UNIVERSITAT DE BARCELONA

Treball final del grau de Matemàtiques

Facultat de Matemàtiques i Informàtica

LA CORBA DE FREY: TEORIA I APLICACIONS

Autora: Mar Curcó Iranzo

Director: Dr. Artur Travesa Grau
Departament de Matemàtiques i Informàtica

Barcelona, 29 de juny de 2017

Abstract

We start this thesis with a brief study on the Rieman-Roch Theorem so we can later introduce the concept of elliptic curve. We'll proceed studying these as Weirstrass plane cubics and their reduction behaviour. Subsequently we'll develop the construction of Frey's curve and study some of its properties. Then, we give a short introduction to modular functions and Galois representation. Finally, we draw an outline for the proof of Fermat's Theorem, where we can appreciate the importance of said curve. We conclude with an application of this method on other diofantic equations.

Resum

Iniciem el treball amb un breu estudi de del teorema de Riemann-Roch, per així poder introduïr el concepte de corba el·líptica. Tot seguit, desenvolupem l'estudi d'aquestes mitjançant la seva interpretació com a cúbiques planes de Weierstrass i el comportament de la seva reducció. A continuació donem la contrucció de la corba de Frey i n'estudiem algunes de les seves propietats. Seguidament, donem una breu introducció a les funcions modulars i a les representacions de Galois i, finalment, dibuixem l'esquema de la demostració del teorema de Fermat, on queda palesa la importància de la corba esmentada. Acabem amb una aplicació d'aquest mètode a altres equacions diofantines.

Agraïments

Vull donar les gràcies a

El Dr. Artur Travessa, per totes les hores dedicades i per guiar-me en el tema que em vaig entossudir a escollir.

La meva família (Mama, Papa, Dídac i Paula), per haver-me aguantat en els meus momens més insoportables sense perdre la paciència i la confiança.

La Ojanta i la Ilona, perquè sí. L'Angels i la Blau, perquè puc.

El Giancarlo, per l'editor de LaTeX; el Bruno, per raons (i persones); el Ioar, per el Club de los Batidos; el Lloyd, per compromís (no som tan amics); el Toni i l'Oriol, perquè estan allí.

L'Oriol i el Pau, pel grup fonamental.

La Clara i l'Àngela Francesca, per ser tant desconsiderades al pis.

Introducció

L'any 1637, Pierre de Fermat va escriure al marge d'un llibre de l'aritmètica de Diofant una frase que podem interpretar, amb notació actual, com *no existeixen nombres naturals $n > 2$, x, y i z tals que*

$$x^n + y^n = z^n.$$

El 1995, Andrew Wiles va publicar en un article de 98 pàgines a la revista *Annals of Mathematics* la demostració del teorema

Tota corba el·líptica semiestable és modular;

amb aquest resultat, restava provada l'afirmació de Fermat.

Entremig d'aquests dos fets, però, hi ha 358 anys de matemàtics encarant-se amb el teorema i fent progressos per a desenvolupar la prova del que semblava un enunciat senzill, o almenys comprensible per tothom. En particular es redueix la prova al cas d'exponent primer més gran que 3.

L'estratègia de la demostració va ser iniciada per Gerhard Frey, el qual va suposar que l'enunciat de Fermat era fals; i, suposant que existia una solució (a, b, c) de l'equació diofantina, va associar a aquesta una corba el·líptica amb molt bones propietats; tant bones, que se sospitava que aquesta no podia existir. Tot i així, provar la no existència d'aquesta corba no és un camí curt. Per a fer-ho s'han d'estudiar molt bé les propietats de les corbes el·líptiques, en particular, les del grup format pels seus punts de n-torsió. A partir d'aquestes propietats, podem associar al grup esmentat una representació de Galois molt natural. Així doncs, Wiles demostra que aquesta representació ha d'estar fortament relacionada amb una funció modular de pes k i nivell N; amb els teoremes de baixades de nivell de Serre i Ribet, aquesta ha de ser equivalent a una altra funció modular amb pes i nivell més petits. Però els coneixements que ja es tenien de funcions modulars indiquen que aquesta no pot exisitr.

L'objectiu del treball és doble; d'una banda, fer un estudi de les corbes el·líptiques i entendre la construcció de la corba de Frey i les seves propietats, d'acord amb l'article original *Links between stable elliptic curves and certain Diophantine equations*, publicat el 1986 per G. Frey ([8]); de l'altra, veure l'aplicació d'aquesta idea en la demostració del teorema de Fermat, tot entenent què significa l'enunciat del teorema de Wiles.

La memòria del treball és estructurada en quatre seccions.

La primera secció consta del capítol 1 i es tracta d'una introducció a les corbes algebraiques. Recordem les definicions i conceptes bàsics de les corbes projectives. A més, hi afegeim un estudi de la teoria de divisors sobre una corba per presentar el teorema de Riemann-Roch, el qual ens permet donar una definició precisa de corba el·líptica.

La secció següent és formada pels capítols 2 i 3 del treball. En el primer, exposem la interpretació de les corbes el·líptiques com a cúbiques planes donades per equacions de Wiertrass i en treballem les seves diferents formes. Mitjançant aquestes, definim els invariants d'una corba el·líptica i construïm l'estructura de grup dels seus punts utilitzant el teorema de Riemann-Roch. En el capítol 3 estudiem la reducció de les corbes el·líptiques definides sobre $\mathbb{Q}$ mòdul un nombre primer p i donem la demostració del teorema de reducció semi-estable que motiva la definició de corba semi-estable. Amb aquest objectiu, introduïm el concepte d'equació minimal i demostrem l'existència d'aquesta en el teorema de Nèron.

Els capítols 4 i 5 conformen la tercera secció. En aquesta, explicitem la construcció de la corba el·líptica de Frey i en veiem algunes de les seves propietats. Al capítol 4 n'exposem

les propietats més directes i al capítol 5 treballem les propietats del grup format pel conjunt dels punts de n-torsió d'una corba el·líptica. En particular, la ramificació del cos de nombres $\mathbb{Q}(E[n])$, traslladant les eines conegudes en l'anàlisi de les corbes el·líptiques definides sobre $\mathbb{C}$ a corbes definides sobre $\mathbb{Q}_p$ mitjançant la parametrització de Tate i l'aparellament de Weil.

L'última secció del treball, on hi figuren els capítols restants, és on mostrem les aplicacions de la corba de Frey, concretament en la resolució d'equacions diofantines. Al capítol 6 donem una breu introducció a les formes i les funcions modulars, així com a la funció L associada a una corba el·líptica; finalment hi enunciem el teorma de modularitat de Wiles donant-li sentit. El capítol 7 recull resultats potents i essencials de la representació associada als punts de n-torsió d'una corba el·líptica per poder donar un esboç de la demostració del teorema de Fermat al capítol 8. Finalment, apliquem el procediment de la demostració de Fermat a altres equacions diofantines.

La realització d'aquest treball m'ha fet conscient de la gran quantitat de propietats aritmètiques que tenen les corbes el·líptiques. L'esudi d'aquestes, a part de resultar molt bonic, proporciona una eina molt bona per a la investigació en molts camps de recerca actual.

Una altra de les principals conclusions a les que he arribat és que la construcció de la corba de Frey és només una petita part de la demostració del teorema de Fermat, i una part encara més ínfima de l'estudi de la teoria de nombres. Tot i això, la realització d'aquest projecte m'ha permés adonar-me de l'esforç que implica obtenir resultats en aquesta branca de les matemàtiques; es necessiten coneixements profunds de totes les altres branques d'aquesta ciència i, per tant, moltes persones implicades. Ho he vist reflectit en la quantitat de noms de matemàtics que m'he trobat en el camí de la realització del treball i la quantitat de documents i llibres diferents que he hagut de consultar.

D'altra banda, per a l'escriptura d'aquesta memòria, he hagut d'apendre a fixar i aclarir idees per tal de donar sentit a allò que estava escrivint, ja que és molt més dificil plasmar sobre un paper amb claredat allò que un té estructurat en la ment.

Índex

1 Corbes el·líptiques **1**

1.1 Preliminars 1

1.2 Teorema de Riemann-Roch i definició de gènere 3

2 Equació de Weierstrass **7**

2.1 L'equació de Weierstrass 7

2.2 La llei de grup 10

2.3 Forma normal de Legendre 13

3 Corbes el·líptiques semi-estables **15**

3.1 Tipus de reducció 15

3.2 Equació minimal de Weierstrass 17

3.3 Teorema de reducció semi-estable 19

4 La corba de Frey **21**

4.1 Construcció i propietats 21

5 Punts de n-torsió i ramificació **25**

5.1 Corbes el·líptiques sobre $\mathbb{C}$ 25

5.2 Punts de n-torsió 28

5.3 L'aparellament de Weil 29

5.4 La parametrització de Tate 32

5.5 Ramificació en el cas de bona reducció 34

6 Funcions modulars **37**

6.1 Grup modular 37

6.2 Funcions modulars 39

6.3 Formes modulars de pes k 40

6.4 Formes modulars de pes k i nivell N 41

6.5 Funció L de E i teorema de modularitat 43

7 Representacions de Galois **45**

7.1 Representació d'un grup 45
7.2 Representacions associades a una corba el·líptica 46

8 Teorema de Fermat i aplicacions **49**
8.1 Teorema de Fermat 49
8.2 Altres equacions diofantines 50

Capítol 1

Corbes el·líptiques

1.1 Preliminars

En tot el treball, utilitzarem lliurement els conceptes bàsics de geometria, anàlisi o aritmètica que s'han treballat a diferents assignatures del grau. Amb la finalitat, però, d'establir les notacions en mencionarem alguns.

Per a nosaltres, una corba C serà una varietat (algebraica) projectiva de dimensió 1 sobre un cos algebraicament tancat k'; i direm que la corba és definida sobre un cert cos k, subcòs de k', si l'ideal homogeni $I(C) \subseteq k'[X_0, \ldots, X_n]$ és l'extensió d'un ideal de $k[X_0, \ldots, X_n]$; és a dir, si és definit per polinomis de $k[X_0, \ldots, X_n]$. Ho denotem per C/k. Notem que els punts d'una corba projectiva és el conjunt de punts P de $\mathbb{P}^n$ que s'anul·len en tots els polinomis de $I(C)$, és a dir, que $C \subset \mathbb{P}^n$; diem que una corba és plana si $n = 2$. A més a més, diem que un punt de P de C és un punt definit sobre un subcòs K que conté a k si les coordenades de P són de K i dentoem per $C(K)$ al conjunt de punts de C definits sobre K.

L'anell de coordenades de C és l'anell quocient

$$k'[C] = \frac{k'[X_0, \ldots, X_n]}{I(C)},$$

i diem que la corba C és irreductible quan $I(C)$ és un ideal primer, o sigui quan aquest anell és un domini d'integritat; en aquest cas podem considerar el cos de fraccions, $k'(C)$, que anomenarem el cos de les funcions (racionals) definides sobre la corba C.

Siguin $P \in C$ un punt de la corba i $f_1, \ldots, f_m \in k'[X_0, \ldots, X_n]$ un conjunt de generadors de $I(C)$. El concepte de corba llisa (o no singular) en el punt P és manllevat de la geometria analítica i es reflecteix en el fet que la matriu

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{i,j}$$

tingui rang $n - dim(C)$, fet que no depèn del conjunt de generadors de $I(C)$. Diem que C és llisa o no singular si ho és a tot punt P.

A fí d'estudiar la corba localment a l'entorn d'un punt no singular P, és útil considerar l'idel maximal de $k'[C]$

$$M_P := \{f \in k'[C] : f(P) = 0\}$$

i l'anell localitzat en M_P, $k'[C]_P$; es té un isomorfisme

$$\chi : \frac{k'[C]}{M_P} \to k'.$$
$$f \to f(P),$$

Aquest és un anell de valoració discreta i la valoració (normalitzada) de $k'[C]_P$ ve donada per

$$ord_P : k'[C]_P \to \mathbb{N} \cup \infty \cup \{\infty\}$$
$$ord_P(f) = max\{d \in \mathbb{N} : f \in M_P^d\}.$$

Utilitzant que $ord_P(f/g) = ord_P(f) - ord_P(g)$, podem estendre ord_P a $k(C)$,

$$ord_P : k(C) \to \mathbb{Z} \cup \{\infty\}.$$

Les relacions entre corbes diferents seran donades per aplicacions racionals, és a dir, donades C_1, C_2 dues corbes projectives, $C_1 \subset \mathbb{P}^m$ i $C_2 \subset \mathbb{P}^n$. Una aplicació racional de C_1 a C_2 serà una aplicació de la forma

$$\Phi : V_1 \to V_2$$
$$\Phi = [f_0, \ldots, f_n]$$

on $f_0, \ldots, f_n \in k'(C_1)$ tenen la propietat que per a cada $P \in C_1$ on estan $f_0, \ldots f_n$ totes definides $\Phi(P) = [f_0(P), \ldots, f_n(P)] \in C_2$. Diem que Φ és regular en P si existeix una funció $g \in k'(V_1)$ tal que

(a) cada gf_i està definida en P, és a dir, que el denominador de gf_i no s'anul·la en P; i

(b) $(gf_i)(P) \neq 0$ per a algun i.

Definim com a morfisme de corbes a una aplicació racional que és regular en cada punt. Diem que és un isomorfisme si existeix un morfisme tal que compost amb el primer és la aplicació identitat i viceversa. Els mateixos conceptes d'aplicació racional i morfisme es poden definir de manera anàloga per a varietats projectives de dimensió arbitrària.

La següent proposició ens resumeix les propietats bàsiques de les aplicacions entre corbes.

Proposició 1.1.1. (a) *Siguin C una corba i $V \subset \mathbb{P}^N$ una varietat, $P \in C$ un punt llis i $\Phi : C \to V$ una aplicació racional. Aleshores, Φ és regular en P. En particular, si C és llisa, Φ és un morfisme.*

(b) *Sigui $\Phi : C_1 \to C_2$ un morfisme de corbes. Aleshores Φ és constant o exhaustiu. Donada una aplicació no constant definida sobre k de corbes, $\Phi : C_1 \to C_2$, definim $\deg(\Phi) = [k(C_1) : \Phi^* k(C_2)]$; on $\Phi^* : k(C_2) \to k(C_1)$ i $\Phi^* f = f \circ \Phi$, i si Φ és constant definim el grau de Φ com zero.*

(c) *Siguin C_1 i C_2 dues corbes llises i $\Phi : C_1 \to C_2$ una aplicació de grau 1. Aleshores Φ és un isomorfisme.*

Dem. [18] □

1.1.2. Amb les mateixes notacions de la proposició, si tenim $\Phi : C_1 \to C_2$ un morfisme no constant de corbes llises, i prenem un punt $P \in C_1$, aleshores anomenem índex de ramificació de Φ en P a

$$e_\phi = ord_P(\Phi^* t_{\Phi(P)});$$

on $t_{\phi(P)} \in k'(C_2)$ és un uniformitzant en $\Phi(P)$. Observem que, amb aquestes definicions, per a tot $\mathbb{Q} \in C_2$ tenim que

$$\sum_{P \in \Phi^{-1}(Q)} e_\phi(P) = \deg(\Phi).$$

1.2 Teorema de Riemann-Roch i definició de gènere

En aquest punt, donarem les definicions i les proposicions necessàries per entendre l'enunciat del teorema de Riemann-Roch per a corbes llises. Aquest ens permetrà donar la definició del gènere d'una corba i, de fet, tindrà diverses aplicacions al llarg de tot el treball. Comencem amb la definició de divisor d'una corba llisa.

Definició 1.2.1. Sigui C una corba llisa. El grup de divisors de C és el grup abelià lliure de base el conjunt dels punts de C, és a dir, $\mathrm{Div}(C) := \bigoplus_{P \in C} \mathbb{Z}P$. Un divisor de C és, doncs, un element de $\mathrm{Div}(C)$; per tant, té l'aspecte

$$D = \sum_{P \in C} n_P P,$$

on $n_P \in \mathbb{Z}$ i $n_P = 0$ excepte per a una quantitat finita de $P \in C$. El grau de D és la suma dels seus coeficients, és a dir, $\deg(D) = \sum_{P \in C} n_P \in \mathbb{Z}$.

Definició 1.2.2. Donada $f \in k'(C)$, $f \neq 0$, una funció racional no nul·la sobre C, aquesta té una quantitat finita de zeros (punts en els quals s'anul·la el numerador de f) i pols (punts en els quals s'anul·la el denominador de f), comptats amb multiplicitats. El divisor de f és, per definició, $\mathrm{div}(z) = \sum_{P \in C} ord_P(z)P$. Observem que la funció $ord_P(f)$ ens diu si P és un zero o un pol de f i quina multiplicitat té, per tant, el divisor d'una funció racional ens desciru els seus pols i zeros. Anomenem divisor prinipal a tot divisor provinent d'una funció racional sobre C, és a dir, a tot $D \in \mathrm{Div}(C)$ tal que existeix $f \in k'(C)$ i $D = \mathrm{div}(f)$.

Ara, si $K := k'(C)$ i considerem K^* com a grup multiplicatiu, es tenen els morfismes de grups

$$K^* \xrightarrow{\mathrm{div}} \mathrm{Div}(C) \qquad \text{i} \qquad \mathrm{Div}(C) \xrightarrow{\deg} \mathbb{Z},$$

de manera que el divisor del producte de funcions és la suma de divisors, i el grau de la suma de dos divisors és la suma de graus.

Definició 1.2.3. Definim el conjunt

$$L(D) := \{f \in K : ord_P(f) \geq n_P, \forall P \in C\} = \{f \in K : \mathrm{div}(f) + D > 0 \text{ o } f = 0\},$$

on $D = \sum n_P P$; és a dir, és el conjunt de les funcions de K tals que tenen zeros en els punts amb $n_P > 0$, poden tenir zeros en els punts amb $n_P = 0$ i poden tenir pols només en els punts amb $n_P < 0$.

Observació 1.2.4. $L(D)$ és un espai vectorial sobre k'. Per tant, podem considerar la seva dimensió com a espai vectorial, la qual dentotarem $l(D)$, i de fet, aquesta és finita. [10]

Definició 1.2.5. Sigui C una corba llisa i siguin D i D' dos divisors de C. Aleshores definim la relació d'equivalència següent

$$D \sim D' \Leftrightarrow \exists f \in \bar{K}(C) \text{ tal que } \operatorname{div}(f) = D - D'.$$

El quocient de $\operatorname{Div}(C)$ per aquesta relació d'equivalència s'anomena grup de classes de divisors o grup de Picard, i el denotem per $\operatorname{Pic}(C)$. Denotem a més a més les seves classes per $[D]$. Definim a més a més $\operatorname{Div}^0(C) = \{D \in \operatorname{Div}(C) : \deg(D) = 0\}$ el subgrup de $\operatorname{Div}(C)$ format pels divisors de grau zero de C i $\operatorname{Pic}^0(C)$ el quocient de $\operatorname{Div}^0(C)$ per la relació d'equivalència $\sim$.

Observació 1.2.6. De les definicions 1.2.3 i 1.2.5, es veu clarament que la dimensió de l'espai vectorial $L(D)$ no depèn de la classe dequivalència del divisor D. És a dir, si D i D' són dos divisors de C tals que $[D] = [D']$, aleshores $l(D) = l(D')$. Diem que D és un divisor principal si $[D] = [0]$, és a dir, si $D = \operatorname{div}(f)$ per alguna $f \in K$. Observem que com que tota funció racional té la mateixa quantitat de pols que de zeros, aleshores per a tot divisor principal D és té que $\deg \operatorname{div}(D) = 0$.

Per tal de parlar de les diferencials sobre una corba, recordem com es definex el mòdul de les diferencials d'un anell qualsevol R sobre k.

