Aritmètica
Curs 2025-2026

UNIVERSITAT DE BARCELONA

Darrera lliçó (problemes)

Artur Travesa

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona
27 de maig de 2026

Un problema d'arrels primitives

Artur Travesa

27 de maig de 2026

Història

En la sessió del Seminari de Teoria de Nombres (UB-UAB-UPC) del dia 21 de gener de 2019, vaig presentar una conferència amb el títol

Història

En la sessió del Seminari de Teoria de Nombres (UB-UAB-UPC) del dia 21 de gener de 2019, vaig presentar una conferència amb el títol

Arrels primitives: fets i qüestions

Història

En la sessió del Seminari de Teoria de Nombres (UB-UAB-UPC) del dia 21 de gener de 2019, vaig presentar una conferència amb el títol

Arrels primitives: fets i qüestions

La classe de problemes d'avui és un extracte d'aquell contingut.

Definicions bàsiques i notació

Sigui $p > 2$ un nombre natural primer.

Definicions bàsiques i notació

Sigui $p > 2$ un nombre natural primer.

Hem vist que el grup multiplicatiu $G(p) := (\mathbb{Z}/p\mathbb{Z})^*$ és cíclic. El seu ordre és $\varphi(p) = p - 1$.

Definicions bàsiques i notació

Sigui $p > 2$ un nombre natural primer.

Hem vist que el grup multiplicatiu $G(p) := (\mathbb{Z}/p\mathbb{Z})^*$ és cíclic. El seu ordre és $\varphi(p) = p - 1$.

Definició : Anomenarem arrel primitiva mòdul p tot nombre enter g tal que la seva reducció mòdul p sigui un generador del grup $G(p)$.

Definicions bàsiques i notació

Sigui $p > 2$ un nombre natural primer.

Hem vist que el grup multiplicatiu $G(p) := (\mathbb{Z}/p\mathbb{Z})^*$ és cíclic. El seu ordre és $\varphi(p) = p - 1$.

Definició (restrictiva): Anomenarem arrel primitiva mòdul p tot nombre enter g, $1 \leq g \leq p$, tal que la seva reducció mòdul p sigui un generador del grup $G(p)$.

Definicions bàsiques i notació

Sigui $p > 2$ un nombre natural primer.

Hem vist que el grup multiplicatiu $G(p) := (\mathbb{Z}/p\mathbb{Z})^*$ és cíclic. El seu ordre és $\varphi(p) = p - 1$.

Definició (restrictiva): Anomenarem arrel primitiva mòdul p tot nombre enter g, $1 \leq g \leq p$, tal que la seva reducció mòdul p sigui un generador del grup $G(p)$.

Observació: Notem que triem un conjunt específic de representants de les classes mòdul p; i que, d'acord amb aquesta restricció, 5 no és una arrel primitiva mòdul 3; només $g = 2$ és una arrel primitiva mòdul $p = 3$.

Exemples: totes les arrels primitives per a $2 < p < 32$

p	$g \pmod p$
3	2
5	2, 3
7	3, 5
11	2, 6, 7, 8
13	2, 6, 7, 11
17	3, 5, 6, 7, 10, 11, 12, 14
19	2, 3, 10, 13, 14, 15
23	5, 7, 10, 11, 14, 15, 17, 19, 20, 21
29	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27
31	3, 11, 12, 13, 17, 21, 22, 24

Algunes propietats bàsiques

- *Tota arrel primitiva, g, mòdul un nombre primer $p > 2$ és no-quadrat mòdul p. És a dir, el símbol de Legendre és* $\left(\frac{g}{p}\right) = -1$.

Per tant, com a màxim hi ha $\frac{p-1}{2}$ arrels primitives mòdul p.

Algunes propietats bàsiques

- *Tota arrel primitiva, g, mòdul un nombre primer $p > 2$ és no-quadrat mòdul p. És a dir, el símbol de Legendre és* $\left(\frac{g}{p}\right) = -1$.

Per tant, com a màxim hi ha $\frac{p-1}{2}$ arrels primitives mòdul p.

- De fet, *el nombre d'arrels primitives mòdul p és exactament* $\varphi(p-1)$.

Algunes propietats bàsiques

- *Tota arrel primitiva, g, mòdul un nombre primer $p > 2$ és no-quadrat mòdul p. És a dir, el símbol de Legendre és* $\left(\frac{g}{p}\right) = -1$.

Per tant, com a màxim hi ha $\frac{p-1}{2}$ arrels primitives mòdul p.

- De fet, *el nombre d'arrels primitives mòdul p és exactament* $\varphi(p-1)$.

I, efectivament, és $\varphi(p-1) \leq \frac{p-1}{2}$.

Algunes propietats bàsiques (cont.)

- Notem que

$$\varphi(p-1) = (p-1) \prod_{\substack{\ell \mid p-1 \\ \text{primer}}} \left(1 - \frac{1}{\ell}\right) = \frac{p-1}{2} \prod_{\substack{\ell \mid p-1 \\ \ell \neq 2 \\ \text{primer}}} \left(1 - \frac{1}{\ell}\right).$$

Algunes propietats bàsiques (cont.)

- Notem que

$$\varphi(p-1) = (p-1) \prod_{\substack{\ell \mid p-1 \\ \text{primer}}} \left(1 - \frac{1}{\ell}\right) = \frac{p-1}{2} \prod_{\substack{\ell \mid p-1 \\ \ell \neq 2 \\ \text{primer}}} \left(1 - \frac{1}{\ell}\right).$$

- Per tant, les arrels primitives mòdul un nombre primer $p > 2$ són exactament els no-quadrats si, i només si, el nombre primer p és de Fermat.

Algunes propietats bàsiques (cont.)

- Notem que

$$\varphi(p-1) = (p-1) \prod_{\substack{\ell \mid p-1 \\ \text{primer}}} \left(1 - \frac{1}{\ell}\right) = \frac{p-1}{2} \prod_{\substack{\ell \mid p-1 \\ \ell \neq 2 \\ \text{primer}}} \left(1 - \frac{1}{\ell}\right).$$

- Per tant, les arrels primitives mòdul un nombre primer $p > 2$ són exactament els no-quadrats si, i només si, el nombre primer p és de Fermat.
- **Exercici:** Per a tot nombre primer de Fermat $p > 3$, el nombre $g = 3$ és una arrel primitiva mòdul p.

Algunes propietats bàsiques (cont.)

- Notem que

$$\varphi(p-1) = (p-1) \prod_{\substack{\ell \mid p-1 \\ \text{primer}}} \left(1 - \frac{1}{\ell}\right) = \frac{p-1}{2} \prod_{\substack{\ell \mid p-1 \\ \ell \neq 2 \\ \text{primer}}} \left(1 - \frac{1}{\ell}\right).$$

- Per tant, les arrels primitives mòdul un nombre primer $p > 2$ són exactament els no-quadrats si, i només si, el nombre primer p és de Fermat.
- **Exercici:** Per a tot nombre primer de Fermat $p > 3$, el nombre $g = 3$ és una arrel primitiva mòdul p. I per a tot nombre primer de Fermat $p > 5$, el nombre $g = 2$ no és arrel primitiva modul p.

La conjectura d'Artin

Qüestió

Quins nombres enters g poden ser arrels primitives mòdul algun nombre primer $p > 2$?

La conjectura d'Artin (cont.)

Recordem la taula.

p	$g \pmod p$
3	2
5	2, 3
7	3, 5
11	2, 6, 7, 8
13	2, 6, 7, 11
17	3, 5, 6, 7, 10, 11, 12, 14
19	2, 3, 10, 13, 14, 15
23	5, 7, 10, 11, 14, 15, 17, 19, 20, 21
29	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27
31	3, 11, 12, 13, 17, 21, 22, 24

La conjectura d'Artin (cont.)

Recordem la taula.

p	$g \pmod p$
3	2
5	2, 3
7	3, 5
11	2, 6, 7, 8
13	2, 6, 7, 11
17	3, 5, 6, 7, 10, 11, 12, 14
19	2, 3, 10, 13, 14, 15
23	5, 7, 10, 11, 14, 15, 17, 19, 20, 21
29	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27
31	3, 11, 12, 13, 17, 21, 22, 24

Notem que la taula conté els nombres naturals 2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 24, 26 i 27.

La conjectura d'Artin (cont.)

Recordem la taula.

p	$g \pmod p$
3	2
5	2, 3
7	3, 5
11	2, 6, 7, 8
13	2, 6, 7, 11
17	3, 5, 6, 7, 10, 11, 12, 14
19	2, 3, 10, 13, 14, 15
23	5, 7, 10, 11, 14, 15, 17, 19, 20, 21
29	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27
31	3, 11, 12, 13, 17, 21, 22, 24

Notem que la taula conté els nombres naturals 2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 24, 26 i 27.
Els únics nombres naturals menors que 31 que no conté són els 1, 4, 9, 16, i 25, i els 23, 28, 29 i 30. (. . . / . . .)

La conjectura d'Artin (cont.)

(. . . / . . .) Però, si ampliem la taula,

La conjectura d'Artin (cont.)

(. . . / . . .) Però, si ampliem la taula,

p	$g \pmod p$
31	3, 11, 12, 13, 17, 21, 22, 24
. . .	. . .
41	6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35
43	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34
47	5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45
53	2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51
59	2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56
. . .	. . .
67	2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63

La conjectura d'Artin (cont.)

(. . . / . . .) Però, si ampliem la taula,

p	$g \pmod p$
31	3, 11, 12, 13, 17, 21, 22, 24
. . .	. . .
41	6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35
43	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34
47	5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45
53	2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51
59	2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56
. . .	. . .
67	2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63

els únics nombres naturals menors que 51 que no conté són els 1, 4, 9, 16, 25, 36 i 49.

La conjectura d'Artin (cont.)

Conjectura (E. Artin, 1927)

La conjectura d'Artin (cont.)

Conjectura (E. Artin, 1927)

Sigui $g \in \mathbb{Z}$ un nombre enter, $g \neq 0$, $g \neq -1$, i g no-quadrat.

La conjectura d'Artin (cont.)

Conjectura (E. Artin, 1927)

Sigui $g \in \mathbb{Z}$ un nombre enter, $g \neq 0$, $g \neq -1$, i g no-quadrat. Llavors, existeix una infinitat de nombres primers $p > 2$ tals que la reducció mòdul p de g és una arrel primitiva mòdul p.

La conjectura d'Artin (cont.)

Conjectura (E. Artin, 1927)

Sigui $g \in \mathbb{Z}$ un nombre enter, $g \neq 0$, $g \neq -1$, i g no-quadrat. Llavors, existeix una infinitat de nombres primers $p > 2$ tals que la reducció mòdul p de g és una arrel primitiva mòdul p.

Observació

Ja hem vist que per a tot nombre primer $p > 2$ els quadrats no poden ser arrels primitives mòdul p.

La conjectura d'Artin (cont.)

Conjectura (E. Artin, 1927)

Sigui $g \in \mathbb{Z}$ un nombre enter, $g \neq 0$, $g \neq -1$, i g no-quadrat. Llavors, existeix una infinitat de nombres primers $p > 2$ tals que la reducció mòdul p de g és una arrel primitiva mòdul p.

Observació

Ja hem vist que per a tot nombre primer $p > 2$ els quadrats no poden ser arrels primitives mòdul p.
D'altra banda, mòdul qualsevol nombre primer $p > 2$, el nombre $g = -1$ és d'ordre 2, de manera que -1 només pot ser arrel primitiva mòdul p si $p - 1 = \varphi(p) = 2$; això és, només per a $p = 3$.

HGR $\Longrightarrow$ la conjectura d'Artin

Sigui $g \in \mathbb{Z}$ un nombre enter, $g \neq 0$, $g \neq -1$, i g no-quadrat. Per a tot nombre real positiu x, denotem per $N(x; g)$ la quantitat de nombres primers p, $2 < p \leq x$, tals que la reducció mòdul p de g és una arrel primitiva mòdul p.

Teorema (C. Hooley, 1967, suposa la validesa de la HGR)

HGR $\Longrightarrow$ la conjectura d'Artin

Sigui $g \in \mathbb{Z}$ un nombre enter, $g \neq 0$, $g \neq -1$, i g no-quadrat. Per a tot nombre real positiu x, denotem per $N(x; g)$ la quantitat de nombres primers p, $2 < p \leq x$, tals que la reducció mòdul p de g és una arrel primitiva mòdul p.

Teorema (C. Hooley, 1967, suposa la validesa de la HGR)

La funció $N(x; g)$ és donada asimptòticament per $C(g)\pi(x)$, on $\pi(x)$ és la funció que compta la quantitat de nombres primers p, $1 < p \leq x$, i $C(g)$ és una constant positiva, que depèn de g.

HGR $\Longrightarrow$ la conjectura d'Artin

Sigui $g \in \mathbb{Z}$ un nombre enter, $g \neq 0$, $g \neq -1$, i g no-quadrat. Per a tot nombre real positiu x, denotem per $N(x; g)$ la quantitat de nombres primers p, $2 < p \leq x$, tals que la reducció mòdul p de g és una arrel primitiva mòdul p.

Teorema (C. Hooley, 1967, suposa la validesa de la HGR)

La funció $N(x; g)$ és donada asimptòticament per $C(g)\pi(x)$, on $\pi(x)$ és la funció que compta la quantitat de nombres primers p, $1 < p \leq x$, i $C(g)$ és una constant positiva, que depèn de g.
A més a més, els valors de $C(g)$ són múltiples racionals (estrictament positius) de la constant d'Artin

$$A := \prod_{p,\ primer} \left(1 - \frac{1}{p(p-1)}\right) \simeq 0,37395581361920228805\ldots \square$$

HGR $\Longrightarrow$ la conjectura d'Artin

Sigui $g \in \mathbb{Z}$ un nombre enter, $g \neq 0$, $g \neq -1$, i g no-quadrat. Per a tot nombre real positiu x, denotem per $N(x; g)$ la quantitat de nombres primers p, $2 < p \leq x$, tals que la reducció mòdul p de g és una arrel primitiva mòdul p.

Teorema (C. Hooley, 1967, suposa la validesa de la HGR)

La funció $N(x; g)$ és donada asimptòticament per $C(g)\pi(x)$, on $\pi(x)$ és la funció que compta la quantitat de nombres primers p, $1 < p \leq x$, i $C(g)$ és una constant positiva, que depèn de g.
A més a més, els valors de $C(g)$ són múltiples racionals (estrictament positius) de la constant d'Artin

$$A := \prod_{p,\ primer} \left(1 - \frac{1}{p(p-1)}\right) \simeq 0,37395581361920228805\ldots \square$$

El teorema també especifica (aquí no ho fem) una infinitat de valors de g per als quals $C(g) = A$.

La conjectura d'Artin (cont.)

Càlculs posteriors recolzen els valors que afirma el teorema; presentem un extracte de la taula dels valors de la constant $C(g)$.

La conjectura d'Artin (cont.)

