment, és negatiu, però el factor $(2,\ 1) - (2,\ 13)$ positiu, $(2,\ 9) - (2,\ 15)$ haurà de ser, necessàriament, negatiu; en conseqüència, en l'expressió donada anteriorment s'haurà d'adoptar el signe superior positiu per a (2, 15), i l'inferior negatiu, per a (2, 9). D'aquí es calcula $(2,\ 9) = -1,9659461994$, $(2,\ 15) = 1,4780178344$. Igualment, com que del desenvolupament del producte de $(2,\ 1) - (2,\ 13)$ per $(2,\ 3) - (2,\ 5)$ apareix $(4,\ 9) - (4,\ 10)$, de manera que una quantitat positiva, concloem que el factor $(2,\ 3) - (2,\ 5)$ és positiu; d'aquí, per un càlcul similar al fet abans, es troba

$$(2,3) = \frac{1}{2}(4,3) + \frac{1}{2}\sqrt{4 + (4,10) - 2(4,9)}$$
$$= 0,8914767116,$$
$$(2,5) = \frac{1}{2}(4,3) - \frac{1}{2}\sqrt{4 + (4,10) - 2(4,9)}$$
$$= -0,5473259801.$$

Finalment, per operacions completament anàlogues, es descobreix

$$(2,10) = \frac{1}{2}(4,10) - \frac{1}{2}\sqrt{4 + (4,3) - 2(4,1)}$$
$$= -1,7004342715,$$
$$(2,11) = \frac{1}{2}(4,10) + \frac{1}{2}\sqrt{4 + (4,3) - 2(4,1)}$$
$$= -1,2052692728.$$

Resta que baixem a les mateixes arrels de Ω. L'equació (D), les arrels de la qual són [1] i [16], surt $xx-(2,1)x+1=0$, d'on les arrels $\frac{1}{2}(2,1) \pm \frac{1}{2}\sqrt{(2,1)^2-4}$, o millor

$$\frac{1}{2}(2,1) \pm \frac{1}{2}i\sqrt{4-(2,1)^2},$$

o sigui,

$$\frac{1}{2}(2,1) \pm \frac{1}{2}i\sqrt{2-(2,15)};$$

prenem el signe superior per a [1], l'inferior per a [16]. Les catorze arrels restants es tindran, o bé per les potències de [1], o bé per la resolució de set equacions quadràtiques, cadascuna de les quals expressa una parella, on la incertesa dels signes de les quantitats radicals es podrà aixecar pel mateix artifici que en els precedents. Així, [4] i [13] són les arrels de l'equació $xx-(2,13)x+1=0$, de manera que $\frac{1}{2}(2,13) \pm \frac{1}{2}i\sqrt{2-(2,9)}$; pel desenvolupament del producte de $[1]-[16]$ per $[4]-[13]$, però, surt $(2,5)-(2,3)$, de manera que una quantitat real

negativa; per tant, com que $[1]-[16]$ és $+i\sqrt{2-(2,15)}$, és a dir, el producte de la imaginària i per una real *positiva*, $[4]-[13]$ també ha de ser el producte de i per una real *positiva*, per causa que $ii=-1$; d'aquí es conclou que s'ha d'agafar el signe superior per a [4], l'inferior per a [13]. De manera similar, per a les arrels [8] i [9] es troba $\frac{1}{2}(2,9)\ \pm\frac{1}{2}i\sqrt{2-(2,1)}$, on, com que el producte de $[1]-[16]$ per $[8]-[9]$ resulta $(2,\,9)-(2,\,10)$, de manera que negatiu, convé agafar per a [8] el signe superior, per a [9], l'inferior. Calculant igualment les arrels restants, obtenim els valors numèrics següents, on s'ha de sobreentendre que els signes superiors corresponen a les primeres arrels, els inferiors, a les darreres.

$$
\begin{aligned}
[1],\ [16]\cdots &\quad 0,9324722294 \pm 0,3612416662i\\
[2],\ [15]\cdots &\quad 0,7390089172 \pm 0,6736956436i\\
[3],\ [14]\cdots &\quad 0,4457383558 \pm 0,8951632914i\\
[4],\ [13]\cdots &\quad 0,0922683595 \pm 0,9957341763i\\
[5],\ [12]\cdots &\quad -0,2736629901 \pm 0,9618256432i\\
[6],\ [11]\cdots &\quad -0,6026346364 \pm 0,7980172273i\\
[7],\ [10]\cdots &\quad -0,8502171357 \pm 0,5264321629i\\
[8],\ [\,9]\cdots &\quad -0,9829730997 \pm 0,1837495178i
\end{aligned}
$$

* * *

Això que s'ha tractat en el que precedeix podria ser suficient, certament, per a la resolució de l'equació $x^n-1=0$, de manera que, també, per a la recerca

de les funcions trigonomètriques corresponents als arcs commensurables amb la perifèria; no obstant això, per la seva importància, no podem posar fi a aquesta disquisició sense que abans afegim aquí quelcom que il·lustri aquest raonament amb una gran quantitat d'observacions, i també d'exemples afins a ella o que en depenen. Entre tals coses, elegirem sobretot les que es poden acabar sense un gran aparell de les altres disquisicions, i no volem que aquestes siguin considerades altrament que com a *manifestacions* d'aquesta amplíssima doctrina, que cal tractar després copiosament.

355. Com que n se suposa sempre imparell, 2 estarà entre els factors de $n-1$, i el complex Ω, format de $\frac{1}{2}(n-1)$ períodes de dos termes. Un període tal com $(2,\ \lambda)$ constarà de les arrels $[\lambda]$ i $[\lambda g^{\frac{1}{2}(n-1)}]$, on g, denota, com més amunt, una arrel primitiva qualsevol per al mòdul n. Però resulta $g^{\frac{1}{2}(n-1)} \equiv -1\,(\text{mòd.}\,n)$, de manera que $\lambda g^{\frac{1}{2}(n-1)} \equiv -\lambda$ (vegeu l'article 62), d'on $[\lambda g^{\frac{1}{2}(n-1)}] \equiv [-\lambda]$. Per tant, suposant $[\lambda] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$ i, en conseqüència, $[-\lambda] = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$, resulta la suma $(2,\ \lambda) = 2\cos\frac{kP}{n}$. D'on, en aquest lloc, només deduïm aquesta conclusió, que el valor de qualsevol suma de dos termes és una quantitat real. Com que qualsevol període, la quantitat de termes del qual és parella, $= 2a$, es pot descompondre en a períodes de dos termes, és clar, més generalment, que el valor de qualsevol suma, la quantitat de termes de la qual és parella, és una quantitat real. Així, si, en l'article 352, entre els factors α, β, γ, etc., es reserva a l'últim lloc el 2, totes les operacions s'acabaran per quantitats

reals fins que s'arribi a les sumes de dos termes, i les imaginàries s'introduiran només llavors, quan es passi d'aquestes sumes a les arrels mateixes.

356. Mereixen summa atenció les equacions auxiliars per les quals es determinen per a qualsevol valor de n les sumes que constitueixen el complex Ω, les quals estan connectades d'una manera sorprenent amb propietats molt recòndites del nombre n. En aquest lloc, però, restringirem la disquisició als dos casos següents: *primer*, tractarem de l'equació quadràtica les arrels de la qual són sumes de $\frac{1}{2}(n-1)$ termes; *segon*, per al cas en què $n-1$ implica un factor 3, de la cúbica les arrels de la qual són sumes de $\frac{1}{3}(n-1)$ termes.

Escrivint, per abreujar, m per $\frac{1}{2}(n-1)$, i designant per g una arrel primitiva qualsevol per al mòdul n, el complex Ω constarà dels dos períodes $(m,\ 1)$ i $(m,\ g)$, i el primer contindrà les arrels $[1]$, $[gg]$, $[g^4]$, $\ldots$, $[g^{n-3}]$, el darrer, les $[g]$, $[g^3]$, $[g^5]$, $\ldots$, $[g^{n-2}]$. Suposant que els residus mínims positius dels nombres gg, g^4, $\ldots$, g^{n-3}, segons el mòdul n són, en ordre arbitrari, R, R', R'', etc., i els residus de g, g^3, g^5, $\ldots$, g^{n-2}, els N, N', N'', etc., les arrels de què consta $(m,\ 1)$ coincidiran amb les $[1]$, $[R]$, $[R']$, $[R'']$, etc., i les arrels del període $(m,\ g)$ amb les $[N]$, $[N']$, $[N'']$, etc. Ara, és clar que tots els nombres 1, R, R', R'', etc., són *residus quadràtics* del nombre n, i, com que tots són diferents i menors que n, i la seva quantitat $= \frac{1}{2}(n-1)$, de manera que igual a la quantitat de tots els residus positius de n per sota de n, aquests residus coincidiran completament amb aquells nombres.

D'aquí se segueix espontàniament que tots els nombres N, N', N'', etc., que són diferents tant entre si com dels 1, R, R', etc., i que, presos simultàniament amb aquests, exhaureixen tots els nombres 1, 2, 3, ..., $n-1$, han de coincidir amb tots els no-residus quadràtics positius de n per sota de n. Ara, si se suposa que l'equació les arrels de la qual són les sumes $(m, 1)$, (m, g), és $xx - Ax + B = 0$, resulta $A = (m,1)+(m,g) = -1$, $B = (m,1)\times(m,g)$. El producte de $(m, 1)$ per (m, g), per l'article 345, resulta $= (m, N+1)+(m, N'+1)+(m, N''+1)+etc. = W$, i, d'aquí, es reduirà a una forma tal com $\alpha(m, 0)+\beta(m, 1)+\gamma(m, g)$. Per a la determinació dels coeficients α, β, γ, observem, *primer*, que resulta $\alpha+\beta+\gamma = m$ (això és, perquè la quantitat de sumes en W és $= m$); *segon*, que és $\beta = \gamma$ (això se segueix de l'article 350, ja que el producte $(m, 1) \times (m, g)$ és una funció invariable de les sumes $(m, 1)$, (m, g), de les quals està composta la suma més gran $(n-1, 1)$); *tercer*, com que tots els nombres $N+1$, $N'+1$, $N''+1$, etc., estan continguts entre els límits 2 i $n+1$, exclusivament, és evident que, *o bé* cap suma de W es redueix a $(m, 0)$, de manera que és $\alpha = 0$, quan entre els nombres N, N', N'', etc., no ocorre $n-1$, *o bé* una, posem (m, n), i, en conseqüència, es té $\alpha = 1$, quan $n-1$ es troba entre els nombres N, N', N'', etc. D'aquí es conclou que, en el primer cas, resulta $\alpha = 0$, $\beta = \gamma = \frac{1}{2}m$, en el darrer, $\alpha = 1$, $\beta = \gamma = \frac{1}{2}(m-1)$; simultàniament, d'aquí se segueix que, com que els nombres β i γ resulten, necessàriament, enters, té lloc el primer cas, o sigui, que $n-1$ (o bé, el que és el mateix, -1) no es troba entre els no-residus de n, quan m és parell, o sigui, n de la forma $4k+1$; el darrer cas, però, o sigui, $n-1$, o bé -1, es troba entre els no-

residus de n, es presenta quan m és imparell, o sigui, n de la forma $4k+3$.* D'aquí, a causa que $(m, 0) = m$, $(m, 1)+(m, g) = -1$, el producte cercat resulta, en el primer cas, $= -\frac{1}{2}m$, en el darrer, $= \frac{1}{2}(m+1)$, de manera que l'equació cercada, en aquell cas, $xx + x - \frac{1}{4}(n-1) = 0$, les arrels de la qual són $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$, però en aquest, $xx+x+\frac{1}{4}(n+1) = 0$, les arrels de la qual són $-\frac{1}{2}\pm\frac{1}{2}i\sqrt{n}$.