Sigui $k \subset R$ un anell commutatiu i sigui M un R-mòdul. Una derivació de R en M sobre k és una aplicació k-lineal $D : R \to M$ tal que

$$D(xy) = xD(y) + yD(x)$$

per a tot $x, y \in R$.

Per cada $x \in R$, considerem $[x]$ un símbol i el R-mòdul lliure F sobre el conjunt $\{[x]|x \in R\}$, és a dir, $\bigoplus_{x \in R} R \cdot [x]$. Sigui N el submòdul de F generat per la reunió dels següents conjunts d'elements:

(a) $\{[x + y] - [x] - [y]|x, y \in R\}$,

(b) $\{[\lambda x] - \lambda[x]|x \in R, \lambda \in k\}$,

(c) $\{[xy] - x[y] - y[x]|x, y \in R\}$.

Aleshores, $\Omega_k(R) = F/N$ és el mòdul quocient, anomenem dx a la classe residual de $[x]$ en $\Omega_k(R)$ i considerem $d : R \to \Omega_k(R)$ la funció $x \mapsto dx$.

Definició 1.2.7. Definim el R-mòdul $\Omega_k(R)$ com el mòdul de les diferencials de R sobre k, i l'aplicació d és una derivació.

Aleshores, si prenem $R = K = k'(C)$, podem parlar de $\Omega_k(K)$ com del mòdul de les diferencials sobre la corba C.

Proposició 1.2.8. *Si tenim $f, t \in K$, $t \notin k$, existeix un únic $v \in k$ tal que $df = vdt$. Aleshores escrivim $v = \dfrac{df}{dt}$ i anomenem a v la derivada de f respecte t. (En una corba l'espai està generat per un dt).*

Dem. [10] □

Definició 1.2.9. Sigui $\omega \in \Omega_k(K)$, $\omega \neq 0$, aleshores, prenent t un uniformitzant de $k_P[C]$ es té que $\omega = fdt$ per a algun $f \in K$. Aleshores definim $ord_P(\omega) = ord_P(f)$ i $\operatorname{div}(\omega) = \sum ord_P(\omega)$. La classe del divisor $\operatorname{div}(\omega)$ no depen de la diferencial ω escollida, i s'anomena divisor canònic de C a qualsevol divisor W de C tal que $[W] = [\operatorname{div}(\omega)]$.

Teorema 1.2.10. (Riemann-Roch) *Sigui C una corba llisa i W un divisor canònic de C. Aleshores existex un nombre enter positiu g que anomenarem el gènere de C, tal que per a tot divisor C de D se satisfà que*

$$l(D) - l(W - D) = \deg(D) - g + 1.$$

Dem. [10], [13] □

Donem finalment la definició de corba el·líptica.

Definició 1.2.11. Una corba el·líptica és (formalment) una parella (E, O), on E es una corba llisa de gènere 1 i $O \in E$ un punt destacat. Per a simplificar la notació, usualment denotarem la corba el·líptica simplement com E. Diem que E està definida sobre k, i escrivim E/k, si E està definida sobre k com a corba i, a més a més, $O \in E(k) := \{P \in E$ tals que les seves cordenades són de $k\}$.

Capítol 2

Equació de Weierstrass

2.1 L'equació de Weierstrass

L'objetiu d'aquest capítol és fer un estudi bàsic de es corbes el·líptiques i veure que admeten models que són corbes cúbiques planes. Amb aquest propòsit serà útil parlar de les equacions de Weierstrass i les seves formes.

Definició 2.1.1. Sigui k un cos. Anomenarem equació (projectiva) de Weierstrass sobre k a una equació cúbica de la forma

$$W : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

on $a_i \in k$, $\forall i$ (notem la numeració dels índexs). Aleshores podem considerar la corba C_W de $\mathbb{P}^2$ definida per aquesta equació amb un sol punt a la recta de l'infinit; el $O = [0, 1, 0]$.

Per facilitar la notació treballarem amb coordenades no-homogènies, és a dir, amb $X = x/z$ i $Y = y/z$, de manera que l'equació W de la corba C_W es transforma en l'equació (afí) de Weierstrass

$$W : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Proposició 2.1.2. *Sigui C_W una corba donada per una equació de Weierstrass W i suposem que té una singularitat; aleshores, existeix una aplicació biracional $\Phi : E \to \mathbb{P}^1$ de grau 1.*

Dem. Fent un canvi de variables lineal podem assumir que el punt sigular de C_W és el $(0, 0)$. Mirant les derivades parcials en $(0, 0)$ veiem que $a_3 = a_4 = a_6 = 0$, i per tant que l'equació de W ha de ser de la forma $Y^2 + a_1XY = X^3 + a_2X^2$. Aleshores, l'aplicació

$$\begin{aligned} \Phi : E &\to \mathbb{P}^1 \\ (x, y) &\mapsto [x, y] \end{aligned}$$

és una aplicació racional de grau 1 amb inversa

$$\begin{aligned} \Phi^{-1} : \mathbb{P}^1 &\to E \\ [1, t] &\mapsto (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t). \end{aligned}$$

□

Estem en disposició de demostrar que tota corba el·líptica admet un model de Weierstrass.

Teorema 2.1.3. *Sigui E una corba el·líptica sobre k.*

(a) *Existeixen funcions $x, y \in k'(E)$ tals que l'aplicació*

$$\Phi : E \to \mathbb{P}^2, \qquad \Phi = [x, y, 1],$$

és un isomorfisme de E/k a una corba donada per una equació de Weierstrass W:

$$C_W : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

de coeficients $a_1, \dots a_6 \in k$, i tal que $\Phi(O) = [0, 1, 0]$.

(b) *Dues equacions qualssevol de Weierstrass per a E com en (a) estan relacionades per un canvi lineal de la forma*

$$X \mapsto u^2X + r, \qquad Y \mapsto u^3Y + su^2X + t;$$

amb $u, r, s, t \in k$, $u \neq 0$.

(c) *Tota corba llisa donada per una equació de Weierstrass sobre k és una corba el·líptica sobre k amb origen $O = [0, 1, 0]$.*

Dem.

(a) El teorema de Riemann-Roch (1.2.10) ens diu que, per a $g = 1$ és $l(nO) = \dim(L(nO)) = n$; per tant, podem escollir $\{1, x\}$ de tal forma que sigui base de $L(2O)$ i $\{1, x, y\}$ que sigui base de $L(3O)$. Així, x ha de tenir un pol d'orde 2 en O i y un pol d'ordre 3 en O. Ara, $L(6O)$ té dimensió 6, però conté 1, x, y, x^2, xy, y^2, x^3, que són 7 elements. Per tant, han d'existir $A_1, \dots, A_7 \in k$ amb algun $A_i \neq 0$ tal que

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0.$$

A més a més, $A_6A_7 \neq 0$, ja que en cas contrari cada terme tindria un pol d'ordre diferent en O, d'on obtindríem que $A_j = 0\ \forall j$. Ara, fent el canvi de variables x, y per $-A_6A_7x$, $A_6A_7^2y$ i dividint la igualtat per $A_6^3A_7^4$, obtenim una equació de Weiestrass. Aleshores podem considerar l'aplicació

$$\Phi : E \to \mathbb{P}^2$$
$$\Phi = [x, y, 1],$$

la imatge de la qual està sobre la corba C_W definida per W. A més a més, utilitzant 1.1.1, Φ és un morfisme exhaustiu tal que $\Phi(O) = [0, 1, 0]$.

A continuació hem de veure que $k'(E) = k'(x, y)$, que és equivalent a veure que $[k'(E) : k'(x, y)] = 1$ que per definició és $\mathrm{gr}(\Phi)$. Si considerem les aplicacions $[x, 1] : E \to \mathbb{P}^1$ i $[y, 1] : E \to \mathbb{P}^1$, com que x i y són funcions amb únic pol d'ordre 2 i 3 respectivament, per 1.1.2 sabem que tenen graus 2 i 3 respectivament. Així, $[k'(E) : k'(x)] = 2$ i $[k'(E) : k'(y)] = 3$; i com que $[k'(E) : k'(x, y)]$ ha de dividir als dos ha de ser $[k'(E) : k'(x, y)] = 1$.

Finalment, per provar (a) ens falta veure que C_W és llisa. Suposem que no fos així. Aleshores utilitant 2.1.2 sabem que existeix una aplicació $\Psi : C_W \to \mathbb{P}^1$ de grau 1. En compondre Φ i Ψ obtindríem una aplicació $\Psi \circ \Phi : E \to \mathbb{P}^1$ de grau 1 entre dues corbes llises; és a dir, un isomorfisme. Però això entraria en contradicció amb que E té gènere 1 i $\mathbb{P}^1$ gènere 0. Per tant C_W és una corba llisa i en conseqüència Φ és un isomorfisme entre E i C_W.

(b) Prenem x, y i x', y' dues parelles de funcions coordenades de Weierstrass de E; de manera que x i x' tinquin un pol d'ordre 2 en O i y i y' tenen un pol d'ordre 3 en O. Aleshores $\{1, x\}$ i $\{1, x'\}$ son dues bases de $L(2O)$, i $\{1, x, y\}$ i $\{1, x', y'\}$ son dues bases de $L(3O)$; per tant existeixen constants $u_1, u_2, r, s_2, t \in K$ amb $u_1 u_2 \neq 0$ tal que

$$x = u_1 x' + r\,, \qquad y = u_2 y' + s_2 x' + t.$$

Ara utilitzant que (x, y) i (x', y') satisfan equacions de Weierstrass on els termes Y^2 i X^3 tenen coeficient 1 obtenim que $u_1^3 = u_2^2$, de manera que prenent $u = u_2/u_1$ i $s = s_2/u^2$ assolim el canvi de variables desitjat.

(c) Sigui C_W la corba donada per una equació de Weierstrass W sense singularitats. La diferencial $\omega = dx/(2y + a_1 x + a_3)$ no té pols ni zeros. Així doncs, per definició, $\mathrm{div}(\omega) = 0$; i aplicant el teorema de Riemann-Roch (1.2.10) tenim que $2\mathrm{gen}(C_W) - 2 = \deg(\mathrm{div}(\omega)) = 0$, d'on treiem que el gènere de $C_W = 1$.

□

Observació 2.1.4. Observem que els canvis de variables de (b) ens donen les fórmules següents.

$ua_1' = a_1 + 2s,$

$u^2 a_2' = a_3 - sa_1 + 3r - s^2,$

$u^3 a_3' = a_3 + ra_1 + 2t,$

$u^4 a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,$

$u^6 a_6' = a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1;$

on els a_i' són els coeficints de l'equació de Weiestrass resultants del canvi.

Per tant, a partir d'ara, per treballar amb E corba el·líptica ens referirem directament a alguna de les seves expressions com a equació de Weierstrass. Si k és un cos de característica diferent de 2 i 3, i tenim E/k una corba el·líptica amb equació de Weierstrass

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

podem manipular aquesta per obtenir equacions equivalents més senzilles o amb les quals ens sigui millor treballar (com que usualment treballarem amb k cos de característica zero, podrem utilitzar aquestes transformacions sense problema). Així doncs, recordant que els únics canvis de variable que ens relacionen dues equacions de Weierstrass de E són del tipus $X \mapsto u^2 X + r$, i $Y \mapsto u^3 Y + su^2 X + t$; procedim de la següent forma.

Com que $\mathrm{car}(k) \neq 2$ podem fer el canvi $X \mapsto X$, $Y \mapsto Y - \frac{a_1}{2} X - \frac{a_3}{2}$; obtenint així una equació del tipus

$$Y^2 = X^3 + \tfrac{b_1}{4} X^2 + \tfrac{b_2}{2} X + \tfrac{b_3}{4},$$

on

$$\begin{aligned} b_1 &= 4a_2 + a_1^2, \\ b_2 &= 2a_4 + a_1 a_3, \\ b_3 &= 4a_6 + a_3^2. \end{aligned}$$

Ara, com que $\text{car}(k) \neq 3$ fem el canvi $X \mapsto X + \frac{b_2}{12}$, i $Y \mapsto Y$ de manera que l'equació es transforma en la forma anomenada normal de Weierstrass

$$W_E : Y^2 = X^3 - g_2X - g_3,$$

on

$$g_2 = \frac{b_1^2 - 24b_2}{48}, \quad g_3 = \frac{-b_1^3 + 36b_1b_2 - 216b_3}{864}.$$

Si a aquesta última equació fem el canvi $X \mapsto X$, $Y \mapsto \frac{Y}{2}$ aleshores recuperem la forma clàssica de Weierstrass

$$Y^2 = 4X^3 - g_2'X - g_3',$$

on $g_2' = 4g_2$ i $g_3' = 4g_3$. Aquesta úlima expressió és la més convenient quan es realitza l'estudi analític de les corbes el·líptiques sobre $\mathbb{C}$. És per això que l'utilitzarem més endavant.

Definició 2.1.5. Siguin E una corba el·líptica i $W_E : Y^2 = X^3 - g_2X - g_3$ una forma normal de Weierstrass; el discriminant de l'equació cúbica és $\Delta_W := 4g_2^3 - 27g_3^2$, que coincideix amb el discriminiant del polinomi $X^3 - g_2X - g_3$, i com que E és llisa, veurem en el capítol 3 que es té $\Delta \neq 0$. Definim el discriminant de E com $\Delta := g_2'^3 - 27g_3'^2$. Aleshores, per les relacions descrites tenim que $\Delta = 16\Delta_W$; per tant, podem utilitzar els dos indiscriminadament per veure si una corba donada per una equació de Weierstrass és llisa o no ho és. Definim, a més a més l'invariant j_E de E com $j_E := \dfrac{12^3 4g_2^3}{\Delta_W} = \dfrac{12^3 g_2'^3}{\Delta}$ i, en el cas que $j_E \neq 0, 12^3$, l'invariant de Hasse de E com $\delta_E := -\dfrac{1}{2}\dfrac{g_2}{g_3} \pmod{\mathbb{Q}^{*2}}$.

Observació 2.1.6. Els únics canvis que respecten la forma normal de Weierstrass són els de la forma $X \mapsto \alpha X$, $Y \mapsto \beta Y$ amb $\alpha^3 = \beta^2$; és a dir, $X \mapsto \lambda^2 X$, $Y \mapsto \lambda^3 Y$, amb $\lambda \in k^*$. Amb aquests canvis, $g_2 \mapsto \lambda^4 g_2$ i $g_3 \mapsto \lambda^6 g_3$, i els invariants j_E i Δ es transformen en $j_E \mapsto j_E$ i $\Delta \mapsto \lambda^{12} = 1728\Delta$.

2.2 La llei de grup

Ara, sigui E una corba el·líptica. Utilitzant la suma natural de $\text{Pic}(E)$ i el teorema de Riemann-Roch, veurem que podem donar estructura de grup als punts de E.

Proposició 2.2.1. *Sigui E una corba el·líptica amb O el seu punt de l'infinit.*

(a) *Siguin $P, Q \in E$. Si considerem els punts com a divisors, $D := P$ i $D' := Q$, aleshores*

$$D \sim D' \Leftrightarrow P = Q.$$

(b) *Per a cada divisor $D \in \text{Div}^0(E)$ existeix un únic punt $P \in E$ tal que $D \sim P - O$. Sigui $\sigma : \text{Div}^0(E) \to E$ l'aplicació donada per aquesta associació.*

(c) *σ és una aplicació exhaustiva.*

(d) *Siguin $D_1, D_2 \in \text{D}^0(E)$. Aleshores*

$$\sigma(D_1) = \sigma(D_2) \Leftrightarrow D_1 \sim D_2.$$

Per tant, σ indueïx a una aplicació bijectiva $\bar{\sigma} : \mathrm{Pic}^0(E) \to E$.

(e) *L'aplicació inversa $\bar{\sigma}^{-1}$ ve donada per*

$$\begin{aligned} \bar{\sigma}^{-1} : E &\to \mathrm{Pic}^0(E) \\ P &\to [P - O] \end{aligned}$$

Dem.

(a) Suposem que $D \sim D'$. Aleshores existeix una $f \in k'(E)$ tal que $\mathrm{div}(f) = D - D' = P - Q$. Per tant, $f \in L(D')$, però pel teorema de Riemann-Roch (1.2.10), $l(D') = l(Q) = 1$. És a dir, que $f \in k'$, ja que $L(Q)$ ja conté el cos de constants, i $P = Q$.

(b) Com que E és una corba de gènere 1, pel teorema de Riemann-Roch 1.2.10 sabem que $l(D + O) = 1$. Prenem f un generador d'aquest espai. Com que $\mathrm{div}(f) \geq -D - O$ i $\deg(\mathrm{div}(f)) = 0$, llavors $\mathrm{div}(f) = -D - O + P$ per a algun $P \in E$; i per tant, $D \sim P - O$ fet que prova l'existència. Per veure la unicitat, suposem que existeix un $P' \in E$ tal que $D \sim P' - O$. Aleshores, $P \sim D + O \sim P'$ i, per l'apartat (a), $P = P'$ i això prova la unicitat.

(c) Per a qualsevol $P \in E$ es té que $\sigma(P - O) = P$.

(d) Siguin $D_1, D_2 \in \mathrm{D}^0(E)$ i prenem $P_i = \sigma(D_i)$. Per la definició de σ tenim que $P_1 - P_2 \sim D_1 - D_2$, ergo, que si $P_1 = P_2$, aleshores $D_1 \sim D_2$. De la mateixa manera, si $D_1 \sim D_2$ aleshores $P_1 \sim P_2$, i per (a), $P_1 = P_2$.

(e) Si considerem les composicions $\sigma \circ \sigma^{-1}$ i $\sigma^{-1} \circ \sigma$, és obvi que obtenim les identitats.

□

Corol·lari 2.2.2. *Sigui E una corba el·liptica i $D = \sum n_P(P) \in \mathrm{Div}(E)$. Aleshores D és principal si i només si $\sum n_P = 0$ i $\sum [n_P]P = O$.*

Dem. Ja hem vist que si D és un divisor principal, aleshores $\deg(D) = 0$. Per tant, $D \in \mathrm{Div}^0(E)$ i

$$D \sim 0 \Leftrightarrow \sigma(D) = O \Leftrightarrow \textstyle\sum [n_P]\sigma((P) - (O)) = O,$$

que és el que volíem ja que $\sigma((P) - (O)) = P$. □

Aquesta suma es pot veure, geomètricament, de la manera següent.

Definició 2.2.3. Sigui E una corba el·líptica donada per una equació de Weierstrass W i siguin $P, Q \in E$. Sigui L la recta que uneix P i Q, o, si $P = Q$, la recta tangent a E que passa per P, i anomenem R al tercer punt d'intersecció de L amb E. Sigui L' la recta que conecta R i O. Aleshores, definim la suma $P \oplus Q$ com el punt tal que L' interseca a R, O i a $P \oplus Q$.

Proposició 2.2.4. *La suma definida per $\oplus$ conincideix amb la suma induïda de Pic^0 per $\bar{\sigma}$.*

Dem. Clarament, és suficient veure que $\bar{\sigma}^{-1}(P \oplus Q) = \bar{\sigma}^{-1}(P) + \bar{\sigma}^{-1}(Q)$. Veiem-ho. Sigui

$$f(X,Y,Z) = \alpha X + \beta Y + \gamma Z = 0$$

la recta L de $\mathbb{P}^2$ que conté a P i Q, i sigui R el tercer punt d'intersecció de L amb E. Sigui L' la recta de $\mathbb{P}^2$ que conté a R i O, donada per

$$f'(X,Y,Z) = \alpha' X + \beta' Y + \gamma' Z = 0.$$

Donat que la recta $Z = 0$ interseca a E en O amb multiplicitat 3, tenim que $\mathrm{div}(f/Z) = P + Q + R - 3O$ i que $\mathrm{div}(f'/Z) = R + (P \oplus Q) - 2O$. Per tant,

$$(P \oplus Q) - P - Q + O = \mathrm{div}(f/f') \sim 0,$$

d'on obtenim que

$$\sigma^{-1}(P \oplus Q) - \sigma^{-1}(P) - \sigma^{-1}(Q) = 0,$$

com volíem. □

Corol·lari 2.2.5. *Propietats de $\oplus$:*

(a) Si L recta interseca a tres punts de E (no necessàriament diferents), aleshores $(P \oplus Q) \oplus R = O$.