Càlculs posteriors recolzen els valors que afirma el teorema; presentem un extracte de la taula dels valors de la constant $C(g)$.

g	$C(g)/A$	aprox.
2	1	1.000000
3	1	1.000000
5	20/19	1.052632
6	1	1.000000
7	1	1.000000
8	3/5	0.600000
10	1	1.000000
11	1	1.000000
12	1	1.000000
13	156/155	1.006452
14	1	1.000000
15	1	1.000000
17	272/271	1.003690
18	1	1.000000
19	1	1.000000
20	20/19	1.052632

g	$C(g)/A$	aprox.
21	204/205	0.995122
22	1	1.000000
23	1	1.000000
24	1	1.000000
26	1	1.000000
27	3/5	0.600000
28	1	1.000000
29	812/811	1.001233
30	1	1.000000
31	1	1.000000
32	15/19	0.789474
33	544/545	0.998165
34	1	1.000000
35	1	1.000000
37	1332/1331	1.000751
38	1	1.000000

La conjectura d'Artin (cont.) (Alguns resultats parcials incondicionals)

Mencionem alguns resultats importants incondicionals.

La conjectura d'Artin (cont.) (Alguns resultats parcials incondicionals)

Mencionem alguns resultats importants incondicionals.

Teorema (R. Murty i R. Gupta; 1984)

La conjectura d'Artin és certa per a una infinitat de valors de g. $\square$

La conjectura d'Artin (cont.) (Alguns resultats parcials incondicionals)

Mencionem alguns resultats importants incondicionals.

Teorema (R. Murty i R. Gupta; 1984)

La conjectura d'Artin és certa per a una infinitat de valors de g. □

Teorema (R. Heath-Brown, 1986)

(a) *Hi ha com a màxim dos nombres* **naturals primers** g *per als quals la conjectura d'Artin no és certa per a* g.

(b) *Hi ha com a màxim tres nombres* **naturals lliures de quadrats** $g > 1$ *per als quals la conjectura d'Artin no és certa per a* g.

(c) *Sigui* $\mathcal{E}$ *el conjunt de les excepcions a la conjectura d'Artin,*

$$\mathcal{E} := \{g \in \mathbb{Z} : \text{ la conjectura d'Artin no és certa per a } g\}.$$

Llavors, per a $x \in \mathbb{R}$, $x > 0$, *és*

$$\#\{g \in \mathcal{E} : |g| \leq x\} = O\big(\log^2(x)\big). \square$$

L'arrel primitiva mínima

Canviem una mica el focus.

L'arrel primitiva mínima

Canviem una mica el focus.

La definició d'arrel primitiva
mòdul un nombre primer $p > 2$

L'arrel primitiva mínima

Canviem una mica el focus.

La definició d'arrel primitiva (restringida a l'interval $1 \leq g \leq p-1$) mòdul un nombre primer $p > 2$, fa que tingui sentit parlar de l'**arrel primitiva mínima** mòdul p.

L'arrel primitiva mínima

Canviem una mica el focus.

La definició d'arrel primitiva (restringida a l'interval $1 \leq g \leq p-1$) mòdul un nombre primer $p > 2$, fa que tingui sentit parlar de l'**arrel primitiva mínima** mòdul p.

Notació

Escriurem $g(p)$ per a l'arrel primitiva mínima mòdul p.

L'arrel primitiva mínima

Canviem una mica el focus.

La definició d'arrel primitiva (restringida a l'interval $1 \leq g \leq p-1$) mòdul un nombre primer $p > 2$, fa que tingui sentit parlar de l'**arrel primitiva mínima** mòdul p.

Notació

Escriurem $g(p)$ per a l'arrel primitiva mínima mòdul p.
Així,

$$g(p) = \min\{g : 1 \leq g \leq p-1,\ g \text{ genera } G(p)\}.$$

L'arrel primitiva mínima

Canviem una mica el focus.

La definició d'arrel primitiva (restringida a l'interval $1 \leq g \leq p-1$) mòdul un nombre primer $p > 2$, fa que tingui sentit parlar de l'**arrel primitiva mínima** mòdul p.

Notació

Escriurem $g(p)$ per a l'arrel primitiva mínima mòdul p.
Així,

$$g(p) = \min\{g : 1 \leq g \leq p-1,\ g \text{ genera } G(p)\}.$$

I com que $\#G(p) > 1$, resulta que $g(p) > 1$.

L'arrel primitiva mínima (cont.)

Qüestió

L'arrel primitiva mínima (cont.)

Qüestió

Quins nombres naturals poden ser arrel primitiva **mínima** mòdul algun nombre primer $p > 2$?

L'arrel primitiva mínima (cont.)

Qüestió

Quins nombres naturals poden ser arrel primitiva **mínima** mòdul algun nombre primer $p > 2$?

Recordem el resultat següent.

L'arrel primitiva mínima (cont.)

Qüestió

Quins nombres naturals poden ser arrel primitiva **mínima** mòdul algun nombre primer $p > 2$?

Recordem el resultat següent.

Proposició

Sigui $g \in G(p)$ un element qualsevol. Llavors, per a tot exponent natural $k \geq 1$, l'ordre de g^k és $\dfrac{\mathrm{ord}(g)}{\mathrm{mcd}(k, \mathrm{ord}(g))}$, on $\mathrm{ord}(g)$ designa l'ordre de g.

□

L'arrel primitiva mínima (cont.)

Qüestió

Quins nombres naturals poden ser arrel primitiva **mínima** mòdul algun nombre primer $p > 2$?

Recordem el resultat següent.

Proposició

Sigui $g \in G(p)$ un element qualsevol. Llavors, per a tot exponent natural $k \geq 1$, l'ordre de g^k és $\dfrac{\mathrm{ord}(g)}{\mathrm{mcd}(k, \mathrm{ord}(g))}$, on $\mathrm{ord}(g)$ designa l'ordre de g.

□

En particular, l'ordre de g^k és menor o igual que l'ordre de g:

$$\mathrm{ord}(g^k) \leq \mathrm{ord}(g).$$

L'arrel primitiva mínima (cont.)

Corol·lari

Sigui $g \in \mathbb{Z}$, $g > 1$, un nombre natural. Si existeixen nombres $a, k \in \mathbb{Z}$, $a, k > 1$, tals que $g = a^k$, llavors g no pot ser arrel primitiva mínima mòdul p per a cap nombre primer $p > 2$. $\square$

L'arrel primitiva mínima (cont.)

Corol·lari

Sigui $g \in \mathbb{Z}$, $g > 1$, un nombre natural. Si existeixen nombres $a, k \in \mathbb{Z}$, $a, k > 1$, tals que $g = a^k$, llavors g no pot ser arrel primitiva mínima mòdul p per a cap nombre primer $p > 2$. $\square$

Així, per exemple, a més a més dels quadrats
1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, . . . ,

L'arrel primitiva mínima (cont.)

Corol·lari

Sigui $g \in \mathbb{Z}$, $g > 1$, un nombre natural. Si existeixen nombres $a, k \in \mathbb{Z}$, $a, k > 1$, tals que $g = a^k$, llavors g no pot ser arrel primitiva mínima mòdul p per a cap nombre primer $p > 2$. $\square$

Així, per exemple, a més a més dels quadrats
1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, . . . ,

els nombres
8, 27, 32, 125, 128, . . . ,

L'arrel primitiva mínima (cont.)

Corol·lari

Sigui $g \in \mathbb{Z}$, $g > 1$, un nombre natural. Si existeixen nombres $a, k \in \mathbb{Z}$, $a, k > 1$, tals que $g = a^k$, llavors g no pot ser arrel primitiva mínima mòdul p per a cap nombre primer $p > 2$. $\square$

Així, per exemple, a més a més dels quadrats
1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, ...,

els nombres
8, 27, 32, 125, 128, ...,

tampoc no poden ser arrel primitiva mínima per a cap nombre primer $p > 2$.

L'arrel primitiva mínima (cont.)

Per a tot $x \in \mathbb{R}$, $x > 2$, posem

$$\pi_2(x) := \#\{p : 2 < p \leq x,\ p \text{ primer}\} = \pi(x) - 1;$$

L'arrel primitiva mínima (cont.)

Per a tot $x \in \mathbb{R}$, $x > 2$, posem

$$\pi_2(x) := \#\{p : 2 < p \leq x,\ p \text{ primer}\} = \pi(x) - 1;$$

i, per a tot nombre natural $g \geq 2$, g no potència exacta, posem

$$n(g; x) := \#\{p : 2 < p \leq x,\ \text{primer i } g(p) = g\},$$

la quantitat de nombres primers senars menors o iguals que x per als quals l'arrel primitiva mínima mòdul p és exactament g.

L'arrel primitiva mínima (cont.)

Per a tot $x \in \mathbb{R}$, $x > 2$, posem

$$\pi_2(x) := \#\{p : 2 < p \leq x,\ p \text{ primer}\} = \pi(x) - 1;$$

i, per a tot nombre natural $g \geq 2$, g no potència exacta, posem

$$n(g; x) := \#\{p : 2 < p \leq x,\ \text{primer i } g(p) = g\},$$

la quantitat de nombres primers senars menors o iguals que x per als quals l'arrel primitiva mínima mòdul p és exactament g.

Per exemple, $\pi_2(1000) = 167$,

L'arrel primitiva mínima (cont.)

Per a tot $x \in \mathbb{R}$, $x > 2$, posem

$$\pi_2(x) := \#\{p : 2 < p \leq x,\ p \text{ primer}\} = \pi(x) - 1;$$

i, per a tot nombre natural $g \geq 2$, g no potència exacta, posem

$$n(g; x) := \#\{p : 2 < p \leq x,\ \text{primer i } g(p) = g\},$$

la quantitat de nombres primers senars menors o iguals que x per als quals l'arrel primitiva mínima mòdul p és exactament g.

Per exemple, $\pi_2(1000) = 167$,
$\max\{g : n(g; 1000) \neq 0\} = \max\{g(p) : 2 < p < 1000, p \text{ primer } \} = 21$,
i

L'arrel primitiva mínima (cont.)

g	$n(g;1000)$	$\frac{n(g;1000)}{\pi_2(1000)}$
2	67	$0.401198\ldots$
3	40	$0.239521\ldots$
5	26	$0.155689\ldots$
6	11	$0.0658683\ldots$
7	10	$0.0598802\ldots$
10	2	$0.011976\ldots$
11	4	$0.0239521\ldots$
12	0	0
13	2	$0.011976\ldots$
14	0	0
15	1	$0.00598802\ldots$
17	2	$0.011976\ldots$
18	0	0
19	1	$0.00598802\ldots$
20	0	0
21	1	$0.00598802\ldots$

L'arrel primitiva mínima (cont.)

g	$n(g;1000)$	$\frac{n(g;1000)}{\pi_2(1000)}$	$n(g;10^6)$	$\frac{n(g;10^6)}{\pi_2(10^6)}$
2	67	0.401198...	29341	0.373785...
3	40	0.239521...	17814	0.226939...
5	26	0.155689...	10882	0.13863...
6	11	0.0658683...	4412	0.056206...
7	10	0.0598802...	5455	0.0694931...
10	2	0.011976...	1847	0.0235296...
11	4	0.0239521...	4412	0.056206...
12	0	0	259	0.00329949...
13	2	0.011976...	1844	0.0234913...
14	0	0	630	0.00802578...
15	1	0.00598802...	342	0.00435685...
17	2	0.011976...	921	0.0117329...
18	0	0	36	0.000458616...
19	1	0.00598802...	579	0.00737608...
20	0	0	17	0.000216569...
21	1	0.00598802...	108	0.00137585...

L'arrel primitiva mínima (cont.)

Se satisfà que

$$\pi_2(10^6) = 78497,$$

$$\max\{g(p) : 2 < p < 10^6, p \text{ primer } \} = 73.$$

(!)

L'arrel primitiva mínima (cont.)

Molts més càlculs (!) permeten assegurar que

$$\pi_2(10^{13}) = 346\,065\,536\,838,$$

i que

$$\max\{g(p) : 2 < p < 10^{13},\ p \text{ primer } \} = 281.$$

$$(!!!)$$

De fet,

L'arrel primitiva mínima (cont.)

g	$n(g; 10^{13})$	$\frac{n(g; 10^{13})}{\pi_2(10^{13})} \times 100$
1	0	0
2	129 413 368 373	37.39562441133250189728041399 . . .
3	78 420 620 939	22.66062713309421965227720 32 . . .
4	0	0
5	48 125 772 062	13.90654859820052198063421 89 . . .
6	19 338 378 468	5.58806827304871753304314795 . . .
7	23 775 539 277	6.87024183171691891625181061 . . .
8	0	0
9	0	0
10	7 985 205 429	2.30742578471141718200980407 . . .
11	12 886 761 577	3.72379223159471768354195947 . . .
12	1 129 345 726	0.32633868611096882250363158 6 . . .
13	8 039 038 115	2.32298141804372444553207088 . . .
14	2 862 155 584	0.82705594152815933973674417 9 . . .
15	1 453 161 633	0.41990937505003660262797543 35 . . .
16	0	0
17	4 003 233 814	1.15678488259118142405428655 . . .
18	140 043 704	0.04046739391607121461043818 64 . . .
19	2 625 244 588	0.75859752230368087364098408 2 . . .
20	58 362 336	0.01686453280880162971855202 10 . . .
21	553 536 226	0.15995127138566272770604534 91 . . .
22	851 040 129	0.24591877503202187265236857 0 . . .
23	1 340 344 888	0.38730955420950843707369904 0 . . .
24	7 911 428	0.00228610686642960726933521952 . . .
25	0	0

L'arrel primitiva mínima (cont.)

g	$n(g;10^{13})$	$\frac{n(g;10^{13})}{\pi_2(10^{13})} \times 100$
26	448 886 281	0.12971135037064739202865172 . . .
27	0	0
28	52 185 195	0.01507957003659364771109285849 . . .
29	762 557 314	0.22035055006270904435699087 02 . . .
30	36 301 436	0.01048975761403060696411662 14 . . .
31	512 108 823	0.14798030097973265901573056 9 . . .
32	0	0
33	120 201 891	0.03473385188779108046757673 83 . . .
34	160 682 167	0.04643113800586807451142015355 . . .
35	52 322 273	0.01511918045294786817612975 62 . . .
36	0	0
37	261 878 201	0.07567300789115856768588802 87 . . .
38	91 338 156	0.02639331175087716551111560355 . . .
39	53 292 942	0.01539966749851415032626982 55 . . .
40	1 097 413	0.00031711132233133306526031673 76 . . .
41	142 809 427	0.04126658444664828523609105 35 . . .
42	3 665 353	0.00105914996144670220009328 9718 . . .
43	99 069 942	0.02862750879651346624854812 26 . . .
44	6 632 897	0.00191665921449583346621517 2479 . . .
45	267 529	0.00007730587750644338836907596758 . . .
46	34 286 432	0.00990749680343065909552203 3370 . . .
47	59 340 198	0.01714709836240593334409303 29 . . .
48	9 533	0.00000275468054031123661854378852 . . .
49	0	0
50	29 375	0.00000848827660459903237907519 0158 . . .

