TREBALL DE FI DE GRAU

Grau en Matemàtiques

Títol: La conjectura de Sato-Tate

Autor: Marta Altarriba Fatsini

Director: Óscar Rivero Salgado

Departament: Departament de Matemàtiques

Convocatòria: 2018-2019

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

La conjectura de Sato–Tate

Marta Altarriba Fatsini

2019

Índex

Introducció

Donada una corba qualsevol, un problema clàssic és comptar el seu nombre de punts sobre un cos finit. És a dir, si C és corba definida per un polinomi $f(x, y)$, trobar el nombre

$$N_p := \#C(\mathbb{F}_p) = \#\{(a, b) \in \mathbb{F}_p^2 \mid f(a, b) = 0\}.$$

Per exemple, per a les còniques és senzill trobar una parametrització de la corba i comptar directament el nombre de solucions en $\mathbb{F}_p$. Però per a la majoria de corbes, el càlcul de N_p no és gens trivial.

Un cas interessant és el de les *corbes el·líptiques*, que prenent el seu model afí podem veure com corbes planes cúbiques no singulars de la forma

$$E : y^2 = x^3 + Ax + B.$$

Un dels motius pels quals les corbes el·líptiques són tan importants és que tenen estructura de grup. L'estudi d'aquest tipus de corbes té diverses aplicacions en criptografia i en la teoria de nombres. Un bon exemple d'això és la relació que tenen amb el famós *últim teorema de Fermat*, que diu que per a $m \geq 3$, no existeixen solucions enteres de l'equació

$$x^m + y^m = z^m$$

amb x, y, z diferents de zero. La clau de la demostració d'aquest teorema (Wiles, 1995) és un resultat sobre modularitat de corbes el·líptiques.

Respecte els nombres N_p, resulta més natural estudiar el nombre de punts de la projectivització de la corba, que fent un petit abús de notació, denotarem també com N_p. Calcular-lo explícitament per a una corba el·líptica arbitrària és difícil, no obstant, se'n coneix una fita:

Teorema (Hasse)**.** *Si N_p és el nombre de punts d'una corba el·líptica sobre $\mathbb{F}_p$, aleshores*

$$|N_p - p - 1| \leq 2\sqrt{p}.$$

Per altra banda, podem pensar el problema globalment i estudiar quin valor pren N_p segons el primer p. Així doncs, ens formulem la següent pregunta: com es distribueix la successió dels nombres N_p?

En teoria de nombres, és habitual estudiar qüestions que tracten la distribució d'uns valors determinats. Un resultat clàssic i molt important en aquest àmbit, és l'anomenat *teorema de Dirichlet*:

Teorema (Dirichlet)**.** *Sigui n un enter positiu fixat, i $1 \leq a \leq n$ un enter tal que $(a, n) = 1$. Existeixen infinits primers $p \equiv a \mod n$, i el límit*

$$\lim_{N \to \infty} \frac{\#\{1 \leq p \leq N \mid p \equiv a \mod n\}}{\#\{1 \leq p \leq N\}}$$

existeix i val $\frac{1}{\phi(n)}$, on ϕ és la funció d'Euler.

Dit d'una altra manera, els nombres primers estan *equidistribuïts* respecte les classes mòdul n coprimeres amb n. La paraula equidistribució, com ens podem imaginar, fa referència a que el nombre de termes d'una successió que pertanyen a un interval depèn únicament de la longitud d'aquest interval.

Un altre exemple representatiu sobre equidistribució, és el *teorema de Chebotarev*. És un resultat que, en termes de polinomis, respon a la pregunta següent: si tenim un polinomi mònic irreductible amb coeficients enters, quina és la seva factorització sobre $\mathbb{F}_p[x]$? El teorema ho relaciona amb el grup de Galois del polinomi en qüestió, i diu que és conseqüència d'un resultat d'equidistribució sobre les classes de conjugació del seu grup de Galois.

De fet, el concepte d'*equidistribució* es pot definir més generalment parlant de mesures. En el cas del teorema de Dirichlet, la mesura utilitzada és la de comptar habitual, però podem considerar-ne qualsevol.

Definició. Siguin X un espai compacte Hausdorff i $C(X)$ l'espai de Banach de les funcions $f : X \to \mathbb{C}$ amb la norma del suprem. Una successió $(x_i) \subset X$ és *equidistribuïda respecte la mesura* μ, o μ*-equidistribuïda*, si per a cada $f \in C(X)$,

$$\mu(f) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(x_i).$$

Tornant al nostre problema, la resposta a quina és la distribució dels N_p per a una corba el·líptica la dóna la *conjectura de Sato-Tate*. Si E és una corba el·líptica i considerem els nombres

$$x_p := \frac{p + 1 - N_p}{\sqrt{p}},$$

que pel teorema de Hasse sabem que es troben en l'interval $[-2, 2]$, aleshores la successió (x_p) és equidistribuïda en $[-2, 2]$.

La mesura per la qual (x_p) és equidistribuïda varia segons les característiques de la corba E. La propietat que la determina és la *multiplicació complexa* (CM), que fa referència a la mida de l'anell d'endomorfismes de la corba. Direm que una corba el·líptica E té CM si $\mathrm{End}(E)$ és estrictament més gran que $\mathbb{Z}$, i que no en té si $\mathrm{End}(E) \cong \mathbb{Z}$. Per als diferents casos, tenim les següents formulacions de la conjectura de Sato–Tate:

- Si la corba té CM, tenim dos possibilitats: si el cos de definició conté el de multiplicació complexa, la successió (x_p) està equidistribuïda en $[-2, 2]$ respecte la mesura

  $$\mu_{\mathrm{CM}} = \frac{1}{\pi} \frac{dz}{\sqrt{4 - z^2}};$$

  altrament, respecte la mesura

  $$\frac{1}{2}\, \delta_0 + \frac{1}{2}\, \mu_{\mathrm{CM}},$$

  on δ_0 és la delta de Dirac en el zero.

- En canvi, si la corba no té multiplicació complexa, se satisfà

  $$\lim_{N\to\infty} \frac{\#\{p \le N \mid x_p \in [a, b]\}}{\#\{p \le N\}} = \frac{1}{2} \int_a^b \sqrt{4 - t^2} dt.$$

L'objectiu principal d'aquest treball és entendre la conjectura de Sato–Tate. Està estructurat en cinc capítols, amb els continguts següents:

1. En primer lloc, veurem els dos exemples de resultats d'equidistribució esmentats per motivar la conjectura de Sato–Tate: el teorema de Dirichlet i el teorema de Chebotarev. Per poder entendre bé el segon, cal una breu introducció a la teoria de nombres algebraica per, en poques paraules, generalitzar la propietat dels enters de factoritzar en nombres primers.

   Un dels motius pels quals es va desenvolupar aquesta teoria, com hem vist abans en el cas de les corbes el·líptiques i la modularitat, és per demostrar l'últim teorema de Fermat. Un altre dels motius és per calcular grups de Galois de polinomis. El teorema de Chebotarev ens permet, fent servir les descomposicions d'un polinomi al reduir-lo sobre diferents cossos finits, determinar el seu grup de Galois.

   En aquest capítol, parlarem d'anells d'enters, de la descomposició en ideals primers, introduirem l'*element de Frobenius* i veurem algunes de les seves propietats. Llavors, enunciarem el teorema de Chebotarev i veurem l'aplicació que té en la descomposició de polinomis estudiant tres exemples: una extensió quadràtica, una cúbica i la ciclotòmica.

2. En el segon capítol, començarem veient amb detall com comptar el nombre de punts d'una cònica exemplificant-ho amb la circumferència. Tot seguit, definirem les corbes el·líptiques sobre un cos $\Bbbk$, de manera projectiva i afí, i n'estudiarem les possibles reduccions sobre els cossos finits $\mathbb{F}_p$, la llei de grup i l'anell d'endomorfismes.

   En concret, pararem especial atenció a l'*endomorfisme de Frobenius*, que per a una corba el·líptica E definida sobre un cos $\Bbbk$ és

   $$\begin{aligned} \phi_q : E(\overline{\Bbbk}) &\longrightarrow E(\overline{\Bbbk}) \\ (x, y) &\longmapsto (x^q, y^q), \end{aligned}$$

   i relacionarem algunes de les seves propietats amb el grup de Galois $\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Aleshores, enunciarem el teorema de Hasse, i després d'un seguit de lemes, el demostrarem.

   Per acabar, construirem el *mòdul de Tate*: un objecte que servirà per relacionar N_p amb els nombres N_{p^r}, per a tot enter $r \geq 1$.

3. A continuació, introduirem les *sèries L*. En general, són uns objectes associats a una representació de Galois, un morfisme d'un grup de Galois d'un cos a un grup de matrius, i permeten entendre millor l'estructura del grup de Galois absolut $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Les sèries L i les seves extensions analítiques, les funcions L, es poden relacionar amb objectes geomètrics però també amb d'altres analítics. Actualment, l'estudi d'aquestes funcions i les seves possibles relacions és un dels grans temes de la teoria de nombres.

   En el nostre context, són especialment rellevants perquè són les eines que s'utilitzen per demostrar la conjectura de Sato–Tate. En el capítol 3, començarem parlant de caràcters i de les seves sèries L associades, i les farem servir per demostrar el teorema de Dirichlet. Llavors, explicarem quina relació tenen amb les corbes i ens definirem la funció L associada a una corba el·líptica.

   L'altra idea important del capítol és el concepte d'*equidistribució*. El presentarem amb rigor i comentarem alguns resultats bàsics connectats amb els caràcters i les sèries L vistos anteriorment.

4. El quart capítol conté la part central del treball, l'enunciat i demostració de la conjectura de Sato–Tate. Primer de tot, explicarem amb detall què és la *multiplicació complexa* per a una corba el·líptica. Després, demostrarem la conjectura per a una corba el·líptica amb CM utilitzant les eines presentades al tercer capítol, distingint dos casos: la corba té CM sobre el cos de definició $\mathbb{k}$ o sobre un cos no contingut en $\mathbb{k}$. Obtindrem dues mesures per les quals la successió de valors $a_p := p + 1 - N_p$ normalitzada és equidistribuïda respectivament.