(b) $P \oplus O = P$ per a tot $P \in E$.

(c) $P \oplus Q = Q \oplus P$.

(d) Sigui $P \in E$. Existeix un punt de E, que denotarem $\ominus P$ tal que $P \oplus (\ominus P) = O$.

(e) Siguin $P, Q, R \in E$. Aleshores $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

(f) Si P i Q són punts k-racionals de E, (és a dr, de coordenades en k), aleshores $P \oplus Q$ també és k-racional.

En definitiva, E amb l'operació $\oplus$ té estructura de grup commutatiu amb element neutre O, i els punts k-racionals de E formen un subgrup de E amb aquesta operació.

Observació 2.2.6. Per simplificar la notació, a partir d'ara utilitzarem $+$ i $-$ per simbolitzar $\oplus$ i $\ominus$ respectivament. Així doncs, si tenim $m \in \mathbb{Z}$ i $P \in E$, escrivim el morfisme multipliar per m com

$$[m]P = P + \cdots + P, \text{ per a } m > 0,\ [0]P = O \text{ i } [m]P = [-m](-P), \text{ per a } m < 0.$$

Observació 2.2.7. Sigui E una corba el·líptica donada per una equació de Weierstrass

$$W : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

(a) Sigui $P_0 = (x_0, y_0) \in E$, $P_0 \neq 0$. Aleshores $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.

(b) Donats $P_1, P_2 \in E$, $P_1 = (x_1, y_1) \neq (0,0)$ i $P_2 = (x_2, y_2) \neq (0,0)$, les fòrmules d'addició que es dedueixen proporcionen que $P_1 + P_2 = P_3 = (x_3, y_3)$, on

(i) $P_1 + P_2 = O$, si $x_1 = x_2$ i $y_1 + y_2 + a_1x_2 + a_3 = 0$.

(ii)

$$x_3 = \alpha^2 + a_1\alpha - a_2 - x_1 - x_2 \text{ i } y_3 = -(\alpha + a_1)x_3 - \beta - a_3$$

i

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1} \text{ i } \beta = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \text{ si } x_1 \neq x_2$$
$$\alpha = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \text{ i } \beta = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \text{ si } x_1 = x_2.$$

$Y = \alpha X + \beta$ és la recta per P_1 i P_2, o tangent en el cas que $P_1 = P_2$.

Corol·lari 2.2.8. *Un cas especial de les fórmules d'addició és la fórmula de duplicació, on podem escriure la coordenada x de $[2]P$ com*

$$x([2]P) = \frac{x^4 - b_2x^2 - 2b_3x - b_4}{4x^3 + b_1x^2 + 2b_2x + b_3},$$

on $P = (x, y)$, b_1, b_2, b_3 són els construïts anteriorment i $b_4 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

2.3 Forma normal de Legendre

Sigui E una corba el·líptica sobre k un cos de característica diferent de 2. Prenem l'equació de Weiestrass de E en forma normal donada per

$$W_E : Y^2 = X^3 + g_2X + g_3.$$

Com que k' és algebraicament tancat, el polinomi cúbic $X^3 + g_2X + g_3$ té tres arrels en k'; factoritzant-lo, obtenim

$$Y^2 = (X - e_1)(X - e_2)(X - e_3);$$

i com que $\Delta \neq 0$ i el discriminant del polinomi cúbic és 16Δ, aquest també és diferent de zero, i per tant els e_1 són tots diferents. Ara fent la substitució

$$X \mapsto (e_2 - e_1)X + e_1 \qquad \text{i} \qquad Y \mapsto (e_2 - e_1)^{3/2}Y,$$

W es transforma en

$$Y^2 = X(X - 1)(X - \lambda),$$

on $\lambda = \dfrac{e_3 - e_1}{e_2 - e_1} \in k'$ i $\lambda \neq 0, 1$.

Capítol 3

Corbes el·líptiques semi-estables

3.1 Tipus de reducció

En general, a partir d'aquest punt treballarem amb corbes el·líptiques definides sobre $\mathbb{Q}$ a no ser que indiquem el contrari. Una eina molt efectiva per estudiar-les és la teoria de la reducció. Donem abans, però, un resultat auxiliar de les corbes donades per equacions de Weierstrass.

Definició 3.1.1. Sigui C_W una corba donada per una equació de Weierstrass W amb una singularitat en $P \in C_W$. Diem que P és un node si existeixen dues rectes tangents diferents a C_W per P, i diem que P és una punta si existeix una única recta tangent a C_W per P.

Proposició 3.1.2. *Sigui C_W una corba donada per una equació de Weierstrass W sobre $\mathbb{Q}$. Aleshores és té la classificació següent.*

(a) *C_W és llisa si i només si $\Delta \neq 0$.*

(b) *C_W té un node si i només si $\Delta = 0$ i $g_2 \neq 0$.*

(c) *C_W té una punta si i només si $\Delta = g_2 = 0$.*

Dem. Escrivim

$$C_W : f_W(X,Y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 = 0.$$

Començarem provant que el punt de l'infinit no és singular. Això és fàcil considerant

$$F_W[X,Y,Z] = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

Aleshores, recordant que $O = [0,1,0]$, tenim que

$$\tfrac{\partial F}{\partial Z}(O) = 1 \neq 0;$$

per tant, O és un punt llis de C_W. Suposem ara que C_W és singular en $P = (x_0, y_0)$. Aleshores, la substitució $X \mapsto X + x_0$, $Y \mapsto Y + y_0$ porta el punt P al $(0,0)$ i deixa δ i g_2 invariants. Per tant, podem suposar que $P = (0,0)$. Aleshores, com que, per ser P singular,

$$a_6 = f_W(0,0) = 0,\ a_4 = \tfrac{\partial f_W}{\partial X}(0,0) = 0 \text{ i } a_3 = \tfrac{\partial f_W}{\partial Y}(0,0) = 0,$$

f_W és de la forma

$$f_W : Y^2 + a_1XY - a_2X^2 - X^3$$

i és clar que $\Delta = 0$. Ara, si considerem el desenvolupament de Taylor de f_W en $(0,0)$, tenim que

$$f_W(X,Y) = (Y + \alpha X)(Y - \beta X) - X^3.$$

Per tant $Y + \alpha X = 0$ i $Y - \beta X = 0$ són les rectes tangents a C_W en $(0,0)$; és a dir que, per definició, C_W tindrà un node a $(0,0)$ si $\alpha \neq \beta$, i una punta si $\alpha = \beta$. Però això equival a dir que $Y^2 + a_1XY - a_2X^2$ tingui dos zeros diferents o un zero doble, és a dir que el discriminant d'aquesta equació quadràtica que és $a_1^2 + 4a_2$ sigui igual a zero o diferent de zero respectivament. Però com que $g_2 = (a_1^2 + 4a_2)^2/27$, és equivalent a dir que g_2 és diferent o igual a zero.

Per tant, ara només ens falta provar que si C_W és llisa, aleshores $\Delta \neq 0$. Prenem W en la forma

$$Y^2 = 4X^3 + b_1X^2 + b_2X + b_3.$$

Aleshores, un punt (x,y) de C_W és singular si $2y = 12x^2 + 2b_1x + b_2 = 0$, és a dir si és de la forma $(x,0)$, amb x arrel doble de $4X^3 + b_1X^2 + b_2X + b_3$, però aquesta equació cúbica té una arrel doble si i només si el seu discriminant, que coincideix amb 16Δ és zero. A més a més, com que cap cúbica no pot tenir dues arrels dobles, C_W només pot tenir un punt singular; i amb això, acaba la demostració. □

Considerem ara E una corba el·líptica donada per una equació de Weierstrass general

$$W : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

de coeficients $a_1, \ldots, a_6 \in \mathbb{Z}$, i sigui ℓ un nombre primer. Aleshores, definim la reducció de E mòdul ℓ com la corba donada per l'equació

$$W(\ell) : Y^2 + \overline{a_1}XY + \overline{a_3}Y = X^3 + \overline{a_2}X^2 + \overline{a_4}X + \overline{a_6},$$

on $\overline{a_i}$ és la classe residual de a_i en $\mathbb{F}_\ell = \mathbb{Z}/\mathbb{Z}\ell$. Òbviament, $W(\ell)$ torna a ser una equació de Weierstrass, per tant, pel teorema anterior, podem tenir tres situacions diferents.

- Bona reducció. És el cas en que $E(\ell)$ torna a ser una corba el·líptica, és a dir, que és llisa. En aquest cas, $v_\ell(\Delta) = 0$.

- Reducció multiplicativa. És el cas en què $E(\ell)$ té un node.

- Reducció additiva. És el cas en què $E(\ell)$ té una punta.

Donem una caracterització de la reducció multiplicativa que ens serà útil.

Proposició 3.1.3. *Sigui ℓ un nombre primer dieferent de 2 i de 3. $E(\ell)$ té reducció multiplicativa si i només si $v_\ell(j_E) < 0$ i l'extensió $\mathbb{Q}(\sqrt{\delta_E})|\mathbb{Q}$ és no ramificada en ℓ.*

Dem. Suposem que $E(\ell)$ te reducció multiplicativa. Per la definició, $j_E = \frac{12^3 4 g_2^3}{\Delta_W} = \frac{12^3 4^3 g_2^3}{\Delta}$. Ara, com que $\ell \neq 2, 3$, podem escriue $E(\ell)$ en la seva forma normal de Weierstrass de manera que es té $v_\ell(12^3 4^3 g_2^3) \leq 0$ i $v_\ell(\Delta) > 0$, i per tant, $v_\ell(j_E) < 0$. Ara, per la definició $\delta_E = -\frac{1}{2}\frac{g_2}{g_3}$ (mod $\mathbb{Q}^{*2}$) en el cas que $j_E \neq 0, 12^3$. Per tant, el discriminant de $\mathbb{Q}(\sqrt{\delta_E})$ serà $2g_2g_3$ o bé $8g_2g_3$. Com que $\ell \neq 2$ i $\ell \nmid g_2$, per veure que $\mathbb{Q}(\sqrt{\delta_E})|\mathbb{Q}$ és no ramificada en ℓ només hem de verue que $\ell \nmid g_3$. Però si $\ell | g_3$, com que $\ell|\Delta$ tindriem $\ell|\Delta + 27g_3^2$, i per tant que $\ell|4g_2^3$; i per tenir

$\ell \neq 2$ $\ell | g_2$ que contradiu que $E(\ell)$ tingui reducció multiplicativa en ℓ. Veiem el recíproc. Per a això hem de veure que $v_l(\Delta) > 0$ i que $v_l(g_2) = 0$. La primera condició és clara del fet que $v_\ell(j_E) = v_\ell(\frac{12^3 4^3 g_2^3}{\Delta}) < 0$ ($\ell \neq 2, 3$); la segona és clara de què $\mathbb{Q}(\sqrt{\delta_E})|\mathbb{Q}$ és no ramificada en ℓ, ja que si no fos així, és a dir, si $\ell | g_2$, aleshores ℓ dividiria el discriminant de l'extensió qudràtica i, per tant, no podria ser no ramificada.

□

Proposició 3.1.4. (Teorema de reducció semi-estable) *Siguin ℓ un nombre primer diferent de 2 i diferent de 3, i $E(\ell)$ una corba el·líptica sobre $k := \mathbb{Q}_l$.*

(a) *Sigui K'/k una extensió no ramificada. Aleshores, el tipus de reducció de E sobre K és el mateix que el tipus de reducció sobre K'.*

(b) *Sigui K'/k una extensió finita. Si E te bona reducció o reducció multiplicativa sobre k, aleshores E te el mateix tipus de reducció sobre K'*

(c) *Existeix una extensió finita K'/K tal que E només te bona reducció o reducció multiplicativa sobre K'.*

Aquest teorema motiva la definició següent.

Definició 3.1.5. Sigui E una corba el·líptica definida per una equació de Weierstras de coeficients a $\mathbb{Z}$. Donat un nombre primer p diem que E té reducció semi-estable mòdul p si E té bona reducció o reducció de tipus multiplicatiu mòdul p.

3.2 Equació minimal de Weierstrass

Per veure la demostració del teorema de reducció semi-estable, necessitem el concepte de corba minimal de Weierstrass. Siguin, doncs, p un nombre primer i E una corba el·líptica sobre $\mathbb{Q}$ donada per l'equació

$$C_W : Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 = 0.$$

Considerem l'anell dels nombres p-enters, és a dir $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} : |x|_p \leq 1\}$. Aleshores diem que l'equació C_W és p-entera si els a_i són p-enters.

Definició 3.2.1. Diem que C_W és minimal en p si és p-entera i $v_p(\Delta_W)$ és mínim d'entre els $\Delta_{W'}$ tal que $C_{W'}$ és una equació equivalent a C_W per un canvi de coordenades de coeficients en $\mathbb{Q}$ i $C_{W'}$ és p-entera.

Lema 3.2.2. *Siguin p un nombre primer diferent de 2 i diferent de 3, i E una corba el·líptica definida sobre $\mathbb{Q}$ donada per*

$$W : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

(a) *W es pot transformar en una equació minimal W' en p mitjançant un canvi de coordenades de coeficients en $\mathbb{Q}$.*

(b) *Si els coeficients de W són p-enters, els nous coeficients del canvi de coordenades del punt anterior també ho són.*

(c) *Dues equacions minimals en p de E estan relacionades per un canvi de coordenades tal que* $|u|_p = 1$ *i* r, s, *i* t *són p-enters.*

Dem. Per hipòtesis, $p > 3$.

(a) Com que podem suposar que W té coeficients enters, tenim que $|\Delta_W|_p \leq 1$; i com que $|\Delta_W|_p > 0$, només hi ha una quantitat finita de possibilitats per a $|\Delta_{W'}|_p$ entre Δ_W i 1, ja que $|\cdot|_p$ és discret. Per tant, l'existència queda provada.

(b) Si la nova equació és minimal en p, com que $u^{12}\Delta_{W'} = \Delta_W$, sabem que $|u|_p \leq 1$. Ara, si a'_i són els coeficients de la nova equació, tenim $u^2 a'_2 = a_3 - sa_1 + 3r - s^2$ i $u^3 a'_3 = a_3 - ra_1 + 2t$, i per tant $r, s, t \in \mathbb{Z}_{(p)}$.

(c) Ara, si W i W' són equacions minimals en p, i considerem el canvi de coordenades que ens transforma W en W', hem vist en (b) que $|u|_p \leq 1$. Ara, si considerem la transformació inversa, de manera anàloga obtenim que $|u^{-1}|_p \leq 1$. Per tant ha de ser $|u_p| = 1$.

□

Definició 3.2.3. Sigui E una corba el·líptica donada per l'equació de Weierstrass

$$W : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Diem que W és minimal (o globalment minimal) si

(i) l'equació W està definida sobre $\mathbb{Z}$.

(ii) Per a cada p primer, W és minimal en p.

Per provar que tota corba el·líptica E admet una equació minimal farem servir el teorema d'aproximació següent, conseqüència del teorema xinès del residu.

Teorema 3.2.4. *Siguin* $p_1, \ldots, p_n$ *un conjunt de nombres primers i* $\epsilon_1, \ldots, \epsilon_n$ *nombres reals positius. Siguin* $x_1, \ldots, x_n \in \mathbb{Z}_{(p)}$. *Aleshores existeix un* $x \in \mathbb{Z}$ *tal que* $|x - x_i|_{p_i} \leq \epsilon_i$ *per a tot i.*

Teorema 3.2.5. (Teorema de Néron) *Donada una corba el·líptica E sobre* $\mathbb{Q}$ *per una equació de Weierstrass W, aleshores existeix un canvi de coordenades (sobre* $\mathbb{Q}$*) que transforma W en una equació minimal.*

Dem. Si tenim

$$W : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

podem suposar que $a_i \in \mathbb{Z}$, de manera que $\Delta_W \in \mathbb{Z}$. Sigui p un nombre primer que divideixi Δ_W, aleshores poem fer un canvi de coordenades donat per $\{u_p, r_p, s_p, t_p\}$ de manera que la nova equació W_p, amb coeficients $a_{i,p}$, és minimal en p. Sabem, doncs que $u_p, r_p, s_p, t_p \in \mathbb{Z}_{(p)}$ i que $|u_p|^{12}|\Delta_{W_p}|_p = |\Delta_W|_p$. Ara, per el lema anterior podem escriure $u_p = p^{n_p}k_p$ amb $k_p \in \mathbb{Z}_{(p)}$, $|k_p|_p = 1$ i $n_p \geq 0$. Prenem $u = \prod_{p|\delta_W} p^{n_p} \in \mathbb{N}$ com a primer coeficient del canvi de coordenades. D'aquesta manera, si p divideix Δ_W i W' és la nova equació, tenim

$$|\Delta_{W'}|_p = |u|_p^{-12} = |u_p|_p^{-12}|\Delta_W|_p = |\Delta_p|_p.$$

Com que, a més a més, $|\Delta_{W'}|_\ell = 1$ si ℓ no divideix Δ_W, la nova equació és minimal si els coeficients d'aquesta, a'_i són enters. Per verue això, escollim, mitjançant el teorema anterior, r, s, t enters de manera que

$$|r - r_p|_p \leq p^{-6n_p},\ |s - s_p| \leq p^{-6n_p},\ |t - t_p|_p \leq p^{-6n_p}.$$

Aleshores les formules el canvi de coordenades del capítol 2 (Observació 2.1.4) mostren que els a'_i són enters, ja que per la propietat ultramétrica de $|\cdot|_p$ tenim que $|a'_i|_\ell \leq 1$ per a tot ℓ primer. □

3.3 Teorema de reducció semi-estable

Vist el concepte de d'equació minimal i l'existència d'aquesta, anem a veure la demostració del teorema de reducció semi-estable.

Dem. (Teorema de reducció semi-estable)

(a) Sigui

$$E : Y^2 = X^3 + AX + B$$

una equació minimal sobre k de E. Siguin $\mathcal{O}'$ l'anell dels enters de K' , v'_ℓ l'extensió de v_ℓ a K' i

$$X \mapsto u'^2 X\,, \qquad Y \mapsto u'^3 Y$$

un canvi de coordenades que doni una equació minimal de E sobre K'. Com que K'/k és no ramificada, podem trobar $u \in k$ amb $u/u' \in (\mathcal{O}')^*$. Aleshores la substitució

$$X \mapsto u^2 X\,, \qquad Y \mapsto u^3 Y$$

també dona una equació minimal per a E/K', ja que $v'_\ell(u^{-12}\Delta) = v'_\ell((u')^{-12}\Delta)$. Però aquesta nova equació té coeficients en $\mathcal{O}$, i, per la minimalitat de l'equació original sobre k tenim que $v_\ell(u) = 0$. Per tant, l'equació inicial ja era minimal sobre K'; i per ser v'_ℓ una extensió de v_ℓ podem concloure que E té el matiex tipus de reducció sobre k i sobre K'.