L'arrel primitiva mínima (cont.)

g	$n(g; 10^{13})$	$\frac{n(g; 10^{13})}{\pi_2(10^{13})} \times 100$
51	14 761 447	0.00426550622025969609242561118 . . .
52	3 527 065	0.00101918990033702420895669 2275 . . .
53	37 600 494	0.01086513680141502261702884811 . . .
54	3 022	0.00000087324500082036683743 2007648 . . .
55	5 912 016	0.00170835156081072861309312645 . . .
56	108 973	0.00003148912226154792699387 10025 . . .
57	8 569 540	0.00247627662618470100200102145 . . .
58	11 979 140	0.00346152353379460264624594973 . . .
59	20 066 806	0.00579855659230051031620835 0649 . . .
60	11 065	0.00000319737125548555891998185461 . . .
61	14 442 844	0.00417344186652165130900193 4833 . . .
62	5 401 437	0.00156081332147457306064799176 . . .
63	115 745	0.00003344597704167880860309 98429 . . .
64	0	0
65	1 994 714	0.00057639775928735844333598 60038 . . .
66	407 962	0.00011788576340988669939551 41199 . . .
67	8 477 342	0.00244963485166926877775298828 . . .
68	668 301	0.00019311399976613235533509 2039 . . .
69	2 138 301	0.00061788903325585414587945 0492 . . .
70	174 389	0.00005039190021444836281036 743273 . . .
71	5 453 311	0.00157580296779242736552057 5466 . . .
72	48	0.00000001387020517517458907899945966 . . .
73	3 992 363	0.00115364362382865724956669 8329 . . .
74	1 556 796	0.00044985583199773124124645 9225 . . .
75	4 753	0.00000137343927495010045609342566 . . .

L'arrel primitiva mínima (cont.)

g	$n(g;10^{13})$	$\frac{n(g;10^{13})}{\pi_2(10^{13})} \times 100$
76	278 282	0.000080413092428290312460044325 7 . . .
77	396 533	0.000114583209765156361067976932 . . .
78	123 482	0.000035681680738352262680271068 3 . . .
79	2 364 107	0.000683138523876384838828878658 . . .
80	5	0.000000001444813039080686362395777048 . . .
81	0	0
82	898 726	0.000259698208672165786346101424 7 . . .
83	1 523 520	0.000440240312260041457367442849 7 . . .
84	704	0.000000203429675902560639825325408 4 . . .
85	267 746	0.000077368582392339490157203944 3 . . .
86	542 235	0.000156685639649183193942734833 5 . . .
87	361 968	0.000104595217225991576244734925 . . .
88	2 451	0.000000708247351757352454846409909 . . .
89	844 326	0.000243978642806967918723235370 4 . . .
90	32	0.000000009246803450116392719332973108 . . .
91	98 518	0.000028468018196830211810101432 65 . . .
92	68 901	0.000019909812641139674211086286 9 . . .
93	221 835	0.000064102020104892811840413440 30 . . .
94	269 232	0.000077797980827554270144107969 3 . . .
95	117 214	0.000033870463112560714256371722 2 . . .
96	1	0.000000000288962607816137272479155409 6 . . .
97	438 735	0.000126778009740212986241142249 . . .
98	7	0.000000002022738254712960907354087 87 . . .
99	4 112	0.000011882142433399564644342870 4 . . .
100	0	0

L'arrel primitiva mínima (cont.)

g	$n(g; 10^{13})$	$\frac{n(g; 10^{13})}{\pi_2(10^{13})} \times 100$
101	325 776	0.000094137082523909936079169332 7 . . .
102	14 542	0.000004202094242862268216391877 97 . . .
103	240 996	0.000069638832633257818118386537 1 . . .
104	634	0.000000183202293355431030751784529 7 . . .
105	742	0.000000214410254999573856179533314 0 . . .
106	91 995	0.000026583115106045548381719901 9 . . .
107	157 259	0.000045441970742557931332799500 6 . . .
108	0	0
109	118 143	0.000034138909375221905782504857 6 . . .
110	2 378	0.000000687153081386774433955431564 . . .
111	34 786	0.000010051853275492151160459900 08 . . .
112	0	0
113	80 254	0.000023190405127676280665542138 25 . . .
114	3 756	0.000001085343554957411595431707 72 . . .
115	14 937	0.000004316234472949642439021144 35 . . .
116	7 151	0.000002066371608493197635498440334 . . .
117	756	0.000000218455731508999777994241490 . . .
118	27 804	0.000008034316347719880724010437 01 . . .
119	8 767	0.000002533335182724075467824755 48 . . .
120	0	0
121	0	0
122	22 822	0.000006594704635579884832519284 76 . . .
123	15 832	0.000004574856006945085297889988 45 . . .
124	4 007	0.000001157873169519262050823975 726 . . .
125	0	0

L'arrel primitiva mínima (cont.)

g	$n(g;10^{13})$	$\frac{n(g;10^{13})}{\pi_2(10^{13})} \times 100$
126	3	0.00000000086688782344841181743746622 9 . . .
127	3 5510	0.00001026106220355103454573480 86 . . .
128	0	0
129	9 695	0.00000280149248277745085668541169 6 . . .
130	795	0.00000022972527321382913162092855 07 . . .
131	24 192	0.00000699058340828799289581572767 0 . . .
132	30	0.00000000866887823448411817437466229 . . .
133	3 397	0.00000098160597875141831461169092 7 . . .
134	8 673	0.00000250617269758935856421171487 . . .
135	1	0.00000000028896260781613727247915540 96 . . .
136	53	0.00000001531501821425527544139523 67 . . .
137	15 015	0.00000433877355635930114627451847 6 . . .
138	739	0.00000021354336717612544436209584 8 . . .
139	11 418	0.00000329937505604465537716699647 . . .
140	1	0.00000000028896260781613727247915540 96 . . .
141	3 162	0.00000091369976591462605557908940 5 . . .
142	3 801	0.00000109834687230913777269326971 . . .
143	1 175	0.00000033953106418396129516300760 6 . . .
144	0	0
145	2 017	0.00000058283757996514887859045646 12 . . .
146	3 063	0.00000088509246774082846560365302 0 . . .
147	0	0
148	616	0.00000017800096641474055984715973 2 . . .
149	5 363	0.00001549706465717944192305710 46 . . .
150	0	0

L'arrel primitiva mínima (cont.)

g	$n(g;10^{13})$	$\frac{n(g;10^{13})}{\pi_2(10^{13})} \times 100$
151	4 048	0.00000116972063643972367899562109 . . .
152	8	0.00000000231170086252909817983324327 7 . . .
153	48	0.00000001387020517517458907899945966 . . .
154	89	0.00000002571767209563621725064483 15 . . .
155	931	0.00000026902418787682380067809368 64 . . .
156	3	0.00000000086688782344841181743746622 9 . . .
157	2 890	0.00000083510193658863671746475913 38 . . .
158	1 034	0.00000029878733648188593974344669 4 . . .
159	697	0.00000020140693764784767891797132 1 . . .
160	0	0
161	382	0.00000011038371618576443808703736 6 . . .
162	0	0
163	1 698	0.00000049065850807180108866960588 56 . . .
164	160	0.00000004623401725058196359666486554 . . .
165	8	0.00000000231170086252909817983324327 7 . . .
166	559	0.00000016153009776922073531584787 4 . . .
167	1 039	0.00000030023214952096662610584247 1 . . .
168	0	0
169	0	0
170	36	0.00000001040265388138094180924959475 . . .
171	11	0.00000000317858868597750999727070950 6 . . .
172	82	0.00000002369493384092325634329074 36 . . .
173	747	0.00000021585506803865454254192909 1 . . .
174	35	0.00000001011369127356480453677043 93 . . .
175	0	0

L'arrel primitiva mínima (cont.)

g	$n(g;10^{13})$	$\frac{n(g;10^{13})}{\pi_2(10^{13})} \times 100$
176	0	0
177	241	0.00000006963998848368908266747645 37 $*$ . . .
178	251	0.00000007252961456185045539226800 78 . . .
179	506	0.00000014621507955496545987445263 7 . . .
180	0	0
181	411	0.00000011876363181243241898893287 3 . . .
182	10	0.00000000288962607816137272479155409 6 . . .
183	99	0.00000002860729817379758997543638555 . . .
184	1	0.00000000028896260781613727247915540 96 . . .
185	91	0.00000002629559731126849179560314 23 . . .
186	9	0.00000000260066347034523545231239869 . . .
187	42	0.00000001213642952827776544412452 72 . . .
188	20	0.00000000577925215632274544958310819 3 . . .
189	0	0
190	11	0.00000000317858868597750999727070950 6 . . .
191	232	0.00000006703932501334384721516405 50 . . .
192	0	0
193	184	0.00000005316911983816925813616459537 . . .
194	67	0.00000001936049472368119725610341 24 . . .
195	1	0.00000000028896260781613727247915540 96 . . .
196	0	0
197	101	0.00000002918522338942986452039469 64 . . .
198	0	0
199	78	0.00000002253908340965870725337412195 . . .
200	0	0

L'arrel primitiva mínima (cont.)

g	$n(g;10^{13})$	$\frac{n(g;10^{13})}{\pi_2(10^{13})} \times 100$
201	25	0.00000000722406519540343181197888524 1 . . .
202	21	0.00000000606821476413888272206226360 2 . . .
203	16	0.00000000462340172505819635966648655 4 . . .
204	0	0
205	18	0.00000000520132694069047090462479737 . . .
206	26	0.00000000751302780321956908445804065 1 . . .
207	1	0.00000000028896260781613727247915540 96 . . .
208	0	0
209	12	0.00000000346755129379364726974986491 6 . . .
210	0	0
211	42	0.00000001213642952827776544412452 72 . . .
212	4	0.00000000115585043126454908991662163 9 . . .
213	8	0.00000000231170086252909817983324327 7 . . .
214	17	0.00000000491236433287433363214564196 . . .
215	9	0.00000000260066347034523545231239869 . . .
216	0	0
217	8	0.00000000231170086252909817983324327 7 . . .
218	9	0.00000000260066347034523545231239869 . . .
219	5	0.00000000144481303908068636239577704 8 . . .
220	0	0
221	4	0.00000000115585043126454908991662163 9 . . .
222	2	0.00000000057792521563227454495831081 93 . . .
223	14	0.00000000404547650942592181470817574 . . .
224	0	0
225	0	0

L'arrel primitiva mínima (cont.)

g	$n(g;10^{13})$	$\frac{n(g;10^{13})}{\pi_2(10^{13})} \times 100$
226	9	0.000000002600663470345235452312398 69 . . .
227	13	0.000000003756513901609784542229020325 . . .
228	0	0
229	8	0.000000002311700862529098179833243277 . . .
230	3	0.000000000866887823448411817437466229 . . .
231	0	0
232	0	0
233	10	0.000000002889626078161372724791554096 . . .
234	0	0
235	0	0
236	0	0
237	1	0.0000000002889626078161372724791554096 . . .
238	1	0.0000000002889626078161372724791554096 . . .
239	4	0.000000001155850431264549089916621639 . . .
240	0	0
241	3	0.000000000866887823448411817437466229 . . .
242	0	0
243	0	0
244	0	0
245	0	0
246	0	0
247	2	0.000000000577925215632274544958310819 3 . . .
248	0	0
249	0	0
250	0	0

L'arrel primitiva mínima (cont.)

g	$n(g;10^{13})$	$\frac{n(g;10^{13})}{\pi_2(10^{13})} \times 100$
251	2	0.00000000057792521563227454495831081 93 . . .
252	0	0
253	0	0
254	0	0
255	0	0
256	0	0
257	0	0
258	0	0
259	0	0
260	0	0
261	0	0
262	1	0.00000000028896260781613727247915540 96 . . .
263	2	0.00000000057792521563227454495831081 93 . . .
264	0	0
265	0	0
266	0	0
267	0	0
268	0	0
269	0	0
270	0	0
271	0	0
272	0	0
273	0	0
274	0	0
275	0	0

L'arrel primitiva mínima (cont.)

g	$n(g;10^{13})$	$\frac{n(g;10^{13})}{\pi_2(10^{13})} \times 100$
276	0	0
277	0	0
278	1	0.00000000028896260781613727247915540 96 . . .
279	0	0
280	0	0
281	1	0.00000000028896260781613727247915540 96 . . .
282	0	0
283	0	0
284	0	0
285	0	0
286	0	0
287	0	0
288	0	0
289	0	0
290	0	0
291	0	0
292	0	0
293	0	0
294	0	0
295	0	0
296	0	0
297	0	0
298	0	0
299	0	0
300	0	0

L'arrel primitiva mínima (cont.)

Observació

Unes quantes observacions dels percentatges en alguns intervals $f < p < F$, per a f, F, de la forma $5 \cdot k \cdot 10^9$, per a $0 \leq k \leq 2000$, semblen palesar que aquests es conserven pràcticament constants en créixer F (òbviament, per als valors petits de g, que són els que apareixen primer).

L'arrel primitiva mínima (cont.)

Observació

Unes quantes observacions dels percentatges en alguns intervals $f < p < F$, per a f, F, de la forma $5 \cdot k \cdot 10^9$, per a $0 \leq k \leq 2000$, semblen palesar que aquests es conserven pràcticament constants en créixer F (òbviament, per als valors petits de g, que són els que apareixen primer).

Això fa pensar en el següent refinament de la conjectura d'Artin per a les arrels primitives mínimes.

L'arrel primitiva mínima (cont.)

Observació

Unes quantes observacions dels percentatges en alguns intervals $f < p < F$, per a f, F, de la forma $5 \cdot k \cdot 10^9$, per a $0 \leq k \leq 2000$, semblen palesar que aquests es conserven pràcticament constants en créixer F (òbviament, per als valors petits de g, que són els que apareixen primer).
Això fa pensar en el següent refinament de la conjectura d'Artin per a les arrels primitives mínimes.

Conjectura (refinament de la conjectura d'Artin)

Sigui $g > 1$ un nombre enter que no és una potència exacta.
Llavors, el conjunt dels nombres primers $p > 2$ per als quals $g(p) = g$ és infinit.

L'arrel primitiva mínima (cont.)

Observacions

• Per als 346 065 536 838 nombres primers p, $2 < p < 10^{13}$, només apareixen 199 valors de g com a mínima arrel primitiva mòdul p, el màxim dels quals és 281.

L'arrel primitiva mínima (cont.)

Observacions

• Per als 346 065 536 838 nombres primers p, $2 < p < 10^{13}$, només apareixen 199 valors de g com a mínima arrel primitiva mòdul p, el màxim dels quals és 281.

• La suma dels percentatges d'aparició dels valors $g = 2$ (37.3956%) i $g = 3$ (22.6606%) és 60.0662%.

L'arrel primitiva mínima (cont.)

Observacions

• Per als 346 065 536 838 nombres primers p, $2 < p < 10^{13}$, només apareixen 199 valors de g com a mínima arrel primitiva mòdul p, el màxim dels quals és 281.

• La suma dels percentatges d'aparició dels valors $g = 2$ (37.3956%) i $g = 3$ (22.6606%) és 60.0662%.

• Els següents percentatges d'aparició corresponen als valors $g = 5$ (13.9065%), $g = 7$ (6.8702%), i $g = 6$ (5.5881%).

L'arrel primitiva mínima (cont.)

Observacions

• Per als 346 065 536 838 nombres primers p, $2 < p < 10^{13}$, només apareixen 199 valors de g com a mínima arrel primitiva mòdul p, el màxim dels quals és 281.

• La suma dels percentatges d'aparició dels valors $g = 2$ (37.3956%) i $g = 3$ (22.6606%) és 60.0662%.

• Els següents percentatges d'aparició corresponen als valors $g = 5$ (13.9065%), $g = 7$ (6.8702%), i $g = 6$ (5.5881%).