   Un cop vist el cas de les corbes amb multiplicació complexa, veurem l'altre cas. Quan la corba no té CM, en la demostració de la conjectura de Sato–Tate es fan servir unes matemàtiques d'un nivell més elevat, i per aquest motiu, veurem simplement una idea general de la prova pas a pas. En particular, parlarem per sobre de *formes modulars* i del teorema de modularitat.

   Al final del capítol, enunciarem la conjectura en termes de grups: definirem el *grup de Sato–Tate* d'una corba el·líptica i explicarem com calcular-lo per, d'aquesta manera, recuperar els resultats demostrats anteriorment.

5. En el darrer capítol, generalitzarem la conjectura per a *varietats abelianes*, ja que les corbes el·líptiques en són un cas particular (dimensió 1). Per començar, les definirem i els hi associarem un grup de Sato–Tate reproduint el procediment seguit en el capítol 4, i enunciarem la conjectura de Sato–Tate per a varietats abelianes en general.

   A continuació, estudiarem la conjectura de Sato–Tate des del punt de vista de la teoria de grups. El nostre objectiu és resoldre el problema de classificació següent: volem trobar els grups que poden ser grups de Sato–Tate per a una varietat abeliana determinada. Per aconseguir-ho, ens definirem dos grups molt relacionats amb el grup de Sato–Tate: el *grup de Mumford–Tate* i el *grup de Hodge*.

   Llavors, enunciarem la conjectura de Mumford–Tate, que fa referència als dos grups esmentats, demostrada únicament en dimensions baixes. Presentarem els *axiomes de Sato–Tate*, unes condicions que s'espera que satisfaci el grup de Sato–Tate d'una varietat abeliana. Veurem que en dimensió 1, el problema de classificació es redueix a l'estudi fet al final del capítol 4, comentarem la solució coneguda en dimensió 2, i per a dimensions més altes veurem que el problema continua obert. Com a últim resultat, més general, veurem que si la conjectura de Mumford–Tate es compleix, aleshores el grup de Sato–Tate d'una varietat abeliana satisfà els axiomes de Sato–Tate.

Capítol 1

Motivació: alguns resultats clàssics d'equidistribució

La conjectura de Sato–Tate és un resultat d'equidistribució, és a dir, ens diu com unes quantitats determinades estan distribuïdes asimptòticament. Per motivar-lo, veurem altres resultats importants d'equidistribució.

Un primer exemple important en l'aritmètica és el teorema de Dirichlet:

Teorema 1.1 (Dirichlet)**.** *Sigui n un enter positiu fixat, i $1 \leq a \leq n$ un enter tal que $(a,n) = 1$. Existeixen infinits primers $p \equiv a \bmod n$, i el límit*

$$\lim_{N\to\infty} \frac{\#\{1 \leq p \leq N \mid p \equiv a \bmod n\}}{\#\{1 \leq p \leq N\}}$$

existeix i val $\frac{1}{\phi(n)}$, on ϕ és la funció d'Euler.

És a dir, els nombres primers estan equidistribuïts entre les diferents classes mòdul n que són coprimeres amb n. Més endavant, un cop haguem parlat de sèries L, veurem una idea de la demostració d'aquest teorema.

Una generalització d'aquest resultat és el teorema de Chebotarev. En aquest capítol introduirem els conceptes de teoria de nombres algebraica necessaris per poder enunciar-lo, i en veurem algunes aplicacions.

1.1 Preliminars algebraics

Els resultats d'aquesta secció es poden trobar demostrats en qualsevol llibre introductori de teoria de nombres algebraica, com per exemple [12], [17] o [26].

Sigui $\Bbbk$ una extensió finita de $\mathbb{Q}$, i considerem el seu anell d'enters

$$\mathcal{O}_\Bbbk := \{\alpha \in \Bbbk \mid \exists f \in \mathbb{Z}[x] \text{ mònic tal que } f(\alpha) = 0\}.$$

Teorema 1.2. *$\mathcal{O}_\Bbbk$ és un domini de Dedekind, i.e.,*

1. *és íntegrament tancat, és a dir, la clausura entera en el cos de fraccions és ell mateix,*
2. *és noetherià, i*
3. *tot ideal primer diferent del 0 és maximal.*

Corol·lari 1.3. *Tot ideal* $\mathfrak{a} \neq 0$ *de* $\mathcal{O}_{\Bbbk}$ *es pot descomposar com a producte d'ideals primers* $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ *de manera única llevat ordre. A més, els primers* $\mathfrak{p}_i$ *són exactament els ideals primers de* $\mathcal{O}_{\Bbbk}$ *que contenen* $\mathfrak{a}$*.*

Tenim doncs que, tot i que en general $\mathcal{O}_{\Bbbk}$ no és un domini de factorització única, hi ha descomposició única en producte d'ideals primers.

Considerem ara una extensió finita $\mathbb{L}/\Bbbk$, el seu anell d'enters $\mathcal{O}_{\mathbb{L}}$, i $\mathfrak{p}$ un ideal primer de $\mathcal{O}_{\Bbbk}$. Tenim que $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ és un ideal de $\mathcal{O}_{\mathbb{L}}$, per tant té una descomposició $\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, on $\mathfrak{P}_i$ són els ideals primers (diferents) de $\mathcal{O}_{\mathbb{L}}$ que contenen $\mathfrak{p}$.

Definició 1.4. Per a un primer $\mathfrak{p}$, considerem la descomposició anterior. L'*índex de ramificació de* $\mathfrak{P}_i$ és l'exponent e_i, i el *grau d'inèrcia de* $\mathfrak{P}_i$ és el grau de l'extensió de cossos residuals ${}^{\mathcal{O}_{\mathbb{L}}}/_{\mathfrak{P}_i}/{}^{\mathcal{O}_{\Bbbk}}/_{\mathfrak{p}}$, $f_i = [{}^{\mathcal{O}_{\mathbb{L}}}/_{\mathfrak{P}_i} : {}^{\mathcal{O}_{\Bbbk}}/_{\mathfrak{p}}]$.

Definició 1.5. Si $e_i > 1$ per a algun i, $\mathfrak{p}$ *ramifica* en $\mathbb{L}/\Bbbk$. Si $e_i = f_i = 1$ $\forall i$, $\mathfrak{p}$ *descompon completament*. Si $g = 1$ i $e_1 = 1$, $\mathfrak{p}$ és *inert*.

Teorema 1.6. *Siguin* $\mathbb{L}/\Bbbk$ *una extensió finita i* $\mathfrak{p}$ *un ideal primer de* $\Bbbk$*. Siguin* e_i*,* f_i *els corresponents índexs de ramificació i graus d'inèrcia de* $\mathfrak{p}$*. Aleshores*

$$\sum_{i=1}^{g} e_i f_i = [\mathbb{L} : \Bbbk].$$

Si $\mathbb{L}/\Bbbk$ és de Galois, podem dir més sobre e_i i f_i:

Teorema 1.7. *Sigui* $\mathbb{L}/\Bbbk$ *una extensió de Galois i* $\mathfrak{p}$ *un primer de* $\Bbbk$*.*

1. *L'acció del grup de Galois* $\mathrm{Gal}(\mathbb{L}/\Bbbk)$ *sobre els primers de* $\mathbb{L}$ *que contenen* $\mathfrak{p}$ *és transitiva, és a dir, si* $\mathfrak{P}$ *i* $\mathfrak{P}'$ *són primers de* $\mathbb{L}$ *que contenen* $\mathfrak{p}$*, existeix* $\sigma \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$ *tal que* $\sigma(\mathfrak{P}) = \mathfrak{P}'$*.*
2. *Els primers* $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ *de* $\mathbb{L}$ *que contenen* $\mathfrak{p}$ *tenen el mateix índex de ramificació* e *i el mateix grau d'inèrcia* f*, i per tant* $[\mathbb{L} : \Bbbk] = efg$*.*

Definició 1.8. Per a un ideal primer $\mathfrak{P}$ de $\mathcal{O}_{\mathbb{L}}$, el seu *grup de descomposició* és

$$D_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(\mathbb{L}/\Bbbk) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

i el seu *grup d'inèrcia* és

$$I_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(\mathbb{L}/\Bbbk) \mid \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}\ \forall \alpha \in \mathcal{O}_{\mathbb{L}}\}.$$

Observem que $I_{\mathfrak{P}} \subset D_{\mathfrak{P}}$. Un element $\sigma \in D_{\mathfrak{P}}$ indueix un automorfisme $\tilde{\sigma} : {}^{\mathcal{O}_{\mathbb{L}}}/_{\mathfrak{P}} \to {}^{\mathcal{O}_{\mathbb{L}}}/_{\mathfrak{P}}$, $\tilde{\sigma} \in \tilde{G} = \mathrm{Gal}({}^{\mathcal{O}_{\mathbb{L}}}/_{\mathfrak{P}} \,/\, {}^{\mathcal{O}_{\Bbbk}}/_{\mathfrak{p}})$, que és la identitat en $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{\Bbbk}$. Això defineix un homomorfisme

$$\begin{aligned} \varphi : D_{\mathfrak{P}} &\longrightarrow \tilde{G} \\ \sigma &\longmapsto \tilde{\sigma}. \end{aligned}$$

Proposició 1.9. *Siguin $D_{\mathfrak{P}}$, $I_{\mathfrak{P}}$ i $\tilde{G}$ com abans. Aleshores,*

1. *l'homomorfisme $\varphi : D_{\mathfrak{P}} \to \tilde{G}$ és exhaustiu, i el seu nucli és $I_{\mathfrak{P}}$. Per tant, ${}^{D_{\mathfrak{P}}}/_{I_{\mathfrak{P}}} \cong \tilde{G}$.*
2. *$|D_{\mathfrak{P}}| = ef$ i $|I_{\mathfrak{P}}| = e$, on e i f són l'índex de ramificació i el grau d'inèrcia de $\mathfrak{p}$ en $\mathfrak{P}$ respectivament.*

Corol·lari 1.10. *El grup de descomposició d'un primer és trivial si i només si descompon completament.*

Recordem que tota extensió de cossos finits és de Galois i té grup de Galois cíclic. En el nostre cas, tenim l'extensió ${}^{\mathcal{O}_{\mathbb{L}}}/_{\mathfrak{P}}$ / ${}^{\mathcal{O}_{\mathbb{k}}}/_{\mathfrak{p}}$, de grau f, on $|{}^{\mathcal{O}_{\mathbb{k}}}/_{\mathfrak{p}}| = q$ i $|{}^{\mathcal{O}_{\mathbb{L}}}/_{\mathfrak{P}}| = q^f$. Per tant, el seu grup de Galois $\tilde{G}$ és isomorf a ${}^{\mathbb{Z}}/_{f\mathbb{Z}}$. També sabem que un generador d'aquest grup és una potència de l'anomenat *endomorfisme de Frobenius*, $\sigma_q : x \mapsto x^q$. Considerem l'element corresponent a σ_q en $\tilde{G}$ per l'homomorfisme φ, el denotem $(\frac{\mathfrak{P}}{\mathbb{L}/\mathbb{k}})$ i el denominem *element de Frobenius*.