Així, qualsevol que sigui l'arrel de Ω que s'ha adoptat per a [1], la diferència entre les sumes $\sum[\mathfrak{R}]$ i $\sum[\mathfrak{N}]$, on s'han de substituir per a $\mathfrak{R}$ tots els residus quadràtics, per a $\mathfrak{N}$ tots els no-residus positius de n per sota de n, serà $= \pm\sqrt{n}$ per a $n \equiv 1$, i $= \pm i\sqrt{n}$ per a $n \equiv 3\,(\text{mòd. } 4)$. I també d'aquí se segueix fàcilment que, si k denota un enter qualsevol no divisible per n, resulta $\sum \cos \frac{k\mathfrak{R}P}{n} - \sum \cos \frac{k\mathfrak{N}P}{n} = \pm\sqrt{n}$, i $\sum \sin \frac{k\mathfrak{R}P}{n} - \sum \sin \frac{k\mathfrak{N}P}{n} = 0$, per a $n \equiv 1\,(\text{mòd. } 4)$; contràriament, per a $n \equiv 3\,(\text{mòd. } 4)$, aquella diferència és $= 0$, aquesta $= \pm\sqrt{n}$, teoremes que, a causa de la seva elegància, són molt memorables. D'altra banda, observem que els signes superiors valen sempre quan s'agafa per a k la unitat, o bé, més generalment, un residu quadràtic de n, els inferiors quan per a k es pren un no-residu, i aquests

* D'aquesta manera, hem obtingut una nova demostració del teorema: -1 és residu de tots els nombres primers de la forma $4k+1$, no-residu de tots els de la forma $4k+3$, que més amunt (articles 108, 109, 262) ja va ser comprovat de moltes maneres diverses. Si agrada més suposar aquest teorema, no serà necessari, per a la distinció dels dos casos diferents, tenir en compte aquesta condició, perquè β i γ ja resulten enters per si.

teoremes també es poden estendre, conservada o, encara més, augmentada la seva elegància, a qualssevol valors compostos de n; però, en aquest lloc, convé callar aquestes coses, que són de recerca més alta, i reservar-nos la seva consideració per a una altra ocasió.

357. Sigui l'equació de m-èsim grau, les arrels de la qual són les m arrels contingudes en el període $(m, 1)$, la $x^m - ax^{m-1} + bx^{m-2} - etc. = 0$, o sigui, $z = 0$, i serà $a = (m, 1)$, i cadascun dels coeficients restants, b, etc., compresos en una forma tal com $\mathfrak{A} + \mathfrak{B}(m, 1) + \mathfrak{C}(m, g)$, de manera que $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, són enters (article 348); i denotant per z' la funció en què es transforma z si se substitueix a tot arreu $(m, 1)$ per (m, g) i (m, g) per (m, gg), o sigui, el que és el mateix, per $(m, 1)$, les arrels de l'equació $z' = 0$ seran les arrels contingudes en (m, g), i el producte $zz' = \dfrac{x^n - 1}{x - 1} = X$. Així, z es pot reduir a una forma $R + S(m, 1) + T(m, g)$, on R, S, T, seran funcions enteres de x, tots els coeficients de les quals també seran enters; fet això, es tindrà $z' = R + S(m, g) + T(m, 1)$. D'aquí, escrivint, per abreujar, p i q per $(m, 1)$ i (m, g), respectivament, resulta $2z = 2R + (S + T)(p + q) - (T - S)(p - q) = 2R - S - T - (T - S)(p - q)$, i, similarment, $2z' = 2R - S - T + (T - S)(p - q)$, d'on, posant $2R - S - T = Y$, $T - S = Z$, resulta $4X = YY - (p - q)^2 ZZ$, de manera que, com que $(p - q)^2 = \pm n$, $4X = YY \mp nZZ$, on val el signe superior quan n és de la forma $4k + 1$, l'inferior quan n és de la forma $4k + 3$. Aquest és el teorema la demostració del qual hem promès més amunt (article 124). Es copsarà fàcilment que els dos termes més alts de la funció Y sempre resulten $2x^m + x^{m-1}$; i el més alt de la funció Z, x^{m-1}; però els coeficients restants, que,

evidentment, tots seran enters, varien segons l'índole diferent del nombre n, i no es poden presentar fórmules analítiques generals.

Exemple. Per a $n = 17$, l'equació les arrels de la qual són les vuit arrels contingudes en (8, 1), pels preceptes de l'article 348, surt $x^8 - px^7 + (4+p+2q)x^6 - (4p+3q)x^5 + (6+3p+5q)x^4 - (4p+3q)x^3 + (4+p+2q)xx - px + 1 = 0$, d'on $R = x^8 + 4x^6 + 6x^4 + 4xx + 1$, $S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + xx - x$, $T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2xx$, i, d'aquí, $Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5xx + x + 2$, $Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + xx + x$. Heus aquí alguns altres exemples.

n	Y	Z
3	$2x + 1$	1
5	$2xx + x + 2$	x
7	$2x^3 + xx - x - 2$	$xx + x$
11	$2x^5 + x^4 - 2x^3 + 2xx$ $-x - 2$	$x^4 + x$
13	$2x^6 + x^5 + 4x^4 - x^3$ $+4xx + x + 2$	$x^5 + x^3 + x$
19	$2x^9 + x^8 - 4x^7 + 3x^6$ $+5x^5 - 5x^4 - 3x^3$ $+4xx - x - 2$	$x^8 - x^6 + x^5 + x^4 - x^3$ $+x$
23	$2x^{11} + x^{10} - 5x^9 - 8x^8$ $-7x^7 - 4x^6 + 4x^5$ $+7x^4 + 8x^3 + 5xx$ $-x - 2$	$x^{10} + x^9 - x^7 - 2x^6$ $-2x^5 - x^4 + xx + x$

358. Passem a la consideració de les equacions cúbiques, per a les quals, en el cas en què n és de la forma $3k+1$, es determinen les tres sumes de $\frac{1}{3}(n-1)$ termes que componen el complex Ω. Sigui g una arrel primitiva qualsevol per al mòdul n, i $\frac{1}{3}(n-1) = m$, que serà un enter parell. Llavors, les tres sumes de què consta Ω seran $(m, 1)$, (m, g), (m, gg), per a les quals escriurem, respectivament, p, p', p''; és clar que la primera conté les arrels $[1]$, $[g^3]$, $[g^6]$, $\ldots$, $[g^{n-4}]$, la segona, les $[g]$, $[g^4]$, $\ldots$, $[g^{n-3}]$, la tercera, les $[gg]$, $[g^5]$, $\ldots$, $[g^{n-2}]$. Suposant que l'equació cercada és $x^3 - Axx + Bx - C = 0$, resulta $A = p + p' + p''$, $B = pp' + p'p'' + pp''$, $C = pp'p''$, d'on, directament, es té $A = -1$. Siguin $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., els residus mínims positius dels nombres g^3, g^6, $\ldots$, g^{n-4}, segons el mòdul n, en un ordre arbitrari, i $\mathfrak{K}$ el complex d'aquests afegint-hi el nombre 1; similarment, siguin $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, etc., els residus mínims dels nombres g, g^4, g^7, $\ldots$, g^{n-3}, i $\mathfrak{K}'$ el seu complex; i, finalment, $\mathfrak{A}''$, $\mathfrak{B}''$, $\mathfrak{C}''$, etc., els residus mínims de gg, g^5, g^8, $\ldots$, g^{n-2}, i $\mathfrak{K}''$ el seu complex; d'on tots els nombres en $\mathfrak{K}$, $\mathfrak{K}'$, $\mathfrak{K}''$, seran diferents i coincidiran amb els 1, 2, 3, $\ldots$, $n-1$. Abans de tot, aquí s'ha d'observar que el nombre $n-1$ s'ha de trobar, necessàriament, en $\mathfrak{K}$, ja que es copsa fàcilment que és residu de $g^{\frac{3}{2}m}$. D'aquí, també fàcilment, és conseqüència que dos nombres tals com h, $n-h$, sempre es troben en el *mateix* dels tres complexos $\mathfrak{K}$, $\mathfrak{K}'$, $\mathfrak{K}''$; en efecte, si un és residu de la potència g^λ, l'altre serà residu de la potència $g^{\lambda+\frac{3}{2}m}$ o bé de la $g^{\lambda-\frac{3}{2}m}$, si $\lambda > \frac{3}{2}m$. Denotem amb el símbol $(\mathfrak{K}\mathfrak{K})$ la quantitat de nombres de la sèrie 1, 2, 3, $\ldots$, $n-1$, que, tant ells com, simultàniament, els nombres més pròxims més grans en una unitat, es contenen en $\mathfrak{K}$; similarment, sigui

$(\mathfrak{K}\mathfrak{K}')$ la quantitat de nombres de la mateixa sèrie que es contenen en $\mathfrak{K}$ però els pròxims següents en $\mathfrak{K}'$, d'on, simultàniament, es coneixerà espontàniament el significat dels signes $(\mathfrak{K}\mathfrak{K}'')$, $(\mathfrak{K}'\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}')$, $(\mathfrak{K}'\mathfrak{K}'')$, $(\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}''\mathfrak{K}')$, $(\mathfrak{K}''\mathfrak{K}'')$. Fet això, afirmo, *primer*, que resulta $(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'\mathfrak{K})$. En efecte, suposant que h, h', h'', etc., són tots els nombres de la sèrie 1, 2, 3, ..., $n-1$, que es contenen en $\mathfrak{K}$, però que els pròxims més grans, $h+1$, $h'+1$, $h''+1$, etc., en $\mathfrak{K}'$, i, així, la quantitat dels quals és $= (\mathfrak{K}\mathfrak{K}')$, és evident que tots els nombres $n-h-1$, $n-h'-1$, $n-h''-1$, etc., es contenen en $\mathfrak{K}'$, però els pròxims més grans, $n-h$, $n-h'$, etc., en $\mathfrak{K}$; per tant, com que es donen en total $(\mathfrak{K}'\mathfrak{K})$ nombres d'aquests, certament no pot ser $(\mathfrak{K}'\mathfrak{K}) < (\mathfrak{K}\mathfrak{K}')$; i es demostra igualment que no pot ser $(\mathfrak{K}\mathfrak{K}') < (\mathfrak{K}'\mathfrak{K})$; conseqüentment, aquests nombres seran, necessàriament, iguals. Completament de la mateixa manera, es prova que $(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}')$. Segon, com que, necessàriament, a qualsevol nombre de $\mathfrak{K}$, exceptuat el màxim, $n-1$, ha de seguir el seu pròxim més gran contingut o bé en $\mathfrak{K}$, o bé en $\mathfrak{K}'$, o bé en $\mathfrak{K}''$, la suma $(\mathfrak{K}\mathfrak{K})+(\mathfrak{K}\mathfrak{K}')+(\mathfrak{K}\mathfrak{K}'')$ resultarà igual a la quantitat de tots els nombres de $\mathfrak{K}$ disminuïda en una unitat, posem $= m-1$, i, per una raó similar, serà $(\mathfrak{K}'\mathfrak{K})+(\mathfrak{K}'\mathfrak{K}')+(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})+(\mathfrak{K}''\mathfrak{K}')+(\mathfrak{K}''\mathfrak{K}'') = m$.