• Els percentatges d'aparició superiors a 1% que resten corresponen als valors $g = 11$, 13, 10 i 17.

L'arrel primitiva mínima (cont.)

Observacions

• Per als 346 065 536 838 nombres primers p, $2 < p < 10^{13}$, només apareixen 199 valors de g com a mínima arrel primitiva mòdul p, el màxim dels quals és 281.

• La suma dels percentatges d'aparició dels valors $g = 2$ (37.3956%) i $g = 3$ (22.6606%) és 60.0662%.

• Els següents percentatges d'aparició corresponen als valors $g = 5$ (13.9065%), $g = 7$ (6.8702%), i $g = 6$ (5.5881%).

• Els percentatges d'aparició superiors a 1% que resten corresponen als valors $g = 11$, 13, 10 i 17.

• I els percentatges d'aparició superiors a 0.25% que resten corresponen als valors $g = 14$, 19, 15, 23 i 12.

L'arrel primitiva mínima (cont.)

Observacions

• Per als 346 065 536 838 nombres primers p, $2 < p < 10^{13}$, només apareixen 199 valors de g com a mínima arrel primitiva mòdul p, el màxim dels quals és 281.

• La suma dels percentatges d'aparició dels valors $g = 2$ (37.3956%) i $g = 3$ (22.6606%) és 60.0662%.

• Els següents percentatges d'aparició corresponen als valors $g = 5$ (13.9065%), $g = 7$ (6.8702%), i $g = 6$ (5.5881%).

• Els percentatges d'aparició superiors a 1% que resten corresponen als valors $g = 11$, 13, 10 i 17.

• I els percentatges d'aparició superiors a 0.25% que resten corresponen als valors $g = 14$, 19, 15, 23 i 12.

• Entre aquests 14 valors de g, la suma dels percentatges d'aparició és de 98.6513%, i corresponen a 341 398 170 473 dels 346 065 536 838 nombres primers p, $2 < p < 10^{13}$.

L'arrel primitiva mínima (cont.)

Sembla, doncs, que les arrels primitives mínimes tendeixen a ser nombres g "petits".

L'arrel primitiva mínima (cont.)

Sembla, doncs, que les arrels primitives mínimes tendeixen a ser nombres g "petits".

Però...

L'arrel primitiva mínima (cont.)

Teorema (usa el teorema dels nombres primers)

Per a tot nombre enter $N > 0$, *existeix una infinitat de nombres primers* $p > 2$ *tals que* $g(p) > N$.

L'arrel primitiva mínima (cont.)

Teorema (usa el teorema dels nombres primers)

Per a tot nombre enter $N > 0$, existeix una infinitat de nombres primers $p > 2$ tals que $g(p) > N$.

És a dir, *l'arrel primitiva mínima mòdul un primer p pot ser tan gran com vulguem!*

L'arrel primitiva mínima (cont.)

Teorema (usa el teorema dels nombres primers)

Per a tot nombre enter $N > 0$, existeix una infinitat de nombres primers $p > 2$ tals que $g(p) > N$.

És a dir, *l'arrel primitiva mínima mòdul un primer p pot ser tan gran com vulguem!*

Demostració

Sigui $F := 4 \prod_{\ell \leq N,\ \text{primer}} \ell$.

L'arrel primitiva mínima (cont.)

Teorema (usa el teorema dels nombres primers)

Per a tot nombre enter $N > 0$, existeix una infinitat de nombres primers $p > 2$ tals que $g(p) > N$.

És a dir, *l'arrel primitiva mínima mòdul un primer p pot ser tan gran com vulguem!*

Demostració

Sigui $F := 4 \prod_{\ell \leq N,\ \text{primer}} \ell$.

Com a conseqüència del teorema dels nombres primers, tenim que el conjunt dels nombres primers p tals que $p \equiv 1 \pmod{F}$ és infinit.

L'arrel primitiva mínima (cont.)

Teorema (usa el teorema dels nombres primers)

Per a tot nombre enter $N > 0$, existeix una infinitat de nombres primers $p > 2$ tals que $g(p) > N$.

És a dir, *l'arrel primitiva mínima mòdul un primer p pot ser tan gran com vulguem!*

Demostració

Sigui $F := 4 \prod_{\ell \leq N,\ \text{primer}} \ell$.

Com a conseqüència del teorema dels nombres primers, tenim que el conjunt dels nombres primers p tals que $p \equiv 1 \pmod{F}$ és infinit.
La llei de reciprocitat quadràtica implica que per a cadascun d'aquests primers, p, tots els nombres primers $\ell \leq N$ són quadrats mòdul p;

L'arrel primitiva mínima (cont.)

Teorema (usa el teorema dels nombres primers)

Per a tot nombre enter $N > 0$, existeix una infinitat de nombres primers $p > 2$ tals que $g(p) > N$.

És a dir, *l'arrel primitiva mínima mòdul un primer p pot ser tan gran com vulguem!*

Demostració

Sigui $F := 4 \prod_{\ell \leq N,\ \text{primer}} \ell$.

Com a conseqüència del teorema dels nombres primers, tenim que el conjunt dels nombres primers p tals que $p \equiv 1 \pmod{F}$ és infinit.
La llei de reciprocitat quadràtica implica que per a cadascun d'aquests primers, p, tots els nombres primers $\ell \leq N$ són quadrats mòdul p; i, pel teorema fonamental de l'Aritmètica, tots els nombres g, $1 \leq g \leq N$, són quadrats mòdul p.

L'arrel primitiva mínima (cont.)

Teorema (usa el teorema dels nombres primers)

Per a tot nombre enter $N > 0$, existeix una infinitat de nombres primers $p > 2$ tals que $g(p) > N$.

És a dir, *l'arrel primitiva mínima mòdul un primer p pot ser tan gran com vulguem!*

Demostració

Sigui $F := 4 \prod_{\ell \leq N,\ \text{primer}} \ell$.

Com a conseqüència del teorema dels nombres primers, tenim que el conjunt dels nombres primers p tals que $p \equiv 1 \pmod{F}$ és infinit.
La llei de reciprocitat quadràtica implica que per a cadascun d'aquests primers, p, tots els nombres primers $\ell \leq N$ són quadrats mòdul p; i, pel teorema fonamental de l'Aritmètica, tots els nombres g, $1 \leq g \leq N$, són quadrats mòdul p.
Per tant, cap d'ells no pot ser arrel primitiva mòdul p. $\square$

L'arrel primitiva mínima (cont.)

- Notem que tots els valors de g, $2 \leq g \leq 99$ i no potències exactes, apareixen com a arrel primitiva mínima mòdul algun nombre primer $p > 2$.

L'arrel primitiva mínima (cont.)

- Notem que tots els valors de g, $2 \leq g \leq 99$ i no potències exactes, apareixen com a arrel primitiva mínima mòdul algun nombre primer $p > 2$.
- Els únics nombres g, $100 < g \leq 150$ i no potències exactes, que no apareixen com a arrel primitiva mínima mòdul un nombre primer $p < 10^{13}$, que són aquells que hem destacat en color vermell a les taules, són

$$108, \quad 112, \quad 120, \quad 147, \quad 150.$$

L'arrel primitiva mínima (cont.)

- Notem que tots els valors de g, $2 \leq g \leq 99$ i no potències exactes, apareixen com a arrel primitiva mínima mòdul algun nombre primer $p > 2$.
- Els únics nombres g, $100 < g \leq 150$ i no potències exactes, que no apareixen com a arrel primitiva mínima mòdul un nombre primer $p < 10^{13}$, que són aquells que hem destacat en color vermell a les taules, són

$$108, \quad 112, \quad 120, \quad 147, \quad 150.$$

- Però també es té que

$g(p)$	p
108	?
112	26 310 950 124 889
120	19 293 869 183 821
147	62 996 766 050 791
150	?

L'arrel primitiva mínima (cont.)

• Notem que tots els valors de g, $2 \leq g \leq 99$ i no potències exactes, apareixen com a arrel primitiva mínima mòdul algun nombre primer $p > 2$.

• Els únics nombres g, $100 < g \leq 150$ i no potències exactes, que no apareixen com a arrel primitiva mínima mòdul un nombre primer $p < 10^{13}$, que són aquells que hem destacat en color vermell a les taules, són

$$108, \quad 112, \quad 120, \quad 147, \quad 150.$$

• Però també es té que

$g(p)$	p
108	?
112	26 310 950 124 889
120	19 293 869 183 821
147	62 996 766 050 791
150	?

• És a dir, els nombres 112, 120 i 147 també són l'arrel primitiva mínima per a algun nombre primer.

L'arrel primitiva mínima (cont.)

- De fet, per a nombres primers $2 < p < 10^{14}$ també s'obtenen els valors de $g(p)$ següents:

$g(p)$	p
112	26 310 950 124 889
120	19 293 869 183 821
147	62 996 766 050 791
175	45 723 648 644 281
231	75 271 918 656 481
235	10 108 817 382 049
236	34 696 311 221 881
244	10 500 982 302 721
246	79 567 164 932 641
249	42 101 611 282 201
253	90 946 855 087 201
254	41 704 619 234 041
257	15 727 353 827 329
259	33 666 594 395 281
265	51 077 463 803 521
267	48 458 307 250 081
269	24 553 499 345 761
271	85 528 088 276 401
274	38 629 825 347 961
277	20 474 220 836 161
290	58 382 742 082 681
293	44 384 069 747 161
335	89 637 484 042 681

L'arrel primitiva mínima (cont.)

- I per a nombres primers $2 < p < 10^{16}$ també s'obtenen els valors de $g(p)$ següents (Tomás Oliveira e Silva):

$g(p)$	p
150	556 763 790 982 351
176	130 398 420 659 641
189	3 607 658 470 877 761
198	326 649 028 004 881
204	124 734 874 915 561
208	7 908 701 933 527 921
210	6 698 953 447 001 401
220	181 806 920 622 601
228	395 249 436 822 241
232	735 027 744 223 081
234	212 921 046 628 921
248	1 419 170 227 555 921
255	1 751 892 611 174 281
258	146 349 865 061 401
261	112 219 414 471 921
266	1 929 701 346 990 481
268	385 702 944 009 769
273	3 240 104 160 528 841
275	9 249 777 751 699 801
276	6 786 179 526 366 241
279	1 171 298 806 619 041
282	863 761 115 217 001

$g(p)$	p
283	288 645 077 565 601
284	697 475 454 991 561
286	5 509 437 582 125 401
287	157 489 901 168 161
291	141 186 510 344 881
292	507 675 571 155 481
295	329 014 129 918 321
298	115 975 649 791 681
299	756 132 760 168 801
301	859 112 508 085 441
302	100 836 851 947 441
303	119 450 390 411 881
305	254 384 692 421 161
307	176 853 800 981 881
309	1 408 667 845 587 601
310	4 371 978 171 442 561
311	263 914 274 447 041
313	2 450 615 204 310 001
314	2 043 889 418 952 481
316	2 317 512 492 640 489
317	641 548 266 280 321
319	112 400 256 696 841

$g(p)$	p
322	1 876 980 294 702 241
323	6 294 741 074 705 329
326	1 962 603 968 297 281
327	847 558 117 476 841
329	2 022 738 564 473 929
331	1 786 292 979 064 441
332	4 584 253 145 204 041
334	2 917 055 672 130 601
337	610 821 130 190 041
339	4 777 020 807 295 801
346	6 616 263 947 370 841
347	358 973 066 123 281
349	2 168 525 352 747 601
355	3 874 584 305 820 001
358	8 104 729 994 426 521
359	2 069 304 073 407 481
362	6 606 116 274 810 361
379	9 017 970 810 061 249
383	6 984 775 112 986 441
401	4 986 561 061 454 281
417	6 525 032 504 501 281

L'arrel primitiva mínima (cont.)

• De manera que els únics nombres g, $2 < g \leq 300$ i no potències exactes, per als quals no s'ha trobat (no hi ha) cap nombre primer $2 < p < 10^{16}$ tal que $g(p) = g$ són els 24 nombres següents:
108, 160, 162, 168, 180, 192, 200, 224, 240, 242, 245, 250, 252, 260, 264, 270, 272, 280, 285, 288, 294, 296, 297, 300.

L'arrel primitiva mínima (cont.)

• De manera que els únics nombres g, $2 < g \leq 300$ i no potències exactes, per als quals no s'ha trobat (no hi ha) cap nombre primer $2 < p < 10^{16}$ tal que $g(p) = g$ són els 24 nombres següents:
108, 160, 162, 168, 180, 192, 200, 224, 240, 242, 245, 250, 252, 260, 264, 270, 272, 280, 285, 288, 294, 296, 297, 300.

Ara bé,
posem
$g_1 := 285 = 3 \cdot 5 \cdot 19$,
$g_2 := 245 = 5 \cdot 7^2$,
$g_3 := 297 = 3^3 \cdot 11$,
$g_4 := 168 = 2^3 \cdot 3 \cdot 7$,
$g_5 := 296 = 2^3 \cdot 37$,
$g_6 := 180 = 2^2 \cdot 3^2 \cdot 5$,
$g_7 := 160 = 2^5 \cdot 5$.

L'arrel primitiva mínima (cont.)

Podem demostrar fàcilment que *per als* 5 *valors següents de* p, *tots de* 122 *xifres decimals, és* $g(p) = g_1 = 285$.

L'arrel primitiva mínima (cont.)

Podem demostrar fàcilment que *per als* 5 *valors següents de* p, *tots de* 122 *xifres decimals, és* $g(p) = g_1 = 285$.

p = 26 769 219 478 121 761 133 156 045 565 040 362 953 828 624 952 981 478 733 829 774 198_
288 950 587 403 349 055 575 812 093 130 457 911 639 958 732 521 762 097 081,
p = 27 087 883 180 286 028 079 554 359 344 601 159 418 855 824 010 241 722 350 333 206 147_
437 488 756 116 198 183 068 266 491 298 723 278 189 186 394 212 322 323 921,
p = 39 520 173 053 662 451 896 181 660 993 272 601 229 548 299 672 754 268 236 591 523 573_
665 710 582 489 381 193 902 915 960 849 573 938 123 570 651 688 280 298 241,
p = 44 232 577 755 252 924 850 062 715 917 745 393 193 936 694 948 091 234 897 234 441 199_
553 539 999 077 090 180 646 170 171 549 866 847 139 568 653 370 343 744 921,
p = 57 064 298 628 577 185 576 461 175 852 317 925 504 571 097 539 519 846 514 778 166 414_
576 242 847 984 351 360 503 619 624 058 174 556 389 113 850 845 529 284 681.

L'arrel primitiva mínima (cont.)

Podem demostrar fàcilment que *per als* 5 *valors següents de* p, *tots de* 122 *xifres decimals, és* $g(p) = g_1 = 285$.

p = 26 769 219 478 121 761 133 156 045 565 040 362 953 828 624 952 981 478 733 829 774 198_
288 950 587 403 349 055 575 812 093 130 457 911 639 958 732 521 762 097 081,
p = 27 087 883 180 286 028 079 554 359 344 601 159 418 855 824 010 241 722 350 333 206 147_
437 488 756 116 198 183 068 266 491 298 723 278 189 186 394 212 322 323 921,
p = 39 520 173 053 662 451 896 181 660 993 272 601 229 548 299 672 754 268 236 591 523 573_
665 710 582 489 381 193 902 915 960 849 573 938 123 570 651 688 280 298 241,
p = 44 232 577 755 252 924 850 062 715 917 745 393 193 936 694 948 091 234 897 234 441 199_
553 539 999 077 090 180 646 170 171 549 866 847 139 568 653 370 343 744 921,
p = 57 064 298 628 577 185 576 461 175 852 317 925 504 571 097 539 519 846 514 778 166 414_
576 242 847 984 351 360 503 619 624 058 174 556 389 113 850 845 529 284 681.