(b) Prenem una equació minimal de Weierstrass per E sobre k. Siguin

$$X \mapsto u^2 X + r\,, \qquad Y \mapsto u^3 Y^2 + su^2 X + t$$

un canvi de coordenades que doni una equació minimal de Weierstrass sobre K'. Per a aquesta nova equació els Δ' i g'_2 associats satisfan la desigualtat

$$0 \leq v'_\ell(\Delta') = v'_\ell(u^{-12}\Delta) \quad \text{i} \quad 0 \leq v'_\ell(g'_2) = v'_\ell(u^{-4} g_2).$$

Ara, com que $u^{12}\Delta' = \Delta$ i $v_\ell(\Delta') = v_\ell(\Delta)$, aleshores tenim que $v_\ell(u) \geq 0$ i, per tant, $u \in \mathcal{O}'$, amb la qual cosa $0 \leq v'_\ell(u) \leq \min\{\frac{1}{12} v'_\ell(\Delta), \frac{1}{4} v'_\ell(g_2)\}$. Però pel cas de bona reducció (resp. reducció multiplicativa) tenim que $v_\ell(\Delta) = 0$) (resp. $v_\ell(g_2) = 0$). Per tant, en ambdós casos $v'_\ell(u) = 0$ i $v'_\ell(\Delta') = v'_\ell(\Delta)$, $v'_\ell(g'_2) = v'_\ell(g_2)$, fet que ens manté el tipus de reducció.

(c) Estenem k a K' de manera que podem escriure l'equació de E en la forma normal de Legendre,

$$Y^2 = X(X-1)(X-\lambda)\,, \qquad \lambda \neq 0, 1.$$

Aleshores, és fàcil comprobar que o bé E té bona reducció en K', o bé E té reducció multiplicativa en K', o bé E té reducció multiplicativa en $K'(\sqrt{\ell})$.

Suposem primer que $\mathrm{car}(k) \neq 2$. Aleshores, els invariants donats per aquesta equació són

$$g_2 = \frac{16(\lambda^2-\lambda+1)}{48} \quad \text{i} \quad \Delta = 16\lambda^2(\lambda-1)^2.$$

Raonem per casos

- Cas 1. Si λ és un enter ℓ-enter, $\lambda \not\equiv 0, 1 \pmod{M_\ell}$ on M_ℓ és l'ideal maximal de k. Aleshores, Δ és un element enter ℓ-enter invertible, i per tant l'equació té bona reducció.
- Cas 2. Si $\lambda \equiv 0$ o $1 \pmod{M_\ell}$. Aleshores, $\Delta \in M_\ell$ i g_2 és un enter ℓ-enter invertible, i per tant l'equació te reducció de tipus multiplicatiu.
- Cas 3. Si λ no és un enter ℓ-enter. Aleshores, escollim r prou gran tal que $V_\ell(\ell^r\lambda) = 0$, és a dir, tal que $\ell^r\lambda$ sigui invertible. Fent el canvi de coordenades

$$X \mapsto \ell^{-r}X \quad , \quad Y \mapsto \ell^{-3r/2}Y$$

i reemplaçant k per $k(\ell^{1/2})$ si és necessàri, obtenim l'equació de coeficients ℓ enters de E

$$Y^2 = X(X-\ell^r)(X-\ell^r\lambda),$$

i per aqueta equació, $\Lambda \in M_\ell$ i g_2 és un element invertible enter ℓ-enter. Per tant, E té reducció de tipus multiplicatiu. □

Per tant, hem vist que després d'una extensió finita de cossos, el tipus de reducció de E és bona o multiplicativa, i que després aquest tipus no torna a canviar. Per això diem que E te reducció estable modul ℓ si existeix un model de E on aquesta té bona reducció o reducció multiplicativa mòdul ℓ.

Definició 3.3.1. Una corba el·líptica E sobre $\mathbb{Q}$ és estable si té reducció semi-estable mòdul tots els primers.

Observació 3.3.2. Si tenim E una corba el·líptica estable i W una equació minimal de E, dels resultats anteriors es dedueix clarament que aquesta equació és òptima per a la reducció de E. És a dir, que per a tot primer p, W tindrà bona reducció o reducció multiplicativa sobre p. Dit d'una altra manera, si tenim E una corba el·líptica estable sempre podem trobar una equació de Weierstrass de E, W, de manera que E te bona reducció o reducció multiplicativa en tot primer per W. Aquesta, és doncs, una equació minimal.

Ara, donada E una corba el·líptica amb reducció estable, podem definir un invariant de E que ens digui en quins primers de $\mathbb{Z}$ E té reducció de tipus multiplicatiu.

Definició 3.3.3. Sigui E una corba el·líptica donada per una equació de Weierstrass de coeficients en $\mathbb{Z}$, definim el conductor de E com $N_E = \prod_{\ell \text{ primer},\ \ell \mid \Delta_E} \ell$, és a dir, el producte dels primers on E té reducció de tipus multiplicatiu.

Capítol 4

La corba de Frey

4.1 Construcció i propietats

L'objectiu d'aquest punt és donar l'associació explícita d'una corba el·líptica estable E a una hipotètica solució no trivial de l'equació de fermat i veure'n algunes propietats. Abans de tractar l'equació $Z_1^p - Z_2^p = Z_3^p$, però, començarem treballant amb l'equació més general $a_1 Z_1^{n_1} - a_2 Z_2^{n_2} = a_3 Z_3^{n_3}$, on a_1, a_2 i a_3 són enters primers entre ells, dos a dos, i $n_1, n_2, n_3 \in \mathbb{N}$.

Considerem A i B dos nombres enters primers entre ells tal que $A \equiv 0 \bmod 2^5$ i $B \equiv 1 \bmod 4$, i escrivim $C := A - B$. Associem a aquests nombres la corba el·líptica donada per

$$E : Y^2 = X^3 + (A+B)X^2 + ABX.$$

Aleshores, realitzant les transformacions $X \mapsto X + \dfrac{AB}{6}$, $Y \mapsto Y$, la seva forma normal de Weierstrass esdevé

$$W_E : Y^2 = X^3 - \tfrac{1}{3}(A^2 + B^2 - AB)X + \tfrac{1}{27}(A+B)(2A^2 + 2B^2 - 5AB),$$

a partir de la qual obtenim que els invariants de E són

$$\Delta_{W_E} = A^2 B^2 C^2,$$

$$j_E = \frac{2^8 (A^2 + B^2 - AB)^3}{A^2 B^2 C^2},$$

$$\delta_E = \frac{1}{2} \frac{A^2 + B^2 - AB}{(A+B)(2A^2 + 2B^2 - 5AB)} \bmod \mathbb{Q}^{*2}.$$

Proposició 4.1.1. *Amb les notacions anteriors, la corba el·lípica E té les propietats següents.*

(a) *Els punts d'ordre dos de E són $\mathbb{Q}$-racionals.*

(b) *E és semiestable sobre $\mathbb{Q}$ i el seu conductor és $N_E = \displaystyle\prod_{\ell \mid ABC,\, \ell \text{ primer}} \ell$.*

(c) *Una equació minimal de E ve donada per*

$$M_E = Y^2 + XY = X^3 + \tfrac{A+B-1}{4} X^2 + \tfrac{A \cdot B}{16} X.$$

El discriminant d'aquesta és $\Delta_{M_E} = \frac{A^2B^2C^2}{2^8}$. *(Notem que, amb les condicions que hem imposat a* A *i* B *tenim que* $\frac{A+B-1}{4}$, $\frac{A\cdot B}{16}$ *i* Δ *són nombres enters).*

(d) *Sigui* p *un primer senar i* $\mathbb{Q}(E[p])$ *el cos obtingut d'adjuntar les coordenades els punts d'ordre* p *de* E *a* $\mathbb{Q}$. *Aleshores* $\mathbb{Q}(E[p])$ *és no ramificat sobre* $\mathbb{Q}_\ell$ *per a tot primer* ℓ *que no divideixi* $2p$.

Dem.

(a) Per calcular els punts d'ordre 2 utilitzem la fórmula per a la coordenada x_{2P} del punt $[2]P$, on $P = (x, y) \in E$:

$$x_{2P} = \frac{x^4 - 2ABx^2 + A^2B^2}{4x^3 + 4(A+B) + 4ABx}.$$

Per tant, els punts d'ordre 2 són aquells tals que $4x^3 + 4(A+B)x^2 + 4ABx = 0$; i les solucions d'aquesta cúbica són $x_1 = 0$, $x_2 = -A$ i $x_3 = -B$. És a dir, els punts d'ordre 2 de E són $P_0 = (0,0)$, $P_1 = (-A,0)$, $P_2 = (-B,0)$, que clarament són $\mathbb{Q}$-racionals.

(b) Veiem la semiestabilitat de E mòdul ℓ, ℓ primer, per casos:

• Cas $\ell = 2$. $v_2(j_E) = 8 - 2 \cdot v_2(A) \leq -2$ i $\delta_E \equiv B \pmod{\mathbb{Q}_2^2}$. D'on obtenim que E té reducció multiplicativa mòdul 2, ja que $B \equiv 1 \pmod 4$.

• Cas $\ell = 3$. Suposem primer que $3 \nmid ABC$. Aleshores es té que $C = A - B \not\equiv 0 \pmod 3$, i per tant $A \not\equiv B \pmod 3$. Així, el polinomi $X^3 + (A+B)X^2 + ABX$ té 3 zeros diferents mòdul 3, ergo E té bona reducció mòdul 3. En el cas que $3|ABC$ tenim que $v_3(j_E) = -v_3(\Delta_{W_E}) < 0$ i $v_3\left(\frac{1}{2}\frac{A^2+B^2-AB}{(A+B)(2A^2+2B^2-5AB)}\right) = 0$; per tant $\mathbb{Q}(\sqrt{\delta_E})|\mathbb{Q}$ és no ramificada en els divisors de 3, i per la caracterització donada en 3.1.3, E té reducció multiplicativa mòdul 3.

• Cas ℓ primer, $\ell \neq 2, 3$. Com que $\mathrm{mcd}(AB(A-B), A^2+B^2-AB) = 1$, E té bona reducció mòdul ℓ si i només si $v_\ell(j_E) \geq 0$. Però $v_\ell(j_E) < 0$ si i només si $\ell|ABC$, i en aquest cas, $v_\ell(\delta_E) = 0$ i per tant E te reducció multiplicativa mòdul ℓ.

Per tant, E es semiestable sobre $\mathbb{Q}$ i, per tant, el seu conductor és $N_E = \prod_{\ell|ABC,\, \ell \text{ primer}} \ell$.

(c) Fent els canvis $X \mapsto X - \frac{1}{12}$ i $Y \mapsto \frac{Y}{2} + \frac{1}{2}\left(X - \frac{1}{12}\right)$, transformem W_E en M_E i, per tant, les dues equacions defineixen la mateixa corba E. Ens falta veure, doncs que M_E és minimal. Però el discriminant de M_E és $\Delta_E = \frac{A^2B^2C^2}{2^8}$, que resulta que, per l'apartat (B), és òptim respecte la reducció de E. Per tant, M_E és una equació minimal de E.

(d) Veurem la demostració en el capítol següent.

□

Si ara prenem l'equació generalitzada

$$a_1 Z_1^{n_1} - a_2 Z_2^{n_2} = a_3 Z_3^{n_3},$$

i suposem que (z_1, z_2, z_3) n'és una solució amb $\gcd(z_1, z_2, z_3) = 1$, $2^5|a_1 z_1^{n_1}$ i $a_2 z_2^{n_2} \equiv 1 \bmod 4$, podem escriure $A = a_1 z_1^{n_1}$, $B = a_2 z_2^{n_2}$ i $C = a_3 z_3^{n_3}$. Aleshores, la corresponent corba el·líptica és estable amb discriminant

$$\Delta_E = \frac{a_1^2 a_2^2 a_3^2 z_1^{2n_1} z_2^{2n_2} z_3^{2n_3}}{2^8}$$

i conductor

$$N = \prod_{v_\ell(\Delta_E)>0,\, \ell \text{ primer}} \ell;$$

i satisfà les propietats de la proposició anterior.

Observació 4.1.2. Amb les notaciona anteriors

$$\frac{2^8 \Delta_E}{N} > a_1^2 a_2^2 a_3^2 z_1^{2n_1-1} z_2^{2n_2-1} z_3^{2n_3-1}.$$

Centrem-nos ara en el cas $a_1 = a_2 = a_3 = 1$ i $n_1 = n_2 = n_3 = p$, amb p primer diferent de 2 i de 3. Aleshores, sigui (z_1, z_2, z_3) una solució entera de

$$Z_1^p - Z_2^p = Z_3^p.$$

Podem assumir sense pèrdua de generalitat que $2|z_1$ i que $z_2 \equiv 1 \bmod 4$; és a dir, podem assumir que z_3 és imparell. Si z_3 fos parell, aleshores o bé z_1 i z_2 serien parells, o bé z_1 i z_2 serien imparells. En el primer cas podriem dividir la igualtat entre 2^p i obtenir una nova solució de l'equació (z_1', z_2', z_3') tal que $|z_i'| < |z_i|$, i repetir aquest procés fins que alguna z_i fos senar. En el segon cas, passant z_1^p restant a l'altra banda de la igualtat i renombrant z_1, z_2 i z_3 obtenim la generalització. Si procedim com anteriorment, és a dir, prenent $A = z_1^p$, $B = z_2^p$ i $C = z_3^p$, la corba el·líptica $E = E_{(z_1,z_2,z_3)}$ associada a (z_1, z_2, z_3) donada per l'equació minimal

$$M_E : Y^2 + XY = X^3 + \frac{z_1^p + z_2^p - 1}{4} X^2 + \frac{z_1^p z_2^p}{16} X$$

és estable sobre $\mathbb{Q}$. Els seus punts d'ordre 2 son $\mathbb{Q}$-racionals, el seu conductor es $N_E = \prod_{\ell | z_1 z_2 z_3,\, \ell \text{ primer}} \ell$, i $\Delta_E = (2^{-4} z_1 z_2 z_3)^{2p}$. I, per l'observació anterior, tenim que $2^8 \Delta_E \geq N^{2p}$. El cos $\mathbb{Q}(E[p])$ es no ramificat en tots els primers ℓ excepte en els divisors de $2p$.

Per tant, resumint els resultats provats, l'existència d'una solució no trivial de l'equació de Fermat implica l'existència d'una corba el·líptica sobre $\mathbb{Q}$ amb propietats molt remarcables.

Capítol 5

Punts de n-torsió i ramificació

5.1 Corbes el·líptiques sobre $\mathbb{C}$

Una referència bàsica per l'estudi d'aquest apartat és [12].

Definició 5.1.1. Una xarxa $\Lambda \subset \mathbb{C}$ és un subgrup discret de $\mathbb{C}$ que conté una $\mathbb{R}$-base de $\mathbb{C}$. Llavors, és un grup abeliá lliure de dimensió 2 i si ω_1, ω_2 és una base de Λ, escrivim $\Lambda = [\omega_1, \omega_2]$.

Definició 5.1.2. Una funció el·líptica relativa a una xarxa Λ, és una funció meromorfa $f : \mathbb{C} \to \mathbb{C}$ tal que $f(z+\omega) = f(z)$ per a tot $\omega \in \Lambda$ i per a tot $z \in \mathbb{C}$.

Definició 5.1.3. Un paral·lelògram fonamental per a Λ és un conjunt de la forma

$$D = a + \{t_1\omega_1 + t_2\omega_2 \,:\, 0 \leq t_1, t_2 < 1\},$$

on $a \in \mathbb{C}$ i $\{\omega_1, \omega_2\}$ és una base de Λ.

Veiem que existeixen funcions el·líptiques no constants. Per fer-ho definirem la funció $\wp$ de Weierstrass.

Definició 5.1.4. Sigui Λ una xarxa, definim la sèrie $\wp$ de Weierstrass associada a Λ com

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda,\omega\neq 0} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

Definim també la sèrie d'Eisenstain de pes $2k$ associada a Λ com la sèrie

$$G_{2k}(\Lambda) = \sum_{\omega\in\Lambda,\omega\neq 0} \frac{1}{\omega^{2k}}.$$

Per facilitar la notació, una vegada tinguem Λ fixada escriurem $\wp(z)$ i G_{2k}.

Proposició 5.1.5. *Sigui Λ una xarxa.*

(a) *La sèrie de Eisenstain G_{2k} per Λ és absolutament convergent per a tot $k > 1$.*

(b) *La sèrie $\wp$ de Weierstrass convergeix absolutament i uniformement en tot compacte de $\mathbb{C} - \Lambda$. Defineix una funció meromorfa en $\mathbb{C}$ que té un pol doble amb residu 0 a cada punt de la xarxa i cap més pol.*

Dem. [12] □

Definició 5.1.6. Donada una xarxa Λ, anomenem funció $\wp(z)$ de Weierstrass associada a Λ a la funció meromorfa donada per la sèrie de Weierstrass associada a Λ i anomenem constant G_{2k} d'Eisenstein associada a Λ a la constant defnida per la sèrie G_{2k} d'Eisenstein associada a Λ.

Proposició 5.1.7. *La funció $\wp$ de Weierstrass és una funció el·líptica.*

Dem. [12] □

Teorema 5.1.8. *Sigui Λ una xarxa i sigui $\mathbb{C}(\Lambda)$ el conjunt de les funcions el·líptiques relatives a Λ. Aleshores $\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$.*

Dem. [12] □

Teorema 5.1.9. (a) *Donada una xarxa Λ, la sèrie de Laurent de $\wp(z)$ en $z = 0$ ve donada per*

$$\wp(z) = z^{-2} + \sum_{k=1}^{\infty} (2k+1)G_{2k+2}z^{2k}.$$

(b) *Per a tot $z \in \mathbb{C}$, $z \notin \Lambda$, és*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Observació 5.1.10. Utilitzarem com a notació habitual $g_2'(\Lambda) := 60G_4$ i $g_3'(\Lambda) := 140G_6$.

Proposició 5.1.11. *Siguin $g_2'(\Lambda)$ i $g_3'(\Lambda)$ les quantitats associades a una xarxa Λ.*

(a) *El polinomi $f(x) = 4x^3 - g_2'(\Lambda)x - g_3'(\Lambda)$ té arrels diferents; el seu discriminant $\Delta(\Lambda) = (g_2'(\Lambda))^3 - 27(g_3'(\Lambda)')^2$ és diferent de zero.*

(b) *Sigui $E/\mathbb{C}$ la corba el·líptica donada per*

$$E : Y^2 = 4X^3 - g_2'(\Lambda)X - g_3'(\Lambda).$$

Aleshores, l'aplicació

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$$
$$z \mapsto \phi(z) = \begin{cases} [\wp(z), \wp'(z), 1] & z \notin \Lambda \\ [0,1,0] & z \in \Lambda \end{cases}$$

és un isomorfisme analític, és a dir, és una aplicació bijectiva i holomorfa.

Proposició 5.1.12. *Sigui E una corba el·líptica donada per*

$$E : Y^2 = 4X^3 - g_2'X - g_3',$$

on ara $g_2', g_3' \in \mathbb{C}$, a priori, no estan associats a cap xarxa Λ. Aleshores, existeix una única xarxa Λ tal que $g_2' = g_2'(\Lambda)$ i $g_3' = g_3'(\Lambda)$.