Proposició 1.11. *L'element de Frobenius satisfà les propietats següents:*

1. *$(\frac{\mathfrak{P}}{\mathbb{L}/\mathbb{k}})$ és l'únic element de $D_{\mathfrak{P}}$ tal que $(\frac{\mathfrak{P}}{\mathbb{L}/\mathbb{k}})(x) \equiv x^q \bmod \mathfrak{P}$, $\forall x \in \mathcal{O}_{\mathbb{L}}$.*
2. *Per a tot $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{k})$, $(\frac{\sigma(\mathfrak{P})}{\mathbb{L}/\mathbb{k}}) = \sigma(\frac{\mathfrak{P}}{\mathbb{L}/\mathbb{k}})\sigma^{-1}$.*

És a dir, actua com l'endomorfisme de Frobenius a nivell de cossos residuals. A més, en cas de prendre un altre primer $\mathfrak{P}'$, l'element de Frobenius obtingut és un conjugat de $(\frac{\mathfrak{P}}{\mathbb{L}/\mathbb{k}})$, de manera que la classe de conjugació és un invariant del primer $\mathfrak{p}$. Per tant, podem fer servir les notacions $(\frac{\mathfrak{p}}{\mathbb{L}/\mathbb{k}})$, o simplement $\mathrm{Frob}_{\mathfrak{p}}$, per referir-nos a l'element de Frobenius.

1.2 Teorema de Chebotarev

Ara ens trobem en condicions d'enunciar el teorema de Chebotarev:

Teorema 1.12 (Chebotarev)**.** *Sigui $\mathbb{L}/\mathbb{k}$ una extensió de Galois, i sigui $\langle\sigma\rangle$ la classe de conjugació d'un element $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{k})$. Aleshores el conjunt $S = \{\mathfrak{p}$ ideal primer de $\mathbb{k} \mid \mathfrak{p}$ no ramifica i $(\frac{\mathfrak{p}}{\mathbb{L}/\mathbb{k}}) \in \langle\sigma\rangle\}$ té densitat $\delta(S) = \frac{|\langle\sigma\rangle|}{|\mathrm{Gal}(\mathbb{L}/\mathbb{k})|} = \frac{|\langle\sigma\rangle|}{[\mathbb{L}:\mathbb{k}]}$.*

Demostració. Veure [14, Capítol V, Teorema 6.4]. □

Vegem algunes aplicacions d'aquest teorema en algunes extensions senzilles. Estudiarem els casos quadràtic, cúbic i ciclotòmic.

Per començar, prenem un ideal primer de $\mathbb{Z}$, (p), on p primer. Volem veure com descomposa en una extensió quadràtica, per exemple $\mathbb{Z}[i]$. Amb la notació anterior, tindríem $\mathbb{k} = \mathbb{Q}$, $\mathcal{O}_{\mathbb{k}} = \mathbb{Z}$, $\mathbb{L} = \mathbb{Q}(i)$ i $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[i]$. El grup de Galois $G = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ té dos elements, per tant, $G \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}}$, i vist com a grup de permutacions, $G \cong \{\mathrm{id}, (1\ 2)\}$. Com que $efg = 2$, tenim tres possibles descomposicions:

(a) **Cas $g = 2$:** el primer (p) decomposa com a producte de dos ideals primers diferents, és a dir, $(p) = \mathfrak{P}_1\mathfrak{P}_2$. Es pot veure que aquest cas correspon als primers de la forma $p = 4k + 1$. Si calculem l'element de Frobenius $\mathrm{Frob}_p = (\frac{(p)}{\mathbb{Q}(i)/\mathbb{Q}})$, observem que només l'element identitat deixa fixos $\mathfrak{P}_1$ i $\mathfrak{P}_2$, així que tenim $\mathrm{Frob}_p = \mathrm{id}$.

(b) **Cas $f = 2$:** el primer (p) també és primer a $\mathbb{Z}[i]$. Tenim doncs, que és de la forma $p = 4k+3$. El grup de descomposició en aquest cas és tot el grup G, i com que Frob_p ha de ser generador, tenim que ha de ser l'element $(1\ 2)$.

(c) **Cas $e = 2$:** el primer ramifica, és a dir, $(p) = \mathfrak{P}^2$. Aquest cas correspon a $p = 2$ i $\mathfrak{P} = (1+i)$.

En general, per a qualsevol extensió quadràtica, el primer (p) pot descomposar completament, ser inert o ramificar, anàlogament als casos (a), (b), i (c). El teorema de Chebotarev ens diu:

$$\lim_{N\to\infty} \frac{\#\{1 \le p \le N \mid \mathrm{Frob}_p = \mathrm{id}\}}{\#\{1 \le p \le N\}} = \lim_{N\to\infty} \frac{\#\{1 \le p \le N \mid p \equiv 1 \bmod 4\}}{\#\{1 \le p \le N\}} = \frac{1}{2},$$

$$\lim_{N\to\infty} \frac{\#\{1 \le p \le N \mid \mathrm{Frob}_p = (1\ 2)\}}{\#\{1 \le p \le N\}} = \lim_{N\to\infty} \frac{\#\{1 \le p \le N \mid p \equiv 3 \bmod 4\}}{\#\{1 \le p \le N\}} = \frac{1}{2}.$$

En altres paraules, asimptòticament, la meitat dels primers descomposa en producte de dos primers diferents en una extensió quadràtica, o equivalentment, la meitat dels primers són de la forma $p = 4k + 1$ i la resta de la forma $p = 4k + 3$.

Per al segon exemple, considerem un polinomi $f \in \mathbb{Z}[x]$ de grau 3. Estudiarem com descomposa en $\mathbb{F}_p[x]$ segons el seu grup de Galois pensat com el grup de permutacions de les arrels, que en aquest cas pot ser $\mathcal{S}_3$ o bé $\mathcal{A}_3$.

Prenem el polinomi $f(x) = x^3 - x - 1$, que té grup de Galois $\mathrm{Gal}(f) = \mathcal{S}_3$. Tenim tres classes de conjugació,

$$C_1 = \mathrm{id},\ C_2 = \{(1\ 2\ 3), (1\ 3\ 2)\},\ C_3 = \{(1\ 2), (1\ 3), (2\ 3)\};$$

en conseqüència, tres possibles descomposicions:

(a) f **factoritza en tres polinomis de grau 1:** totes les arrels queden fixes, és a dir, $\mathrm{Frob}_p = \mathrm{id}$.

(b) f **és irreductible en $\mathbb{F}_p$:** com que totes les arrels poden permutar, tenim que $\mathrm{Frob}_p \in C_2$.

(c) f **factoritza en un polinomi de grau 2 i un polinomi de grau 1:** una de les arrels es queda fixa, i les altres dues es poden permutar, per tant, l'element de Frobenius pertany a C_3.

Aplicant el teorema de Chebotarev, tenim:

$$\lim_{N\to\infty} \frac{\#\{1 \le p \le N \mid \mathrm{Frob}_p \in C_1\}}{\#\{1 \le p \le N\}} = \frac{1}{6},$$

$$\lim_{N\to\infty} \frac{\#\{1 \le p \le N \mid \mathrm{Frob}_p \in C_2\}}{\#\{1 \le p \le N\}} = \frac{1}{3},$$

$$\lim_{N\to\infty} \frac{\#\{1 \le p \le N \mid \mathrm{Frob}_p \in C_3\}}{\#\{1 \le p \le N\}} = \frac{1}{2}.$$

És a dir, per a la meitat dels primers, el polinomi factoritza en un irreductible de grau 2 i un de grau 1; per a un sisè, factoritza en tres polinomis de grau 1; i per a la resta, és irreductible. En el nostre cas particular, si ho comprovem per als primers 50 nombres primers pels quals no ramifica, efectivament tenim que per a un 52% factoritza en un de grau 2 i un de grau 1, per a un 12% en tres de grau 1, i per a un 36% és irreductible.

Si ho mirem per al polinomi $f(x) = x^3 - 3x - 1$, que té grup de Galois $\mathrm{Gal}(f) = \mathcal{A}_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$, fent servir el mateix raonament veiem que només podem tenir dues possibles factoritzacions:

(a) f factoritza en tres polinomis de grau 1 $\Leftrightarrow \mathrm{Frob}_p \in C_1$.

(b) f és irreductible $\Leftrightarrow \mathrm{Frob}_p \in C_2$.