Preparat això així, desenvolupem, pels preceptes de l'article 345, el producte pp', en $(m, \mathfrak{A}'+1)+(m, \mathfrak{B}'+1)+(m, \mathfrak{C}'+1)+$ *etc.*, expressió que es copsarà fàcilment que es redueix a $(\mathfrak{K}'\mathfrak{K})p+(\mathfrak{K}'\mathfrak{K}')p'+(\mathfrak{K}'\mathfrak{K}'')p''$, i, com que, per l'article 345, I, el producte $p'p''$ s'origina d'aquell substituint per $(m, 1)$, (m, g), (m, gg), respectivament, (m, g), (m, gg), (m, g^3), és a dir, per p, p', p'', respectivament, p', p'', p, resultarà $p'p'' =$

$(\mathfrak{K}'\mathfrak{K})p'+(\mathfrak{K}'\mathfrak{K}')p''+(\mathfrak{K}'\mathfrak{K}'')p$, i, de manera completament similar, $p''p = (\mathfrak{K}'\mathfrak{K})p'' + (\mathfrak{K}'\mathfrak{K}')p + (\mathfrak{K}'\mathfrak{K}'')p'$. D'aquí se segueix directament, *primer*, que $B = m(p + p' + p'') = -m$; *segon*, com que, per una raó similar a com abans s'ha desenvolupat pp', també pp'' es redueix a $(\mathfrak{K}''\mathfrak{K})p + (\mathfrak{K}''\mathfrak{K}')p'+(\mathfrak{K}''\mathfrak{K}'')p''$, i aquesta equació ha de ser idèntica a l'anterior, que serà, necessàriament, $(\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}'\mathfrak{K}')$ i $(\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K})$. D'aquí es conclou, establint $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}') = a$, $(\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}') = b$, $(\mathfrak{K}'\mathfrak{K}') = (\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}'') = c$, que resulta $m-1 = (\mathfrak{K}\mathfrak{K})+(\mathfrak{K}\mathfrak{K}')+(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}\mathfrak{K})+b+c$, i $a+b+c = m$, d'on $(\mathfrak{K}\mathfrak{K}) = a-1$, de manera que aquelles nou quantitats desconegudes s'han reduït a les tres a, b, c, o, millor, a dues, a causa de l'equació $a+b+c = m$. Finalment, és clar que el quadrat pp es desenvolupa en $(m,\ 1 + 1) + (m,\ \mathfrak{A} + 1) + (m,\ \mathfrak{B} + 1) + (m,\ \mathfrak{C} + 1) + etc.$; entre les parts d'aquesta expressió s'hi trobarà $(m,\ n)$, que es redueix a $(m,\ 0)$, o sigui, a m; però es copsarà fàcilment que les restants es redueixen a $(\mathfrak{K}\mathfrak{K})p + (\mathfrak{K}\mathfrak{K}')p' + (\mathfrak{K}\mathfrak{K}'')p''$, d'on es té $pp = m + (a-1)p + bp' + cp''$.

Així, d'aquesta manera, per les disquisicions precedents hem obtingut aquestes quatre reduccions:

$$\begin{aligned} pp &= m + (a-1)p + bp' + cp'', \\ pp' &= bp + cp' + ap'', \\ pp'' &= cp + ap' + bp'', \\ p'p'' &= ap + bp' + cp'', \end{aligned}$$

on, entre les tres incògnites a, b, c, hi ha l'equació condicional $a+b+c = m$ ... (I), i, a sobre, és cert que aquestes són nombres enters. D'aquí es conclou que $C = p \times p'p'' = app+bpp'+cpp'' = am+(aa+bb+cc-a)p+(ab+bc+$

$ac)p'+(ab+bc+ac)p''$. Però com que $pp'p''$ és una funció invariable de les sumes p, p', p'', els coeficients pels quals han estan multiplicats aquests en l'expressió precedent seran, necessàriament, iguals (article 350), d'on es té la nova equació $aa+bb+cc-a = ab+bc+ac \ldots$ II; i, d'aquí, $C = am+(ab+bc+ac)(p+p'+p'')$, o sigui (per causa de I, i de $p+p'+p'' = -1$), $C = aa-bc \ldots$ III. Ara, encara que C depèn aquí de tres incògnites entre les quals només es tenen dues equacions, no obstant això, aquestes, amb l'ajut de la condició segons la qual a, b, c, són enters, són suficients per a la plena determinació de C. Per mostrar-ho, expressarem l'equació (II) així: $12a+12b+12c+4 = 36aa+36bb+36cc-36ab-36ac-36bc-24a+12b+12c+4$; la primera part, per I, resulta $= 12m + 4 = 4n$; la darrera, però, es redueix a $(6a - 3b - 3c - 2)^2 + 27(b - c)^2$, o bé, escrivint k per $2a - b - c$, a $(3k - 2)^2 + 27(b - c)^2$. D'aquí és clar que el nombre $4n$ (és a dir, en general, el quàdruple de qualsevol primer de la forma $3n+1$) es pot representar per la forma $xx + 27yy$, cosa que, certament sense dificultat, es pot deduir de la teoria general de les formes binàries; no obstant això, és bastant sorprenent que una tal descomposició estigui lligada als valors de a, b, c. Però el nombre $4n$ sempre es pot descompondre només d'una única manera en un quadrat i 27 vegades un quadrat, la qual cosa demostrem així.* Si se suposa que $4n = tt + 27uu = t't' + 27u'u'$, resultaria, *primer*, $(tt' - 27uu')^2 + 27(tu' + t'u)^2 = 16nn$, *segon*, $(tt' + 27uu')^2 + 27(tu' - t'u)^2 = 16nn$, *tercer*, $(tu' + t'u)(tu' - t'u) = 4n(u'u' - uu)$; de l'equació tercera se segueix que n, com que és un nombre primer, divideix un dels dos nombres $tu' + t'u$, $tu' - t'u$; però,

* Aquesta proposició es podria provar més directament pels principis de la secció V.

de la primera i la segona, és clar que aquests dos nombres són menors que n; per tant, el que n divideix ha de ser, necessàriament, $= 0$, de manera que, també, $u'u' - uu = 0$, d'on, $u'u' = uu$ i $t't' = tt$, és a dir, aquelles dues descomposicions no diferiran. Així, si suposem coneguda la descomposició de $4n$ en un quadrat i 27 vegades un quadrat (que es pot descobrir, o bé pel mètode directe de la secció V, o bé per l'indirecte transmès en els articles 323, 324), posem, si es té $4n = MM + 27NN$, els quadrats $(3k-2)^2$, $(b-c)^2$ hauran estat determinats, i, en lloc de l'equació (II), n'haurem obtingut dues. Però és clar fàcilment que, no només el quadrat $(3k-2)^2$, sinó també l'arrel $3k-2$, han estat perfectament determinats; en efecte, com que, necessàriament, és o bé $= +M$ o bé $= -M$, l'ambigüitat s'aixecarà d'aquí perquè k ha de ser enter; per la qual cosa, s'establirà $3k - 2 = +M$ o bé $= -M$, segons si M és de la forma $3z + 1$ o bé $3z + 2$.* Ara, com que resulta $k = 2a - b - c = 3a - m$, serà $a = \frac{1}{3}(m + k)$, $b + c = m - a = \frac{1}{3}(2m - k)$ d'on $C = aa - bc = aa - \frac{1}{4}(b + c)^2 + \frac{1}{4}(b - c)^2 = \frac{1}{9}(m+k)^2 - \frac{1}{36}(2m-k)^2 + \frac{1}{4}NN = \frac{1}{12}kk + \frac{1}{3}km + \frac{1}{4}NN$, i, així, s'han descobert tots els coeficients de l'equació cercada. *Q. E. F.* Aquesta fórmula encara surt més simple si se substitueix NN pel seu valor [deduït] de l'equació $(3k - 2)^2 + 27NN = 4n = 12m + 4$, on, fet

* Evidentment, M no pot ser de la forma $3z$; en efecte, altrament, $4n$ resultaria divisible per 3. Aquí no és necessari considerar l'ambigüitat de si $b - c$ s'ha d'establir $= N$ o bé $= -N$, ni tampoc no es podria fer de cap manera per la naturalesa de la qüestió, ja que depèn de l'elecció d'una arrel primitiva g, de manera que per a unes arrels primitives la diferència $b - c$ sortirà positiva, i, per a altres, negativa.

el càlcul, s'obté $C = \frac{1}{9}(m + k + 3km) = \frac{1}{9}(m + kn)$. El mateix valor també es pot reduir a $(3k - 2)NN + k^3 - 2kk + k - km + m$, expressió que, certament, menys idònia per a l'ús, mostra directament que C, tal com ha de ser, surt, en veritat, enter.

Exemple. Per a $n = 19$, resulta $4n = 49 + 27$, d'on $3k - 2 = +7$, $k = 3$, $C = \frac{1}{9}(6 + 57) = 7$, i, l'equació cercada, $x^3 + xx - 6x - 7 = 0$, com més amunt (article 351). De manera similar, per a $n = 7$, 13, 31, 37, 43, 61, 67, el valor de k es troba, respectivament, 1, -1, 2, -3, -2, 1, -1, d'on $C = 1$, -1, 8, -11, -8, 9, -5.

D'altra banda, encara que el problema resolt en aquest article és bastant intricat, no obstant això, no hem volgut suprimir-lo, tant per causa de l'elegància de la solució, com perquè ha donat ocasió d'utilitzar diversos artificis, que també es podran aplicar amb profit en altres qüestions importants.