Aquests dos últims resultats ens ens diuen que tota corba el·líptica E sobre $\mathbb{C}$ està parametritzada per funcions el·líptiques, de manera que les coordenades dels punts de E es poden escriure com

$$x(\phi(z)) = \wp(z) \quad \text{i} \quad y(\phi(z)) = \wp'(z).$$

Ara, sigui Λ una xarxa de $\mathbb{C}$; podem prendre una base de Λ, $\{\omega_1, \omega_2\}$, de forma que $Im(\omega_1/\omega_2) > 0$, i aleshores prenent $\tau = \omega_1/\omega_2$ tenim que τ pertany al semiplà superior de $\mathbb{C}$ i $\{1, \tau\}$ és la base d'una xarxa Λ_τ homotètica a Λ. Anomenem Λ_τ a la xarxa normalitzada de Λ, i a més a més, les corbes que defineixen Λ i Λ_τ són isomorfes. Per tant, utilitzant els resultats anteriors, per a tota corba el·líptica E donada per una equació de Weierstrass de la forma

$$W_E : Y^2 = 4X^3 - g_2'X - g_3',$$

podem trobar una xarxa Λ_τ tal que la corba el·líptica donada per

$$Y^2 = 4X^3 - g_2'(\Lambda_\tau)X - g_3'(\Lambda_\tau),$$

és isomorfa a E, i podem prendre aquesta equació en lloc de W_E. Aleshores, escriurem $g_2'(\tau)$ i $g_3'(\tau)$ en lloc de $g_2'(\Lambda)$ i $g_3'(\Lambda)$ respectivament. Per tant, sigui E una corba el·líptica sobre $\mathbb{C}$ donada per l'equació $Y^2 = 4X^3 - g_2'X - g_3'$ i amb xarxa associada $\Lambda = [1, \tau]$; i sigui j_E l'invariant j de E definit anteriorment. Aleshores prenent $q = e^{2\pi i\tau}$ i $w = e^{2\pi iz}$ podem calcular els desenvolupaments en sèrie de g_2', g_3', j_E i els desenvolupaments en sèrie de Fourier de $\wp(z)$ i $\wp'(z)$; de manera que utilitzant la parametrització donada per ϕ obtenim expressions

$$g_2' = \frac{1}{12}\left[1 + 240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}\right],$$

$$g_3' = \frac{1}{6^3}\left[-1 + 504\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n}\right],$$

$$j_E = \frac{12^3 g_2'^3}{\Delta} = \frac{1}{q} + 744 + 196884q\cdots,$$

$$x(w) = \frac{1}{12} + \sum_{m\in\mathbb{Z}}\frac{q^m w}{(1-q^m w)^2} - 2\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n},$$

$$y(w) = \sum_{m\in\mathbb{Z}}\frac{q^m w(1+q^m w)}{(1-q^m w)^3}.$$

Ara, fent els canvis $X \mapsto X - \frac{1}{12}$ i $Y \mapsto \frac{Y}{2} + \frac{1}{2}\left(X - \frac{1}{12}\right)$, l'equació de Weierstrass es transforma en

$$E : Y^2 - XY = X^3 - h_2X - h_3,$$

on

$$h_2 = 5\sum_{n=1}^{\infty}\frac{q^n}{1-q^n},$$

$$h_3 = \sum_{n=1}^{\infty}\frac{5n^3+7n^5}{12}\frac{q^n}{1-q^n},$$

$$X(w) = \sum_{m\in\mathbb{Z}}\frac{q^m w}{(1-q^m w)^2} - 2\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n},$$

$$Y(w) = \sum_{m\in\mathbb{Z}} \frac{(q^m w)^2}{(1-q^m w)^3} - \sum_{n=1}^{\infty} \frac{nq^n}{1-q^n}.$$

Aquesta s'anomena l'equació (complexa) de Tate.

5.2 Punts de n-torsió

Definició 5.2.1. Donada una corba el·líptica E sobre $\mathbb{Q}$, posem $E_n := \{P \in E(\bar{\mathbb{Q}}) : [n]P = O\}$, el conjunt de punts de n-torsió de E, és a dir, el nucli de la multiplicació per $[n]$.

Acabem de veure que podem parametritzar tota corba el·líptica $E/\mathbb{Q}$ per una corba el·líptica sobre $\mathbb{C}$ associada a una xarxa $\Lambda = [\omega_1, \omega_2]$, de manera que aquesta parametrització manté l'estructura de grup. Per tant, ens podem mirar els punts de n-torsió de E com els punts de n-torsió de E sobre $\mathbb{C}$, és a dir d'aquesta parametrització. Denotem per $E[n]$ el grup dels punts de n-torsió de E sobre $\mathbb{C}$ (clarament, $E_n \cong E[n]$).

Proposició 5.2.2. *Sigui E una corba el·líptica sobre $\mathbb{Q}$. Aleshores*

$$E[n] \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}},$$

i per tant, $\#E[n] = n^2$.

Dem. Sigui $\Lambda = [\omega_1, \omega_2]$ la xarxa associada a E. Ja hem vist que E és isomorfa a $\mathbb{C}/\Lambda$, aleshores podem escriure l'isomorfisme explícit

$$\begin{aligned} \Phi : \frac{\mathbb{Z}}{n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}} &\to \mathbb{C}[n] \subset \frac{\mathbb{C}}{\Lambda} \\ (a_1, a_2) &\to \frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2. \end{aligned}$$

□

Teorema 5.2.3. *Sigui $\mathbb{Q}(E[n])$ el cos extensió de $\mathbb{Q}$ obtingut d'adjuntar a $\mathbb{Q}$ les coordenades dels punts de $E[n]$. Aleshores, $\mathbb{Q}(E[n])|\mathbb{Q}$ és una extensió de Galois.*

Dem. Com que $\#(E[n]) = n^2$, les coordenades $(x, y) = P \in E[n]$ només poden tenir un nombre finit de conjugats sota l'acció de $\mathrm{Aut}(\mathbb{C})$; per tant, x i y han de ser nombres algebraics sobre $\mathbb{Q}$. Sigui ara $\sigma : \mathbb{Q}(E[n]) \to \mathbb{C}$ un morfisme de cossos. Per veure que $\mathbb{Q}(E[n])$ és Galois sobre $\mathbb{Q}$ és suficient veure que $\sigma(\mathbb{Q}(E[n])) \subseteq \mathbb{Q}(E[n])$. Ara, si posem $E[n] = \{O, P_1, \ldots, P_{n^2-1}\}$ amb $P_i = (x_i, y_i)$, clarament σ ve determinat per les imatges de x_i i y_i. Però com que x_i i y_i són nombres algebraics i les fòrmules d'addició venen donades per funcions racionals de coeficients en $\mathbb{Q}$, si definim

$$\sigma(P) = \begin{cases} (\sigma(x_i), \sigma(y_i)), & \text{si } P = P_i, \\ O, & \text{si } P = O, \end{cases}$$

aleshores $\sigma(P + Q) = \sigma(P) + \sigma(Q)$, per a tot $P, Q \in E[n]$. Així doncs, $n\sigma(P_i) = \sigma(nP_i) = \sigma(O) = O$ per a tot $P_i \in E[n]$, és a dir, que $\sigma(P_i)$ és un dels P_j's de $E[n]$. Per tant, $\sigma(x_i), \sigma(y_i) \in \mathbb{Q}(E[n])$ per a tot i, és a dir que $\sigma(\mathbb{Q}(E[n])) \subseteq \mathbb{Q}(E[n])$, fet que completa la prova del teorema. □

5.3 L'aparellament de Weil

Siguin k un cos de característica p (es permet $p = 0$), $k' \supseteq k$ un cos algebraicament tancat, E/k una corba el·líptica i m un enter més gran o igual que 2 primer amb p (si $p > 0$). Prenem un punt $T \in E[m]$, aleshores per el corol·lari 2.2.2 sabem que $m(T) - m(O)$ és un divisor principal, és a dir, que existeix $f \in k'(E)$ tal que

$$\operatorname{div}(f) = m(T) - m(O).$$

Ara, prenent $T' \in E$ tal que $[m]T' = T$, de la mateixa manera, existeix una funció $g \in \bar{K}(E)$ tal que

$$\operatorname{div}(g) = \sum_{R \in E[m]} (T' \oplus R) - (R);$$

(notem que $\#E[m] = m^2$ i que $[m^2]T' = O$). Anomearem a f i g funcions associades a T. Clarament, $f \circ [m]$ i g^m tenen el mateix divisor, i com que $\operatorname{gen}(E) = 1$, existeix $\lambda \in k^*$ tal que $\lambda(f \circ [m]) = g^m$. Suposem ara que tenim un altre $S \in E[m]$; aleshores per a qualsevol $X \in E$ és

$$g(X \oplus S)^m = \lambda f([m]X \oplus [m]S) = \lambda f([m]X) = g(X)^m,$$

de manera que podem definir un aparellament

$$e_m : E[m] \times E[m] \to \mu_m,$$

on μ_m denota el conjunt de les arrels de la unitat, de la manera següent

$$e_m(S, T) := g(X \oplus S)/g(X),$$

on X es qualsevol punt de E tal que $g(S \oplus X)$ i $g(X)$ estiguin ambdós definits i siguin diferents de zero. Observem que e_m no depèn de l'elecció de X, ja que $g(x)$ i $g(x \oplus S)$ són funcions racionals amb el mateix divisor, i per tant el seu quocient és constant. Aquest s'anomena l'**aparellament de Weil**.

Observació 5.3.1. Multiplicant f per λ, és a dir, prenent, com a funció associada a T, λf en lloc de f, suposarem que $f \circ [m] = g^m$.

Proposició 5.3.2. *Propietats de l'aparellament de Weil.*

(a)

$$e_m(S_1 \oplus S_2, T) = e_m(S_1, T) + e_m(S_2 T),$$
$$e_m(S, T_1 \oplus T_2) = e_m(S, T_1) + e_m(S, T_2),$$

(b)

$$e_m(S, T) = e_m(T, S)^{-1} \ .$$

(c) *Si* $e_m(S, T) = 1$ *per a tot* $S \in E[m]$, *aleshores* $T = O$.

(d) *Per tot* $\sigma \in G_{k'/k}$,

$$\sigma(e_m(S,T)) = e_m(\sigma(S), \sigma(T)).$$

(e) *Si* $S \in E[mm']$ *i* $T \in E[m]$, *aleshores*

$$e_{mm'}(S,T) = e_m([m']S, T).$$

Dem.

(a) Provem la linealitat del primer factor

$$e_m(S_1 \oplus S_2, T) = \frac{g(X \oplus S_1 \oplus S_2)}{g(X \oplus S_1)} g(X) = e_m(S_2, T) e_m(S_1, T),$$

ja que prenent $Y = X + S_1$ tenim la igualtat. Per veure la linealitat del segon factor comencem prenent $f_1, f_2, f_3, g_1, g_2, g_3$ funcions associades als punts T_1, T_2 i $T_3 = T_1 + T_2$. Utilitzant el corol·lari 2.2.2, prenem $h \in k'(E)$ tal que el seu divisor és

$$\mathrm{div}(h) = (T_1 \oplus T_2) - (T_1) - (T_2) + (O).$$

En conseqüència $\mathrm{div}(f_3/f_1 f_2) = m\mathrm{div}(h)$ i per tant $f_3 = c f_1 f_2 h^m$ per a alguna constant $c \in k'^*$. Ara, com que podem suposar que $f_i \circ [m] = g_i^m$, és fàcil veure que

$$g_3 = c' g_1 g_2 (h \circ [m]),$$

per a algún $c' \in \mathbb{C}$; i aplicant això, obtenim que

$$e_m(S, T_1 \oplus T_2) = \frac{g_3(X \oplus S)}{g_3(X)} = \frac{g_1(X \oplus S) g_2(X \oplus S) h([m]X \oplus [m]S)}{g_1(X) g_2(X) h([m]X)}.$$

(b) Per l'apartat anterior, tenim que

$$e_m(S \oplus T, S \oplus T) = e_m(S,S) e_m(S,T) e_m(T,S) e_m(T,T);$$

per tant, és suficient veure que $e_m(P,P) = 1$ per a tot $P \in E[m]$. Denotem per $\tau_Q : E \to E$ la translació pel punt Q, és a dir, $\tau_Q(P) = P \oplus Q$. Aleshores

$$\mathrm{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]P}\right) = m \sum_{i=0}^{m-1} ([1-i]P) - ([-i]P) = 0,$$

d'on veiem que

$$\prod_{i=0}^{m-1} f \circ \tau_{[i]P}$$

és constant. Ara, prenent P' tal que $[m]P' = P$, aleshores

$$\prod_{i=0}^{m-1} g \circ \tau_{[i]P'}$$

també és constant. En conseqüència, el producte de les g's pren el mateix valor en X i en $X \ominus P'$,

$$\prod_{i=0}^{m-1} g(X \oplus [i]P') = \prod_{i=0}^{m-1} g(X \oplus [i+1]P')$$

i cancelant els termes iguals de cada costat de la igualtat obtenim l'expressió $g(X) = g(X \oplus [m]P') = g(X \oplus P)$, d'on $e_m(P,P) = \dfrac{g(X \oplus P)}{g(X)} = 1$, com volíem veure.

(c) Si tenim que $e_m(S,T) = 1$ per a tot $S \in E[m]$, aleshores $g(X \oplus S) = g(X)$ per a tot $S \in E[m]$, aleshores existeix $h \in k'(E)$ tal que $g = h \circ [m]$ ([18]), amb la qual cosa

$$(h \circ [m])^m = g^m = f \circ [m],$$

i $f = h^m$. Aleshores, per les propietats dels divisors, $m\mathrm{div}(h) = \mathrm{div}(f) = m(T) - m(O)$, i, per la proposició 2.2.1, $T = O$.

(d) Sigui $\sigma \in G_{k'/k}$. Si f i g són les funcions associades a T, aleshores f^σ i g^σ són les funcions associades a $\sigma(T)$, on f^σ i g^σ denoten les funcions resultants d'aplicar σ als coeficients de f i g respectivament. Aleshores,

$$e_m(\sigma(S), \sigma(T)) = \frac{g^\sigma(\sigma(X) \oplus \sigma(S))}{g^{\sigma(\sigma(X))}} = \sigma\left(\frac{g(X \oplus S)}{g(X)}\right) = \sigma(e_m(S,T)).$$

(e) Prenem f i g com anteriorment, i tenim que

$$\mathrm{div}(f^{m'}) = mm'(T) - mm'(O) \text{ i } (g \circ [m'])^{mm'} = (f \circ [mm'])^{m'}.$$

Per les definicions de $e_{mm'}$ i e_m,

$$e_{mm'}(S,T) = \frac{g \circ [m'](X \oplus S)}{g \circ [m'](X)} = \frac{g(Y \oplus [m']S)}{g(Y)} = e_m([m']S, T).$$

□

Les propietats de l'aparallemant de Weil impliquen que e_m és exhaustiu, i en particular el resultat següent.

Corol·lari 5.3.3. *Existeixen punts $S, T \in E[m]$ tal que $e_m(S,T)$ és una arrel primitiva m-èsima de la unitat. En particular, si $E[m] \subset E(K)$, alehsores $\mu_m \subset k^*$.*

Dem. La imatge de $e_m(S,T)$ en moure S i T per $E[m]$ és un subgrup de μ_m, o sigui, μ_d per a algun $d|n$, d'on

$$1 = \sigma(e_m(S,T)) = e_m([d]S, T) \text{ per a tot } S, T \in E[m].$$

Per l'apartat (c) de la proposició anterior, tenim que $[d]S = O$, i com que S és arbitrari, ha de ser $d = m$. Finalment, si $E[m] \subset E(K)$, l'apartat (d) implica que $e_m(S,T) \in k^*$ per a tot $S, T \in E[m]$, i per tant $\mu_m \subset k^*$.

La construcció de l'aparellament de Weil és completament algebraica, fet que mostra que $\mu_m \subset E[m]$ essent m un nombre enter.

5.4 La parametrització de Tate

Per estudiar localment les corbes el·líptiques definides sobre $\mathbb{Q}$ farem una cosa similar al que hem fet sobre $\mathbb{C}$ però sobre $\mathbb{Q}_p$. Considerem doncs k una extensió finita de $\mathbb{Q}_p$ i denotem per $|\cdot|$ el valor absolut normalitzat donat per la valoració p-àdica, tal que $|p| = p^{-1}$. Considerem les sèries formals de $k(w)[[q]]$, on q és una variable de k i w és una indeterminada sobre k^* (notem que $k(w)$ denota el cos de fraccions de $k[w]$), donades per

$$x(w) = \frac{1}{12} + \sum_{m\in\mathbb{Z}} \frac{q^m w}{(1-q^m w)^2} - 2\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n},$$
$$y(w) = \sum_{m\in\mathbb{Z}} \frac{q^m w(1+q^m w)}{(1-q^m w)^3}.$$

Aleshores, utilitzant les identitats,

$$\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n} = \sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2} \quad \text{en } k[[q]] \text{ i}$$
$$\frac{w}{(1-w)^2} = \frac{1}{w+w^{-1}-2} = \frac{w^{-1}}{(1-w^{-1})^2} \quad \text{en } k(w),$$

transformem les sèries $x(w)$ i $y(w)$ en

$$X(w) = \frac{w}{(1-w)^2} + \sum_{n=1}^{\infty} \left(\frac{q^n w}{(1-q^n w)^2} + \frac{q^n w^{-1}}{(1-q^n w^{-1})^2} - 2\frac{q^n}{(1-q^n)^2} \right) \text{ i}$$
$$Y(w) = \frac{w^2}{(1-w)^3} + \sum_{n=1}^{\infty} \left(\frac{q^{2n} w^2}{(1-q^n w)^3} - \frac{q^n w^{-1}}{(1-q^n w^{-1})^3} - \frac{q^n}{(1-q^n)^2} \right),$$

que faran el paper de les sèries $\wp$ i $\wp'$ de Weierstrass. Aleshores, comparant aquestes sèries amb $\sum q^n$, es veu clarament que aquestes sèries convergeixen per a tot $w \in k'$ (k' cos algebraicament tancat, $k \subset k'$), $w \notin q^{\mathbb{Z}}$ ($q^{\mathbb{Z}}$ és el grup ciclic infinit generat per q en k^*) sempre que $0 < |q| < 1$; i es té que $X(qw) = X(w) = X(w^{-1})$, $Y(qw) = Y(w)$ i $Y(w^{-1}) + Y(w) = -X(w)$. Considerem ara les sèries de $k[[q]]$ donades per

$$h_2(q) = 5\sum_{n=1}^{\infty} \frac{q^n}{1-q^n} \text{ i}$$
$$h_3(q) = \sum_{n=1}^{\infty} \frac{5n^3+7n^5}{12} \frac{q^n}{1-q^n}.$$

Aquestes són convergents sempre que $|q| < 1$ i que els coeficients són enters de valor absolut més petit o igual que 1. Per tant, les sèries de potències descrites, utilitzant els resultats obtingut en l'anàlisi sobre $\mathbb{C}$, satisfan l'equació (p-àdica) de Tate

$$E_q : Y^2 - XY = X^3 - h_2 X - h_3.$$

Com és usual, definim

$$\Delta = h_3(q) + (h_2(q))^2 + 72h_2(q)h_3(q) - 432(h_3(q))^2 + 64(h_2(q))^3 = q - 24q^2 + 252q^3 + \cdots \in k[[q]].$$

Aquesta definició prové de la relació

$$g_2'^3 - 27g_3'^2 = \left(4h_2 + \tfrac{1}{12}\right)^3 - 27\left(4h_3 - \tfrac{1}{3}h_2 - \tfrac{1}{216}\right)^2.$$

Alesores, $\Delta \equiv q \pmod{q^2}$, amb la qual cosa $|\Delta| = |q| \neq 0$ i l'invariant

$$j = \frac{(12g_2'^3)}{\Delta} = \frac{(1+48h_2)^3}{\Delta}$$

està ben definit i $j = \dfrac{1}{q} + 744 + \cdots$, com esperavem.

És a dir, hem obtingut que la equació de Tate definex una corba el·líptica E_q/k, que anomenarem Corba de Tate. Observem que, per tenir $j = \dfrac{1}{q} + 744 + \cdots$ sabem que $|j| > 1$ i per tant que $j \notin \mathcal{O}_p$. A més a més, la reducció mòdul p de E_q és donada per l'equació

$$Y^2 + XY = X^3,$$

que, en cooredenades homogènies, és

$$z(y^2 + xy) = x^3.$$

Per tant, clarament E_q té un punt doble en $(0,0,1)$ amb dues tangents diferents, és a dir, que E_q té reducció estable multiplicativa en p. Recíprocament, si tenim una corba el·líptica definida sobre k amb invariant j tal que $|j| > 1$ i amb reducció estable multiplicativa en p, aquesta és isomorfa sobre k a una corba de Tate E_q.