Per Chebotarev, sabem que f mai descomposa en un de grau 2 i un de grau 1, per a un terç dels primers factoritza en producte de tres de grau 1, i per a la resta és irreductible. En el nostre exemple, si ho mirem pels primers fins al 29, tenim que $f(x) = (x-3)(x-4)(x-10)$ en $\mathbb{F}_{17}$, $f(x) = (x-10)(x-12)(x-14)$ en $\mathbb{F}_{19}$ i per a la resta és irreductible.

I per acabar, vegem el cas ciclotòmic. Considerem l'extensió $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Es pot veure que existeix un isomorfisme

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^* &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ r &\longmapsto \sigma_r : (\zeta_n \mapsto \zeta_n^r).\end{aligned}$$

Sigui p un primer tal que $p \nmid n$, i $\mathfrak{p}$ un primer de $\mathbb{Q}(\zeta_n)$. L'element de Frobenius $\mathrm{Frob}_\mathfrak{p}$ està caracteritzat per:

(i) $\mathrm{Frob}_\mathfrak{p}(\mathfrak{p}\mathcal{O}_{\mathbb{Q}(\zeta_n)}) = \mathfrak{p}\mathcal{O}_{\mathbb{Q}(\zeta_n)}$, i

(ii) $\mathrm{Frob}_\mathfrak{p}(x) \equiv x^p \bmod \mathfrak{p}\mathcal{O}_{\mathbb{Q}(\zeta_n)}\ \forall x \in \mathcal{O}_{\mathbb{Q}(\zeta_n)}$.

Aquesta segona condició ens diu que $\mathrm{Frob}_\mathfrak{p} = \sigma_a$ per a certa $1 \leq a < n$, és a dir, $\mathrm{Frob}_\mathfrak{p}(\zeta) = \sigma_a(\zeta) = \zeta^a$. Com que $\zeta^a \equiv \zeta^p \bmod \mathfrak{p}\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ implica $a \equiv p \bmod n$, aleshores $\mathrm{Frob}_\mathfrak{p} = \sigma_p$. Això ens diu que l'element de Frobenius de $\mathfrak{p}$ ve donat per la classe de p mod n.

Aquest resultat ens permet recuperar el teorema de Dirichlet, ja que per Chebotarev tenim que la densitat d'ideals primers $\mathfrak{p}$ tal que $\mathrm{Frob}_\mathfrak{p} = \sigma_a$ és $\frac{1}{\phi(n)}$, o en altres paraules, que la densitat de primers p tal que $p \equiv a \bmod n$ és $\frac{1}{\phi(n)}$.

Capítol 2

Teorema de Hasse

La conjectura de Sato–Tate és un resultat sobre el nombre de punts d'una corba el·líptica sobre cossos finits. Però, de fet, podem comptar els punts de qualsevol corba. Si les distingim pel seu *gènere*, un invariant topològic relacionat amb el grau i el nombre de singularitats de la corba, podem diferenciar tres casos:

- Si la corba és de gènere 0, és una cònica. Si té un punt, la podem parametritzar i comptar-ne fàcilment el nombre de punts. Més endavant en veurem un exemple concret detallat.
- Si la corba és de gènere > 1, la corba té un nombre finit de punts racionals. Aquest resultat s'anomena teorema de Faltings. La prova de Faltings consisteix en veure un cas particular de la conjectura de Tate i usar un ampli repertori de tècniques de geometria algebraica (veure [5]).
- Si la corba és de gènere 1, o bé no té cap punt o bé és una corba el·líptica. En aquest cas, no tenim manera de comptar els punts, sinó que en tenim una fita, el teorema de Hasse: si N_q és el nombre de punts d'una corba el·líptica E sobre $\mathbb{F}_q$, aleshores

$$|N_q - q - 1| < 2\sqrt{q}.$$

L'objectiu d'aquesta part del treball és presentar les corbes el·líptiques, veure'n les propietats més importants i demostrar aquest teorema.

2.1 Exemple senzill: les còniques

Considerem la circumferència $C : x^2 + y^2 = 1$. Prenem el punt $(1, 0)$, evidentment de C, i considerarem la projecció estereogràfica per l'eix y. Sigui

$$L : y = (1 - x)t$$

la recta que passa per $(1, 0)$ i cada punt de l'eix vertical $(0, t)$, i prenem l'altre punt d'intersecció de L amb C. Com que aquest punt és de C, ha de complir l'equació de la circumferència, i tenim

$$x^2 + (1 - x)^2t^2 = 1 \Leftrightarrow (1 + t^2)x^2 - 2t^2x + t^2 - 1 = 0.$$

Si resolem l'equació de segon grau, quan $t^2+1 \neq 0$ tenim

$$x = \frac{-2t^2 \pm \sqrt{4t^2 - 4(t^2-1)(t^2+1)}}{2(t^2+1)} \Leftrightarrow x = 1,\ \frac{t^2-1}{t^2+1}.$$

A partir de l'equació de L calculem el valor de la coordenada y, obtenint la següent parametrització de la circumferència:

$$(x,y) = \left(\frac{t^2-1}{t^2+1},\ \frac{2t}{t^2+1} \right),\ t = 0, 1, \ldots, \infty.$$

A partir de la parametrització, observem que el nombre de solucions en $\mathbb{F}_p$ depèn de les arrels de t^2+1 en aquest cos. En $\mathbb{F}_2$ té una arrel doble, i per tant tenim p solucions. Per a la resta, si -1 no és un quadrat mòdul p, que és el cas dels primers de la forma $p = 4k+3$, tenim $p+1$ solucions projectives; en cas contrari, és a dir, pels primers de la forma $p = 4k+1$, en tenim $p-1$.

Si C és una cònica qualsevol, si té un punt podem trobar una parametrització seguint el mateix procediment que per a la circumferència, i de manera similar podem comptar el nombre de punts de C.

2.2 Corbes el·líptiques

Sigui C una corba sobre un cos $\Bbbk$ definida per un polinomi $f \in \Bbbk[x,y]$, és a dir $C : f(x,y) = 0$. Li podem associar el conjunt de *punts* $\Bbbk$*-racionals*

$$C(\Bbbk) := \{(a,b) \in \Bbbk^2 \mid f(a,b) = 0\}.$$

Si $\Bbbk$ és algebraicament tancat i f és irreductible, $C(\Bbbk)$ determina de manera única f. Per tant, considerarem també els punts sobre les extensions de $\Bbbk$, en particular els punts $\overline{\Bbbk}$-racionals, als que anomenarem simplement punts de la corba.

Definició 2.1. Una *corba el·líptica* sobre un cos $\Bbbk$ és una corba plana projectiva no singular de gènere 1 amb un punt $\Bbbk$-racional O.

Per entendre aquesta primera definició, ens cal tenir coneixements previs de geometria algebraica. El teorema de Riemann–Roch (veure [9]) permet donar una caracterització alternativa més elemental:

Definició 2.2. Una *corba el·líptica projectiva* $\tilde{E}$ sobre un cos $\Bbbk$ és la corba definida per l'equació

$$\tilde{E} : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

anomenada *equació de Weierstrass projectiva*, amb $\Delta \neq 0$, on $a_1, a_2, a_3, a_4, a_6 \in \Bbbk$ i Δ és el discriminant.

És a dir, una corba el·líptica és una corba plana cúbica no singular, i recíprocament, tota corba definida per l'equació de Weierstrass és una corba el·líptica.

La condició $\Delta \neq 0$ ens assegura que E no té cap punt singular. Segons el valor de la coordenada z, podem distingir els punts de $\tilde{E}$. Considerem primers els punts que tenen $z = 0$, i que per tant compleixen l'equació $x^3 = 0$. Obtenim un únic punt, $O = (0:1:0)$, al que anomenarem *punt de l'infinit*. Per a la resta de punts, que tenen $z \neq 0$, considerem el representant amb $z = 1$. D'aquesta manera, obtenim $E : f(x,y,1) = 0$, la versió afí de la corba. Podem descriure-la tal com hem fet amb la projectiva:

Definició 2.3. Una *corba el·líptica* E sobre un cos $\Bbbk$ és la corba definida per l'equació

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

anomenada *equació de Weierstrass*, on $a_1, a_2, a_3, a_4, a_6 \in \Bbbk$ i $\Delta \neq 0$.

Si $\text{char}(\Bbbk) \neq 2, 3$, amb un canvi de variables adequat es pot reescriure com

$$E : y^2 = x^3 + Ax + B,$$

amb $A, B \in \Bbbk$ i $\Delta = -16(4A^3 + 27B^2)$.

L'estreta relació entre E i $\tilde{E}$ justifica que a partir d'ara, considerem simplement una corba el·líptica E, sense especificar afí o projectiva.

Si la nostra corba té coeficients en $\mathbb{Q}$, podem estudiar la seva *reducció mòdul* p, és a dir, si

$$E : y^2 = x^3 + Ax + B,\ A, B \in \mathbb{Q},$$

podem fer un canvi de variables i obtenir

$$E_p : y^2 = x^3 + \overline{A}x + \overline{B},\ \overline{A}, \overline{B} \in \mathbb{F}_p.$$

Tot i que E és una corba el·líptica no singular, és possible que E_p tingui punts singulars. Hi ha tres possibles casos:

(a) **Bona reducció**: si $p \neq 2$ i $p \nmid \Delta = -16(4A^3 + 27B^2)$, E_p és una corba el·líptica no singular sobre $\mathbb{F}_p$.

(b) **Reducció additiva**: si $p \neq 2, 3$, quan $p \mid \Delta$ i $p \mid -2AB$, la corba E_p té una cúspide. Sense el punt singular, la corba té estructura de grup additiu. Correspon al cas $\overline{A} = \overline{B} = 0$, és a dir, a la corba $y^2z = x^3$. A part del punt $(0, 0, 1)$, tenim els p punts solució de la corba $z = x^3$; en total, $p + 1$.