359. Les disquisicions precedents versaven sobre la *trobada* d'equacions auxiliars; ara explicarem una propietat molt remarcable de la seva *solució*. Se sap que tots els esforços dels més eminents geòmetres per a trobar una solució general de les equacions que superen el quart ordre, o sigui (per tal que jo defineixi més acuradament el que es desitjava), de la reducció A PURES DE LES AFECTADES, sempre han estat, fins ara, inútils, i a penes resten dubtes de si aquest problema no solament supera la força de l'anàlisi contemporània, sinó de si es proposa quelcom més aviat impossible (compareu amb el que hem dit d'aquesta qüestió en *Demonstr. noua etc. p.*

22*)*. No obstant això, és cert que es donen innombrables equacions afectades de qualsevol grau que admeten una tal reducció a pures, i esperem que seria grat als geòmetres si mostréssim que les nostres equacions auxiliars sempre s'han de remetre a aquestes. Però, a causa de l'àmbit ampli d'aquesta disquisició, en aquest lloc només transmetem les consideracions més importants que són necessàries per a mostrar-ne la possibilitat, i ajornem per a un altre moment un tractament més complet, del qual és molt digna aquesta qüestió. S'han de presentar, en primer lloc, algunes observacions generals sobre les arrels de l'equació $x^e - 1 = 0$, que també apleguen el cas en què e és un nombre compost.

I. Aquestes arrels (com és conegut dels llibres elementals) s'expressen per $\cos \frac{kP}{e} + i \sin \frac{kP}{e}$, on per a k s'han d'agafar els e nombres 0, 1, 2, 3, $\ldots$, $e - 1$, o bé qualssevol altres congrus a aquests segons el mòdul e. Una arrel, per a $k = 0$, o bé, en general, per a k divisible per e, resulta $= 1$; a qualsevol altre valor de k li correspon una arrel diferent de 1.

II. Com que és $\left(\cos \frac{kP}{e} + i \sin \frac{kP}{e}\right)^\lambda = \cos \frac{\lambda kP}{e} + i \sin \frac{\lambda kP}{e}$, és clar que si R és una arrel tal que correspongui a un valor de k primer amb e, en la progressió R, RR, R^3, etc., el terme e-èsim és, certament, $= 1$, però tots els anteriors, diferents de 1. D'aquí se segueix immediatament que totes les e quantitats 1, R, RR, R^3, $\ldots$, R^{e-1}, són diferents, i, com que, evidentment, totes satisfan l'equació $x^e - 1 = 0$, expressaran totes les arrels d'aquesta equació.

III. Finalment, en la mateixa suposició, la suma $1 + R^{\lambda} + R^{2\lambda} + \cdots + R^{\lambda(e-1)}$ resulta $= 0$ per a qualsevol valor enter de λ no divisible per e; en efecte, és $= \dfrac{1 - R^{\lambda e}}{1 - R^{\lambda}}$, el numerador d'aquesta fracció resulta $= 0$, però el denominador, no $= 0$. Però quan λ és divisible per e, aquella suma resulta, evidentment, $= e$.

360. Sigui, com sempre en el que precedeix, n un nombre primer, g una arrel primitiva per al mòdul n, i $n - 1$ el producte de tres enters positius α, β, γ; per abreujar, farem la disquisició constantment de manera que també s'estengui als casos en què α o bé $\gamma = 1$; quan $\gamma = 1$, convindrà agafar les arrels $[1]$, $[g]$, etc., per a les sumes $(\gamma, 1)$, (γ, g), etc. Així, suposem que de totes les α sumes conegudes de $\beta\gamma$ termes, $(\beta\gamma, 1)$, $(\beta\gamma, g)$, $(\beta\gamma, gg)$, $\ldots$, $(\beta\gamma, g^{\alpha-1})$, s'han de deduir les sumes de γ termes, qüestió que hem reduït més amunt a una equació afectada del β-èsim grau, però que ara ensenyarem a resoldre per una de pura igualment alta. Per abreujar, per a les sumes $(\gamma, 1)$, (γ, g^{α}), $(\gamma, g^{2\alpha})$, $\ldots$, $(\gamma, g^{\alpha\beta-\alpha})$, que estan contingudes en $(\beta\gamma, 1)$, escriurem a, b, c, $\ldots$, m, respectivament; per a les (γ, g), $(\gamma, g^{\alpha+1})$, $\ldots$, $(\gamma, g^{\alpha\beta-\alpha+1})$, contingudes en $(\beta\gamma, g)$, a', b', $\ldots$, m', respectivament; per a les (γ, gg), $(\gamma, g^{\alpha+2})$, $\ldots$, $(\gamma, g^{\alpha\beta-\alpha+2})$, a'', b'', $\ldots$, m'', respectivament; etc., fins aquelles que estan contingudes en $(\beta\gamma, g^{\alpha-1})$.

I. Ara, designi formalment R una arrel de l'equació $x^{\beta} - 1 = 0$, i suposem que del desenvolupament de la potència β-èsima de la funció $t = a + Rb + RRc + \cdots + R^{\beta-1}m$, s'origina, pels preceptes de l'article 345,

$$\begin{aligned} & N + Aa + Bb + Cc + \cdots + Mm \\ & \quad + A'a' + B'b' + C'c' + \cdots + M'm' \\ & \quad + A''a'' + B''b'' + C''c'' + \cdots + M''m'' \\ & \quad + etc. = T, \end{aligned}$$

on tots els coeficients N, A, B, A', etc., seran funcions racionals enteres de R. Si també se suposa que les potències β-èsimes d'unes altres dues funcions $u = R^\beta a + Rb + RRc + \cdots + R^{\beta-1}m$, $u' = b + Rc + RRd + \cdots + R^{\beta-2}m + R^{\beta-1}a$, es desenvolupen, respectivament, en U i U', es copsarà fàcilment de l'article 350 que, com que u' s'origina de t commutant les sumes a, b, c, $\ldots$, m, respectivament, amb b, c, d, $\ldots$, a, serà $U' =$

$$\begin{aligned} & N + Ab + Bc + Cd + \cdots + Ma \\ & \quad + A'b' + B'c' + C'd' + \cdots + M'a' \\ & \quad + A''b'' + B''c'' + C''d'' + \cdots + M''a'' \\ & \quad + etc. \end{aligned}$$

A més a més, és clar que, com que és $u = Ru'$, serà $U = R^\beta U'$; per tant, per causa que $R^\beta = 1$, els coeficients corresponents en U i U' seran iguals; finalment, com que t i u només difereixen en el fet que a es multiplica en t per la unitat, en u, per R^β, s'entendrà fàcilment que tots els coeficients corresponents (és a dir, que multipliquen les mateixes sumes) són iguals en T i U i, en conseqüència, també tots els coeficients corresponents en T i U'. D'aquí, finalment, es conclou que $A = B = C = etc. = M$; $A' = B' = C' = etc.$, $A'' = B'' = C'' = etc.$, etc., d'on T es redueix a una forma tal com $N + A(\beta\gamma, 1) + A'(\beta\gamma, g) + A''(\beta\gamma, gg)$ *etc.*, on cadascun dels coeficients N, A, A', etc., es pot reduir

a una forma tal com $pR^{\beta-1}+p'R^{\beta-2}+p''R^{\beta-3}+etc.$, de manera que p, p', p'', etc., són nombres enters donats.

II. Si per a R s'agafa una arrel determinada de l'equació $x^\beta - 1 = 0$ (la solució de la qual suposem que ja es té), i tal, certament, que cap potència d'aquesta menor que la β-èsima no és igual a la unitat, T també serà una quantitat determinada, de la qual es podrà derivar t per l'equació pura $t^\beta - T = 0$. I com que aquesta equació té β arrels, que seran t, Rt, RRt, $\ldots$, $R^{\beta-1}t$, pot semblar dubtós quina arrel convé adoptar. Però, que això és completament arbitrari es veurà fàcilment així. Convé recordar que, després que s'han determinat totes les sumes de $\beta\gamma$ termes, l'arrel [1] només està definida fins al punt que alguna de les $\beta\gamma$ arrels contingudes en ($\beta\gamma$, 1) s'ha de denotar amb aquest símbol, i, en conseqüència, és completament arbitrari quina de les β sumes que constitueixen ($\beta\gamma$, 1) volem designar per a. Si, ara, expressada per a alguna suma determinada, se suposa que resulta $t = \mathfrak{T}$, es copsarà fàcilment que si, després, es vol designar per a la suma que abans es designava per b, les que abans eren c, d, $\ldots$, a, b, ara resulten b, c, $\ldots$, m, a, de manera que el valor de t ara és $= \dfrac{\mathfrak{T}}{R} = \mathfrak{T}R^{\beta-1}$. De manera similar, si plau expressar la suma que a l'inici era c, per a, el valor de t resultarà $= \mathfrak{T}R^{\beta-2}$; i així, a més a més, t es pot considerar igual a qualsevol de les quantitats $\mathfrak{T}$, $\mathfrak{T}R^{\beta-1}$, $\mathfrak{T}R^{\beta-2}$, etc.; és a dir, a qualsevol arrel de l'equació $x^\beta - T = 0$, segons se suposi expressada per (γ, 1) l'una o l'altra suma continguda en ($\beta\gamma$, 1). *Q. E. D.*

III. Després que la quantitat t s'ha determinat d'aquesta manera, convé investigar les altres $\beta - 1$ que

surten de t si en la seva expressió se substitueixen per a R, successivament, RR, R^3, R^4, $\ldots$, R^β; posem $t' = a + RRb + R^4c + \cdots + R^{2\beta-2}m$, $t'' = a + R^3b + R^6c + \cdots + R^{3\beta-3}m$, etc. Certament, ja es té l'última, ja que, evidentment, resulta $= a+b+c+\cdots+m = (\beta\gamma, 1)$; les restants, però, es poden trobar de la manera següent. Si pels preceptes de l'article 345 es desenvolupa el producte $t^{\beta-2}t'$ de manera similar com abans t^β en I, es provarà per un mètode completament anàleg al precedent que això que apareix aquí es pot reduir a una forma tal com $\mathfrak{N} + \mathfrak{A}(\beta\gamma, 1) + \mathfrak{A}'(\beta\gamma, g) + \mathfrak{A}''(\beta\gamma, gg)\text{etc.} = T'$, de manera que $\mathfrak{N}$, $\mathfrak{A}$, $\mathfrak{A}'$, etc., siguin funcions racionals enteres de R, i, així, T' una quantitat coneguda; d'on es tindrà $t' = \dfrac{T'tt}{T}$. Exactament de la mateixa manera, si se suposa que del desenvolupament del producte $t^{\beta-3}t''$ surt T'', aquesta expressió tindrà una forma similar i, en conseqüència, del seu valor conegut es derivarà t'' per l'equació $t'' = \dfrac{T''t^3}{T}$; igualment, t''' es trobarà per una equació tal com $t''' = \dfrac{T'''t^4}{T}$, de manera que T''' és una quantitat coneguda, etc.

Aquest mètode no seria aplicable si pogués resultar $t = 0$, d'on també hauria de ser $T = T' = T'' = etc. = 0$; però es pot provar que això és impossible, encara que convé suprimir la demostració en aquest lloc a causa de l'extensió. També es donen artificis peculiars pels quals les fraccions $\dfrac{T'}{T}$, $\dfrac{T''}{T}$, etc., es poden convertir en funcions racionals *enteres* de R; i també mètodes més breus per a trobar valors de t', t'', etc., en el cas en què $\alpha = 1$, tots els quals aquí hem de deixar en silenci.