Teorema 5.4.1. *Sigui E_T la Corba de Tate. Definim $\phi : k^* \to E(k)$ per*

$$\begin{cases} \phi(w) = (X(w), Y(w)), & \text{si } w \notin q^{\mathbb{Z}}, \\ \phi(w) = O, & \text{si } w \in q^{\mathbb{Z}}; \end{cases}$$

on O és el punt de l'infinit de E_T. Aleshores ϕ és un morfisme de k^* en el conjunt dels punts k-racionals de E_T, amb nucli $q^{\mathbb{Z}}$.

Dem. Comencem provant que ϕ està ben definida. Clarament, $O \in E_T$, per tant és suficient que provem que $\phi(w) \in E_T$ per a $w \notin q^{\mathbb{Z}}$. Com que tant $X(w)$ com $Y(w)$ tenen període multiplicatiu q, només ens cal considerar w tal que $|q| < |w| \leq 1$ i $w \neq 1$. Si prenem el segon desenvolupament per a $X(w)$ que hem donat, aquest expressa $X(w)$ com una sèrie de potències en w on els coeficients són funcions racionals de w, i es té el mateix resultat per a $Y(w)$. Ara, si $w \neq 1$ i $q \neq 0$ i tenim que $|q| < |w| < |q|^{-1}$ i que se satisfà que $|q^n w| < 1$ i $|q^n w^{-1}|$ per a tot n enter de manera que $X(w)$ i $Y(w)$ convergeixen absolutament, i , per tant, sota aquestes condicions, $\phi(w)$ és un punt de la corba de Tate. Si fixem $w < 1$, i fem variar q, les sèries de potències en q de coeficients complexos són iguals coeficient a coeficient. Aleshores, variant w, concloem que els coeficients són formalment iguals com a funcions racionals d'una indeterminada. I per tant, ja hem acabat.

Provem doncs que ϕ és un morfisme. Siguin w_1, w_2 dos elements de k^*, i sigui $w_3 = w_2 w_1$, hem de veure que $\phi(w_3) = \phi(w_1) + \phi(w_2)$. Anomenem $P_i = \phi(w_i)$, $i = 1, 2, 3$. Per la periodicitat de X i Y ens podem restringir al cas en què $|q| < |w_1| \leq 1$ i $1 \leq |w_2| < |q^{-1}|$, ja que aleshores tindrem que $|q| < |w_3| < |q|^{-1}$, i tots els w_i estaran en el domini de convergència de les sèries

de potències per a X i Y considerades anteriorment. Com que $\phi(1) = O$, si $w_1 = 1$ o $w_2 = 1$, tenim la igualtat de forma trivial. Ara, si recordem les fòrmules per a la suma definida sobre una corba el·líptica qualsevol, tenim que $P_1 + P_2 = O$ si i només si $X_1 = X_2$ i $Y_1 + Y_2 = -X_1$ i això passa si i només si $w_1 w_2 = 1$ (estem utilitzant $P_i = (X_i, Y_i)$).

En general, suposem que els tres P_i són diferents de O. Si $X_1 \neq X_2$, aleshores per les fórmules de addició tenim

$$(X_1 - X_2)^2 X_3 = (Y_1 - Y_2)^2 + (Y_1 - Y_2)(X_1 + X_2) - (X_1 - X_2)^2(X_1 + X_2) \text{ i}$$
$$(X_1 - X_2)Y_3 = -(X_1 - X_2)(Y_1 + X_3) + (Y_1 - Y_2)(X_1 - X_3)$$

Ara, podem raonar igual que quan hem vist que $\phi(w)$ pertany a E_T. Finalment, per continuïtat, el cas en què $X_1 = X_2$ queda demostrat també. □

Ara, recordem que $E := E_{A,B,C}$ és la corba el·líptica associada a tres nombres enters A, B, C tals que $A - B = C$; en concret, prenem $A = a^p$, $B = b^p$ i $C = c^p$ on (a, b, c) és una hipotètica solució de l'equació de Fermat. Considerem $\mathbb{Q}(E[p])$ el cos associat a aquesta corba; hem vist que aquest és un cos extensió de Galois de $\mathbb{Q}$ i que sempre conté un arrel primitiva p-èsima de la unitat ζ_p. Ara veurem que si ℓ és un nombre primer que divideix Δ_E, és a dir, un nombre primer que divideix abc, aleshores, $\mathbb{Q}(E[p])$ és no ramificat sobre $\mathbb{Q}_\ell(\zeta_p)$.

Teorema 5.4.2. *Sigui ℓ un nombre primer que divideixi abc. Aleshores, el cos $\mathbb{Q}(E[p])$ associat a E es pot considerar un subcòs de $\mathbb{Q}_\ell(\zeta_p, 2^{1/p})$.*

Dem. Com ja haviem vist, l'invariant j de E és $j_E = \dfrac{(c^{2p} - a^p b^p)^3}{2^8 (abc)^{2p}}$; per tant, excepte per una potència de 2, j és una potència $2p$-èsima d'un element de $\mathbb{Q}_l$ amb valor absolut ℓ-àdic més gran que 1. Per tant, E és isomorfa a una corba el·líptica de Tate E_q sobre $\mathbb{Q}_l$, o potser, sobre una extensió quadràtica no ramificada d'aquest cos.

Ara, si prenem $L := \mathbb{Q}_l(2^{1/p}, \zeta_p)$, sabem, pel teorema 5.4.1 i el teorema d'isomorfia que $E_q(L)$ és isomorf a $L^*/q^{\mathbb{Z}}$. A més a més, com que j és una potència p-èsima en L, q també ho és, és a dir, que existiex $q' \in L$ tal que $q = (q')^p$. Per tant, $L^*/q^{\mathbb{Z}}$ conté el grup $(q', \zeta_p)/q^{\mathbb{Z}}$, que és isomorf a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, i en conseqüència $E_q[p] \subset E_q(L)$.

Observació 5.4.3. Aquest teorema ens diu que si p és un primer i tenim ℓ un altre primer dividint el conductor de E, és a dir, que E te reducció de tipus multiplicatiu en ℓ, aleshores $\mathbb{Q}(E[p])$ és no ramificat sobre $\mathbb{Q}_\ell$ exepte per a ℓ dividint $2p$.

5.4.4. Aquests resultats van ser donats per Tate, però mai van arribar a ser publicats per ell. Per veure una profundització de la teoria de corbes el·líptiques sobre cossos locals es pot consultar [15].

5.5 Ramificació en el cas de bona reducció

Amb les notacions anteriors, ja hem vist quin és el comportament de $\mathbb{Q}(E[p])$ en el cas en què E té reducció de tipus multiplicatiu en un primer ℓ. En aquest capítol com ja hem avançat, veurem que si E té bona reducció en ℓ, aleshores $\mathbb{Q}(E[p])$ és una extensió no ramificada de Q_ℓ. Recordem que $E(\ell)$ denota la reducció de E mòdul ℓ.

Definició 5.5.1. Com que $E(\ell)$ pot ser o no ser llisa, denotem per $E_{ns}(\ell)$ el conjunt dels punts no singulars (o llisos) de $E(\ell)$, és a dir, tots els punts de $E(\ell)$ excepte potser un punt S que és un node de $E(\ell)$.

Proposició 5.5.2. *$E_{ns}(\ell)$ és un grup abelià.*

Dem. Si $E(\ell)$ és llisa, $E(\ell) = E_{ns}(\ell)$ i per tant el resultat és evident. Suposem doncs que tenim un punt $S \in E(\ell)$ que és un node. Aleshores

$$y = \alpha_1 x + \beta_1 \text{ i } y = \alpha_2 x + \beta_2$$

són dues rectes tangents a E en S. Aleshores, l'aplicació

$$E_{ns}(l) \to k'^*$$
$$(x, y) \to \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}$$

és un isomorfisme de grups abelians. □

Definició 5.5.3. Sigui E una corba el·líptica sobre $k := \mathbb{Q}_\ell$ i sigui $\bar{k}$ el cos residual de $\mathbb{Z}_\ell$, és a dir, de l'anell d'enters de k. Prenem $P \in E(k)$, $P = (x, y)$, aleshores denotem per $P(\ell)$ a la reducció en $\bar{k}$ del punt P. Defnim $E_0(k) := \{P \in E(k) : P(\ell) \in E_{ns}(\ell)(\bar{k})\}$ i $E_1(k) := \{P \in E(k) : P(l) = O(\ell)\}$, és a dir, $E_0(k)$ és el conjunt de punts amb reducció no singular i $E_1(k)$ el nucli de la reducció.

Proposició 5.5.4. *Hi ha una successió exacta de grups abelians*

$$0 \to E_1(k) \to E_0(k) \xrightarrow{red} E_{ns}(l)(\bar{k}) \to 0,$$

on red és el morfisme de reducció.

Dem. La suma que estableix l'estructura de grup en $E_{ns}(l)(\bar{k})$ i en $E(k)$ estan definides mitjançant les interseccions de E amb rectes de $\mathbb{P}^2$, i com que el morfisme de reducció $\mathbb{P}^2(k) \to \mathbb{P}^2(\bar{k})$ porta rectes a rectes, tenim que $E_0(k)$ té estructura de grup i que l'aplicació $E_0(k) \to E_{ns}(\ell)(\bar{k})$ és un morfisme. Per tant, l'exactitud del morfisme de l'esquerre i del morfisme central provenen directament de la definició de $E_1(k)$. Per tant només ens queda provar que el morfisme de reducció és exhaustiu. Per això utilitzarem el lema de Hensel. Recordem-ne l'enunciat.

Lema 5.5.5. *(Lema de Hensel) Siguin k un cos complet respecte una valoració discreta v i $\mathcal{O}_k$ l'anell d'enters de K. Prenem π un uniformitzant de k i considerem $\bar{k} = \mathcal{O}_k/\pi\mathcal{O}_k$ el cos residual. Sigui $f(X) \in \mathcal{O}_k[X]$ un polinomi mònic de coeficients en $\mathcal{O}_K$. Si la reducció $\bar{f}(X) \in \bar{k}[X]$ te una arrel simple x_0, aleshores existeix un únic element $a \in \mathcal{O}_K$ tal que $f(a) = 0$, a és una arrel simple de f, i tal que $\bar{a} = x_0$ en k.*

Prosseguim amb la demostració. Prenem

$$f(X, Y) = Y^2 + a_1XY + a_3Y - a_2X^2 - a_4X - a_6 = 0$$

un model minimal de Weierstrass de E, i sigui $\bar{f}(X, Y)$ la corresponent reducció de f mòdul ℓ. Sigui $P(\ell) = (\alpha, \beta)$ qualsevol punt de $E_{ns}(\ell)(k)$. Com que $P(\ell)$ és un punt no singular de $E(\ell)$ sabem que o bé

$$\tfrac{\partial \bar{f}}{\partial x}(P(\ell)) \neq 0 \text{ o bé } \tfrac{\partial \bar{f}}{\partial y}(P(\ell)) \neq 0,$$

Suposem que estem en el cas (l'altre es fa de manera anàloga)

$$\frac{\partial \bar{f}}{\partial x}(P(\ell)) \neq 0$$

i prenem y_0 tal que $\bar{y_0} = \beta$. Aleshores, si ens fixem en el polinomi en una variable $f(X, y_0)$, sabem que aquest, reduït mòdul l tè una arrel simple en α, per tant, pel lema de Hensel, existeix un $x_0 \in \mathbb{Z}_l$ tal que $\bar{x_0} = \alpha$ i $f(x_0, y_0) = 0$. Per tant el punt $P = (x_0, y_0) \in E_0(K)$ i redueix a $P(l)$.

Proposició 5.5.6. *Sigui E una corba el·líptica sobre $k := \mathbb{Q}_\ell$, i $m \geq 1$ un nombre enter, $\ell \nmid m$. El subgrup $E_1(k)$ no te punts no trivials d'ordre m.*

Dem. [18] □

Proposició 5.5.7. *Siguin E una corba el·líptica sobre $k := \mathbb{Q}_\ell$, i $m \geq 1$ un nombre enter. Aleshores, si E te bona reducció sobre ℓ, el morfisme de reducció*

$$E(k)[m] \to E(\ell)(\bar{k}),$$

on $\bar{k}$ és el cos residual de $\mathbb{Z}_\ell$, és injectiu.

Dem. Per la proposicó 5.5.4, sabem que tenim la successió exacta

$$0 \to E_1(k) \to E_0(k) \to E_{ns}(l)(\bar{k}) \to 0;$$

però si $E(\ell)$ és no singular, aleshores, $E_0(k) = E(k)$ i $E_{ns}(\bar{k})(\ell) = E(\bar{k})(l)$, per tant utilitzant que $E_1(k)$ no té punts no trivials d'orde m, $E(k)[m]$ s'injecta en $E(l)(\bar{k})$. □

Ara reinterpretarem aquetsa injectivitat en termes de l'acció del grup de Galois.

Definició 5.5.8. Sigui k^{nr} la màxima extenxió no ramificada de $k := \mathbb{Q}_\ell$. Definim el subgrup d'inèrcia de $G_{k'/k}$ com $I = G_{k'/k^{nr}}$, on k' és la calusura algebràica de k. A més a més, tenim la descomposició següent

$$1 \to G_{k'/k^{nr}} \to G_{k'/k} \to G_{k^{nr}/k} \to 1,$$

però $G_{k^{nr}/k} = G_{\bar{k}'/\bar{k}}$, per tant, I és el conjunt de elements de $G_{k'/k}$ que actua trivialment en el cos residual $\bar{k}'$.

Definició 5.5.9. Sigui Σ un conjunt en el qual actua I. Diem que Σ és no ramificat sobre I si l'acció de I sobre Σ és trivial.

Proposició 5.5.10. *Sigui E una corba el·líptica sobre $k := \mathbb{Q}_\ell$ i suposem que E té bona reducció mòdul ℓ. Sigui $m \geq 1$ un enter. Aleshores $E[m]$ és no ramificat sobre I.*

Dem. Sigui K' una extensió finita de k tal que $E[m] \subset E(K')$ i denotem per $\mathcal{O}'$ l'anell dels enters de K', per m' el seu idel maximal, per $\bar{K}'$ el cos residual de $\mathcal{O}'$ i per v' la valoració en K' extensió de la valoració ℓ-àdica v_ℓ. Si agafem una equació minimal de E, el discriminant Δ_E compleix $v_\ell(\Delta_E) = 0$, i per tant, com que v' és un múltiple de v_ℓ, també es té que $v_\ell(\Delta_E)$. Per tant, l'equació minimal tambe ho és a K' i E també té bona reducció sobre $\bar{K}'$. Ara, sabem que el morfisme $E[m] \to E(\ell)(\bar{K}')$ és injectiu. Sigui $\sigma \in I$ i prenem $P \in E[m]$. Volem veure que $\sigma(P) = P$. Per la definició de I, σ actua trivialment en $E(\bar{K}')(\ell)$, per tant

$$(\sigma(P) - P)(\ell) = (\sigma(P))(\ell) - (P)(\ell) = (O)(\ell).$$

Però $\sigma(P) - P$ esta clarament en $E[m]$, per tant, per la injectivitat, tenim que $\sigma(P) - P = O$.

Per tant, $\mathbb{Q}(E[m])$ és invariant per I, amb la qual cosa tenim que $\mathbb{Q}(E[m]) \subset k^{nr}$, i per tant, per definició, $\mathbb{Q}(E[m])$ és no ramificat sobre $\mathbb{Q}_\ell$ i per tant tampoc ho és en $Q_\ell(\zeta_m)$. □

Capítol 6

Funcions modulars

En aquest capítol veurem què són les formes modulars de pes k i nivell N, i donarem un petit estudi dels espais de formes modulars de pes k i nivell 1.

Recordem que donada una xarxa $\Lambda = [\omega_1, \omega_2]$ de $\mathbb{C}$, hem definit funcions $g_2'(\Lambda)$ i $g_3'(\Lambda)$ associades a Λ, $G_{2k}(\Lambda)$ i que $g_2'(\Lambda) = 60G_4$ i $g_3'(\Lambda) = 140G_6$. A més a més, el discriminant associat a Λ és $\Delta(\Lambda) = (g_2'(\Lambda)^3 - 27(g_3'(\Lambda))^2$. Amb aquestes definicions, $g_2'(\lambda\Lambda) = \lambda^{-4}g_2'(\Lambda)$ i $g_3'(\lambda\Lambda) = \lambda^{-6}g_3'(\Lambda)$ per a tot $\lambda \in \mathbb{C} - \{0\}$, d'on $\Delta(\lambda\Lambda) = \lambda^{-12}\Delta(\Lambda)$. Així doncs, podem definir la funció J (de Klein) com

$$J(\Lambda) = \frac{(g_2'(\Lambda))^3}{\Delta(\Lambda)}.$$

Observem que J ens dóna el valor de j_E on E és la corba el·líptica associada a Λ. Clarament $J(\Lambda) = J(\lambda\Lambda)$, de manera que si donem una base normalitzada $\{1, \tau\}$ de Λ amb $\tau \in H := \{z \in \mathbb{C} | \mathrm{Im}(z) \geq 0\}$, $J(\Lambda) = J(\frac{1}{\omega_1}\Lambda) = J([1, \tau])$. Per tant, podem escriure J com una funció sobre H, és a dir, $J(\tau)$, $\tau \in H$.

6.1 Grup modular

Sigui $\tau \in H$, definim el grup modular com el grup donat per les transformacions $\tau \to \dfrac{a\tau + b}{c\tau + d}$, on a, b, c, d són enters tals que $ad - bc = 1$. El denotem per Γ. Aquest és isomorf al grup $PSL(2, \mathbb{Z})$, és a dir, el quocient de $SL(2, \mathbb{Z})$ pel seu centre. Usualment no farem distinció entre la transformació i la matriu que la representa, i si

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

aleshores,

$$A\tau = \frac{a\tau + b}{c\tau + d}.$$

Definició 6.1.1. Sigui G un subgrup de Γ. Aleshores diem que $\tau, \tau' \in H$ són equivalents sota G si i només si existeix un $A \in G$ tal que $A\tau = \tau'$.

Definició 6.1.2. Sigui G un subgrup de Γ. Definim R_G, una regió fonamental de G com un tancat de H tal que

1. L'interior de R_G no conté dos punts equivalents mòdul G; i
2. Per a tot $\tau \in H$ existeix $\tau' \in R_g$ tal que τ i τ' són equivalents mòdul G.

Lema 6.1.3. *Sigui $\tau' \in H$, aleshores existeix un $\tau \in H$ tal que $\tau \sim \tau' \pmod{\Gamma}$ i tal que*

$$|\tau| \geq 1,\ |\tau+1| \geq |\tau| \text{ i } |\tau-1| \geq |\tau|$$

Dem. Escrivim $\omega_1' = 1$ i $\omega_2' = \tau'$. Definim $\Omega = \{m\omega_1' + n\omega_2' : m, n \in \mathbb{Z}\} = \{0, w_1, w_2, \ldots\}$ de manera que $0 < |w_1| \leq |w_2| \leq \cdots$ i $\arg(w_n) < \arg(w_{n+1})$ si $|w_n| = |w_{n+1}|$ (on l'argument de w és el definit en la franja $(-\pi, \frac{3}{2}pi)$). Prenem $\omega_1 = w_1$ i ω_2 el primer element d'aquest grup que no és un múltiple de ω_1. Aleshores, ω_1 i ω_2 són generadors de Ω, i per tant, existeixen nombres enters a, b, cd de manera que

$$\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix},$$

i $ad - bc = \pm 1$. Si tinguéssim $ab - cd = -1$, aleshores canviant ω_1 per $-\omega_1$, c per $-c$ i d per $-d$, obtindriem una equació equivalent però amb $ad - bc = 1$. Ara, per com hem triat aquests nous generadors, es compleix

$$|\omega_2| \leq |\omega_2| \text{ i } |\omega_1 \pm \omega_2| \leq |\omega_2|.$$

Per tant, agafant $\tau = \frac{\omega_2}{\omega_1}$ tenim que $\tau \sim \tau'$ mòdul Γ, que $|\tau| \geq 1$ i $|\tau \pm 1| \geq |\tau|$, com volíem. □

Teorema 6.1.4. *El conjunt tancat*

$$R_\Gamma := \{\tau \in H || \tau| \geq 1, |\tau + \overline{\tau}| \leq 1\}$$

és un domini fonamental de Γ. A més a més si tenim $A \in \Gamma$ i es compleix $\tau = A\tau$ per algun $\tau \in \overset{\circ}{R}_\Gamma$, aleshores $A = Id$, si $\tau = A\tau$ per algun $\tau \in R_\Gamma$ amb $|\tau| = 1$, aleshores $A = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$, i si $\tau = A\tau$ per algun $\tau \in R_\Gamma$ amb $|\tau + \overline{\tau}| = 1$, aleshores $A = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$.