(c) **Reducció multiplicativa**: si $p \neq 2, 3$, quan $p \mid \Delta$ i $p \nmid -2AB$, la corba té un node, i sense ell, té estructura de grup multiplicatiu. En aquesta situació podem distingir dos subcasos: la *reducció multiplicativa dividida*, si $-2AB$ és un quadrat mòdul p (que es dóna quan les tangents al node són racionals sobre $\mathbb{F}_p$), i la *reducció multiplicativa no dividida* en cas contrari. En aquest cas, $\overline{A} \neq 0$ i $\overline{B} = 0$, i la corba que obtenim és $zy^2 = x^3 + \overline{A}x^2z$. Quan $x = 0$, tenim el punt $(0, 1, 0)$, que prendrem com a punt de l'infinit. Dividint l'equació de la corba per x^2, prenent $z = 1$ i fent el canvi de variable $t = \frac{y}{x}$, la resta de punts de la corba vénen donats per les solucions de l'equació $t^2 = x + \overline{A}$. En total, quan p és de reducció dividida tenim p punts i quan és no dividida, en tenim $p + 2$.

Una particularitat interessant de les corbes el·líptiques és que podem definir una operació additiva amb la qual els seus punts tenen estructura de grup.

Teorema 2.4. *Sigui $E/\Bbbk$ una corba el·líptica, prenent el model de Weierstrass amb el punt de l'infinit O. Considerem la següent operació:*

> *Siguin P, Q dos punts de E. Si $P = Q$, prenem L la recta tangent a la corba en el punt P, i si són diferents, prenem L la recta per P i Q. Sigui R el tercer punt d'intersecció de L amb E, i L' la recta que passa per P i O. Aleshores $P + Q$ és l'altre punt d'intersecció de L' amb E.*

L'operació anterior defineix una llei de grup sobre $E(\Bbbk')$ per a totes les extensions $\Bbbk'/\Bbbk$.

Si $\Bbbk$ és algebraicament tancat, podem prendre un tercer punt d'intersecció perquè una recta talla la corba en tres punts. Si no ho és però sabem que talla en dos punts, per les fórmules de Cardano de la resolució d'equacions de tercer grau, podem assegurar que talla en un tercer, de manera que la suma de dos punts està ben definida.

Una altra característica a estudiar de les corbes el·líptiques és el seu anell d'endomorfismes. Com que la suma de dos punts ve donada per una expressió polinòmica, tenim per a cada $m \in \mathbb{Z}$, el morfisme *multiplicar per* m,

$$\begin{aligned}[m] : E(\overline{\Bbbk}) &\longrightarrow E(\overline{\Bbbk}) \\ P &\longmapsto mP,\end{aligned}$$

i identifiquem tots aquests endomorfismes amb $\mathbb{Z}$. Per tant, acabem de veure que $\mathrm{End}(E)$ sempre conté $\mathbb{Z}$. Però no tenen perquè ser els únics endomorfismes. Quan la característica del cos $\Bbbk$ és positiva, $\mathrm{End}(E)$ conté un altre endomorfisme rellevant, l'*endomorfisme de Frobenius*, definit per

$$\begin{aligned}\phi_q : E(\overline{\Bbbk}) &\longrightarrow E(\overline{\Bbbk}) \\ (x, y) &\longmapsto (x^q, y^q).\end{aligned}$$

De fet, es pot demostrar que l'anell d'endomorfismes d'una corba el·líptica pot ser isomorf a:

- $\mathbb{Z}$,
- un ordre en un cos quadràtic imaginari, o
- un ordre en una àlgebra de quaternions sobre $\mathbb{Q}$.

Recordem que $\mathcal{O}$ és un *ordre* en una àlgebra A de dimensió finita sobre $\mathbb{Q}$ si és un subanell tal que és un $\mathbb{Z}$-reticle en A i $\mathbb{Q}\mathcal{O} = A$. Un exemple bàsic seria $A = \mathbb{Q}(i)$ i l'ordre $\mathbb{Z}[i]$.

L'última possibilitat correspon al particular cas de les anomenades corbes *supersingulars*, que és quan l'anell d'endomorfismes és extremadament gran. Només es pot donar quan $\mathrm{char}(\Bbbk) \neq 0$. Durant tot el treball les evitarem i tractarem la resta de corbes, denominades *ordinàries*.

En la resta del capítol, estudiarem algunes propietats de l'endomorfisme de Frobenius que ens permetran demostrar el teorema de Hasse i les relacionarem amb el grup de Galois de $\overline{\Bbbk}/\Bbbk$.

2.3 Demostració del teorema de Hasse

Abans de veure la demostració, enunciarem un parell de teoremes clàssics de la geometria algebraica que farem servir, dels quals podem trobar-ne les demostracions en [22].

Siguin C_1, C_2 dues corbes sobre $\Bbbk$, i $\psi : C_1 \to C_2$ un morfisme.

Teorema 2.5. *ψ és constant o exhaustiu.*

Si $\Bbbk(C_1)$, $\Bbbk(C_2)$ són els cossos de funcions definides sobre $\Bbbk$ de C_1 i C_2 respectivament, la composició amb ψ indueix

$$\begin{aligned}\psi^* : \Bbbk(C_2) &\longrightarrow \Bbbk(C_1) \\ f &\longmapsto \psi^* f := f \circ \psi,\end{aligned}$$

una injecció de cossos de funcions que fixa $\Bbbk$.

Teorema 2.6. *Sigui $\psi : C_1 \to C_2$ un morfisme no constant sobre $\Bbbk$. Aleshores $\Bbbk(C_1)$ és una extensió finita de $\psi^*\Bbbk(C_2)$.*

Aquest teorema ens permet traslladar característiques pròpies de l'extensió $\Bbbk(C_1)/\psi^*\Bbbk(C_2)$ a l'endomorfisme ψ.

Definició 2.7. Sigui $\psi : C_1 \to C_2$. Si ψ és no constant, el seu *grau* és

$$\deg \psi := [\Bbbk(C_1) : \psi^*\Bbbk(C_2)].$$

Si és constant, definim $\deg \psi := 0$. ψ és *separable* si l'extensió $\Bbbk(C_1)/\psi^*\Bbbk(C_2)$ ho és.

Un cop definits aquests conceptes generals sobre morfismes de corbes, vegem algunes propietats de l'endomorfisme de Frobenius ϕ_q.

Lema 2.8. *Un punt P pertany a $E(\mathbb{F}_q)$ si i només si $\phi_q(P) = P$, i en aquest cas $\#E(\mathbb{F}_q) = \#\ker(\phi_q - \mathrm{Id})$.*

Lema 2.9. *$\phi_q - \mathrm{Id}$ és separable, i $\#\ker(\phi_q - \mathrm{Id}) = \deg(\phi_q - \mathrm{Id})$.*

Lema 2.10. deg *és una forma quadràtica definida positiva.*

Les demostracions dels lemes les podem trobar en [22]. Finalment, ja podem enunciar i demostrar el teorema de Hasse, que ens dóna una fita pel nombre de punts d'una corba el·líptica sobre $\mathbb{F}_q$.

Teorema 2.11 (Hasse)**.** *Sigui E una corba el·líptica sobre $\mathbb{F}_q$. Aleshores*

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Demostració. Recordem la desigualtat de Cauchy–Schwarz per a una forma quadràtica d:

$$|d(\alpha - \beta) - d(\alpha) - d(\beta)| \leq 2\sqrt{d(\alpha)d(\beta)}.$$

Per a $d = \deg$, $\alpha = \phi_q$, $\beta = \mathrm{Id}$ obtenim

$$|\deg(\phi_q - \mathrm{Id}) - \deg \phi_q - \deg \mathrm{Id}| \leq 2\sqrt{\deg \phi_q \deg \mathrm{Id}},$$

i com que $\deg \phi_q = q$, $\deg \mathrm{Id} = 1$, finalment arribem a la desigualtat

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

□

2.4 Mòdul de Tate

L'objectiu d'aquesta secció és relacionar el nombre de punts d'una corba el·líptica en $\mathbb{F}_{p^r}$ amb $\#E(\mathbb{F}_p)$.

Sigui E una corba el·líptica sobre un cos $\Bbbk = \mathbb{F}_q$ de característica p. Considerem per a cada $m \in \mathbb{Z}$, el nucli del morfisme de multiplicació per m vist en l'apartat 2.2, $E[m] := \ker[m]$.

Lema 2.12. *Sigui m un enter. Si m és primer amb p, aleshores $[m]$ és separable i $\#E[m] = \deg[m] = m^2$.*

Tenim doncs que, si $(m,p)=1$, $E[m]$ és un grup commutatiu d'ordre m^2 que s'anul·la amb la multiplicació per m. De fet, es té $E[m] \cong {}^{\mathbb{Z}}/_{m\mathbb{Z}} \times {}^{\mathbb{Z}}/_{m\mathbb{Z}}$. Si $m = p^r$, $E[m] = 1$ o m.

El grup de Galois $G = \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ actua sobre $E[m]$. Considerem una representació $G \to \mathrm{Aut}(E[m])$. Escollint una base per $E[m]$, tenim $\mathrm{Aut}(E[m]) \cong \mathrm{GL}(2, {}^{\mathbb{Z}}/_{m\mathbb{Z}})$. Aquesta representació no és prou bona, ja que els coeficients de les matrius són d'un anell de característica positiva. Per millorar-la, el que farem és trobar una representació sobre els nombres p-àdics. Però abans de fer-ho per a la nostra corba el·líptica E, ho veurem en un context més senzill per entendre bé el procediment que seguirem.