Aquests nombres són els $p = t \cdot n + 1$, per a $n = 8 \prod_{2<\ell<285,\ \ell\neq 19} \ell$, i

$t \in \{18229, 18446, 26912, 30121, 38859\}$.

L'arrel primitiva mínima (cont.)

Podem demostrar fàcilment que *per als* 5 *valors següents de* p, *tots de* 122 *xifres decimals, és* $g(p) = g_1 = 285$.

p = 26 769 219 478 121 761 133 156 045 565 040 362 953 828 624 952 981 478 733 829 774 198_
288 950 587 403 349 055 575 812 093 130 457 911 639 958 732 521 762 097 081,
p = 27 087 883 180 286 028 079 554 359 344 601 159 418 855 824 010 241 722 350 333 206 147_
437 488 756 116 198 183 068 266 491 298 723 278 189 186 394 212 322 323 921,
p = 39 520 173 053 662 451 896 181 660 993 272 601 229 548 299 672 754 268 236 591 523 573_
665 710 582 489 381 193 902 915 960 849 573 938 123 570 651 688 280 298 241,
p = 44 232 577 755 252 924 850 062 715 917 745 393 193 936 694 948 091 234 897 234 441 199_
553 539 999 077 090 180 646 170 171 549 866 847 139 568 653 370 343 744 921,
p = 57 064 298 628 577 185 576 461 175 852 317 925 504 571 097 539 519 846 514 778 166 414_
576 242 847 984 351 360 503 619 624 058 174 556 389 113 850 845 529 284 681.

Aquests nombres són els $p = t \cdot n + 1$, per a $n = 8 \prod_{2<\ell<285,\ \ell\neq 19} \ell$, i

$t \in \{18229, 18446, 26912, 30121, 38859\}$.

Demostració

Com que podem calcular fàcilment (per divisió) la factorització dels nombres t, i també la factorització de n, obtenim immediatament la llista de nombres primers que divideixen $p - 1$; per tant, podem certificar (com hem ensenyat en el curs) que els nombres p són primers, calculant-ne una arrel primitiva a l'atzar...; o cercant-ne la menor! □

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8$ $\prod_{2<\ell<295,\, \ell\neq 11} \ell$, i $t \in \{32058, 37153\}$

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8 \prod_{2<\ell<295,\, \ell\neq 11} \ell$, i $t \in \{32058, 37153\}$, els nombres $p := tn + 1 =$

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8 \prod_{2<\ell<295,\, \ell\neq 11} \ell$, i $t \in \{32058, 37153\}$, els nombres $p := tn + 1 =$

23 825 269 629 865 179 051 711 761 997 949 640 885 300 427 755 078 077_
016 650 904 179 912 006 042 029 665 677 166 034 745 745 464 595 596 659_
609 122 655 751 817 521,

27 611 836 126 969 274 356 112 268 186 094 672 400 385 763 066 455 043_
839 279 775 500 538 734 808 145 491 574 762 919 985 921 805 668 482 210_
195 824 256 945 139 321,

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8 \prod_{2<\ell<295,\, \ell\neq 11} \ell$, i $t \in \{32058, 37153\}$, els nombres $p := tn + 1 =$

23 825 269 629 865 179 051 711 761 997 949 640 885 300 427 755 078 077_
016 650 904 179 912 006 042 029 665 677 166 034 745 745 464 595 596 659_
609 122 655 751 817 521,

27 611 836 126 969 274 356 112 268 186 094 672 400 385 763 066 455 043_
839 279 775 500 538 734 808 145 491 574 762 919 985 921 805 668 482 210_
195 824 256 945 139 321, són primers (de 125 xifres decimals),

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8 \prod_{2<\ell<295,\, \ell\neq 11} \ell$, i $t \in \{32058, 37153\}$, els nombres $p := tn + 1 =$

23 825 269 629 865 179 051 711 761 997 949 640 885 300 427 755 078 077_
016 650 904 179 912 006 042 029 665 677 166 034 745 745 464 595 596 659_
609 122 655 751 817 521,

27 611 836 126 969 274 356 112 268 186 094 672 400 385 763 066 455 043_
839 279 775 500 538 734 808 145 491 574 762 919 985 921 805 668 482 210_
195 824 256 945 139 321, són primers (de 125 xifres decimals), i $g(p) = g_3 = 297$, en els dos casos.

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8$ $\prod_{2<\ell<295,\ \ell\neq 11} \ell$, i $t \in \{32058, 37153\}$, els nombres $p := tn + 1 =$

23 825 269 629 865 179 051 711 761 997 949 640 885 300 427 755 078 077_
016 650 904 179 912 006 042 029 665 677 166 034 745 745 464 595 596 659_
609 122 655 751 817 521,

27 611 836 126 969 274 356 112 268 186 094 672 400 385 763 066 455 043_
839 279 775 500 538 734 808 145 491 574 762 919 985 921 805 668 482 210_
195 824 256 945 139 321, són primers (de 125 xifres decimals), i $g(p) = g_3 = 297$, en els dos casos.

I per a $n = 8$ $\prod_{2<\ell<245,\ \ell\neq 5,7} \ell$, i $t = 6280$

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8 \prod_{2<\ell<295,\, \ell\neq 11} \ell$, i $t \in \{32058, 37153\}$, els nombres $p := tn + 1 =$

23 825 269 629 865 179 051 711 761 997 949 640 885 300 427 755 078 077_
016 650 904 179 912 006 042 029 665 677 166 034 745 745 464 595 596 659_
609 122 655 751 817 521,
27 611 836 126 969 274 356 112 268 186 094 672 400 385 763 066 455 043_
839 279 775 500 538 734 808 145 491 574 762 919 985 921 805 668 482 210_
195 824 256 945 139 321, són primers (de 125 xifres decimals), i $g(p) = g_3 = 297$, en els dos casos.

I per a $n = 8 \prod_{2<\ell<245,\, \ell\neq 5,7} \ell$, i $t = 6280$, el nombre $p := tn + 1 =$

183 764 397 570 616 409 697 546 449 280 596 543 923 655 126 600_
025 419 217 965 661 703 376 384 432 687 907 022 360 050 389 305 479 361
és un primer (de 102 xifres decimals)

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8 \prod_{2<\ell<295,\, \ell\neq 11} \ell$, i $t \in \{32058, 37153\}$, els nombres $p := tn + 1 =$

23 825 269 629 865 179 051 711 761 997 949 640 885 300 427 755 078 077_
016 650 904 179 912 006 042 029 665 677 166 034 745 745 464 595 596 659_
609 122 655 751 817 521,
27 611 836 126 969 274 356 112 268 186 094 672 400 385 763 066 455 043_
839 279 775 500 538 734 808 145 491 574 762 919 985 921 805 668 482 210_
195 824 256 945 139 321, són primers (de 125 xifres decimals), i $g(p) = g_3 = 297$, en els dos casos.

I per a $n = 8 \prod_{2<\ell<245,\, \ell\neq 5,7} \ell$, i $t = 6280$, el nombre $p := tn + 1 =$

183 764 397 570 616 409 697 546 449 280 596 543 923 655 126 600_
025 419 217 965 661 703 376 384 432 687 907 022 360 050 389 305 479 361
és un primer (de 102 xifres decimals) i $g(p) = g_4 = 168$.

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 16 \prod_{2<\ell<245,\, \ell\neq 5} \ell$, i $t_6 = 626724$, el nombre

$p := nt_6 + 1 =$

256 747 422 968 576 111 865 922 199 411 633 158 840 147 085 650 611 565_
553 414 706 865 512 110 859 981 933 402 793 331 701 054 016 154 433

és primer, de 105 xifres decimals, i $g(p) = g_6 = 180$.

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 16 \prod_{2<\ell<245,\, \ell\neq 5} \ell$, i $t_6 = 626724$, el nombre

$p := nt_6 + 1 =$

256 747 422 968 576 111 865 922 199 411 633 158 840 147 085 650 611 565_
553 414 706 865 512 110 859 981 933 402 793 331 701 054 016 154 433

és primer, de 105 xifres decimals, i $g(p) = g_6 = 180$.

I per a $t_7 = 618692$ o $t_7 = 980592$, el nombres $p := nt_7 + 1 =$

253 456 986 825 579 189 248 458 870 887 954 095 118 630 020 097 121 174_
097 965 375 221 050 125 561 146 441 401 384 041 423 000 413 838 657,

401 715 059 553 490 829 594 571 743 487 487 606 176 526 686 407 899 643_
685 504 359 550 083 053 804 244 618 108 309 110 101 735 309 017 857,

són primers, de 105 xifres decimals, i $g(p) = g_7 = 160$, per a tots dos.

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8$ $\displaystyle\prod_{2<\ell<295,\, \ell\neq 37} \ell$,

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8$ $\displaystyle\prod_{2<\ell<295,\ \ell\neq 37} \ell$,

i $t \in \{375, 2439, 5235, 5370, 8422, 10131, 12666,$
$13321, 14115, 15582, 15685, 17921, 19263, 19802, 20639, 21880,$
$24192, 24861, 26920, 28693, 29005, 29046, 32049, 33516, 34148,$
$34710, 36901, 38529, 38715, 40852, 42605, 44068, 46125, 49046\}$,

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8$ $\displaystyle\prod_{2<\ell<295,\ \ell\neq 37} \ell$,

i $t \in \{375, 2439, 5235, 5370, 8422, 10131, 12666,$
$13321, 14115, 15582, 15685, 17921, 19263, 19802, 20639, 21880,$
$24192, 24861, 26920, 28693, 29005, 29046, 32049, 33516, 34148,$
$34710, 36901, 38529, 38715, 40852, 42605, 44068, 46125, 49046\}$,

obtenim 34 nombres primers $p = t \cdot n + 1$ per als quals és $g(p) = g_5 = 296$.

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8$ $\displaystyle\prod_{2<\ell<295,\ \ell\neq 37} \ell$,

i $t \in \{375, 2439, 5235, 5370, 8422, 10131, 12666,$
$13321, 14115, 15582, 15685, 17921, 19263, 19802, 20639, 21880,$
$24192, 24861, 26920, 28693, 29005, 29046, 32049, 33516, 34148,$
$34710, 36901, 38529, 38715, 40852, 42605, 44068, 46125, 49046\}$,

obtenim 34 nombres primers $p = t \cdot n + 1$ per als quals és
$g(p) = g_5 = 296$.

Per exemple, per a $t = 375$, és
$p = 82\,855\,936\,135\,344\,100\,632\,056\,271\,522\,681\,245\,522\,780\,723\,865\,103\_$
$509\,764\,974\,109\,209\,268\,525\,901\,004\,067\,727\,168\,403\,658\,740\,190\,041\,391\_$
$380\,898\,836\,192\,995\,001$.

L'arrel primitiva mínima (cont.)

Anàlogament, per a $n = 8$ $\displaystyle\prod_{2<\ell<295,\ \ell\neq 37} \ell$,

i $t \in \{375, 2439, 5235, 5370, 8422, 10131, 12666,$
$13321, 14115, 15582, 15685, 17921, 19263, 19802, 20639, 21880,$
$24192, 24861, 26920, 28693, 29005, 29046, 32049, 33516, 34148,$
$34710, 36901, 38529, 38715, 40852, 42605, 44068, 46125, 49046\}$,

obtenim 34 nombres primers $p = t \cdot n + 1$ per als quals és $g(p) = g_5 = 296$.

Per exemple, per a $t = 375$, és
$p = 82\,855\,936\,135\,344\,100\,632\,056\,271\,522\,681\,245\,522\,780\,723\,865\,103\_$
$509\,764\,974\,109\,209\,268\,525\,901\,004\,067\,727\,168\,403\,658\,740\,190\,041\,391\_$
$380\,898\,836\,192\,995\,001.$

Aquests càlculs recolzen el refinament que hem fet de la conjectura d'Artin.

Mòdul p^2, amb $p > 2$ primer

I per a potències de p?

Mòdul p^2, amb $p > 2$ primer

I per a potències de p?

Sigui $p > 2$ un nombre natural primer. Recordem que

Mòdul p^2, amb $p > 2$ primer

I per a potències de p?

Sigui $p > 2$ un nombre natural primer. Recordem que

per a tot exponent natural $r \geq 1$, el grup multiplicatiu

$$G(p^r) := (\mathbb{Z}/p^r\mathbb{Z})^*$$

també és cíclic. El seu ordre és $\varphi(p^r) = p^{r-1}(p-1)$.

Mòdul p^2, amb $p > 2$ primer

I per a potències de p?

Sigui $p > 2$ un nombre natural primer. Recordem que

per a tot exponent natural $r \geq 1$, el grup multiplicatiu

$$G(p^r) := (\mathbb{Z}/p^r\mathbb{Z})^*$$

també és cíclic. El seu ordre és $\varphi(p^r) = p^{r-1}(p-1)$.

Definició (restrictiva): Anomenarem arrel primitiva mòdul p^r tot nombre natural g, $1 \leq g \leq p^r$, tal que la seva reducció mòdul p^r sigui un generador del grup $G(p^r)$.

Mòdul p^2, amb $p > 2$ primer

I per a potències de p?

Sigui $p > 2$ un nombre natural primer. Recordem que

per a tot exponent natural $r \geq 1$, el grup multiplicatiu

$$G(p^r) := (\mathbb{Z}/p^r\mathbb{Z})^*$$

també és cíclic. El seu ordre és $\varphi(p^r) = p^{r-1}(p-1)$.

Definició (restrictiva): Anomenarem arrel primitiva mòdul p^r tot nombre natural g, $1 \leq g \leq p^r$, tal que la seva reducció mòdul p^r sigui un generador del grup $G(p^r)$.

El nombre d'arrels primitives mòdul p^r és

$$\varphi\big(\varphi(p^r)\big) = \varphi\big(p^{r-1}(p-1)\big).$$

Mòdul p^2, amb $p > 2$ primer (cont.)

- Ens fixarem en el cas $r = 2$; és a dir, mòdul p^2.

En aquest cas, $\#G(p^2) = p(p-1)$, i hi ha
$\varphi\big(p(p-1)\big) = (p-1)\varphi(p-1)$ arrels primitives mòdul p^2.

Mòdul p^2, amb $p > 2$ primer (cont.)

• Ens fixarem en el cas $r = 2$; és a dir, mòdul p^2.
En aquest cas, $\#G(p^2) = p(p-1)$, i hi ha
$\varphi\big(p(p-1)\big) = (p-1)\varphi(p-1)$ arrels primitives mòdul p^2.

• La reducció mòdul p, $G(p^2) \longrightarrow G(p)$, és un morfisme exhaustiu de grups.

Mòdul p^2, amb $p > 2$ primer (cont.)