Dem. Per el lema anterior, sabem que si tenim $\tau' \in H$, aleshores existeix un $\tau \in R_\Gamma$ equivalent a τ'. Veiem, doncs que no tenim dos punts equivalents sota Γ en R_Γ. Posem $\tau' = A\tau$ amb $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$, amb $\tau \in R_\Gamma$ i $c \neq 0$. Aleshores, $\mathrm{Im}(\tau') = \dfrac{\mathrm{Im}(\tau)}{|c\tau + d|^2}$, de manera que

$$|c\tau + d|^2 = (c\tau + d)(c\overline{\tau} + d) = c^2\tau\overline{(\tau)} + cd(\tau + \overline{(\tau)}) + d^2 > c^2 - |cd| + d^2,$$

ja que $\tau \in R_\Gamma$ i $c \neq 0$. I com que $c^2 - |cd| + d^2 \geq 1$, tenim $|c\tau + d|^2 > 1$, i per tant $\mathrm{Im}(\tau') < \mathrm{Im}(\tau)$. Suposem doncs que τ i τ' són punts interiors de R_Γ i que són equivalents sota Γ. Aleshores

$$\tau' = \frac{a\tau + b}{c\tau + d} \text{ i } \tau = \frac{d\tau' - b}{-c\tau' + a},$$

I si $c \neq 0$ tindriem $\mathrm{Im}(\tau') < \mathrm{Im}(\tau)$ i $\mathrm{Im}(\tau) < \mathrm{Im}(\tau')$ que aeria contradictori. Per tant ha de ser $c = 0$, la qual cosa implica que $a = d = \pm 1$ i que $b = 0$, és a dir que $\tau = \tau'$. Finalment, si $A\tau = \tau$ per algun τ, utilitzant el mateix argument obtenim que $c = 0$ i que per tant $A = Id$. Els altres dos casos es fan de manera similar.

□

6.2 Funcions modulars

Definició 6.2.1. Una funció $f : H \to \mathbb{C}$ diem que és modular si

1. f és meromorfa en H.
2. $f(A\tau) = f(\tau)$ per tot $A \in \Gamma$.
3. f té desenvolupament de Fourier de la forma

$$f(\tau) = \sum_{n=-m}^{\infty} a(n)e^{2\pi n\tau}.$$

Observació 6.2.2. La condició (3) fa referència al comportament de f en el punt $i\infty$. Concretament, si $m > 0$, f té un pol d'ordre m en $i\infty$; i per altra banda si $m \leq 0$ aleshores f és analítica en $i\infty$. És a dir, si considerem el semiplà de Poincaré i el compactifiquem adjuntant-li $\mathbb{P}(\mathbb{Q})$ i identificant-la amb el punt de l'infinit pel quocient $H \cup \mathbb{P}^1(\mathbb{Q})/SL(2,\mathbb{Z})$, podem dotar d'estructura anal·lítica a aquest conjunt definint una base d'entorns de $i\infty$ com $B_a := \{z \in h : |\mathrm{Im}(z)| > a\}$. Observem que per a tot nombre racional $\frac{a}{b} \in \mathbb{P}^1(\mathbb{Q})$, podem suposar que és una fracció irreductible, i aleshores existeixen $x, y \in \mathbb{Z}$ tal que $xa - yb = 1$; i per tant, prenent $A = \begin{pmatrix} a & y \\ b & x \end{pmatrix} \in SL(2,\mathbb{Z})$, és clar que $Ai\infty = \frac{a}{b}$.

Teorema 6.2.3. *La funció $J(\tau)$ és una funció modular.*

Dem. El punt (1) és clar de la definicó de les funcions g_2' i g_3'. A més a més, $J(\tau)$ ens dona l'invariant j de la coba el·líptica associada a la xarxa generada per $\{1, \tau\}$. Per tant, conm ja haviem dit tenim que $J(\tau) = \dfrac{1}{q} + 744 + \cdots$, on $q = e^{2\pi i\tau}$ i clarament compleix (3). Ens falta veure doncs que compleix (2). Suposem que tenim $\tau \in H$ i $A \in \Gamma$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ i escrivim $\tau' = \dfrac{a\tau + b}{c\tau + d}$. Aleshores es que $\{1, \tau\}$ és equivalent a $\{1, \tau'\}$, i per tant que generen la mateixa xarxa Λ. Aleshores, per definició de les sèries d'Eisenstein, $g_2'(\tau) = g_2'(\tau')$ i $g_3'(\tau) = g_3'(\tau')$, i per tant, $J(\tau) = J(\tau')$. □

Teorema 6.2.4. *Si f és una funció modular no idènticament zero, aleshores f té el mateix nombre de pols que de zeros en la clausura de R_Γ en $H \cup i\infty$.*

Observació 6.2.5. La demostració d'aquest teorema consisteix a aplicar el teorema dels residus en els diferents casos possibles de la situació dels zeros i els pols de J. Es poden trobar els detalls de la prova en [1].

Teorema 6.2.6. *Tota funció racional de J és una funció modular i, recíprocament, tota funció modular pot ser expressada com una funció racional de J.*

Dem. La primera implicació es clara. Veiem el recíproc. Suposem, doncs que tenim f una funció modular amb zeros en els punts $z_1, \ldots, z_n$ i pols en $p_1, \ldots, p_n$ i escrivim

$$g(\tau) = \prod_{k=1}^{n} \frac{J(\tau) - J(z_k)}{J(\tau) - J(p_k)},$$

on multipliquem per 1 cada vegada que z_k o p_k són ∞. Aleshores, g és una funció amb el mateix nombre de zeros i de pols que f en la clausura de R_Γ.Per tant f/g no te zeros ni pols, i per resultats bàsics d'anàlisi complexa, f/g ha de ser constant, d'on veiem que f ha de ser una funció racional de J. □

6.3 Formes modulars de pes k

Continuem utilitzant les matiexes notacions.

Definició 6.3.1. Una funció f es diu que és una forma modular entera de pes k si satisfà les condicions següents.

1. f és analítica en H.
2. $f(A\tau) = (c\tau + d)^k f(\tau)$ per tota $A \in \Gamma$ i $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
3. El desenvolupament de Fourier de f té la forma

$$f(\tau) = \sum_{n=0}^{\infty} c(n) e^{2\pi i n \tau},$$

on $c(n) \in \mathbb{C}$. A més a més, el terme constant $c(0)$ és el valor de f en $i\infty$ i es denota per $f(i\infty)$. Denotem per M_k el conjunt de les formes modulars de pes k.

Teorema 6.3.2. *Sigui f una forma modular entera de pes k no identicament zero a la clausura de la regió fonamental R_Γ. Aleshores, tenim la fòrmula*

$$k = 12N + 6N(i) + 4N(\rho) + 12N(i\infty),$$

on i i ρ són vètexs del domini fonamental i $N(P)$ és l'ordre de f en P.

Dem. Com en el teorema 6.2.4, la demostració es realitza mitjançant el teorema dels residus distingint diferents casos. [1] □

Observació 6.3.3. Siguin f i g dues formes modulars de pesos k_f i k_g respectivament, aleshores, fg és una forma modular de pes $k_f + k_g$. De la mateixa manera, si g no té zeros en H ni en $i\infty$ aleshores f/g és una forma modular de pes $k_f - k_g$.

Corol·lari 6.3.4. (a) *Les úniques funcions modulars enteres de pes 0 són les funcions constants.*

(b) *Si k és senar, si $k < 0$ o si $k = 2$, la única funció modular entera de pes k és la funció zero.*

(c) *Tota funció modular entera no constant te pes més gran o igual que 4 i parell.*

(d) *L'única fomra parabòlica de pes $k < 0$ és la funció zero.*

Dem. [1] □

Teorema 6.3.5. *Sigui f una forma modular entera de pes parell $k \geq 0$ i definim $G_0(\tau) = 1$, per a tot τ. Aleshores f s'expressa de forma única com a combinació lineal*

$$f = \sum_{r=0, k-12r \neq 2}^{[k/12]} a_r G_{k-12r} \Delta^r,$$

on a_r són nombres complexos. Anomenem formes parabòliques a les formes modulars de pes parell k i amb $a_0 = 0$.

Dem. Si $k < 12$, aleshores, el sumatori de l'enunciat te com a màxim un terme. Pel teorema 6.3.2, sabem que si $k < 12$, aleshores $N = N(i\infty) = 0$, així que els únics possibles zeros de f són als vèrtexs ρ i i. Per exemple, si $k = 4$, ha de ser $N(\rho) = 1$ i $N(i) = 0$, com en G_4. Per tant, f/G_4 és una constant $a_0 \in \mathbb{C}$, és a dir, $f = a_0 G_4$. Els casos $k = 6, 8, 10$ és resolen de forma anàloga a aquest, i per a $k = 0$ i $k = 2$ el resultat es trivial, ja que en el primer cas f seria una funció constant i en el segon cas la suma és buida, i sabem que l'única funció modular de pes 2 és la funció zero pel corol·lari 6.3.4. Per tant, només ens resta suposar que k és un nombre parell més gran o igual que 12.

Farem inducció sobre k. Observem que si tenim una forma parabòlica en M_k, podem escriure-la com a producte Δh, on $h \in M_{k-12}$. Suposem que el teorema es cert per a formes modulars de pes més petit que k. Aleshores, G_k és una forma modular de pes k que no s'anula en $i\infty$. Aleshores, si escrivim $c = \dfrac{f(i\infty)}{G_k(i\infty)}$, la forma entera $f - cG_k$és una forma parabòlica en M_k, per tant, existeix un $h \in M_{k-12}$ tal que $f - cG_k = \Delta h$. Aplicant la hipòtesis d'inducció a h, tenim que

$$\sum_{r=0,k-12-12r\neq 2}^{[(k-12)/12]} b_r G_{k-12-12r}\Delta^r = \sum_{r=1,k-12r\neq 2}^{[k/12]} b_{r-1} G_{k-12r}\Delta^{r-1}.$$

Per tant, $f = cG_k + \Delta h$ té la representació que buscàvem. La unicitat provè de la independència lineal dels productes $G_{k-12r}\Delta^r$. □

Observació 6.3.6. Durant la prova, hem vist que M_k és un espai vectorial sobre $\mathbb{C}$ i de dimensió finita. És més, hem vist que els G_{k-12r} que apareixen en la suma del teorema formen una base d'aquest espai vectorial. Per tant, tenim que

$$\dim M_k = \begin{cases} \left[\frac{k}{12}\right] & \text{si } k \equiv 2 \pmod{12}, \\ \left[\frac{k}{12}\right] + 1 & \text{si } k \not\equiv 2 \pmod{12}. \end{cases}$$

Observació 6.3.7. El conjunt de les formes parabòliques és un subespai lineal de M_k que denotem per S_k. A més a més, pel teorema 6.3.5, $\dim(S_k) = \dim(M_k) - 1$.

6.4 Formes modulars de pes k i nivell N

Hem vist que el grup de les transformacions modulars és isomorf al grup $PSL(2,\mathbb{Z})$, és a dir, a $SL(2,\mathbb{Z})/\{Id, -Id\}$. Definirem els subgrups de congruència de $SL(2,\mathbb{Z})$ de manera similar.

Definició 6.4.1. Donat un nombre enter N, considerem ara la projecció

$$\begin{gathered} SL(2,\mathbb{Z}) \xrightarrow{\pi_N} SL(2,\mathbb{Z}/N\mathbb{Z}) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}. \end{gathered}$$

Aleshores, anomenem subgrup principal de congruència de nivell N al nucli de π_N mòdul $\{Id, -Id\}$, és a dir

$$\overline{\Gamma(N)} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}); \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} / \{Id, -Id\} \subset PSL(2,\mathbb{Z}).$$

Considerem el subgrup de $SL(2,\mathbb{Z})$

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}); c \equiv 0 \pmod{N} \right\}.$$

Anomenem subgrup de Hecke de nivell N al subgrup quocient següent

$$\overline{\Gamma_0(N)} := \Gamma_0(N)/\{Id, -Id\} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL(2,\mathbb{Z}); c \equiv 0 \pmod{N} \right\} /\{Id, -Id\};$$

és un subgrup de $PSL(2,\mathbb{Z})$.

Observació 6.4.2. Els elements de $\overline{\Gamma_0(N)}$ els denotarem per $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ enlloc de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Definició 6.4.3. Una funció f és diu que és una forma modular entera de pes k i nivell N si satisfà les següents condicions:

1. f és analítica en H.
2. $f(A\tau) = (c\tau + d)^k f(\tau)$ per a tota $A \in \Gamma_0(N)$ i $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.
3. La sèrie de Fourier de f té la forma

$$f(\tau) = \sum_{n=0}^{\infty} c(n) e^{2\pi i n \tau}.$$

De la mateixa manera que per a $N = 1$, denotem una forma parabòlica de pes k i nivell N a una forma modular tal que la seva sèrie de Fourier és de la forma

$$f(\tau) = \sum_{n=1}^{\infty} c(n) e^{2\pi i n \tau}.$$

Anomenem $M_k(N)$ a l'espai de les formes modulars de pes k i nivell N i $S_k(N)$ al de les formes parabòliques amb les mateixes condicions.

Clarament, $M_k(N)$ i $S_k(N)$ formen espais vectorials sobre $\mathbb{C}$, de manera que, com per al cas $N = 1$ es pot calcular la seva dimensió, que explicitem en el cas $k = 2$.

Teorema 6.4.4. *Siguin*

$$\begin{cases} \mu = [SL(2,\mathbb{Z}) : \Gamma_0(N)] = N \prod_{l|N} (1 + l^{-1}), \\ v_2 = \prod_{l|N,\ l\ primer} \left(1 + \left(\frac{-1}{l}\right)\right) \text{ si 4 no divideix } N, \quad 0 \text{ altrament} \\ v_3 = \prod_{l|N,\ l\ primer} \left(1 + \left(\frac{-3}{l}\right)\right) \text{ si 9 no divideix } N, \quad 0 \text{ altrament} \\ v_\infty = \sum_{d|N,\ d>0} \varphi\left(\left(d, \frac{N}{d}\right)\right) \end{cases},$$

on, $\left(\frac{-1}{l}\right)$ *i* $\left(\frac{-3}{l}\right)$ *són els símbols de Legendre, donats per*

$$\left(\frac{-1}{l}\right) = \begin{cases} 0 & si\ l = 2 \\ 1 & si\ l \equiv 1 \pmod 4 \\ -1 & si\ l \equiv 3 \pmod 4 \end{cases}$$

i

$$\left(\frac{-3}{l}\right) = \begin{cases} 0 & si\ l = 3 \\ 1 & si\ l \equiv 1 \pmod 3; \\ -1 & si\ l \equiv 2 \pmod 3 \end{cases}$$

i φ és la funció d'Euler. Aleshores, tenim que

$$\dim(S_2(N)) = 1 + \frac{\mu}{12} - \frac{v_2}{4} - \frac{v_3}{4} - \frac{v_\infty}{2}.$$

Dem. [17] □

Com a conseqüència d'aquest teorema, tenim la taula de dimensions següent, contrastada a [11]. (ref. [3])

N	1	2	3	4	5	6	7	8	9	10	11	12	13
μ	1	3	4	6	6	12	8	12	12	18	12	24	14
v_2	1	1	0	0	2	0	0	0	0	2	0	0	2
v_3	1	0	1	0	0	0	2	0	0	0	0	0	2
v_∞	1	2	2	3	2	4	2	4	4	4	2	6	2
$\dim(S_2(N))$	0	0	0	0	0	0	0	0	0	0	1	0	0

Observació 6.4.5. v_2 i v_3 són el nombre de punts el·líptics d'ordres 2 i 3, i v_∞ el de punts parabòlics de $\overline{\Gamma_0(N)}$.

6.5 Funció L de E i teorema de modularitat

Ara associarem a E una sèrie L de manera que aquesta codifiqui algunes propietats aritmètiques de E. Per això utilitzarem els polinomis χ_{σ_p} ja que aquests ens determinen analíticament la informació sobre els punts d'orde finit de E. Comencem definit el producte d'Euler associat a E.

Definició 6.5.1. Definim el producte infinit d'Euler associat a E com la funció complexa

$$L_E(s) = \prod_{p|\Delta_E} \frac{1}{(1 - t_p p^{-s})} \prod_{p\nmid\Delta} \frac{1}{1 - t_p p^{-s} + p^{1-2s}},$$

on $t_p = 1 + p - a_p$ i a_p és el nombre de punts $\mathbb{F}_p$-racionals de $E(p)$. $L_E(s)$ convergeix per a tot s complex tal que $\mathrm{Re}(s) > \frac{3}{2}$.

Cada factor d'aquest producte es pot escriure en forma de sèrie geomètrica, de manera que

$$\frac{1}{(1 - t_p p^{-s})} = \sum_{k=0}^{\infty} (t_p p^{-s})^k, \text{ si } p|\Delta,$$

$$\frac{1}{1 - t_p p^{-s} + p^{1-2s}} = \sum_{k=0}^{\infty} (t_p p^{-s} + p^{1-2s})^k, \text{ si } p \nmid \Delta.$$

Doncs, podem escriure $L_E(s) = \prod_{p|\Delta_E} \sum_{k=0}^{\infty}(t_p p^{-s})^k \prod_{p\nmid\Delta} \sum_{k=0}^{\infty}(t_p p^{-s} + p^{1-2s})^k = \sum_{n\in\mathbb{N}} b_n n^{-s}$, és a dir, en forma de sèrie de Dirichlet. A més a més, del desenvolupament d'aquest producte es dedueix que $b_p = t_p$ per a tot p primer. El següent teorema, conjecturat per E. Artin i provat més tard per Hasse ens permet assgurar la convergància de la sèrie per a $Re(s) > \frac{3}{2}$.

Teorema 6.5.2. *Sigui t_p definit com anteriorment. Aleshores $|t_p| \leq 2\sqrt{p}$.*

Dem. [18] □

Per tant, la sèrie també convergeix per a $Re(s) > \frac{3}{2}$ i en conseqüència, L_E és analítica en aquesta regió del pla complex.

Observació 6.5.3. Així doncs, la funció L_E ens dóna informació sobre els punts de E d'ordre p primer finit. De fet, L_E determina la corba E.

Com en el cas de la funció zeta de Riemann, que a priori està definida per als nombres complexos de part real més gran que 1, però que es pot extendre a una funció meromorfa de tot el pla complex, a L_E també li passa el mateix. El teorema següent, degut a Hasse, ens en dóna més detall.

Teorema 6.5.4. *La funció L_E té una extensió analítica a tot $\mathbb{C}$ i a més a més satisfà una equació funcional que relaciona els valors de s i $s-2$. Concretament, si N_E és el conductor de E i $\Gamma(s)$ és la funció gamma de Euler, definim*

$$\xi_E(s) = N_E^{s/2}(2\Pi)^{-s}\Gamma(s)L_E(s);$$

$\xi_E(s)$ és holomorfa en tot $\mathbb{C}$ i compleix $\xi_E(s) = \mp\xi_E(2-s)$.