IV. Finalment, al mateix temps que s'han trobat t, t', t'', etc., es tindrà immediatament, per l'observació III de l'article precedent, que $t+t'+t''+etc. = \beta a$, d'on serà conegut el valor de a, del qual, per l'article 346, es podran derivar els valors de totes les restants sumes de γ termes. Els valors de b, c, d, etc., també es poden obtenir per les equacions següents, la raó de les quals serà fàcilment evident a qualsevol que s'hi fixi: $\beta b = R^{\beta-1}t+R^{\beta-2}t'+R^{\beta-3}t''+etc.$, $\beta c = R^{2\beta-2}t+R^{2\beta-4}t'+R^{2\beta-6}t''+etc.$, $\beta d = R^{3\beta-3}t+R^{3\beta-6}t'+R^{3\beta-9}t''+etc.$, etc.

Del gran nombre d'observacions pertinents a la disquisició precedent, aquí només en tenim una en compte. Pel que fa a la solució de l'equació pura $x^\beta - T = 0$, és clar fàcilment que T, en la majoria dels casos, té un valor imaginari $P + iQ$, d'on aquella solució dependrà en part de la secció d'un angle (la tangent del qual és $= \frac{Q}{P}$), en part, com se sap, de la secció en β parts d'una raó (de la unitat a $\sqrt{PP+QQ}$). On és molt sorprenent (fet, però, que aquí no exposem més extensament) que el valor de $\sqrt[\beta]{PP+QQ}$ sempre es pot expressar *racionalment* per quantitats ja conegudes, de manera que, excepte l'extracció d'una arrel quadrada, *només* requereix, per a la solució, la secció d'un angle; per exemple, per a $\beta = 3$, només la trisecció d'un angle, mentre que, per a la majoria de les altres equacions cúbiques, les arrels de les quals són totes reals, no es pot evitar simultàniament la trisecció de l'angle i de la raó.

Finalment, com que res no obsta que establim $\alpha = 1$, $\gamma = 1$, de manera que $\beta = n - 1$, és evident que la solució de l'equació $x^n - 1 = 0$ es pot reduir immediata-

ment a la solució de l'equació pura de $n-1$-èsim grau, $x^{n-1}-T=0$, on T es determinarà per les arrels de l'equació $x^{n-1}-1=0$. D'on, amb l'ajut de l'observació feta fa un moment, es conclou que la secció de tot el cercle en n parts requereix: 1r, la secció de tot el cercle en $n-1$ parts; 2n, la secció en $n-1$ parts d'un altre arc que es pot construir un cop feta aquella secció; 3r, l'extracció d'una arrel quadrada; i, certament, es pot provar que aquesta sempre és $\sqrt{n}$.

361. Resta que contemplem encara més extensament el nexe entre les arrels de Ω i les funcions trigonomètriques dels angles $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$, $\ldots$, $\frac{(n-1)P}{n}$. El mètode que hem exposat per a trobar les arrels de Ω (llevat que fossin consultades les taules de sinus durant la tasca, de la manera que hem dit més amunt, però això seria menys directe) s'ha establert de manera que encara deixa incert *quines* arrels corresponen a *cadascun* dels angles; és a dir, quina arrel és $=\cos\frac{P}{n}+i\sin\frac{P}{n}$, quina $=\cos\frac{2P}{n}+i\sin\frac{2P}{n}$, etc. Però aquesta incertesa es dissipa fàcilment reflectint que els cosinus dels angles $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$, $\ldots$, $\frac{(n-1)P}{2n}$, decreixen contínuament (suposat que també es tinguin en compte els signes) i que tots els sinus són positius; en canvi, els angles $\frac{(n-1)P}{n}$, $\frac{(n-2)P}{n}$, $\frac{(n-3)P}{n}$, $\ldots$, $\frac{(n+1)P}{2n}$, tenen respectivament els mateixos cosinus que aquells, però els sinus negatius i iguals en magnitud absoluta als sinus d'aquells. Per tant, de les arrels de Ω, les dues que tenen les parts reals màximes (iguals entre si) correspon-

dran als angles $\frac{P}{n}$, $\frac{(n-1)P}{n}$, i, certament, al primer aquella en què la quantitat imaginària i està multiplicada per una quantitat positiva, al darrer aquella en què i [ho està] per una quantitat negativa. De les $n-3$ arrels restants, novament les que tenen les parts reals màximes correspondran als angles $\frac{2P}{n}$, $\frac{(n-2)P}{n}$, i així successivament. Tan bon punt s'ha reconegut l'arrel a la qual correspon l'angle $\frac{P}{n}$, les que corresponen als angles restants també es podran distingir d'aquí, perquè si se suposa que aquella és $= [\lambda]$, les arrels $[2\lambda]$, $[3\lambda]$, $[4\lambda]$, etc., correspondran, evidentment, als angles $\frac{2P}{n}$, $\frac{3P}{n}$, $\frac{4P}{n}$, etc. Així, es veu tot seguit en l'exemple de l'article 353 que a l'angle $\frac{1}{19}P$ no li pot correspondre cap altra arrel que la [11], i a l'angle $\frac{18}{19}P$, l'arrel [8]; similarment, als angles $\frac{2}{19}P$, $\frac{17}{19}P$, $\frac{3}{19}P$, $\frac{16}{19}P$, etc., els corresponen les arrels [3], [16], [14], [5], etc. En l'exemple de l'article 354, a l'angle $\frac{1}{17}P$ li correspon, evidentment, l'arrel [1]; a l'angle $\frac{2}{17}P$, la [2]; etc. Així, d'aquesta manera, els cosinus i els sinus dels angles $\frac{P}{n}$, $\frac{2P}{n}$, etc., seran plenament determinats.

362. Pel que fa a les funcions trigonomètriques restants d'aquests angles, certament es podrien derivar fàcilment dels cosinus i els sinus corresponents pels mètodes coneguts vulgarment; posem, les secants i les tangents, dividint la unitat i els sinus pels cosinus; i també

les cosecants i les cotangents, dividint la unitat i els cosinus pels sinus. Però, sovint, s'obtindrà el mateix més còmodament sense divisions, per meres addicions, amb l'ajuda de les fórmules següents. Sigui ω qualsevol angle dels $\frac{P}{n}$, $\frac{2P}{n}$, …, $\frac{(n-1)P}{n}$, i $\cos\omega + i\sin\omega = R$, d'on R serà alguna de les arrels de Ω, $\cos\omega = \frac{1}{2}\left(R + \frac{1}{R}\right) = \frac{1+RR}{2R}$, $\sin\omega = \frac{1}{2i}\left(R - \frac{1}{R}\right) = \frac{i(1-RR)}{2R}$. D'aquí resulta $\sec\omega = \frac{2R}{1+RR}$, $\tan\omega = \frac{i(1-RR)}{1+RR}$, $\operatorname{cosec}\omega = \frac{2Ri}{RR-1}$, $\cot\omega = \frac{i(RR+1)}{RR-1}$. Ara mostrarem que els numeradors d'aquestes quatre fraccions es transformen de manera que surten divisibles pels denominadors.

I. A causa que $R = R^{n+1} = R^{2n+1}$, resulta $2R = R + R^{2n+1}$, expressió que és clar que és divisible per $1+RR$, ja que n és un nombre imparell. D'aquí resulta $\sec\omega = R - R^3 + R^5 - R^7 + \cdots + R^{2n-1}$, de manera que (com que, per causa que $\sin\omega = -\sin(2n-1)\omega$, $\sin 3\omega = -\sin(2n-3)\omega$, etc., evidentment resulta $\sin\omega - \sin 3\omega + \sin 5\omega + \cdots + \sin(2n-1)\omega = 0$) $\sec\omega = \cos\omega - \cos 3\omega + \cos 5\omega - \cdots + \cos(2n-1)\omega$, o sigui, finalment (com que $\cos\omega = \cos(2n-1)\omega$, $\cos 3\omega = \cos(2n-3)\omega$, etc.), $= 2(\cos\omega - \cos 3\omega + \cos 5\omega - \cdots \mp \cos(n-2)\omega) \pm \cos n\omega$, on val el signe superior o bé l'inferior segons si n és de la forma $4k+1$ o bé $4k+3$. Evidentment, aquesta fórmula també es pot expressar així:

$$\sec\omega = \pm(1 - 2\cos 2\omega + 2\cos 4\omega + \cdots \pm 2\cos(n-1)\omega).$$

II. De manera similar, substituint $1 - R^{2n+2}$ per $1 - RR$, surt $\tan\omega = i(1 - RR + R^4 - R^6 + \cdots - R^{2n})$,

o sigui (com que $1 - R^{2n} = 0$, $RR - R^{2n-2} = 2i \sin 2\omega$, $R^4 - R^{2n-4} = 2i \sin 4\omega$, etc.),

$$\tan \omega = 2(\sin 2\omega - \sin 4\omega + \sin 6\omega + \cdots \mp \sin(n-1)\omega).$$

III. Com que es té $1 + RR + R^4 + \cdots + R^{2n-2} = 0$, resulta $n = n - 1 - RR - R^4 + \cdots - R^{2n-2} = (1 - 1) + (1 - RR) + (1 - R^4) + \cdots + (1 - R^{2n-2})$, suma de la qual cada part és divisible per $1 - RR$. D'aquí, $\dfrac{n}{1-RR} = 1 + (1 + RR) + (1 + RR + R^4) + \cdots + (1 + RR + R^4 + \cdots + R^{2n-4}) = (n-1) + (n-2)RR + (n-3)R^4 + \cdots + R^{2n-4}$; conseqüentment, multiplicant per 2, restant $0 = (n-1)(1 + RR + R^4 + \cdots + R^{2n-2})$ i multiplicant de nou per R, resulta $\dfrac{2nR}{1-RR} = (n-1)R + (n-3)R^3 + (n-5)R^5 + \cdots - (n-3)R^{2n-3} - (n-1)R^{2n-1}$, d'on es dedueix directament $\operatorname{cosec} \omega = \dfrac{1}{n}((n-1)\sin\omega + (n-3)\sin 3\omega + \cdots - (n-1)\sin(2n-1)\omega) = \dfrac{2}{n}((n-1)\sin\omega + (n-3)\sin 3\omega + etc. + 2\sin(n-2)\omega)$, fórmula que també es pot expressar així:

$$\operatorname{cosec} \omega = -\frac{2}{n}(2\sin 2\omega + 4\sin 4\omega + 6\sin 6\omega + \\ + \cdots + (n-1)\sin(n-1)\omega).$$

IV. Multiplicant el valor de $\dfrac{n}{1-RR}$ transmès més amunt per $1+RR$ i restant $0 = (n-1)(1+RR+R^4+\cdots+R^{2n-2})$, surt $\dfrac{n(1+RR)}{1-RR} = (n-2)RR + (n-4)R^4 + (n-6)R^6 + \cdots - (n-2)R^{2n-2}$, d'on se segueix immediatament que $\cot\omega = \dfrac{1}{n}((n-2)\sin 2\omega + (n-4)\sin 4\omega + (n-$

6) $\sin 6\omega + \cdots - (n-2)\sin(n-2)\omega) = \frac{2}{n}((n-2)\sin 2\omega + (n-4)\sin 4\omega + \cdots + 3\sin(n-3)\omega + \sin(n-1)\omega)$, fórmula que també es pot expressar d'aquesta manera:

$$\cot\omega = -\frac{2}{n}(\sin\omega + 3\sin 3\omega + \cdots + (n-2)\sin(n-2)\omega).$$

363. De la mateixa manera que, suposant que $n-1 = ef$, la funció X es pot descompondre en e factors de f dimensions sempre que es coneguin els valors de totes les e sumes de f termes (article 348), llavors, així també, suposant que $Z = 0$ és una equació d'ordre $(n-1)$-èsim les arrels de la qual són els sinus o bé qualsevol altra de les funcions trigonomètriques dels angles $\frac{P}{n}$, $\frac{2P}{n}$, …, $\frac{(n-1)P}{n}$, la funció Z es podrà descompondre en e factors de f dimensions; qüestió de la qual les consideracions més importants són aquestes.