• Ens fixarem en el cas $r = 2$; és a dir, mòdul p^2.
En aquest cas, $\#G(p^2) = p(p-1)$, i hi ha
$\varphi\big(p(p-1)\big) = (p-1)\varphi(p-1)$ arrels primitives mòdul p^2.

• La reducció mòdul p, $G(p^2) \longrightarrow G(p)$, és un morfisme exhaustiu de grups.

• De fet, per a $1 \leq g \leq p-1$, les antiimatges de g són exactament les p classes de representants $g + \lambda p$, per a $0 \leq \lambda \leq p-1$.

Mòdul p^2, amb $p > 2$ primer (cont.)

Proposició

Fixem un nombre enter g, $1 \leq g \leq p-1$, i pensem-lo com a element de $G(p)$. I sigui $d \mid p-1$ l'ordre de g mòdul p.

Mòdul p^2, amb $p > 2$ primer (cont.)

Proposició

Fixem un nombre enter g, $1 \leq g \leq p-1$, *i pensem-lo com a element de* $G(p)$. *I sigui* $d \mid p-1$ *l'ordre de* g *mòdul* p.

(*Notem que, com que* $g^p \equiv g \pmod{p}$, *resulta que* $\dfrac{g^p - g}{p} \in \mathbb{Z}$.)

Mòdul p^2, amb $p > 2$ primer (cont.)

Proposició

Fixem un nombre enter g, $1 \leq g \leq p-1$, *i pensem-lo com a element de* $G(p)$. *I sigui* $d \mid p-1$ *l'ordre de* g *mòdul* p.

(*Notem que, com que* $g^p \equiv g \pmod{p}$, *resulta que* $\dfrac{g^p - g}{p} \in \mathbb{Z}$.)

Sigui $\lambda_0 \in \mathbb{Z}$, $0 \leq \lambda_0 \leq p-1$, *l'únic nombre d'aquest l'interval tal que* $\lambda_0 \equiv \dfrac{g^p - g}{p} \pmod{p}$.

Mòdul p^2, amb $p > 2$ primer (cont.)

Proposició

Fixem un nombre enter g, $1 \leq g \leq p-1$, *i pensem-lo com a element de* $G(p)$. *I sigui* $d \mid p-1$ *l'ordre de* g *mòdul* p.

(*Notem que, com que* $g^p \equiv g \pmod{p}$, *resulta que* $\dfrac{g^p - g}{p} \in \mathbb{Z}$.)

Sigui $\lambda_0 \in \mathbb{Z}$, $0 \leq \lambda_0 \leq p-1$, *l'únic nombre d'aquest l'interval tal que* $\lambda_0 \equiv \dfrac{g^p - g}{p} \pmod{p}$.

Llavors, l'ordre de $g + \lambda_0 p$ *mòdul* p^2 *és exactament* d,

Mòdul p^2, amb $p > 2$ primer (cont.)

Proposició

Fixem un nombre enter g, $1 \leq g \leq p-1$, *i pensem-lo com a element de* $G(p)$. *I sigui* $d \mid p-1$ *l'ordre de* g *mòdul* p.

(*Notem que, com que* $g^p \equiv g \pmod{p}$, *resulta que* $\dfrac{g^p - g}{p} \in \mathbb{Z}$.)

Sigui $\lambda_0 \in \mathbb{Z}$, $0 \leq \lambda_0 \leq p-1$, *l'únic nombre d'aquest l'interval tal que* $\lambda_0 \equiv \dfrac{g^p - g}{p} \pmod{p}$.

Llavors, l'ordre de $g + \lambda_0 p$ *mòdul* p^2 *és exactament* d, *mentre que per als altres valors de* λ, $0 \leq \lambda \leq p-1$, $\lambda \neq \lambda_0$, *l'ordre de* $g + \lambda p$ *mòdul* p^2 *és exactament* pd.

Mòdul p^2, amb $p > 2$ primer (cont.)

Demostració

L'antiimatge del subgrup de $G(p)$ generat per g és un subgrup de $G(p^2)$ d'ordre pd.

Mòdul p^2, amb $p > 2$ primer (cont.)

Demostració

L'antiimatge del subgrup de $G(p)$ generat per g és un subgrup de $G(p^2)$ d'ordre pd. Per tant, l'ordre de qualsevol dels seus elements és un divisor de pd.

Mòdul p^2, amb $p > 2$ primer (cont.)

Demostració

L'antiimatge del subgrup de $G(p)$ generat per g és un subgrup de $G(p^2)$ d'ordre pd. Per tant, l'ordre de qualsevol dels seus elements és un divisor de pd.

D'altra banda, l'ordre de d ha de dividir l'ordre de qualsevol de les seves antiimatges;

Mòdul p^2, amb $p > 2$ primer (cont.)

Demostració

L'antiimatge del subgrup de $G(p)$ generat per g és un subgrup de $G(p^2)$ d'ordre pd. Per tant, l'ordre de qualsevol dels seus elements és un divisor de pd.

D'altra banda, l'ordre de d ha de dividir l'ordre de qualsevol de les seves antiimatges; per tant, les antiimatges són elements d'ordre d o bé dp.

Mòdul p^2, amb $p > 2$ primer (cont.)

Demostració

L'antiimatge del subgrup de $G(p)$ generat per g és un subgrup de $G(p^2)$ d'ordre pd. Per tant, l'ordre de qualsevol dels seus elements és un divisor de pd.

D'altra banda, l'ordre de d ha de dividir l'ordre de qualsevol de les seves antiimatges; per tant, les antiimatges són elements d'ordre d o bé dp.

I com que

$$(g + \lambda_0 p)^d \equiv \left(g + \frac{g^p - g}{p}\, p\right)^d = g^{pd} \equiv 1 \pmod{p^2},$$

Mòdul p^2, amb $p > 2$ primer (cont.)

Demostració

L'antiimatge del subgrup de $G(p)$ generat per g és un subgrup de $G(p^2)$ d'ordre pd. Per tant, l'ordre de qualsevol dels seus elements és un divisor de pd.

D'altra banda, l'ordre de d ha de dividir l'ordre de qualsevol de les seves antiimatges; per tant, les antiimatges són elements d'ordre d o bé dp.

I com que

$$(g + \lambda_0 p)^d \equiv \left(g + \frac{g^p - g}{p}\, p\right)^d = g^{pd} \equiv 1 \pmod{p^2},$$

l'ordre de $g + \lambda_0 p$ modul p^2 és exactament d.

Mòdul p^2, amb $p > 2$ primer (cont.)

Demostració

L'antiimatge del subgrup de $G(p)$ generat per g és un subgrup de $G(p^2)$ d'ordre pd. Per tant, l'ordre de qualsevol dels seus elements és un divisor de pd.

D'altra banda, l'ordre de d ha de dividir l'ordre de qualsevol de les seves antiimatges; per tant, les antiimatges són elements d'ordre d o bé dp.

I com que

$$(g + \lambda_0 p)^d \equiv \left(g + \frac{g^p - g}{p}\, p\right)^d = g^{pd} \equiv 1 \pmod{p^2},$$

l'ordre de $g + \lambda_0 p$ modul p^2 és exactament d.

D'aquí es dedueix el resultat immediatament, perquè el nombre d'elements de $G(p^2)$ d'ordre d és exactament el mateix, $\varphi(d)$, que el nombre d'elements de $G(p)$ d'ordre d. $\square$

Mòdul p^2, amb $p > 2$ primer (cont.)

Corol·lari

Siguin $p > 2$ un nombre primer i g una arrel primitiva mòdul p. Existeix un únic valor de λ en l'interval $0 \leq \lambda \leq p - 1$ tal que $g + \lambda p$ **no** *és una arrel primitiva mòdul p^2.* $\square$

Mòdul p^2, amb $p > 2$ primer (cont.)

- Anàlogament, si l'ordre d'un element g mòdul p^r, per a algun $r \geq 2$, és d, llavors l'ordre mòdul p^{r+1} és pd.

Mòdul p^2, amb $p > 2$ primer (cont.)

- Anàlogament, si l'ordre d'un element g mòdul p^r, per a algun $r \geq 2$, és d, llavors l'ordre mòdul p^{r+1} és pd.
- En particular, tal com hem vist en el curs, si g és una arrel primitiva mòdul p^2, llavors ho és mòdul p^r, per a tot $r \geq 2$, i la seva reducció mòdul p és una arrel primitiva mòdul p.

Mòdul p^2, amb $p > 2$ primer (cont.)

- Anàlogament, si l'ordre d'un element g mòdul p^r, per a algun $r \geq 2$, és d, llavors l'ordre mòdul p^{r+1} és pd.
- En particular, tal com hem vist en el curs, si g és una arrel primitiva mòdul p^2, llavors ho és mòdul p^r, per a tot $r \geq 2$, i la seva reducció mòdul p és una arrel primitiva mòdul p.
- Així, donada una arrel primitiva mòdul p, existeix un únic valor de λ, $0 \leq \lambda \leq p-1$, tal que $g + \lambda p$ **no** és arrel primitiva mòdul p^r, per a tot $r \geq 2$.

Mòdul p^2, amb $p > 2$ primer (cont.)

- Anàlogament, si l'ordre d'un element g mòdul p^r, per a algun $r \geq 2$, és d, llavors l'ordre mòdul p^{r+1} és pd.
- En particular, tal com hem vist en el curs, si g és una arrel primitiva mòdul p^2, llavors ho és mòdul p^r, per a tot $r \geq 2$, i la seva reducció mòdul p és una arrel primitiva mòdul p.
- Així, donada una arrel primitiva mòdul p, existeix un únic valor de λ, $0 \leq \lambda \leq p-1$, tal que $g + \lambda p$ **no** és arrel primitiva mòdul p^r, per a tot $r \geq 2$.
- I és suficient fixar-se en el cas $r = 2$. Així ho farem.

Exemples

Valors de λ_0 per a totes les arrels primitives mòdul p.

p	g											
	λ_0											
3	2											
	2											
5	2	3										
	1	3										
7	3	5										
	4	2										
11	2	6	7	8								
	10	8	3	10								
13	2	6	7	11								
	6	1	11	6								
17	3	5	6	7	10	11	12	14				
	13	9	2	4	12	14	7	3				
19	2	3	10	13	14	15						
	6	16	17	6	15	13						
23	5	7	10	11	14	15	17	19	20	21		
	1	15	11	8	15	5	2	1	17	11		
29	2	3	8	10	11	14	15	18	19	21	26	27
	2	16	24	14	21	0	28	7	14	4	12	26
31	3	11	12	13	17	21	22	24				
	20	13	7	23	16	4	3	3				
37	2	5	13	15	17	18	19	20	22	24	32	35
	2	24	13	9	11	0	36	25	27	23	12	34

Mòdul p^2, amb $p > 2$ primer (cont.)

- Notem que el mateix valor de λ_0 pot aparèixer per a diferents arrels primitives mòdul p.

Mòdul p^2, amb $p > 2$ primer (cont.)

- Notem que el mateix valor de λ_0 pot aparèixer per a diferents arrels primitives mòdul p.
- I més d'un valor de λ_0 es pot repetir per a diferents arrels primitives mòdul p.

Mòdul p^2, amb $p > 2$ primer (cont.)

- Notem que el mateix valor de λ_0 pot aparèixer per a diferents arrels primitives mòdul p.
- I més d'un valor de λ_0 es pot repetir per a diferents arrels primitives mòdul p.
- Per a algun nombre primer $p > 2$, apareix algun cop el valor $\lambda_0 = 0$; és a dir, alguna arrel primitiva mòdul p **no** és arrel primitiva mòdul p^2.

Mòdul p^2, amb $p > 2$ primer (cont.)

• Notem que el mateix valor de λ_0 pot aparèixer per a diferents arrels primitives mòdul p.
• I més d'un valor de λ_0 es pot repetir per a diferents arrels primitives mòdul p.
• Per a algun nombre primer $p > 2$, apareix algun cop el valor $\lambda_0 = 0$; és a dir, alguna arrel primitiva mòdul p **no** és arrel primitiva mòdul p^2.
• I també hi ha nombres primers $p > 2$ per als quals més d'una arrel primitiva mòdul p no és una arrel primitiva mòdul p^2;

Mòdul p^2, amb $p > 2$ primer (cont.)

• Notem que el mateix valor de λ_0 pot aparèixer per a diferents arrels primitives mòdul p.
• I més d'un valor de λ_0 es pot repetir per a diferents arrels primitives mòdul p.
• Per a algun nombre primer $p > 2$, apareix algun cop el valor $\lambda_0 = 0$; és a dir, alguna arrel primitiva mòdul p **no** és arrel primitiva mòdul p^2.
• I també hi ha nombres primers $p > 2$ per als quals més d'una arrel primitiva mòdul p no és una arrel primitiva mòdul p^2; per exemple, per a $p = 367$, les arrels primitives $g = 159$ i $g = 205$ **no** són arrels primitives mòdul p^2.

Mòdul p^2, amb $p > 2$ primer (cont.)

En tots els exemples mostrats, la mínima arrel primitiva mòdul p és arrel primitiva mòdul p^2. Una primera qüestió que podem posar-nos és:

Mòdul p^2, amb $p > 2$ primer (cont.)

En tots els exemples mostrats, la mínima arrel primitiva mòdul p és arrel primitiva mòdul p^2. Una primera qüestió que podem posar-nos és:

és aquest un fet general?

Mòdul p^2, amb $p > 2$ primer (cont.)

En tots els exemples mostrats, la mínima arrel primitiva mòdul p és arrel primitiva mòdul p^2. Una primera qüestió que podem posar-nos és:

és aquest un fet general?

és a dir,

Qüestió

és cert que, per a tot nombre primer $p > 2$, la **mínima** arrel primitiva mòdul p també és arrel primitiva mòdul p^2? (I, per tant, mòdul p^r per a tot $r \geq 2$.)

Mòdul p^2, amb $p > 2$ primer (cont.)

En tots els exemples mostrats, la mínima arrel primitiva mòdul p és arrel primitiva mòdul p^2. Una primera qüestió que podem posar-nos és:

és aquest un fet general?

és a dir,

Qüestió

és cert que, per a tot nombre primer $p > 2$, la **mínima** arrel primitiva mòdul p també és arrel primitiva mòdul p^2? (I, per tant, mòdul p^r per a tot $r \geq 2$.)

La resposta és

NO!

Mòdul p^2, amb $p > 2$ primer (cont.)

Proposició

Per a tot nombre primer p, $2 < p < 40487$, la mínima arrel primitiva mòdul p també és arrel primitiva mòdul p^r per a tot $r \geq 1$.

Mòdul p^2, amb $p > 2$ primer (cont.)

Proposició

Per a tot nombre primer p, $2 < p < 40487$, la mínima arrel primitiva mòdul p també és arrel primitiva mòdul p^r per a tot $r \geq 1$.
Per a $p = 40487$, la mínima arrel primitiva és $g = 5$ i **no** *és arrel primitiva mòdul p^2.*

Mòdul p^2, amb $p > 2$ primer (cont.)

Proposició

Per a tot nombre primer p, $2 < p < 40487$, la mínima arrel primitiva mòdul p també és arrel primitiva mòdul p^r per a tot $r \geq 1$.
Per a $p = 40487$, la mínima arrel primitiva és $g = 5$ i **no** *és arrel primitiva mòdul p^2.*

Demostració

Càlcul! $\square$

Mòdul p^2, amb $p > 2$ primer (cont.)