Prenem el cercle C sobre un cos $\Bbbk$, i fixem un primer ℓ. La ℓ^n-torsió ve donada per les arrels ℓ^n-èsimes de la unitat, $\zeta_{\ell^n}^i$, on ζ_{ℓ^n} és una arrel primitiva i $i \in \{0, \dots, \ell^n - 1\}$. Si $C[\ell^n]$ és el grup de les arrels ℓ^n-èsimes de la unitat, tenim un isomorfisme

$$\begin{aligned} C[\ell^n] &\longrightarrow {}^{\mathbb{Z}}/_{\ell^n\mathbb{Z}} \\ \zeta_{\ell^n}^i &\longmapsto i. \end{aligned}$$

A partir de l'aplicació elevar a ℓ, $C[\ell^{n+1}] \xrightarrow{\zeta \mapsto \zeta^\ell} C[\ell^n]$, tenim $\dots \leftarrow C[\ell^3] \leftarrow C[\ell^2] \leftarrow C[\ell]$, i prenent-ne el *límit projectiu* podem definir $T_\ell(C) := \varprojlim_n C[\ell^n]$. Gràcies a l'isomorfisme anterior, tenim la identificació $T_\ell(C) \cong \mathbb{Z}_\ell$.

Un element del grup de Galois de $\overline{\Bbbk}/\Bbbk$ permuta les arrels ℓ^n-èsimes, és a dir, indueix una acció

$$\begin{aligned} \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \times C[\ell^n] &\longrightarrow C[\ell^n] \\ (\sigma, \zeta) &\longmapsto \zeta^{a_n(\sigma)}, \end{aligned}$$

on $a_n(\sigma) \in ({}^{\mathbb{Z}}/_{\ell^n\mathbb{Z}})^\times$. És a dir, per a cada $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ tenim una col·lecció d'elements $a_n(\sigma)$, per a tot n. Prenent el límit, tenim un element a $\mathbb{Z}_\ell^\times$, i per tant, una representació

$$\mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \longrightarrow \mathrm{Aut}(\mathbb{Z}_\ell) = \mathrm{GL}(1, \mathbb{Z}_\ell) \cong \mathbb{Z}_\ell^\times.$$

En el cas de l'element de Frobenius $\phi_p \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$, amb $p \neq \ell$, el seu element associat a $\mathbb{Z}_\ell^\times$ és p. Per tant, el polinomi característic de ϕ_p és simplement $T - p$, sense cap dependència en ℓ.

El nostre objectiu és seguir la mateixa construcció, prenent una corba el·líptica E, per arribar a una representació del grup de Galois G que ens permeti trobar el polinomi característic de l'element de Frobenius.

Definició 2.13. Sigui E una corba el·líptica i $\ell \in \mathbb{Z}$ un primer. El *mòdul de Tate (ℓ-àdic) de E* és el grup

$$T_\ell(E) := \varprojlim_n E[\ell^n],$$

prenent el límit projectiu respecte $E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n]$.

Com que $E[\ell^n]$ és un ${}^{\mathbb{Z}}/_{\ell^n\mathbb{Z}}$-mòdul, el mòdul de Tate té estructura de $\mathbb{Z}_\ell$-mòdul.

Proposició 2.14. *Com a $\mathbb{Z}_\ell$-mòdul, el mòdul de Tate $T_\ell E$ té la següent estructura:*

(a) $T_\ell E \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ *si* $\ell \neq \mathrm{char}(\Bbbk)$.

(b) $T_p E \cong \{0\}$ *o bé* $\mathbb{Z}_p$ *si* $p = \mathrm{char}(\Bbbk) > 0$.

Definició 2.15. La *representació ℓ-àdica de $G = \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ associada a E* és l'homomorfisme

$$\rho_\ell : G \longrightarrow \mathrm{Aut}(T_\ell(E))$$

induït per l'acció de G en els punts de la ℓ^n-torsió d'E, $E[\ell^n]$.

Si ens mirem el cas $\ell \neq \mathrm{char}(\Bbbk)$, tenim $\mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}(2, \mathbb{Z}_\ell)$, és a dir, a cada element del grup de Galois li associem una matriu 2×2 amb coeficients a $\mathbb{Z}_\ell$. Com per a tot endomorfisme, el polinomi característic de l'element de Frobenius ϕ_q serà de la forma

$$T^2 - \mathrm{tr}(\phi_q)T + \deg(\phi_q).$$

Per trobar la traça, observem que per a qualsevol matriu 2×2 A, tenim

$$\det(A - \mathrm{Id}) = \det A - \mathrm{tr}A + 1.$$

Si ho calculem per a la matriu de ϕ_q, tenim

$$\deg(\phi_q - \mathrm{Id}) = \deg(\phi_q) - \mathrm{tr}(\phi_q) + 1,$$

i com que $\deg(\phi_q - \mathrm{Id}) = \#E(\mathbb{F}_q)$ i $\deg(\phi_q) = q$, si definim $a_q := q+1-\#E(\mathbb{F}_q)$, obtenim el polinomi característic

$$T^2 - a_q T + q.$$

Observem que tot i que la representació depèn del primer ℓ escollit, ni la traça ni el determinant de la matriu en depenen. Com que la traça també es pot expressar com $a_q = \alpha + \beta$, on $\alpha, \beta \in \mathbb{C}$ són els valors propis de la matriu, tenim

$$\#E(\mathbb{F}_q) = q + 1 - (\alpha + \beta),$$

i aquesta expressió ens permet trobar $\#E(\mathbb{F}_{q^r})$ a partir dels càlculs anteriors observant que $\phi_{q^r} = \phi_q^r$. Aleshores, seguint el mateix raonament tenim

$$\#E(\mathbb{F}_{q^r}) = q^r + 1 - (\alpha^r + \beta^r).$$

De fet, α i β són les arrels del polinomi característic de l'element de Frobenius ϕ_p. Pel teorema de Hasse (2.11), es compleix la desigualtat

$$|a_q| \leq 2\sqrt{q} \;\Rightarrow\; a_q^2 - 4q \leq 0,$$

és a dir, tenim dues arrels d'un polinomi amb coeficients reals i discriminant negatiu. D'aquí podem deduir $\beta = \overline{\alpha}$.

Capítol 3

Sèries L

Per una banda, un dels objectius centrals d'aquest capítol és introduir les sèries L. Tenen especial interès perquè ens serviran per demostrar la conjectura de Sato–Tate en el proper capítol. Primer de tot, recordarem què és un caràcter i definirem la seva sèrie L associada. Com a aplicació, demostrarem el teorema de Dirichlet. A continuació, veurem que podem relacionar algunes corbes el·líptiques amb una sèrie L. I per altra banda, presentarem de manera rigorosa el concepte d'equidistribució i en veurem caracteritzacions en termes de caràcters i sèries L.

3.1 Sèrie L d'un caràcter

Definició 3.1. Sigui G un grup abelià finit. Un *caràcter de Dirichlet* G és un homomorfisme de grups $\chi : G \to \mathbb{C}^\times$.

Per exemple, considerem G el grup cíclic d'ordre n generat per un element g. Si χ és un caràcter tal que $\chi(g) = \omega$, es compleix $\omega^n = 1$, és a dir, ω és una arrel n-èsima de la unitat. Recíprocament, cada arrel n-èsima defineix un caràcter $\chi(g) = \omega$, i $g^k \mapsto \omega^k$. Per tant, el grup d'homomorfismes de G a $\mathbb{C}^\times$ és un grup cíclic d'ordre n.

Definició 3.2. Un *caràcter mòdul* n és una funció $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$.

Es poden estendre a caràcters mòdul un múltiple de n, inclús a tot $\mathbb{Z}$, definint $\chi(m) = 0$ per a tot $m \in \mathbb{Z}$ no primer amb n i assignant a cada enter el valor que pren la seva classe mòdul n. Siguin $\chi_1 \bmod n_1$ i $\chi_2 \bmod n_2$ dos caràcters. Si n_1, n_2 divideixen un enter N i $\chi_1(m) = \chi_2(m)$ per a tot m coprimer amb N, pel que acabem de dir, els dos indueixen un mateix caràcter mòdul N. Aquest fet defineix una relació d'equivalència en els caràcters de Dirichlet. Anomenarem *conductor* d'un caràcter χ al mòdul més petit possible dels caràcters de la classe d'equivalència de χ.

Hi ha molts caràcters importants en l'aritmètica. Un exemple típic és el *caràcter de Legendre*, que és el caràcter d'ordre 2 que obtenim si prenem $G = (\mathbb{Z}/p\mathbb{Z})^\times$, on $p \neq 2$ primer. Es defineix, per a tot $x \in \mathbb{Z}$, el *símbol de Legendre*

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ és quadrat en } \mathbb{F}_p, \\ -1 & \text{si } x \text{ no és quadrat en } \mathbb{F}_p. \end{cases}$$

Els caràcters de Legendre estan relacionats amb la *llei de reciprocitat quadràtica*, un teorema que relaciona les dues congruències quadràtiques

$$x^2 \equiv p \bmod q$$

$$y^2 \equiv q \bmod p$$

de la següent manera:

> *Si p o q són primers de la forma $4k+1$, aleshores o bé les dues equacions tenen solució o bé cap en té. En cas contrari, una d'elles té solució si i només si l'altra no en té.*

Aquesta llei va ser enunciada per Legendre i Euler, i Gauss en va donar una demostració per primera vegada pels volts del 1800 en el seu conegut llibre *Disquisitiones Arithmeticae*, veient uns quants casos i fent servir inducció. Amb els símbols de Legendre, es pot enunciar de la següent manera:

Teorema 3.3 (Llei de reciprocitat quadràtica)**.** *Siguin p i q dos primers senars diferents. Aleshores*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Després d'aquest breu resum sobre caràcters, veurem què són les sèries de Dirichlet amb algun exemple, i veurem la connexió que tenen amb els caràcters.

Definició 3.4. Sigui (λ_k) una successió de nombres reals que tendeix a $+\infty$. Una *sèrie de Dirichlet amb exponents* (λ_k) és una sèrie de la forma

$$\sum a_k e^{-\lambda_k z},$$

amb $a_k, z \in \mathbb{C}$. Si $\lambda_k = \log k$, la sèrie s'anomena *ordinària* i s'escriu $\sum \frac{a_k}{k^z}$.