Consti Ω dels e períodes de f termes $(f, 1) = P$, P', P'', etc., i el període P de les arrels [1], $[a]$, $[b]$, $[c]$, etc.; P' de les $[a']$, $[b']$, $[c']$, etc.; P'' de les $[a'']$, $[b'']$, $[c'']$, etc., etc. Correspongui a l'arrel [1] l'angle ω, de manera que a les arrels $[a]$, $[b]$, etc., els angles $a\omega$, $b\omega$, etc.; a les arrels $[a']$, $[b']$, etc., els angles $a'\omega$, $b'\omega$, etc.; a les arrels $[a'']$, $[b'']$, etc., els angles $a''\omega$, $b''\omega$, etc.; etc., i es copsarà fàcilment que tots aquests angles presos simultàniament coincideixen amb els angles $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$, …, $\frac{(n-1)P}{n}$, respecte a les funcions trigonomètriques.* Així, si la

* Respecte a això, dos angles la diferència dels quals és igual o bé a la perifèria sencera o bé a un dels seus múltiples coincideixen; podríem anomenar-los *congrus segons la perifèria* si es volgués entendre congruència en un sentit una mica més ampli.

funció de què es tracta es denota pel caràcter ϕ prefixat a l'angle, s'estableix $= Y$ el producte dels e factors $x-\phi\omega$, $x-\phi a\omega$, etc.; $= Y'$ el producte dels $x-\phi a'\omega$, $x-\phi b'\omega$, etc.; $= Y''$ el producte dels $x-\phi a''\omega$, $x-\phi b''\omega$, etc.; etc., necessàriament el producte $YY'Y''\cdots$ serà $= Z$. Ara resta que demostrem que tots els coeficients de les funcions Y, Y', Y'', etc., es poden reduir a una forma tal com $A+B(f,1)+C(f,g)+D(f,gg)+\cdots+L(f,g^{e-1})$; fet això, tots s'hauran de tenir per coneguts, evidentment, així que s'han conegut els valors de totes les sumes de f termes; farem això de la manera següent.

De la mateixa manera que $\cos\omega = \frac{1}{2}[1]+\frac{1}{2}[1]^{n-1}$, $\sin\omega = -\frac{1}{2}i[1]+\frac{1}{2}i[1]^{n-1}$, així també, per l'article precedent, les funcions trigonomètriques restants de l'angle ω es poden reduir a una forma tal com $\mathfrak{A}+\mathfrak{B}[1]+\mathfrak{C}[1]^2+\mathfrak{D}[1]^3+$ *etc.*, i es copsarà sense cap dificultat que, llavors, la funció de l'angle $k\omega$ resulta $= \mathfrak{A}+\mathfrak{B}[k]+\mathfrak{C}[k]^2+\mathfrak{D}[k]^3+$ *etc.*, on k denota un enter qualsevol. Ara, com que cadascun dels coeficients de Y són funcions racionals enteres invariants de les $\phi\omega$, $\phi a\omega$, $\phi b\omega$, etc., és evident que si se substitueixen aquestes quantitats pels seus valors, cadascun dels coeficients resulten funcions racionals enteres invariants de les $[1]$, $[a]$, $[b]$, etc.; per la qual cosa, per l'article 347, es reduiran a la forma $A+B(f,1)+C(f,g)+$ *etc.* I per una raó completament similar, tots els coeficients de Y', Y'', etc., també es podran reduir a una forma similar. *Q. E. D.*

364. Sobre el problema de l'article precedent, encara afegim algunes observacions.

I. Com que cadascun dels coeficients de Y' són funcions de les arrels contingudes en el període P' (que es pot establir $= (f, a')$), tals com les funcions de les arrels de P són els coeficients corresponents de Y, és evident, per l'article 347, que Y' es pot derivar de Y sempre que en Y se substitueixin a tot arreu $(f, 1)$, (f, g), (f, gg), etc. per (f, a'), $(f, a'g)$, $(f, a'gg)$, etc., respectivament. Igualment, Y'' es derivarà de Y substituint a tot arreu en Y $(f, 1)$, (f, g), (f, gg), etc., per (f, a''), $(f, a''g)$, $(f, a''gg)$, etc., respectivament; etc. Així, doncs, al mateix temps que s'ha desenvolupat la funció Y, les restants Y', Y'', etc., se segueixen d'aquí sense cap dificultat.

II. Suposant que $Y = x^f - \alpha x^{f-1} + \beta x^{f-2} - etc.$, els coeficients α, β, etc., seran, respectivament, sumes de les arrels de l'equació $Y = 0$, és a dir, de les quantitats $\phi\omega$, $\phi a\omega$, $\phi b\omega$, etc., suma de productes de dues en dues, etc. Però, sovint, aquests coeficients es troben molt més còmodament per un mètode similar al que s'ha transmès en l'article 349, calculant la suma de les arrels $\phi\omega$, $\phi a\omega$, $\phi b\omega$, etc., la suma dels quadrats, dels cubs, etc., i deduint d'aquí, pel teorema de Newton, aquells coeficients. Quan ϕ designa la tangent, la secant, la cotangent o bé la cosecant encara es donen altres estalvis que aquí, però, passem en silenci.

III. Mereix una consideració peculiar el cas en què f és un nombre parell, de manera que qualsevol període P, P', P'', etc., és compost de $\frac{1}{2}f$ períodes de dos termes. Consti P de $(2, 1)$, $(2, \mathfrak{a})$, $(2, \mathfrak{b})$, $(2, \mathfrak{c})$, etc., i els nombres 1, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, etc. i $n-1$, $n-\mathfrak{a}$, $n-\mathfrak{b}$, $n-\mathfrak{c}$, etc., presos simultàniament, coincidiran amb els 1, a, b, c, etc.,

o almenys (cosa que aquí rendeix el mateix) seran congrus a ells segons el mòdul n. Però és $\phi(n-1)\omega = \pm\phi\omega$, $\phi(n-\mathfrak{a})\omega = \pm\phi\mathfrak{a}\omega$, etc., on valen els signes superiors quan ϕ designa el cosinus o bé la secant, els inferiors quan ϕ expressa el sinus, la tangent, la cotangent o bé la cosecant. D'aquí es conclou que, en els dos primers casos, els factors dels quals està compost Y són iguals per parells, de manera que Y és quadrat, i, certament, $Y = yy$, si y es posa igual al producte de $x-\phi\omega$, $x-\phi\mathfrak{a}\omega$, $x-\phi\mathfrak{b}\omega$, etc. Similarment, en els mateixos casos, les funcions restants Y', Y'', etc., seran quadrats, i suposant, certament, que P' consta de $(2, \mathfrak{a}')$, $(2, \mathfrak{b}')$, $(2, \mathfrak{c}')$, etc.; P'' de $(2, \mathfrak{a}'')$, $(2, \mathfrak{b}'')$, $(2, \mathfrak{c}'')$, etc.; etc., el producte dels $x-\phi\mathfrak{a}'\omega$, $x-\phi\mathfrak{b}'\omega$, $x-\phi\mathfrak{c}'\omega$, etc., és $= y'$; el producte dels $x-\phi\mathfrak{a}''\omega$, $x-\phi\mathfrak{b}''\omega$, etc., $= y''$; etc., serà $Y' = y'y'$, $Y'' = y''y''$, etc.; i la funció Z també serà un quadrat (confronteu l'article 337 més amunt) i l'arrel igual al producte de y, y', y'', etc. D'altra banda, es copsarà fàcilment que y', y'', etc., es deriven de y igualment com hem dit abans en I que Y', Y'', etc., se segueixen de Y; i cadascun dels coeficients de y també es pot [reduir] a la forma $A + B(f, 1) + C(f, g) + etc.$, ja que les sumes de cadascuna de les potències de l'equació $y = 0$ són evidentment la meitat de les potències de l'equació $Y = 0$, de manera que reductibles a la tal forma. Però en els quatre casos posteriors, Y serà el producte dels factors $xx - (\phi\omega)^2$, $xx - (\phi\mathfrak{a}\omega)^2$, $xx - (\phi\mathfrak{b}\omega)^2$, etc., de manera que de la forma $x^f - \lambda x^{f-2} + \mu x^{f-4} - etc.$, i és clar que els coeficients λ, μ, etc., es poden deduir de les sumes de quadrats, biquadrats, etc., de les arrels $\phi\omega$, $\phi\mathfrak{a}\omega$, $\phi\mathfrak{b}\omega$, etc.; i les funcions Y', Y'', etc., es comporten similarment.