Notem que 40487 és el 4244-èsim nombre primer

Mòdul p^2, amb $p > 2$ primer (cont.)

Notem que 40487 és el 4244-èsim nombre primer; és a dir, amb la notació usual, p_n, per al n-èsim nombre primer, és $p_{4244} = 40487$.

Mòdul p^2, amb $p > 2$ primer (cont.)

Notem que 40487 és el 4244-èsim nombre primer; és a dir, amb la notació usual, p_n, per al n-èsim nombre primer, és $p_{4244} = 40487$.

Qüestió

és gaire freqüent el fet que l'arrel primitiva **mínima** mòdul un nombre primer $p > 2$ **no** sigui una arrel primitiva mòdul p^2?

Resultats experimentals

Proposició

Entre els nombres primers p, $2 < p < 10^{13}$, la mínima arrel primitiva mòdul p també és arrel primitiva mòdul p^r per a tot $r \geq 1$, excepte per als dos nombres primers

$$p_{4244} = 40487, \qquad p_{310\,221\,731} = 6\,692\,367\,337.$$

Resultats experimentals

Proposició

Entre els nombres primers p, $2 < p < 10^{13}$, la mínima arrel primitiva mòdul p també és arrel primitiva mòdul p^r per a tot $r \geq 1$, excepte per als dos nombres primers

$$p_{4244} = 40487, \qquad p_{310\,221\,731} = 6\,692\,367\,337.$$

Per a aquests dos nombres, p, la mínima arrel primitiva mòdul p és $g(p) = 5$.

Resultats experimentals

Proposició

Entre els nombres primers p, $2 < p < 10^{13}$, *la mínima arrel primitiva mòdul* p *també és arrel primitiva mòdul* p^r *per a tot* $r \geq 1$, *excepte per als dos nombres primers*

$$p_{4244} = 40487, \qquad p_{310\,221\,731} = 6\,692\,367\,337.$$

Per a aquests dos nombres, p, *la mínima arrel primitiva mòdul* p *és* $g(p) = 5$.
La mínima arrel primitiva mòdul 40487^2 *és* $g = 10$.

Resultats experimentals

Proposició

Entre els nombres primers p, $2 < p < 10^{13}$, *la mínima arrel primitiva mòdul* p *també és arrel primitiva mòdul* p^r *per a tot* $r \geq 1$, *excepte per als dos nombres primers*

$$p_{4244} = 40487, \qquad p_{310\,221\,731} = 6\,692\,367\,337.$$

Per a aquests dos nombres, p, *la mínima arrel primitiva mòdul* p *és* $g(p) = 5$.
La mínima arrel primitiva mòdul 40487^2 *és* $g = 10$.
I la mínima arrel primitiva mòdul $6\,692\,367\,337^2$ *és* $g = 7$.

Resultats experimentals

Proposició

Entre els nombres primers p, $2 < p < 10^{13}$, *la mínima arrel primitiva mòdul* p *també és arrel primitiva mòdul* p^r *per a tot* $r \geq 1$, *excepte per als dos nombres primers*

$$p_{4244} = 40487, \qquad p_{310\,221\,731} = 6\,692\,367\,337.$$

Per a aquests dos nombres, p, *la mínima arrel primitiva mòdul* p *és* $g(p) = 5$.
La mínima arrel primitiva mòdul 40487^2 *és* $g = 10$.
I la mínima arrel primitiva mòdul $6\,692\,367\,337^2$ *és* $g = 7$.

Demostració

Resultats experimentals

Proposició

Entre els nombres primers p, $2 < p < 10^{13}$, la mínima arrel primitiva mòdul p també és arrel primitiva mòdul p^r per a tot $r \geq 1$, excepte per als dos nombres primers

$$p_{4244} = 40487, \qquad p_{310\,221\,731} = 6\,692\,367\,337.$$

Per a aquests dos nombres, p, la mínima arrel primitiva mòdul p és $g(p) = 5$.
La mínima arrel primitiva mòdul 40487^2 és $g = 10$.
I la mínima arrel primitiva mòdul $6\,692\,367\,337^2$ és $g = 7$.

Demostració

Molt més càlcul! $\square$

Resultats experimentals (cont.)

Per a cada nombre primer p, $2 < p < 10^{13}$, he calculat

- la mínima arrel primitiva, $g(p)$, mòdul p,
- i el valor de λ, $0 \leq \lambda \leq p-1$, tal que $g(p) + \lambda p$ no és arrel primitiva mòdul p^2.

Resultats experimentals (cont.)

Per a cada nombre primer p, $2 < p < 10^{13}$, he calculat
- la mínima arrel primitiva, $g(p)$, mòdul p,
- i el valor de λ, $0 \leq \lambda \leq p-1$, tal que $g(p) + \lambda p$ no és arrel primitiva mòdul p^2.

I he tabulat el nombre de vegades, $n(\lambda)$, que apareix cada valor de λ, per a $0 \leq \lambda \leq 1000$.

Resultats experimentals (cont.)

Per a cada nombre primer p, $2 < p < 10^{13}$, he calculat
- la mínima arrel primitiva, $g(p)$, mòdul p,
- i el valor de λ, $0 \leq \lambda \leq p-1$, tal que $g(p) + \lambda p$ no és arrel primitiva mòdul p^2.

I he tabulat el nombre de vegades, $n(\lambda)$, que apareix cada valor de λ, per a $0 \leq \lambda \leq 1000$.
En particular, $\lambda = 0$ només apareix dues vegades.

Resultats experimentals (cont.)

Per als valors $1 \leq \lambda \leq 100$, la taula és la següent:

λ	$n(\lambda)$	λ	$n(\lambda)$	λ	$n(\lambda)$	λ	$n(\lambda)$
1	4	2	5	3	1	4	6
5	0	6	7	7	1	8	2
9	1	10	2	11	5	12	2
13	5	14	1	15	2	16	3
17	1	18	2	19	3	20	3
21	5	22	3	23	0	24	1
25	0	26	3	27	1	28	1
29	4	30	1	31	2	32	1
33	2	34	1	35	5	36	0
37	1	38	2	39	3	40	1
41	3	42	2	43	2	44	1
45	2	46	3	47	2	48	1
49	3	50	5	51	1	52	0
53	4	54	1	55	4	56	0
57	1	58	4	59	3	60	5
61	0	62	0	63	3	64	3
65	2	66	0	67	1	68	1
69	1	70	3	71	3	72	1
73	2	74	4	75	2	76	2
77	1	78	1	79	1	80	3
81	0	82	1	83	3	84	1
85	3	86	2	87	1	88	2
89	2	90	1	91	1	92	3
93	2	94	2	95	2	96	4
97	3	98	4	99	3	100	4

Resultats experimentals (cont.)

- En particular, per a $1 \leq \lambda \leq 100$, els valors de $n(\lambda)$ oscil·len entre $n(\lambda) = 0$

Resultats experimentals (cont.)

- En particular, per a $1 \leq \lambda \leq 100$, els valors de $n(\lambda)$ oscil·len entre $n(\lambda) = 0$ (per a $\lambda = 5$, 23, 25, 36, 52, 56, 61, 62, 66 i 81),

Resultats experimentals (cont.)

- En particular, per a $1 \leq \lambda \leq 100$, els valors de $n(\lambda)$ oscil·len entre $n(\lambda) = 0$ (per a $\lambda = 5$, 23, 25, 36, 52, 56, 61, 62, 66 i 81), i $n(\lambda) = 7$ (per a $\lambda = 6$).

Resultats experimentals (cont.)

- En particular, per a $1 \leq \lambda \leq 100$, els valors de $n(\lambda)$ oscil·len entre $n(\lambda) = 0$ (per a $\lambda = 5$, 23, 25, 36, 52, 56, 61, 62, 66 i 81), i $n(\lambda) = 7$ (per a $\lambda = 6$).
En total, entre els 346 065 536 838 nombres primers menors que 10^{13}, apareixen 218 valors de p per als quals $1 \leq \lambda \leq 100$.

Resultats experimentals (cont.)

- En particular, per a $1 \leq \lambda \leq 100$, els valors de $n(\lambda)$ oscil·len entre $n(\lambda) = 0$ (per a $\lambda = 5$, 23, 25, 36, 52, 56, 61, 62, 66 i 81), i $n(\lambda) = 7$ (per a $\lambda = 6$).
En total, entre els 346 065 536 838 nombres primers menors que 10^{13}, apareixen 218 valors de p per als quals $1 \leq \lambda \leq 100$.

- I per a $1 \leq \lambda \leq 1000$, els valors de $n(\lambda)$ també oscil·len entre $n(\lambda) = 0$ i $n(\lambda) = 7$.

Resultats experimentals (cont.)

• En particular, per a $1 \leq \lambda \leq 100$, els valors de $n(\lambda)$ oscil·len entre $n(\lambda) = 0$ (per a $\lambda = 5$, 23, 25, 36, 52, 56, 61, 62, 66 i 81), i $n(\lambda) = 7$ (per a $\lambda = 6$).
En total, entre els 346 065 536 838 nombres primers menors que 10^{13}, apareixen 218 valors de p per als quals $1 \leq \lambda \leq 100$.

• I per a $1 \leq \lambda \leq 1000$, els valors de $n(\lambda)$ també oscil·len entre $n(\lambda) = 0$ i $n(\lambda) = 7$.
I apareixen 1634 valors de p per als quals $1 \leq \lambda \leq 1000$.

Resultats experimentals (cont.)

• En particular, per a $1 \leq \lambda \leq 100$, els valors de $n(\lambda)$ oscil·len entre $n(\lambda) = 0$ (per a $\lambda = 5$, 23, 25, 36, 52, 56, 61, 62, 66 i 81), i $n(\lambda) = 7$ (per a $\lambda = 6$).
En total, entre els 346 065 536 838 nombres primers menors que 10^{13}, apareixen 218 valors de p per als quals $1 \leq \lambda \leq 100$.

• I per a $1 \leq \lambda \leq 1000$, els valors de $n(\lambda)$ també oscil·len entre $n(\lambda) = 0$ i $n(\lambda) = 7$.
I apareixen 1634 valors de p per als quals $1 \leq \lambda \leq 1000$.

Notem que $\pi_2(1000) = 167$, i que per a tots els nombres primers $2 < p < 1000$ és $\lambda < 1000$.

Resultats experimentals (cont.)

• En particular, per a $1 \leq \lambda \leq 100$, els valors de $n(\lambda)$ oscil·len entre $n(\lambda) = 0$ (per a $\lambda = 5$, 23, 25, 36, 52, 56, 61, 62, 66 i 81), i $n(\lambda) = 7$ (per a $\lambda = 6$).
En total, entre els 346 065 536 838 nombres primers menors que 10^{13}, apareixen 218 valors de p per als quals $1 \leq \lambda \leq 100$.

• I per a $1 \leq \lambda \leq 1000$, els valors de $n(\lambda)$ també oscil·len entre $n(\lambda) = 0$ i $n(\lambda) = 7$.
I apareixen 1634 valors de p per als quals $1 \leq \lambda \leq 1000$.

Notem que $\pi_2(1000) = 167$, i que per a tots els nombres primers $2 < p < 1000$ és $\lambda < 1000$.
I notem que $1634 - 167 = 1467$ i que
$\log(\log 10^{13}) - \log(\log 1000) \simeq 1.46634\ldots$

Resultats experimentals (cont.)

Hem mirat les taules dels valors de λ, $1 \leq \lambda \leq 1000$, per als nombres primers d'alguns intervals diferents $f < p < F$, amb f, F múltiples de 5×10^9, i $F \leq 10^{13}$.

Resultats experimentals (cont.)

Hem mirat les taules dels valors de λ, $1 \leq \lambda \leq 1000$, per als nombres primers d'alguns intervals diferents $f < p < F$, amb f, F múltiples de 5×10^9, i $F \leq 10^{13}$.
En tots els casos, hem obtingut resultats numèrics aproximats

$$\begin{aligned} \#\{p : f < p < F \text{ i } 1 \leq \lambda(p) \leq 1000\} & \\ & \simeq 1000\,(\log(\log F) - \log(\log f)) \\ & \simeq 1000 \sum_{f<p<F} \frac{1}{p}. \end{aligned}$$

Resultats experimentals (cont.)

Notem que, per a tot nombre primer $p > 2$, i per a una arrel primitiva g mòdul p (per exemple, la mínima), el valor corresponent de λ, posem $\lambda(p)$, per al qual $g + \lambda(p)p$ no és arrel primitiva mòdul p^2 és un dels p nombres $0 \leq \lambda \leq p - 1$.

Resultats experimentals (cont.)

Notem que, per a tot nombre primer $p > 2$, i per a una arrel primitiva g mòdul p (per exemple, la mínima), el valor corresponent de λ, posem $\lambda(p)$, per al qual $g + \lambda(p)p$ no és arrel primitiva mòdul p^2 és un dels p nombres $0 \leq \lambda \leq p - 1$.
O, dit d'una altra manera, i si suposem equirepartició per als valors de λ, el valor esperat que, fixat un nombre λ i un nombre primer $p > \lambda$, sigui $\lambda(p) = \lambda$ és $\frac{1}{p}$.

Resultats experimentals (cont.)

Notem que, per a tot nombre primer $p > 2$, i per a una arrel primitiva g mòdul p (per exemple, la mínima), el valor corresponent de λ, posem $\lambda(p)$, per al qual $g + \lambda(p)p$ no és arrel primitiva mòdul p^2 és un dels p nombres $0 \leq \lambda \leq p - 1$.
O, dit d'una altra manera, i si suposem equirepartició per als valors de λ, el valor esperat que, fixat un nombre λ i un nombre primer $p > \lambda$, sigui $\lambda(p) = \lambda$ és $\frac{1}{p}$.
Per tant, per als primers p d'un interval $f < p < F$, el valor esperat d'aparicions de cada valor particular λ és

$$\sum_{f<p<F} \frac{1}{p} \simeq \log(\log F) - \log(\log f).$$

Qüestions

Per a tot nombre primer $p > 2$, posem $\lambda(p)$, $0 \leq \lambda(p) \leq p-1$, l'únic valor tal que per a l'arrel primitiva **mínima** mòdul p, $g(p)$, el nombre $g(p) + \lambda(p)p$ no és arrel primitiva mòdul p^2.

Qüestions

Per a tot nombre primer $p > 2$, posem $\lambda(p)$, $0 \leq \lambda(p) \leq p-1$, l'únic valor tal que per a l'arrel primitiva **mínima** mòdul p, $g(p)$, el nombre $g(p) + \lambda(p)p$ no és arrel primitiva mòdul p^2.

Qüestió $P(\lambda, \infty)$

és cert que per a tot nombre natural $\lambda \geq 0$, el conjunt de nombres primers $p > 2$ per als quals $\lambda(p) = \lambda$ és infinit?

Qüestions

Per a tot nombre primer $p > 2$, posem $\lambda(p)$, $0 \leq \lambda(p) \leq p-1$, l'únic valor tal que per a l'arrel primitiva **mínima** mòdul p, $g(p)$, el nombre $g(p) + \lambda(p)p$ no és arrel primitiva mòdul p^2.