Quan tots els coeficients són 1, apareix l'anomenada *funció zeta de Riemann*

$$\zeta(s) = \sum_{m=1}^{\infty} \frac{1}{m^s}.$$

Els enters parells negatius anul·len aquesta funció, i se'ls anomena zeros trivials. Un dels problemes oberts més famosos de les matemàtiques, la *hipòtesi de Riemann*, consisteix en veure que la part real de qualsevol zero no trivial de $\zeta(s)$ és $1/2$. En el nostre context, ens seran útils la propera proposició i dos corol·laris, uns resultats bàsics sobre aquesta funció que necessitarem més endavant. Podem trobar-ne la demostració en [19, Capítol VI].

Proposició 3.5. *La funció $\zeta(s)$ és holomorfa i no s'anul·la si $\Re(s) > 1$. Podem reescriure-la com*

$$\zeta(s) = \frac{1}{s-1} + h(s),$$

on $h(s)$ és una funció holomorfa en $\Re(s) > 0$.

Corol·lari 3.6. *$\zeta(s)$ té un pol simple en $s = 1$.*

Corol·lari 3.7. *Quan $s \to 1$,*

(i) $\sum_p p^{-s} \sim \log \frac{1}{s-1}$.

(ii) $\sum_{p,m\geq 2} p^{-ms}$ *està fitada.*

Un gran exemple de sèries de Dirichlet són les sèries L. Igual que per a la funció zeta, en veurem la definició i un parell de proposicions útils, demostrades també en [19]:

Definició 3.8. Sigui $n \geq 1$ un enter i sigui χ un caràcter mòdul n. La *sèrie L associada a χ* és

$$L(\chi, s) := \sum_{m\geq 1} \frac{\chi(m)}{m^s}.$$

Proposició 3.9. *Si $\chi = 1$, $L(1,s) = F(s)\zeta(s)$, on $F(s) = \prod_{p|n}(1-p^{-s})$. En particular, $L(1,s)$ es pot estendre analítcament en $\Re(s) > 0$ i té un pol simple en $s = 1$.*

Proposició 3.10. *Si $\chi \neq 1$,*

(i) $L(\chi, s)$ convergeix en el semiplà $\Re(s) > 0$.

(ii) $L(\chi, s)$ convergeix absolutament en $\Re(s) > 1$ i

$$L(\chi, s) = \prod_{p \text{ primer}} \frac{1}{1-\chi(p)p^{-s}}.$$

La prolongació analítica d'aquestes sèries s'anomenen *funcions L*.

Teorema 3.11. *Per a tot $\chi \neq 1$, $L(\chi, 1) \neq 0$.*

Demostració. Suposem que $L(\chi, 1) = 0$ per a algun caràcter $\chi \neq 1$, i considerem la funció

$$\zeta_n = \prod_{p\nmid n} \frac{1}{(1-p^{-f(p)s})^{g(p)}},$$

on $f(p)$ és l'ordre de p en $(\mathbb{Z}/n\mathbb{Z})^\times$ i $g(p) = \frac{\phi(n)}{f(p)}$, amb ϕ la funció d'Euler.

Llavors, ζ_n és holomorfa en $s = 1$ i per tant tenim que ho és $\forall s \in \mathbb{C}$ tal que $\Re(s) > 0$, i convergeix en aquest domini ja que és una sèrie de Dirichlet amb coeficients positius.

Però això és impossible, ja que el factor p-èsim de ζ_n és

$$\frac{1}{(1-p^{-f(p)s})^{g(p)}} = (1 + p^{-f(p)s} + p^{-2f(p)s} + \ldots)^{g(p)} > \sum_{k=0}^{\infty} p^{-k\phi(n)s},$$

i $\zeta_n(s) > \sum_{(m,n)=1} m^{-\phi(n)s}$, sèrie que divergeix per a $s = \frac{1}{\phi(n)}$. □

Aquest resultat purament analític, que pot semblar poc rellevant en el nostre context, és la clau de la prova del teorema de Dirichlet, que havíem enunciat al primer capítol.

Teorema 3.12 (Dirichlet)**.** *Sigui n un enter positiu fixat, i $1 \leq a \leq n$ un enter tal que $(a, n) = 1$. Existeixen infinits primers $p \equiv a \bmod n$, i el límit*

$$\lim_{N\to\infty} \frac{\#\{1 \leq p \leq N \mid p \equiv a \bmod n\}}{\#\{1 \leq p \leq N\}}$$

existeix i val $\frac{1}{\phi(n)}$.

Demostració. Sigui χ un caràcter de $(\mathbb{Z}/n\mathbb{Z})^\times$. Considerem la funció

$$f_\chi(s) = \sum_{p \nmid n} \frac{\chi(p)}{p^s}.$$

Observem que el seu comportament segons χ és

1. $f_\chi \sim \log \frac{1}{s-1}$ quan $s \to 1$ si $\chi = 1$,
2. $f_\chi(s)$ està fitada quan $s \to 1$ si $\chi \neq 1$.

El primer cas és conseqüència de resultats vistos anteriorment. A continuació veurem que el segon també és cert.

Si $L(\chi, s) = \prod \frac{1}{1-\chi(p)p^{-s}}$, quan $\Re(s) > 1$ definim el seu logaritme com

$$\log L(\chi, s) = \sum_{m,p} \frac{\chi(p)^m}{mp^{-ms}} = f_\chi(s) + F_\chi(s),$$

on $F_\chi(s) = \sum_{p,m\geq 2} \frac{\chi(p)^m}{mp^{-ms}}$.

El teorema 3.11 i el corol·lari 3.7 ens asseguren que $F_\chi(s)$ està fitada quan $s \to 1$, i per tant la funció $f_\chi(s)$ també.

Per acabar, considerem la funció

$$g_a(s) = \sum_{p \in P_a} \frac{1}{p^s} = \frac{1}{\phi(n)} \sum_{\chi} \frac{f_\chi(s)}{\chi(a)},$$

on $P_a := \{p \equiv a \mod n \mid p \text{ primer}\}$ i el sumatori es fa sobre els caràcters χ de $(\mathbb{Z}/n\mathbb{Z})^\times$. Per l'observació anterior sobre el comportament de f_χ, tenim que $g_a(s) \sim \frac{1}{\phi(n)} \log \frac{1}{s-1}$, d'on finalment deduïm que la densitat de P_a és precisament $\frac{1}{\phi(n)}$. □

A partir de la definició que hem donat al principi d'aquesta secció de caràcter de Dirichlet, podem construir una *representació*. A la secció 2.4 ja havia sortit aquest concepte. Recordarem amb detall la seva definició i veurem com podem obtenir-ne una amb un caràcter de Dirichlet.

Definició 3.13. Sigui G un grup i $\Bbbk$ un cos. Una *representació* de G sobre $\Bbbk$ n-dimensional és un homomorfisme continu

$$\rho : G \longrightarrow \mathrm{GL}(n, \Bbbk).$$

Si $G_\mathbb{L}$ és el grup de Galois d'una extensió separable d'un cos $\mathbb{L}$, la representació de $G_\mathbb{L}$ sobre $\Bbbk$ s'anomena *representació de Galois*.

A cada representació podem associar-li un *caràcter*: a cada element del grup G, li assignem la traça de la matriu que li correspon per la representació ρ,

$$\begin{aligned} \chi_\rho : G &\longrightarrow \Bbbk \\ g &\longmapsto \mathrm{tr}(\rho(g)). \end{aligned}$$

Definició 3.14. Una *representació d'Artin* n-dimensional ρ d'un $\Bbbk$ és una representació de $\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ sobre $\mathbb{C}$ per la qual existeix una extensió finita de Galois $\mathbb{L}/\Bbbk$

$$\rho : \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \longrightarrow \mathrm{Gal}(\mathbb{L}/\Bbbk) \longrightarrow \mathrm{GL}(n, \mathbb{C}).$$

Si tenim un caràcter de Dirichlet $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$, considerant la projecció de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sobre una extensió ciclotòmica $\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q})$, ens podem construir

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times,$$

una representació d'Artin de dimensió 1 sobre $\mathbb{C}$.

3.2 Sèrie L d'una corba el·líptica

Considerem una corba plana afí $C : f(X, Y) = 0$ sobre $\mathbb{F}_p$.

Definició 3.15. La *funció zeta de C* és

$$\zeta(C, s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

si $\Re(s) > 1$, on el productori es fa sobre els ideals primers diferents de zero de $\mathbb{F}_p[x, y] = {}^{\mathbb{F}_p[X,Y]}\!/_{(f(X,Y))}$.

Per a cada ideal primer $\mathfrak{p}$, el quocient ${}^{\mathbb{F}_p[x,y]}\!/_{\mathfrak{p}}$ és finit i és un domini, o sigui, és un cos, i denotem per $\deg \mathfrak{p}$ el seu grau sobre $\mathbb{F}_p$. Gràcies a la igualtat

$$\#{}^{\mathbb{F}_p[x,y]}\!/_{\mathfrak{p}} = p^{\deg \mathfrak{p}},$$

podem fer el canvi de variables $T = p^{-s}$ en la funció zeta de C i obtenir

$$Z(C, T) = \prod_{\mathfrak{p}} \frac{1}{1 - T^{\deg \mathfrak{p}}},$$

de manera que $\zeta(C, s) = Z(C, p^{-s})$.

El que volem ara és trobar la relació entre la funció zeta i els punts de C. Ve donada pel següent resultat:

Proposició 3.16. *Sigui $Z(C, T)$ la funció zeta d'una corba afí C sobre $\mathbb{F}_p$, i sigui $N_m = \#C(\mathbb{F}_{p^m})$ per a tot m enter positiu. Aleshores*

$$\log Z(C, T) = \sum_{m \geq 1} N_m \frac{T^m}{m},$$

i per tant

$$Z(C, T) = \exp\Big(\sum_{m \geq 1} N_m \frac{T^m}{m}\Big).$$

Demostració. Veure [11, Capítol IV]. □

Observem que si C és una corba projectiva podem definir de la mateixa manera la seva funció zeta, és a dir,

$$Z(C, T) = \exp\Big(\sum_{m \geq 1} N_m \frac{T^m}{m}\Big),$$

i $\zeta(C,s) = Z(C,p^{-s})$. De fet, si E és una corba el·líptica projectiva, es pot veure

$$Z(E,T) = \frac{1}{1-T} Z(E^{\text{afí}},T),$$

on $E^{\text{afí}} = E \cap \{z=0\}$.