Exemple I. Sigui $n = 17$, $f = 8$, i designi ϕ el cosinus. D'aquí resulta $Z = (x^8 + \frac{1}{2}x^7 - \frac{7}{4}x^6 - \frac{3}{4}x^5 + \frac{15}{16}x^4 + \frac{5}{16}x^3 - \frac{5}{32}xx - \frac{1}{32}x + \frac{1}{256})^2$, i, així, convé descompondre $\sqrt{Z}$ en dos factors y, y', de quatre dimensions. El període $P = (8, 1)$ consta de $(2, 1)$, $(2, 9)$, $(2, 13)$, $(2, 15)$, d'on y serà el producte dels factors $x - \phi\omega$, $x - \phi 9\omega$, $x - \phi 13\omega$, $x - \phi 15\omega$. Substituint $\phi k\omega$ per $\frac{1}{2}[k] + \frac{1}{2}[n - k]$, es troba $\phi\omega + \phi 9\omega + \phi 13\omega + \phi 15\omega = \frac{1}{2}(8, 1)$; $(\phi\omega)^2 + (\phi 9\omega)^2 + (\phi 13\omega)^2 + (\phi 15\omega)^2 = 2 + \frac{1}{4}(8, 1)$; igualment, la suma dels cubs $= \frac{3}{8}(8, 1) + \frac{1}{8}(8, 3)$, la suma dels biquadrats $= 1\frac{1}{2} + \frac{5}{16}(8, 1)$; d'aquí, determinats els coeficients de y pel teorema de Newton, surt $y = x^4 - \frac{1}{2}(8, 1)x^3 + \frac{1}{4}((8, 1) + 2(8, 3))xx - \frac{1}{8}((8, 1) + 3(8, 3))x + \frac{1}{16}((8, 1) + (8, 3))$; y', però, es deriva de y commutant $(8, 1)$ amb $(8, 3)$; així, substituint $(8, 1)$, $(8, 3)$ pels valors $-\frac{1}{2} + \frac{1}{2}\sqrt{17}$, $-\frac{1}{2} - \frac{1}{2}\sqrt{17}$, resulta

$$y = x^4 + \left(\frac{1}{4} - \frac{1}{4}\sqrt{17}\right)x^3 - \left(\frac{3}{8} + \frac{1}{8}\sqrt{17}\right)xx + \left(\frac{1}{4} + \frac{1}{8}\sqrt{17}\right)x - \frac{1}{16},$$

$$y' = x^4 + \left(\frac{1}{4} + \frac{1}{4}\sqrt{17}\right)x^3 - \left(\frac{3}{8} - \frac{1}{8}\sqrt{17}\right)xx + \left(\frac{1}{4} - \frac{1}{8}\sqrt{17}\right)x - \frac{1}{16}.$$

De manera similar, $\sqrt{Z}$ es pot descompondre en quatre factors de dues dimensions, el primer dels quals serà $(x-\phi\omega)(x-\phi 13\omega)$, el segon $(x-\phi 9\omega)(x-\phi 15\omega)$, el tercer $(x-\phi 3\omega)(x-\phi 5\omega)$, el quart $(x-\phi 10\omega)(x-\phi 11\omega)$, i tots els coeficients d'aquests factors es podran expressar per les quatre sumes (4, 1), (4, 9), (4, 3), (4, 10). Evidentment, però, el producte del primer factor pel segon serà y; el producte del tercer pel quart, y'.

Exemple II. Si, mantenint totes les [hipòtesis] restants, se suposa que ϕ indica el sinus, de manera que convé descompondre $Z = x^{16} - \frac{17}{4}x^{14} + \frac{119}{16}x^{12} - \frac{221}{32}x^{10} + \frac{935}{256}x^8 - \frac{561}{512}x^6 + \frac{357}{2048}x^4 - \frac{51}{4096}xx + \frac{17}{65536}$ en dos factors y, y', de 8 dimensions, y serà el producte dels quatre factors dobles $xx - (\phi\omega)^2$, $xx - (\phi 9\omega)^2$, $xx - (\phi 13\omega)^2$, $xx - (\phi 15\omega)^2$. Ara, com que és $\phi k\omega = -\frac{1}{2}i[k] + \frac{1}{2}i[n-k]$, serà $(\phi k\omega)^2 = -\frac{1}{4}[2k] + \frac{1}{2}[n] - \frac{1}{4}[2n-2k] = \frac{1}{2} - \frac{1}{4}[2k] - \frac{1}{4}[2n-2k]$; d'aquí es dedueix que la suma dels quadrats de les arrels $\phi\omega$, $\phi 9\omega$, $\phi 13\omega$, $\phi 15\omega$ és la $2 - \frac{1}{4}(8, 1)$; la suma dels biquadrats de les mateixes, $= \frac{3}{2} - \frac{3}{16}(8, 1)$; la suma de les potències sisenes $= \frac{5}{4} - \frac{9}{64}(8, 1) - \frac{1}{64}(8, 3)$; la suma de les vuitenes $\frac{35}{32} - \frac{27}{256}(8, 1) - \frac{1}{32}(8, 3)$. D'aquí resulta $y = x^8 - \left(2 - \frac{1}{4}(8, 1)\right)x^6 + \left(\frac{3}{2} - \frac{5}{16}(8, 1) + \frac{1}{8}(8, 3)\right)x^4 - \left(\frac{1}{2} - \frac{9}{64}(8, 1) + \frac{5}{64}(8, 3)\right)xx + \frac{1}{16} - \frac{5}{256}(8, 1)$

$+\frac{3}{256}(8,3)$; y' es deriva de y commutant $(8,1)$, $(8,3)$, de manera que per substitució dels valors d'aquestes sumes es té $y = x^8 - \left(\frac{17}{8} - \frac{1}{8}\sqrt{17}\right)x^6 + \left(\frac{51}{32} - \frac{7}{32}\sqrt{17}\right)x^4 - \left(\frac{17}{32} - \frac{7}{64}\sqrt{17}\right)xx + \frac{17}{256} - \frac{1}{64}\sqrt{17}$, $y' = x^8 - \left(\frac{17}{8} + \frac{1}{8}\sqrt{17}\right)x^6 + \left(\frac{51}{32} + \frac{7}{32}\sqrt{17}\right)x^4 - \left(\frac{17}{32} + \frac{7}{64}\sqrt{17}\right)xx + \frac{17}{256} + \frac{1}{64}\sqrt{17}$. Igualment, Z es pot descompondre en quatre factors, els coeficients dels quals es poden expressar per sumes de quatre termes, i, certament, el producte de dos serà y, el producte dels dos restants, y'.

365. Així, per les disquisicions precedents, hem reduït la secció del cercle en n parts, si n és un nombre primer, a la solució de tantes equacions com en factors es pot descompondre el nombre $n-1$, i els graus d'aquestes equacions es determinen per la magnitud dels factors. Així, quan $n-1$ és una potència del nombre 2, cosa que succeeix per als valors 3, 5, 17, 257, 65537, etc., de n, la secció del cercle es reduirà a equacions només quadràtiques, i les funcions trigonomètriques dels angles $\frac{P}{n}$, $\frac{2P}{n}$, etc., es podran expressar per arrels quadrades més o menys complicades (per a la magnitud de n); conseqüentment, en aquests casos, la secció del cercle en n parts, o sigui, la descripció d'un polígon regular de n costats, es podrà acabar evidentment per construccions geomètriques. Així, per exemple, per a $n = 17$, dels articles 354, 361, per al cosinus de l'angle $\frac{1}{17}P$ es deriva fàcilment l'expressió

$$-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}$$
$$+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}};$$

els cosinus dels múltiples d'aquell angle tenen una forma similar, però els sinus, un signe radical més. És realment sorprenent en gran manera que, encara que la divisibilitat geomètrica del cercle en tres i cinc parts ja fos coneguda en temps d'Euclides, no s'hagi afegit res a aquests descobriments en l'interval de 2000 anys, i tots els geòmetres han presentat com a cert que, excepte aquelles seccions i les que en dimanen espontàniament, posem les seccions en 15, $3\cdot 2^\mu$, $5\cdot 2^\mu$, $15\cdot 2^\mu$, i també en 2^μ parts, cap altra no es pugui acabar per construccions geomètriques. D'altra banda, es prova fàcilment que si el nombre primer n és $= 2^m+1$, tampoc l'exponent m no pot implicar altres factors primers que el nombre 2, de manera que ha de ser o bé $= 1$ o bé $= 2$ o bé una potència més alta del nombre 2; en efecte, si m fos divisible per algun nombre imparell ζ (més gran que la unitat) i $m = \zeta\eta$, $2^m + 1$ seria divisible per $2^\eta + 1$, de manera que, necessàriament, compost. Així, tots els valors de n per als quals arribem a meres equacions quadràtiques es contenen en la forma $2^{2^\nu}+1$; així, els cinc nombres 3, 5, 17, 257, 65537 surten establint $\nu = 0$, 1, 2, 3, 4, o sigui, $m = 1$, 2, 4, 8, 16. De cap manera, però, la secció del cercle no es pot realitzar geomètricament per a *tots* els nombres continguts en aquella forma, sinó només per a aquells que són nombres primers. Certament, Fermat, enganyat per l'indici, va afirmar que tots els nombres continguts en aquella forma són necessàriament primers; però l'il·lm. Euler advertí el primer que aquesta regla ja

és errònia per a $\nu = 5$, o sigui, $m = 32$, perquè el nombre $2^{32} + 1 = 4294967297$ involucra el factor 641.

Però, quan $n - 1$ implica altres factors primers a part de 2, sempre arribem a equacions més altes; posem a una o més cúbiques quan 3 es troba una o més vegades entre els factors primers de $n - 1$; a equacions de cinquè grau quan $n - 1$ és divisible per 5; etc.; I PODEM DEMOSTRAR AMB TOT RIGOR QUE AQUESTES EQUACIONS ELEVADES, NO ES PODEN NI EVITAR NI REDUIR DE CAP MANERA A INFERIORS, encara que els límits d'aquesta obra no permetin transmetre aquí aquesta demostració; cosa, però, que hem considerat que s'ha d'advertir perquè ningú no esperi conduir a construccions geomètriques encara altres seccions excepte les que la nostra teoria suggereix, és a dir, les seccions en 7, 11, 13, 19, etc., parts, i consumeixi el temps inútilment.

366. Si el cercle s'ha de seccionar en a^α parts, on a designa un nombre primer, això es pot fer, evidentment, geomètricament, quan $a = 2$, però no per a cap altre valor de a, suposat que $\alpha > 1$; en efecte, llavors, a part de les equacions que es requereixen per a la secció en a parts, encara en convindrà resoldre necessàriament unes altres $\alpha - 1$ de grau a; i tampoc aquestes no es poden ni evitar ni rebaixar de cap manera. Així, els graus de les equacions necessàries es poden conèixer en general a partir dels factors primers del nombre $(a-1)a^{\alpha-1}$ (això és, també per al cas en què $\alpha = 1$).

Finalment, si el cercle s'ha de seccionar en $N = a^\alpha b^\beta c^\gamma \cdots$ parts, on a, b, c, etc., denoten nombres primers diferents, és suficient haver efectuat les seccions en a^α, b^β, c^γ, etc., parts (article 336); per tant, per

a conèixer els graus de les equacions necessàries per a aquesta finalitat convé considerar els factors primers dels nombres $(a-1)a^{\alpha-1}$, $(b-1)b^{\beta-1}$, $(c-1)c^{\gamma-1}$, etc., o sigui, cosa que aquí rendeix el mateix, els del producte d'aquests nombres. Observeu que aquest producte expressa la quantitat de nombres primers amb N i menors que ell (article 38). Així, llavors, la secció només s'acaba geomètricament quan aquest nombre és una potència binària; però quan implica factors primers diferents de 2, posem p, p', etc., no es poden evitar de cap manera equacions de grau p, p', etc. D'aquí es conclou en general que perquè es pugui seccionar geomètricament el cercle en N parts, N ha de ser, *o bé* 2, *o bé* una potència més alta de 2, *o bé* un nombre primer de la forma 2^m+1, *o bé* el producte de molts nombres primers d'aquest tipus, *o bé* el producte d'un tal primer o bé més per 2 o bé una potència més alta de 2; o sigui, més breument, es requereix que N no impliqui cap factor primer imparell que no sigui de la forma 2^m+1, ni tampoc cap factor primer de la forma 2^m+1 més d'una vegada. D'aquesta manera, es troben els 38 valors de N per sota de 300:

2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.