Qüestió $P(\lambda, \infty)$

és cert que per a tot nombre natural $\lambda \geq 0$, el conjunt de nombres primers $p > 2$ per als quals $\lambda(p) = \lambda$ és infinit?
Amb més precisió: és cert que per a tot nombre natural $\lambda \geq 0$ i tot $F >> 0$,

$$\#\{p : 2 < p < F,\ p \text{ primer, i } \lambda(p) = \lambda\}$$

és asimptòticament equivalent a $\log(\log F)$?

Qüestions

Per a tot nombre primer $p > 2$, posem $\lambda(p)$, $0 \leq \lambda(p) \leq p-1$, l'únic valor tal que per a l'arrel primitiva **mínima** mòdul p, $g(p)$, el nombre $g(p) + \lambda(p)p$ no és arrel primitiva mòdul p^2.

Qüestió $P(\lambda, \infty)$

és cert que per a tot nombre natural $\lambda \geq 0$, el conjunt de nombres primers $p > 2$ per als quals $\lambda(p) = \lambda$ és infinit?
Amb més precisió: és cert que per a tot nombre natural $\lambda \geq 0$ i tot $F >> 0$,

$$\#\{p : 2 < p < F,\ p \text{ primer, i } \lambda(p) = \lambda\}$$

és asimptòticament equivalent a $\log(\log F)$? (?)

Qüestions (cont.)

En particular, per a $\lambda = 0$, la pregunta és

Qüestió $P(0, \infty)$

és cert que hi ha una infinitat de nombres primers $p > 2$ per als quals l'arrel primitiva mínima mòdul p no és arrel primitiva mòdul p^2?

Qüestions (cont.)

En particular, per a $\lambda = 0$, la pregunta és

Qüestió $P(0, \infty)$

és cert que hi ha una infinitat de nombres primers $p > 2$ per als quals l'arrel primitiva mínima mòdul p no és arrel primitiva mòdul p^2?
O, amb més precisió, és cert que, per a tot $F >> 0$,

$$\#\{p : 2 < p < F,\ p \text{ primer, i } \lambda(p) = 0\}$$

és asimptòticament equivalent a $\log(\log F)$?

$$(?)$$

Qüestions (cont.)

A causa de l'heurística anterior, hom està temptat de contestar afirmativament aquesta qüestió. Però potser podríem afinar encara més.

Qüestions (cont.)

A causa de l'heurística anterior, hom està temptat de contestar afirmativament aquesta qüestió. Però potser podríem afinar encara més. Definim els conjunts següents.

Qüestions (cont.)

A causa de l'heurística anterior, hom està temptat de contestar afirmativament aquesta qüestió. Però potser podríem afinar encara més. Definim els conjunts següents.
Per a tot nombre natural $g > 1$ i no potència exacta, posem

$$P(g, 0) := \{p > 2 : \ p \text{ primer}, \ g(p) = g, \ \lambda(p) = 0\}.$$

Qüestions (cont.)

A causa de l'heurística anterior, hom està temptat de contestar afirmativament aquesta qüestió. Però potser podríem afinar encara més. Definim els conjunts següents.
Per a tot nombre natural $g > 1$ i no potència exacta, posem

$$P(g, 0) := \{p > 2 : \ p \text{ primer}, \ g(p) = g, \ \lambda(p) = 0\}.$$

Per exemple, $40487, 6\,692\,367\,337 \in P(5, 0)$, de manera que $P(5, 0) \neq \varnothing$.

Qüestions (cont.)

A causa de l'heurística anterior, hom està temptat de contestar afirmativament aquesta qüestió. Però potser podríem afinar encara més. Definim els conjunts següents.
Per a tot nombre natural $g > 1$ i no potència exacta, posem

$$P(g,0) := \{p > 2 : \ p \text{ primer}, \ g(p) = g, \ \lambda(p) = 0\}.$$

Per exemple, $40487, 6\,692\,367\,337 \in P(5,0)$, de manera que $P(5,0) \neq \varnothing$.
I siguin

$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\} = \bigcup_g P(g,0),$$

$$G(0) := \{g > 1 : \ g \text{ no potència exacta,} \\ \text{i existeix } p, \text{ primer}, \ g(p) = g, \ \lambda(p) = 0\}.$$

Qüestions (cont.)

A causa de l'heurística anterior, hom està temptat de contestar afirmativament aquesta qüestió. Però potser podríem afinar encara més. Definim els conjunts següents.
Per a tot nombre natural $g > 1$ i no potència exacta, posem

$$P(g,0) := \{p > 2 : \ p \text{ primer}, \ g(p) = g, \ \lambda(p) = 0\}.$$

Per exemple, $40487, 6\,692\,367\,337 \in P(5,0)$, de manera que $P(5,0) \neq \varnothing$.
I siguin

$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\} = \bigcup_g P(g,0),$$

$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, \ g(p) = g, \ \lambda(p) = 0\}.$$

Per exemple, $5 \in G(0)$, de manera que $G(0) \neq \varnothing$.

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Sigui $g > 1$ un nombre enter que no sigui una potència exacta.

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Sigui $g > 1$ un nombre enter que no sigui una potència exacta.

Qüestió $P(g, 0, \infty)$: és cert que $\#P(g, 0) = +\infty$?

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Sigui $g > 1$ un nombre enter que no sigui una potència exacta.

Qüestió $P(g, 0, \infty)$: és cert que $\#P(g,0) = +\infty$?

Qüestió $P(g, 0, > 0)$: és cert que $\#P(g,0) > 0$?

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Sigui $g > 1$ un nombre enter que no sigui una potència exacta.

Qüestió $P(g, 0, \infty)$: és cert que $\#P(g,0) = +\infty$?

Qüestió $P(g, 0, > 0)$: és cert que $\#P(g,0) > 0$?

En particular, sabem que $P(5,0) \neq \varnothing$; és a dir, sabem que $P(5, 0, > 0)$ és certa.

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Sigui $g > 1$ un nombre enter que no sigui una potència exacta.

Qüestió $P(g, 0, \infty)$: és cert que $\#P(g,0) = +\infty$?

Qüestió $P(g, 0, > 0)$: és cert que $\#P(g,0) > 0$?

En particular, sabem que $P(5,0) \neq \varnothing$; és a dir, sabem que $P(5,0,>0)$ és certa.

Òbviament, per a tot nombre natural $g > 1$ i no potència exacta, $P(g,0,\infty) \implies P(g,0,>0)$. És certa $P(5,0,\infty)$?

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Sigui $g > 1$ un nombre enter que no sigui una potència exacta.

Qüestió $P(g, 0, \infty)$: és cert que $\#P(g,0) = +\infty$?

Qüestió $P(g, 0, > 0)$: és cert que $\#P(g,0) > 0$?

En particular, sabem que $P(5,0) \neq \varnothing$; és a dir, sabem que $P(5,0,>0)$ és certa.

Òbviament, per a tot nombre natural $g > 1$ i no potència exacta, $P(g,0,\infty) \implies P(g,0,>0)$. És certa $P(5,0,\infty)$?

És certa $P(g,0,>0)$ per a algun altre valor $g \neq 5$?

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Sigui $g > 1$ un nombre enter que no sigui una potència exacta.

Qüestió $P(g, 0, \infty)$: és cert que $\#P(g,0) = +\infty$?

Qüestió $P(g, 0, > 0)$: és cert que $\#P(g,0) > 0$?

En particular, sabem que $P(5,0) \neq \varnothing$; és a dir, sabem que $P(5,0,>0)$ és certa.

Òbviament, per a tot nombre natural $g > 1$ i no potència exacta, $P(g,0,\infty) \implies P(g,0,>0)$. És certa $P(5,0,\infty)$?

És certa $P(g,0,>0)$ per a algun altre valor $g \neq 5$? És certa $P(g,0,>0)$ per a tot valor de g?

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Sigui $g > 1$ un nombre enter que no sigui una potència exacta.

Qüestió $P(g, 0, \infty)$: és cert que $\#P(g,0) = +\infty$?

Qüestió $P(g, 0, > 0)$: és cert que $\#P(g,0) > 0$?

En particular, sabem que $P(5,0) \neq \varnothing$; és a dir, sabem que $P(5,0,>0)$ és certa.

Òbviament, per a tot nombre natural $g > 1$ i no potència exacta, $P(g,0,\infty) \implies P(g,0,>0)$. És certa $P(5,0,\infty)$?

És certa $P(g,0,>0)$ per a algun altre valor $g \neq 5$? És certa $P(g,0,>0)$ per a tot valor de g? És certa $P(g,0,\infty)$ per a algun g?

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Sigui $g > 1$ un nombre enter que no sigui una potència exacta.

Qüestió $P(g, 0, \infty)$: és cert que $\#P(g,0) = +\infty$?

Qüestió $P(g, 0, > 0)$: és cert que $\#P(g,0) > 0$?

En particular, sabem que $P(5,0) \neq \varnothing$; és a dir, sabem que $P(5,0,>0)$ és certa.

Òbviament, per a tot nombre natural $g > 1$ i no potència exacta, $P(g,0,\infty) \implies P(g,0,>0)$. És certa $P(5,0,\infty)$?

És certa $P(g,0,>0)$ per a algun altre valor $g \neq 5$? És certa $P(g,0,>0)$ per a tot valor de g? És certa $P(g,0,\infty)$ per a algun g? És certa $P(g,0,\infty)$ per a tot g?

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$

$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Afirmació $P(0, > 0)$: és cert que $P(0) \neq \varnothing$, perquè $40487, 6\,692\,367\,337 \in P(0)$.

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, \ g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, \ g(p) = g, \ \ \lambda(p) = 0\}.$$

Afirmació $P(0, > 0)$: és cert que $P(0) \neq \varnothing$, perquè $40487, 6\,692\,367\,337 \in P(0)$.

Qüestió $P(0, \infty)$: és cert que $\#P(0) = +\infty$?

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Afirmació $P(0, > 0)$: és cert que $P(0) \neq \varnothing$, perquè $40487, 6\,692\,367\,337 \in P(0)$.

Qüestió $P(0, \infty)$: és cert que $\#P(0) = +\infty$?

Afirmació $G(0, > 0)$: és cert que $G(0) \neq \varnothing$, perquè $5 \in G(0)$.

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, \ g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, \ g(p) = g, \ \ \lambda(p) = 0\}.$$

Afirmació $P(0, > 0)$: és cert que $P(0) \neq \varnothing$, perquè $40487, 6\,692\,367\,337 \in P(0)$.

Qüestió $P(0, \infty)$: és cert que $\#P(0) = +\infty$?

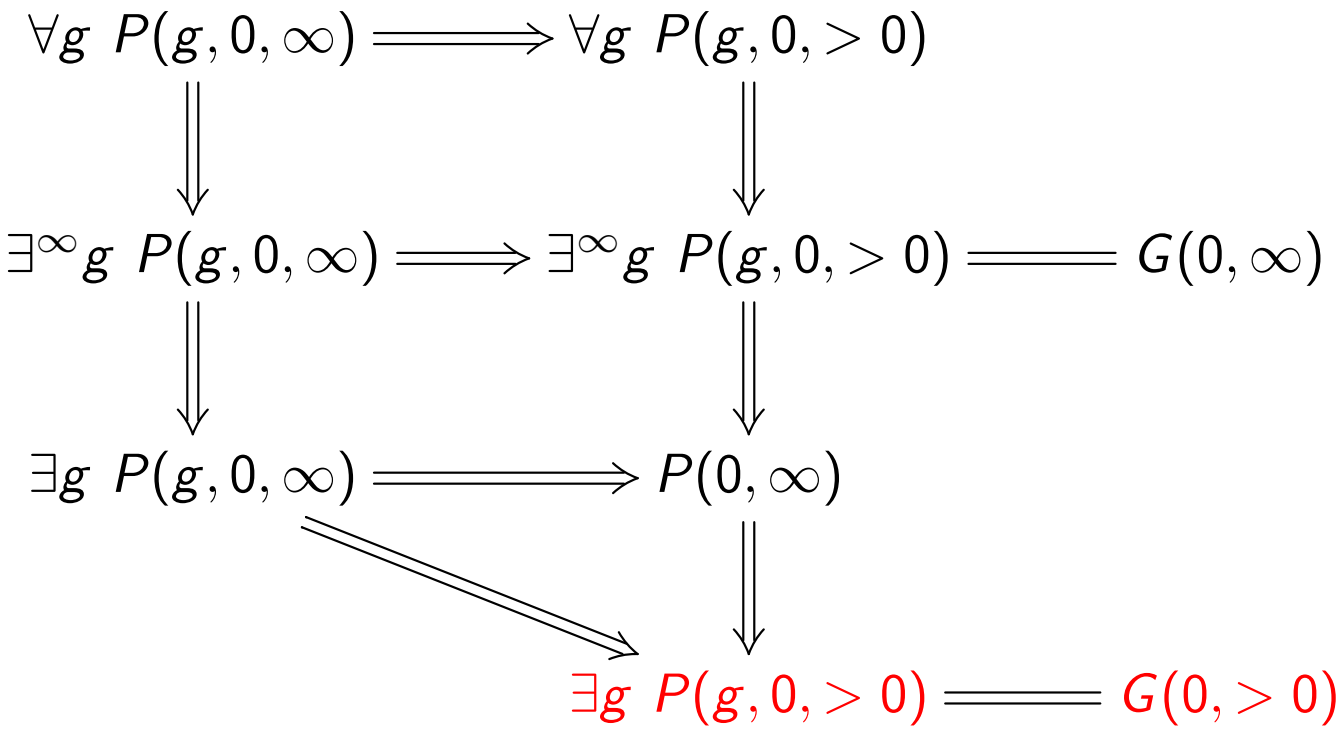
Afirmació $G(0, > 0)$: és cert que $G(0) \neq \varnothing$, perquè $5 \in G(0)$.

Qüestió $G(0, \infty)$: és cert que $\#G(0) = +\infty$?

Qüestions (cont.)

$$P(g,0) := \{p > 2 : \ p \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$
$$P(0) := \{p : \ p \text{ primer, i } \lambda(p) = 0\},$$
$$G(0) := \{g > 1 : \ g \text{ no potència exacta, i existeix } p, \text{ primer}, g(p) = g, \ \ \lambda(p) = 0\}.$$

Relació entre les qüestions.



Especificacions del càlcul

Per a la realització del càlcul, que s'ha programat en `pari`,

Especificacions del càlcul

Per a la realització del càlcul, que s'ha programat en `pari`, s'han utilitzat

4 nuclis d'un processador $x86\_64$, a $2.7\,GHz$, amb $15.6\,GiB$ de RAM;

4 nuclis d'un processador $i686$, a $3.2\,GHz$, amb $3.7\,GiB$ de RAM;

i 2 nuclis d'un processador $x86\_64$, a $3.3\,GHz$, amb $7,8\,GiB$ de RAM,

Especificacions del càlcul

Per a la realització del càlcul, que s'ha programat en `pari`, s'han utilitzat

4 nuclis d'un processador $x86\_64$, a $2.7 GHz$, amb $15.6 GiB$ de RAM;

4 nuclis d'un processador $i686$, a $3.2 GHz$, amb $3.7 GiB$ de RAM;

i 2 nuclis d'un processador $x86\_64$, a $3.3 GHz$, amb $7,8 GiB$ de RAM,

amb un temps acumulat de càlcul de (més de) 3 anys i 284 dies.

UNIVERSITAT DE BARCELONA