Dem. [4], [21], [19] □

Enunciem ara el conegut teorema de modularitat provat per Andrew Wiles el 1995.

Teorema 6.5.5. *Tota corba el·líptica semiestable és modular.*

Dem. [22] □

En el nostre context, interpretem el teorema amb el següent corol·lari que li dona sentit.

Corol·lari 6.5.6. *Sigui E una corba el·líptica de Frey i L_E la sèrie L associada a E,*

$$L_E(s) = \sum_{n=1}^{\infty} b_n n^{-s} \qquad , \qquad b_n \in \mathbb{C}.$$

Aleshores,

$$f_E(z) := \sum_{n=1}^{\infty} b_n e^{2\pi i n z}$$

és una forma parabòlica de pes 2 i nivell el conductor de E, N_E.

Capítol 7

Representacions de Galois

7.1 Representació d'un grup

Per entendre la idea de la representació de Galois associada a una corba el·líptica hem seguit l'article [9] i una referència bàsica ha estat [16].

Definició 7.1.1. Siguin G un grup topològic, A un anell commutatiu i topològic i V un A-mòdul lliure de dimensió finita, n. Aleshores, definim una representació n dimensional de G sobre A com un morfisme continu

$$\rho : G \to GL(V) \cong GL(n, A).$$

Diem que la representació és irreductible si $V \neq \{0\}$ i no existeix cap submòdul M no tivial de V estable (invariant) per tots els automorfismes de $\rho(G)$, és a dir, tal que $\rho(G)M \subset M$.

A nosaltres, tot i això, ens interessen les representacions 2-dimensionals de grups de Galois sobre $\mathbb{Z}/n\mathbb{Z}$. És a dir, sigui $L|\mathbb{Q}$ una extensió de Galois de $\mathbb{Q}$, i sigui G el seu grup de Galois, ens interessaran les representacions de la forma

$$\begin{aligned} \rho : G &\to GL(2, \mathbb{Z}/n\mathbb{Z}) \\ \sigma &\to \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \end{aligned}$$

Donada una representació d'aquest tipus, podem considerar el polinomi característic de $\rho(\sigma)$

$$\chi_{\rho(\sigma)}(T) = T^2 - \mathrm{Tr}(\rho(\sigma))T + \det(\rho(\sigma))$$

on $\mathrm{Tr}(\rho(\sigma)) = a_\sigma + d_\sigma$ i $\det(\rho(\sigma)) = a_\sigma d_\sigma - b_\sigma c_\sigma$. Aquest ens dóna molta informació sobre la matriu, i de fet tenim la seguent definició.

Definició 7.1.2. ρ és semisimple si i només si ρ està determinada per $\{\chi_{\rho(\sigma)}(T)\}$.

Recordem ara la definició de automorfisme de Forbenius. Suposem que tenim K un cos de nombres tal que $A \subset K$.

Definició 7.1.3. Sigui p un nombre primer, aleshores, $\sigma \in G$ és un automorfisme de Frobenius per a p si i només si existeix un ideal primer $\mathfrak{p}$ de l'anell dels enters de K que conté p i tal que per a tot x d'aquest anell d'enters es té que $\sigma(x) - x^p \in \mathfrak{p}$.

Per a cada p primer, en general, hi ha infinits automorfismes de Frobenius; agafem-ne un per a cada p primer i l'anomenem σ_p. Aleshores tenim el teorema següent.

Teorema 7.1.4. (Teorema de densitat de Chevotarev). *Si ρ es semisimple, aleshores, ρ ve determinada per $\{\chi_{\rho(\sigma_p)}(T); p \text{ primer}\}$. A més a més, podem ometre un conjunt finit arbitrari de primers p.*

Dem. [20], [2]. □

7.2 Representacions associades a una corba el·líptica

Recordem que donada E una corba el·líptica sobre $\mathbb{Q}$, aleshores

$$E[n] \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}},$$

i, per tant, $\#E[n] = n^2$.

En la demostació del teorema 5.2.3, es veu que cada $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])|\mathbb{Q})$ indueix una permutació del conjunt $E[n]$, és a dir, dóna una aplicació de $E[n]$ en ell mateix. Ara, com que $E[n]$ es pot generar per dos elements P_1 i P_2, aleshores, els n^2 elements de $E[n]$ venen donats pel conjunt

$$\{a_1P_1 + a_2P_2 | a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}\}.$$

És a dir, cada element de $E[n]$ es pot expressar com $a_1P_1 + a_2P_2$ per a uns únics $a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}$.

Ara, si tenim $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])|\mathbb{Q})$, aquest indueix un morfisme de $E[n]$ en ell mateix de manera que $\sigma(a_1P_1 + a_2P_2) = a_1\sigma(P_1) + a_2\sigma(P_2)$ per a tot $a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}$. Això en diu que la imatge de qualsevol punt de $E[n]$ queda determinada per la imatge per σ de P_1 i P_2. Però $\sigma(P_1), \sigma(P_2) \in E[n]$ i per tant $\sigma(P_1) = \alpha_\sigma P_1 + \gamma_\sigma P_2$ i $\sigma(P_2) = \beta_\sigma P_1 + \delta_\sigma P_2$. Així doncs, $\alpha_\sigma, \beta_\sigma, \gamma_\sigma, \delta_\sigma$ són elements de $\mathbb{Z}/n\mathbb{Z}$ unívocament determinats per σ.

Prenem, doncs per a σ, la notació de matriu $\begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}$.

Aleshores, si τ és un altre element de $\mathrm{Gal}(\mathbb{Q}(E[n])|\mathbb{Q})$, el morfisme composició $\tau\circ\sigma$ conicideix amb el producte usual de matrius

$$\begin{pmatrix} \alpha_{\tau\circ\sigma} & \beta_{\tau\circ\sigma} \\ \gamma_{\tau\circ\sigma} & \delta_{\tau\circ\sigma} \end{pmatrix} = \begin{pmatrix} \alpha_\tau & \beta_\tau \\ \gamma_\tau & \delta_\tau \end{pmatrix} \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}.$$

A més, σ és en realitat un isomorfisme, ja que el determinant de

$$M_\sigma = \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}$$

és invertible, i per tant en podem calcular la matriu inversa

$$M_{\sigma^{-1}} = \begin{pmatrix} \alpha_{\sigma^{-1}} & \beta_{\sigma^{-1}} \\ \gamma_{\sigma^{-1}} & \delta_{\sigma^{-1}} \end{pmatrix},$$

que determina un automorfisme σ^{-1} de $E[n]$ donat per

$$\sigma(P_1) = \alpha_{\sigma^{-1}} P_1 + \gamma_{\sigma^{-1}} P_2,$$
$$\sigma(P_2) = \beta_{\sigma^{-1}} P_1 + \delta_{\sigma^{-1}} P_2,$$

de manera que $M_\sigma M_{\sigma^{-1}} = Id$ i per tant σ^{-1} és el morfisme invers de σ.

Tot això ens permet construir un morfisme

$$\rho_{E,n} : \mathrm{Gal}(\mathbb{Q}(E[n])|\mathbb{Q}) \to GL_2(\frac{\mathbb{Z}}{n\mathbb{Z}})$$
$$\sigma \mapsto \rho_n(\sigma) = \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}.$$

És a dir, que tenim una representació del grup de Galois $\mathrm{Gal}(\mathbb{Q}(E[n])|\mathbb{Q})$. Podem resumir aquests fets en el teorema següent.

Teorema 7.2.1. *Siguin E una corba el·líptica donada per una equació de Weierstrass de coeficients en $\mathbb{Q}$, i $n \geq 2$ in nombre enter. Fixem dos generadors P_1 i P_2 de $E[n]$. Aleshores $\rho_{E,n}$ és un isomorfisme de grups.*

Dem. És clar que ρ_n és un morfisme. Veiem, doncs, que és un isomorfisme. Suposem doncs que tenim σ un element del nucli de ρ_n, és a dir, tal que $\rho_n(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Això ens diu que $\sigma(P_1) = P_1$ i $\sigma(P_2) = P_2$, i per tant que $\sigma(P) = P$ per a tot $P \in E[n]$. Ara, aplicant aquest fet a la definició, tenim que $(x, y) = (\sigma(x), \sigma(y))$, i per tant que σ fixa totes les coordenades dels punts de $E[n]$. Així doncs, σ fixa a tots els elements de $\mathbb{Q}(E[n])$ i per tant ha de ser la identitat, i ρ_n és un isomorfisme.

Teorema 7.2.2. *$\rho_{E,n}$ és semisimple per a quasi tots els nombres naturals n.*

Aleshores, aplicant el teroema de densitat de Chevotarev, sabem que $\rho_{E,n}$ queda determinada pels polinomis característics dels automorfismes de Frobenius σ_p amb p primer. A més a més, podem ometre els primers que divideixin $n \cdot N_E$; aquests venen donats pel resultat següent.

Teorema 7.2.3. (Hasse) *Siguin $E(p)$ la reducció de E mòdul p, i a_p el nombre de punts $\mathbb{F}_p$-racionals de $E(p)$; aleshores*

$$\mathrm{Tr}(\rho_{E,n}(\sigma_p)) \equiv p + 1 - a_p \ mod\ n,$$
$$\det(\rho_{E,n}(\sigma_p)) \equiv p \ mod\ n.$$

Dem. [16] □

Corol·lari 7.2.4. *Els polinomis*

$$\{\chi_p(T) = T^2 + (a_p - p - 1)T + p\,;\ p \text{ nombre primer que no divideix } N_E\}$$

determinen totes les representacions de $\rho_{E,n}$.

Corol·lari 7.2.5. *La representació $\rho_{E,n}$ és irreductible*

Capítol 8

Teorema de Fermat i aplicacions

8.1 Teorema de Fermat

Definició 8.1.1. Una representació

$$\rho : G_{\mathbb{Q}} \to GL_(2, \mathbb{Z}/p^k)$$

és modular de nivell N si existeix una forma parabòlica de pes 2 i nivell N donada per

$$f(z) = \sum_{n=1}^{\infty} c_n e^{2\pi i n z}, \text{ amb } c_n \in \bar{\mathbb{Z}} \text{ i } c_1 = 1,$$

tal que per a tots els primers ℓ excepte potser un conjunt finit, es té que

$$\mathrm{Tr}(\rho(\sigma_\ell)) \equiv c_\ell \pmod{\mathfrak{p}_k},$$

on $\mathfrak{p}_k$ és un ideal de $\overline{\mathbb{Z}}$, la clausura entera de $\mathbb{Z}$ en $\overline{\mathbb{Q}}$, que conté p^k i σ_ℓ és un automorfisme de Frobenius per a ℓ.

Teorema 8.1.2. *Sigui E una corba el·líptica semiestable sobre $\mathbb{Q}$ amb $L_E(s) = \sum_{n=1}^{\infty} b_n n^{-s}$. Aleshores la representació ρ_{E,ℓ^k} és modular per a tot primer ℓ i tota $k \in \mathbb{N}$.*

Dem. La demostració d'aquest teorema és consequència del coroll·lari del teorema de modularitat 6.5.6 i del teorema 7.2.3. □

Ara, donada ρ una repsresentació irreductible modular de nivell N, J-P. Serre es va preguntar quin era el nivell N_ρ mímim tal que ρ era una representació modular de nivell N_ρ, va conjecturar que N_ρ venia donat pel conductor d'Artin, definició del qual no donarem en aquest treball. Però per al cas que ens ocupa, prenent $E = E_{A,B,C}$ la corba el·líptica de Frey associada a A, B i C nombres enters com en el capítol 4 i $\rho_{E,p}$ és la representació associada als punts de p-torsió de E, aleshores, el conductor d'Artin d'aquesta ve donat per

$$N_{\rho_{E,p}} = \prod_{\ell \neq p \text{ primer},\ v_\ell(j_E) \not\equiv 0 \pmod{p}} \ell = \prod_{\ell \neq p \text{ primer},\ v_\ell(ABC/2^4) \not\equiv 0 \pmod{p}} \ell.$$

Definició 8.1.3. Diem que una representació mòdular de nivell N és finita en p un primer no senar, si N és una potència p-èsima, excepte una potència de 2.

Observació 8.1.4. Per els resultats de ramificació vistos en el capítol 5, és clar que $\rho_{E,p}$ és una representació finita en p.

Teorema 8.1.5. (Mazur-Ribet) *Sigui k un cos de característica $p \geq 3$, k' la seva clausura algebraica i $\rho : G_{\mathbb{Q}} \to GL(2, F)$ una representació de $G_{\mathbb{Q}}$ irreductible sobre k' i modular de nivell N en el grup lineal d'un espai vectorial 2-dimensional sobre k. Si ρ és finita en p i de pes 2, aleshores ρ satisfà la conjectura de Serre, és a dir, podem prendre N com el conductor d'Artin N_ρ.*

Dem. [14] □

Tornant al cas de la corba de Frey associada a una hipotètica solució de l'equació de Fermat, recordant que aquesta venia donada per

$$E = E_{a^p,b^p,c^p} : Y^2 = X^3 + (A+B)X^2 + ABX$$

amb $A = a^p$, $B = b^p$ i $C = c^p$, $A \equiv 0 \bmod 2^5$ i $B \equiv 1 \bmod 4$; hem vist que aquesta és una corba semiestable 4.1.1, per tant pel teorema de Wiles (6.5.6),

$$f_E(z) := \sum_{n=1}^{\infty} b_n e^{2\pi i n z}$$

és una forma parabòlica de pes el conductor de E, $N_E = \prod_{\ell \text{ primer},\ \ell | ABC} \ell$. Ara, com que la representació $\rho_{E,p} : G_{\mathbb{Q}} \to E[p]$ satisfà totes les hipòtesis del teorema de Mazur-Ribet (8.1.5), podem prendre com a N el conductor d'Artin de $\rho_{E,p}$. Ara, per les propietats de la ramificació del cos $\mathbb{Q}(E[p])$ (cap. 5) i per la definició del conductor d'Artin que hem donat per al nostre cas, es veu clarament que $N_{\rho_{E,p}} = 2$, ja que

$$N_{E,p} = 2 \prod \ell,$$

on ℓ recorre el cojunt de primers que divideixen $AB(A-B)$ amb multiplicitat una potència diferent de p, però les propietats de ramificació del capítol 5 i la proposició 4.1.1 ens diuen que si ℓ és un primer senar, l'exponent de ℓ en el discriminant minimal de $E = E_{a^p,b^p,c^p}$, Δ_E és sempre divisible per p. És a dir, $\rho_{E,p}$ és una representació modular de pes 2 i nivell 2, la qual cosa implicaria l'existència d'una forma parabòlica no trivial de pes dos i nivell 2, però per les dimensions que es mostren en la taula del capítol 6, és clar que aquesta no pot existir; això prova el teorema de Fermat.

8.2 Altres equacions diofantines

La idea d'utilitzar la corba de Frey per resoldre el problema de l'equació de Fermat, es pot aplicar de manera anàloga o similar per resoldre altres equacions diofantines. Per exemple, si considerem l'equació

$$Z_1^p - Z_2^p = L^m Z_3^p,$$

on p és un nombre primer, m és un nombre enter posititu i $L \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$, podem prendre un solució hipotètica no tivial de l'equació (a, b, c); és a dir, tal que $abc \neq 0$. Aleshores, prenent $A = a^p$, $B = b^p$ i $C = L^m c^p$, i suposant, sense pèrdua de

generalitat que $A \equiv 0 \pmod{2^5}$ i $B \equiv 1 \pmod 4$, podem prendre la corba $E := E_{A,B,C}$ com la descrita en al capítol 4. Els invariants d'aquesta corba venen donats per

$$\Delta = a^{2p}b^{2p}c^{2p}L^{2m} \quad , \quad N_E = L \prod_{\ell prime,\, \ell | abc,\, \ell \neq L} \ell.$$

El conductor d'Artin de la representació associada als punts de $E[p]$ vindria donat per $N_{\rho_{E,p}} = 2 \cdot L$. Aplicant el mateix procediment que en el capítol anterior, arribaríem a la conclusió que l'existència d'aquests (a, b, c) implicaria l'existència d'una forma modular de pes 2 i nivell $2L$. En al cas que $L = 3, 5$, la taula del capítol 6 ens mostra una contradicció directa amb aquets fet. En els casos restants, la contradicció no és tant directa. Pe trobar-la, s'ha de probar l'existència d'una forma modular provinent de dues de pes i nivell més petits, una de les quals no ha de poder existir. Això porta una mica més de feina, però el resultat acaba sent el mateix.

No obstant, la corba de Frey és pot aplicar a molts més tipus d'equacions diofantines, tot i que per resoldre-les cal combinar-la amb eines molt tècniques. Se'n poden trobar exemples a [5], [6], [7].

Bibliografia

[1] Apostol, T. M. *Modular functions and Dirichlet series in number theory*, vol. 41. Springer Science & Business Media, 2012.

[2] Artin, E. The collected papers of emil artin (s. lang and j. tate, eds.), 1965.

[3] Bayer, P., and Travesa, A. "corbes modulars: Taules,"notes del seminari de teoria de nombres de barcelona. Tech. rep., UB-UAB-UPC, Barcelona, 1992.

[4] Deuring, M. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg 14*, 1 (1941), 197–272.

[5] Dieulefait, L., and Freitas, N. Fermat-type equations of signature (13, 13, p) via hilbert cuspforms. *arXiv preprint arXiv:1112.4521* (2011).

[6] Freitas, N. Recipes to fermat-type equations of the form xˆ r+ yˆ r= czˆ p. *arXiv preprint arXiv:1203.3371* (2012).

[7] Freitas, N., Naskrecki, B., and Stoll, M. The generalized fermat equation with exponents 2, 3, n. *arXiv preprint arXiv:1703.05058* (2017).

[8] Frey, G. Links between stable elliptic curves and certain diophantine equations. *Ann. Univ. Sareviensis, Ser Math. 1* (1986), 1–40.

[9] Frey, G. The way to the proof of fermat last theorem. *preprint 1997* (1997).

[10] Fulton, W. *Algebraic curves*. WA Benjamin, 1969.

[11] Hellegouarch, Y. *Invitation to the mathematics of Fermat-Wiles*. Academic Press, 2001.

[12] Lang, S. *Elliptic functions*. Springer, 1987.

[13] Lang, S. *Introduction to algebraic and abelian functions*. Springer Science & Business Media, 2012.

[14] Ribet, K. A. On modular representations of arising from modular forms. *Inventiones mathematicae 100*, 1 (1990), 431–476.

[15] Roquette, P. *Analytic theory of elliptic functions over local fields*. No. 1. Vandenhoeck u. Ruprecht, 1970.

[16] Serre, J.-P., Kuyk, W., and Labute, J. *Abelian l-adic representations and elliptic curves*, vol. 2. WA benjamin New York, 1968.

[17] Shimura, G. *Introduction to the arithmetic theory of automorphic functions*, vol. 1. Princeton university press, 1971.

[18] Silverman, J. H. *The arithmetic of elliptic curves*, vol. 106. Springer Science & Business Media, 2009.

[19] Tate, J. T. The arithmetic of elliptic curves. *Inventiones mathematicae 23*, 3 (1974), 179–206.

[20] Tschebotareff, N. Die bestimmung der dichtigkeit einer menge von primzahlen, welche zu einer gegebenen substitutionsklasse gehören. *Mathematische Annalen 95*, 1 (1926), 191–228.

[21] Weil, A. Jacobi sums as"grossencharaktere". *Transactions of the American Mathematical Society 73*, 3 (1952), 487–495.

[22] Wiles, A. Modular elliptic curves and fermat's last theorem. *Annals of mathematics 141*, 3 (1995), 443–551.