Secció A

AFEGIMENTS

A *l'article* 28. La solució de l'equació indeterminada $ax = by \pm 1$ no fou trobada primer per l'il·lm. Euler (com es diu allí) sinó ja pel geòmetra del segle 17è., Bachet de Meziriac, cèlebre editor i comentarista de Diofant, per al qual l'il·lm. La Grange va vindicar aquest honor (Add. à l'Algèbre d'Euler p. 525, on juntament és indicada l'índole del mètode). Bachet transmeté el seu descobriment en la segona edició del llibre *Problèmes plaisants et delectables qui se font par les nombres,* 1624; en la primera edició (a Lió, 1612), que és l'única que m'ha estat possible veure, encara no hi és, però, tot i així, ja s'anuncia.

Als articles 151, 296, 297. L'il·lm. Le Gendre va exposar de nou la seva demostració en l'admirable obra *Essai d'une theorie des nombres*, p. 214 i s., però de manera que no es va canviar res d'essencial; per la qual cosa, aquest mètode encara queda sotmès a totes les objeccions adduïdes en l'article 297. Certament, el teo-

rema (que es recolza en una suposició) que en qualsevol progressió aritmètica l, $l + k$, $l + 2k$, etc., es troben nombres primers si k i l no tenen divisor comú, s'ha considerat més extensament en aquesta obra, p. 12 i següents; però sembla que encara no és satisfet el rigor geomètric. No obstant això, també llavors, quan aquest teorema s'haurà demostrat plenament restarà l'altra suposició (es donen nombres primers de la forma $4n + 3$ dels quals un nombre primer donat de la forma $4n + 1$ pres positivament és un no-residu quadràtic), que no sé si es pot demostrar *rigorosament*, llevat que ja *se suposi* el propi teorema fonamental. D'altra banda, convé observar que l'il·lm. Le Gendre no va assumir tàcitament aquesta suposició posterior, sinó que ell mateix tampoc no la va dissimular, p. 221.

Als articles 288–293. Sobre el mateix argument, que aquí s'exposa com a aplicació especial de la teoria de les formes ternàries, i que respecte del rigor i de la generalitat sembla ser absolut, de manera que no es pot desitjar res més, l'il·lm. Le Gendre, en la part III de la seva obra, p. 321–400, va instituir una disquisició molt més àmplia.* Va utilitzar uns principis i uns mètodes completament diferents dels nostres; no obstant això, per aquesta via es va implicar en moltes dificultats que van fer que no pogués proveir de demostració rigorosa uns teoremes mereixedors de la palma. Ell mateix va indicar amb sinceritat aquestes dificultats, però, si no ens equivoquem, aquestes, certament, potser es podran

* Fins i tot no avisant nosaltres, els lectors hauran d'anar amb compte de no confondre les nostres formes ternàries amb el que l'il·lm. Le Gendre va anomenar *forme trinaire d'un nombre*. Això és, va indicar per aquesta expressió la descomposició d'un nombre en tres quadrats.

vèncer més fàcilment que la que també s'ha suposat en aquesta disquisició, el teorema recordat fa un moment (En qualsevol progressió aritmètica, etc.), notes al final de la p. 371.

A l'article 306, VIII. En el tercer miler de determinants negatius se n'han trobat 37 d'irregulars, entre els quals 18 tenen índex d'irregularitat 2 i els 19 restants, índex 3.

Al mateix X. No fa gaire he aconseguit resoldre plenament la qüestió proposada aquí; transmetrem aquesta disquisició, que il·lustra admirablement moltes parts tant de l'Aritmètica superior com de l'Anàlisi, a continuació d'aquesta obra, tan aviat com es pugui. Al mateix temps he ensenyat que el coeficient m de l'article 304, p. 489 és $= \gamma = 2,3458847616$, on γ designa la mateixa quantitat que en l'article 302, i π, com allí, la semicircumferència d'un cercle de radi 1.

TAULA I (articles 58, 91)

		2	3	5	7	11	13	17	19	23	29	31	37	41
		43	47											
3	2	1												
5	2	1	3											
7	3	2	1	5										
9	2	1	*	5	4									
11	2	1	8	4	7									
13	6	5	8	9	7	11								
16	5	*	3	1	2	1	3							
17	10	10	11	7	9	13	12							
19	10	17	5	2	12	6	13	8						
23	10	8	20	15	21	3	12	17	5					
25	2	1	7	*	5	16	19	13	18	11				
27	2	1	*	5	16	13	8	15	12	11				
29	10	11	27	18	20	23	2	7	15	24				
31	17	12	13	20	4	29	23	1	22	21	27			
32	5	*	3	1	2	5	7	4	7	6	3	0		
37	5	11	34	1	28	6	13	5	25	21	15	27		
41	6	26	15	22	39	3	31	33	9	36	7	28	32	
43	28	39	17	5	7	6	40	16	29	20	25	32	35	18
47	10	30	18	17	38	27	3	42	29	39	43	5	24	25
		37												
49	10	2	13	41	*	16	9	31	35	32	24	7	38	27
		36	23											
53	26	25	9	31	38	46	28	42	41	39	6	45	22	33
		30	8											

		2	3	5	7	11	13	17	19	23	29	31	37	41
		43	47	53	59	61	67	71	73	79	83	89		
59	10	25	32	34	44	45	23	14	22	27	4	7	41	2
		13	53	28										
61	10	47	42	14	23	45	20	49	22	39	25	13	33	18
		41	40	51	17									
64	5	*	3	1	10	5	15	12	7	14	11	8	9	14
		13	12	5	1	3								
67	12	29	9	39	7	61	23	8	26	20	22	43	44	19
		63	64	3	54	5								
71	62	58	18	14	33	43	27	7	38	5	4	13	30	55
		44	17	59	29	37	11							
73	5	8	6	1	33	55	59	21	62	46	35	11	64	4
		51	31	53	5	58	50	44						
79	29	50	71	34	19	70	74	9	10	52	1	76	23	21
		47	55	7	17	75	54	33	4					
81	11	25	*	35	22	1	38	15	12	5	7	14	24	29
		10	13	45	53	4	20	33	48	52				
83	50	3	52	81	24	72	67	4	59	16	36	32	60	38
		49	69	13	20	34	53	17	43	47				
89	30	72	87	18	7	4	65	82	53	31	29	57	77	67
		59	34	10	45	19	32	26	68	46	27			
97	10	86	2	11	53	82	83	19	27	79	47	26	41	71
		44	60	14	65	32	51	25	20	42	91	18		

TAULA II (article 99)

	–1	2	3	5	7	11	13	17	19	23	29	31	37
3			–		–		–		–			–	–
5	–			–		–			–		–	–	
7		–			–	–				–	–		–
11			–	–		–				–		–	–
13	–		–				–	–		–	–		
17	–	–					–	–	–				
19				–	–	–		–	–	–			
23		–	–				–			–	–	–	
29	–			–	–		–			–	–		
31		–		–	–				–			–	
37	–		–		–	–							–
41	–	–		–						–		–	–
43						–	–	–		–		–	
47		–	–		–			–					–
53	–				–	–	–	–			–		–
59			–	–	–			–	–		–		
61	–		–	–			–		–				
67								–	–	–	–		–
71		–	–	–					–		–		–
73	–	–	–						–	–			–
79		–		–		–	–		–	–		–	
83			–		–	–		–		–	–	–	–
89	–	–		–		–		–					
97	–	–	–			–						–	

	41	43	47	53	59	61	67	71	73	79	83	89	97
3		–				–	–		–	–			–
5	–				–	–		–		–		–	
7		–		–			–	–		–			
11			–	–	–		–	–				–	–
13		–		–		–				–			
17		–	–	–	–		–				–	–	
19		–	–			–			–		–		
23	–		–		–			–	–				
29				–	–		–	–			–		
31	–		–		–		–	–					–
37	–		–	–			–	–	–		–		
41	–	–			–	–			–		–		
43	–	–	–	–	–		–			–	–		–
47			–	–	–	–		–		–	–	–	–
53		–	–	–	–							–	–
59	–			–	–			–		–			
61	–		–			–			–		–		–
67			–		–		–	–	–		–	–	
71		–						–	–	–	–	–	
73	–					–	–	–	–	–		–	–
79							–		–	–	–	–	–
83	–				–	–					–		
89			–	–			–	–	–	–		–	–
97		–	–	–		–			–	–		–	–

TAULA III (article 316)

3	(0)	3;	(1)	6
7	(0)	142857		
9	(0)	1;	(1)	2;
	(2)	4;	(3)	8;
	(4)	7;	(5)	5
11	(0)	09;	(1)	18;
	(2)	36;	(3)	72;
	(4)	45		
13	(0)	076923;	(1)	461538
17	(0)	0588235294	117647	
19	(0)	0526315789	47368421	
23	(0)	0434782608	6956521739	13
27	(0)	037;	(1)	074;
	(2)	148;	(3)	296;
	(4)	592;	(5)	185
29	(0)	0344827586	2068965517	24137931
31	(0)	0322580645	16129;	
	(1)	5483870967	74193	
37	(0)	027;	(1)	135;
	(2)	675;	(3)	378;
	(4)	891;	(5)	459;
	(6)	297;	(7)	486;
	(8)	432;	(9)	162;
	(10)	810;	(11)	054

41	(0)	02439;	(1)	14634;
	(2)	87804;	(3)	26829;
	(4)	60975;	(5)	65853;
	(6)	95121;	(7)	70731
43	(0)	0232558139	5348837209	3
	(1)	6511627906	9767441860	4
47	(0)	0212765957	4468085106	3829787234
		0425531914	893617	
49	(0)	0204081632	6530612244	8979591836
		7346938775	51	
53	(0)	0188679245	283;	
	(1)	4905660377	358;	
	(2)	7547169811	320;	
	(3)	6226415094	339	
59	(0)	0169491525	4237288135	5932203389
		8305084745	7627118644	06779661
61	(0)	0163934426	2295081967	2131147540
		9836065573	7704918032	7868852459
67	(0)	0149253731	3432835820	8955223880
		597		
	(1)	1791044776	1194029850	7462686567
		164		
71	(0)	0140845070	4225352112	6760563380
		28169		
	(1)	8732394366	1971830985	9154929577
		46478		

73	(0)	01369863;	(1)	06849315;
	(2)	34246575;	(3)	71232876;
	(4)	56164383;	(5)	80821917;
	(6)	04109589;	(7)	20547945;
	(8)	02739726		
79	(0)	0126582278	481;	
	(1)	3670886075	949;	
	(2)	6455696202	531;	
	(3)	7215189873	417;	
	(4)	9240506329	113;	
	(5)	7974683544	303	
81	(0)	012345679;	(1)	135802469;
	(2)	493827160;	(3)	432098765;
	(4)	753086419;	(5)	283950617
83	(0)	0120481927	7108433734	9397590361
		4457831325	3	
	(1)	6024096385	5421686746	9879518072
		2891566265	0	
89	(0)	0112359550	5617977528	0898876404
		4943820224	7191	
	(1)	3370786516	8539325842	6966292134
		8314606741	5730	
97	(0)	0103092783	5051546391	7525773195
		8762886597	9381443298	9690721649
		4845360824	7422680412	3711340206
		185567		