Teorema 3.17. *Sigui E una corba el·líptica sobre $\mathbb{F}_p$. Aleshores*

$$Z(E,T) = \frac{1-(p+1-N_1)T+pT^2}{(1-T)(1-pT)},$$

on $N_1 = \#E(\mathbb{F}_p)$.

Demostració. La proposició 3.16 ens diu que

$$\log Z(E,T) = \sum_{m\geq 1} N_m \frac{T^m}{m}.$$

En l'apartat 2.4 havíem vist que els nombres N_m són de la forma

$$N_m = 1 + p^m - \alpha^m - \overline{\alpha}^m,$$

on $\alpha, \overline{\alpha}$ són les arrels del polinomi característic $T^2 - a_pT + p$. Per tant,

$$\log Z(C,T) = \sum_{m\geq 1} \frac{T^m}{m} + \sum_{m\geq 1} \frac{(pT)^m}{m} - \sum_{m\geq 1} \frac{(\alpha T)^m}{m} - \sum_{m\geq 1} \frac{(\overline{\alpha}T)^m}{m} =$$

$$= -\log(1-T) - \log(1-pT) + \log(1-\alpha T) + \log(1-\overline{\alpha}T) =$$

$$= \log \frac{(1-\alpha T)(1-\overline{\alpha}T)}{(1-T)(1-pT)} = \log \frac{1-(p+1-N_1)T+pT^2}{(1-T)(1-pT)}.$$

□

D'aquest teorema es pot deduir que, si E és una corba el·líptica, la desigualtat del teorema de Hasse (2.11),

$$|N_1 - p - 1| \leq 2\sqrt{p},$$

és equivalent a la hipòtesi de Riemann per a E, que podem formular de la manera següent:

$$\textit{Si } Z(E,p^{-s}) = 0, \textit{ aleshores } \Re(s) = 1/2.$$

El resultat anterior s'espera que sigui cert per a corbes més generals. Weil (1949) va conjecturar el següent:

Teorema 3.18 (Conjectures de Weil)**.** *Sigui V una varietat algebraica projectiva sobre $\mathbb{F}_q$ de dimensió n. Aleshores*

1. *$Z(V,T) \in \mathbb{Q}(T)$.*
2. *Existeix un enter ϵ, la característica d'Euler de V, tal que*

$$Z(V, \frac{T}{q^n}) = \pm q^{n\frac{\epsilon}{2}} T^\epsilon Z(V,T).$$

3. Hipòtesi de Riemann:

$$Z(V,T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)P_2(T)\cdots P_{2n}(T)},$$

on $P_i(T) \in \mathbb{Z}[T]$*, amb* $P_0(T) = 1 - T$ *i* $P_{2n}(T) = 1 - q^n T$*, i per a cada* $0 \leq i \leq 2n$*,*

$$P_i(T) = \prod_{j=1}^{b_i}(1 - \alpha_{ij}T)$$

sobre $\mathbb{C}$*, amb* $|\alpha_{ij}| = q^{1/2}$*,* $b_i = \deg P_i(T)$*.*

Nosaltres hem vist que és cert en el cas de les corbes el·líptiques. El mateix Weil el va demostrar per a corbes i varietats abelianes. El resultat general, va ser provat per parts: Dwork (1960) va provar la racionalitat de la funció zeta usant anàlisis funcional p-àdic, i més tard es va donar una demostració alternativa fent servir cohomologia ℓ-àdica on també es veia l'equació funcional (b). Finalment, Deligne (1973) va demostrar la hipòtesi de Riemann.

Un cop tenim definida la funció zeta d'una corba el·líptica sobre $\mathbb{F}_p$, el nostre objectiu és definir-la per a la corba vista sobre $\mathbb{Q}$.

Definició 3.19. Sigui E una corba el·líptica sobre $\mathbb{Q}$, i sigui S el conjunt de primers pels quals E té mala reducció. La *funció zeta de* E és

$$\zeta(E,s) := \prod_{p\notin S}\zeta(E_p,s),$$

que podem escriure com

$$\zeta(E,s) = \prod_{p\notin S}\frac{1-(p+1-N_p)p^{-s}+p^{1-2s}}{(1-p^{-s})(1-p^{1-s})} = \frac{\zeta_S(s)\zeta_S(s-1)}{L_S(E,s)},$$

on $\zeta_S(s)$ és la funció zeta sense els factors corresponents als primers de S i

$$L_S(E,s) := \prod_{p\notin S}\frac{1}{1-(p+1-N_p)p^{-s}+p^{1-2s}} = \prod_{p\notin S}\frac{1}{1-\alpha_p p^{-s}}\frac{1}{1-\beta_p p^{-s}},$$

on l'última igualtat surt de $1-(p+1-N_p)T+pT^2 = (1-\alpha_p T)(1-\beta_p T)$.

A la funció $L_S(E,s)$ volem afegir-li factors pels primers de S, que sabem que n'hi ha un nombre finit. Definim $L_p(E,T) := 1 - a_pT + \det(\mathrm{Frob}_p)T^2$. Aleshores, si $a_p = p+1-\#E(\mathbb{F}_p)$, recordant el càlcul del nombre de punts d'una corba pels primers de mala reducció vist en 2.2, tenim

$$L_p(E,T) = \begin{cases} 1-a_pT+pT^2 & \text{si } p \text{ és de bona reducció,}\\ 1-T & \text{si } p \text{ és de reducció multiplicativa dividida,}\\ 1+T & \text{si } p \text{ és de reducció multiplicativa no dividida,}\\ 1 & \text{si } p \text{ és de reducció additiva.}\end{cases}$$

Definició 3.20. Sigui E una corba el·líptica. La *funció L associada a* E és

$$L(E,s) := \prod_p \frac{1}{L_p(E,p^{-s})} = \prod\frac{1}{1-a_pp^{-s}+p^{1-2s}}\prod\frac{1}{1-p^{-s}}\prod\frac{1}{1+p^{-s}},$$

on el primer productori és sobre els primers de bona reducció i els altres sobre els de reducció multiplicativa, dividida i no dividida respectivament.

3.3 Equidistribució

En aquesta secció, veurem la definició d'equidistribució, i veurem una caracterització de l'equidistribució d'una successió en termes de caràcters.

Sigui X un espai compacte Hausdorff i sigui $C(X)$ l'espai de Banach de les funcions $f : X \to \mathbb{C}$ amb la norma del suprem.

Definició 3.21. Una *mesura de Radon* sobre X és una aplicació contínua $\mu : C(X) \to \mathbb{C}$ tal que $\mu(f) \geq 0$ per a tot $f \geq 0$ i $\mu(\mathbb{1}_X) = 1$.

Al llarg del capítol apareixerà el terme *grup compacte*, que consisteix en un grup G amb una topologia per la qual les operacions de grup són contínues i G com a espai topològic és compacte.

Definició 3.22. Sigui G un grup compacte. La *mesura de Haar* de G és una mesura de Radon μ invariant per translacions, és a dir, μ tal que $\forall S \subseteq X$ mesurable i $\forall g \in G$,

$$\mu(gS) = \mu(Sg) = \mu(S).$$

La mesura de Haar és única llevat escalament, i si G és un grup finit aleshores és la mesura de comptar ($\mu(S) = \#S$) normalitzada.

Definició 3.23. Una successió $(x_i) \subset X$ és *equidistribuïda respecte la mesura* μ, o *μ-equidistribuïda*, si per a cada $f \in C(X)$

$$\mu(f) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(x_i).$$

A continuació tenim un seguit de resultats elementals de mesures i equidistribució, que podem trobar demostrats en [20].

Lema 3.24. *Sigui (f_j) una família de funcions tal que la família de les seves combinacions lineals és densa en $C(X)$. Si $(x_i) \subset X$ és una successió tal que $\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f_j(x_i)$ convergeix per a tota f_j, aleshores existeix una única mesura μ en X per la qual (x_i) és μ-equidistribuïda.*

Proposició 3.25. *Si (x_i) és una successió μ-equidistribuïda en X i $S \subseteq X$ és un conjunt amb frontera de mesura zero, aleshores*

$$\mu(S) = \lim_{n\to\infty} \frac{\#\{x_i \in S : i \leq n\}}{n}.$$

Sigui G un grup compacte. Considerem $X := \mathrm{conj}(G)$, el conjunt de les seves classes de conjugació, i la projecció $\pi : G \to X$. Si μ és la mesura de Haar en G normalitzada, considerem la mesura $\mu(f) := \mu(f \circ \pi)$ en X.

Proposició 3.26. *Sigui G un grup compacte amb mesura de Haar μ, i sigui $X = \mathrm{conj}(G)$. Una successió $(x_i) \subset X$ és μ-equidistribuïda si i només si per a tot caràcter irreductible χ de G,*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi(x_i) = \mu(\chi).$$

Corol·lari 3.27. *Una successió $(x_i) \subset X$ és μ-equidistribuïda si i només si per a tot caràcter irreductible no trivial χ de G,*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi(x_i) = 0.$$

La proposició següent reuneix els conceptes i resultats vistos en capítols anteriors sobre l'element de Frobenius i els d'aquest apartat per veure que la successió de les traces del Frobenius és equidistribuïda:

Proposició 3.28. *Sigui E una corba el·líptica ordinària sobre $\mathbb{F}_q$, i sigui $a_{q^r} = q^r + 1 - \#E(\mathbb{F}_{q^r})$ per a tot enter $r \geq 1$. Sigui $x_r := \frac{a_{q^r}}{q^{r/2}}$. Aleshores la successió (x_r) està equidistribuïda en $[-2,2]$ respecte la mesura*

$$\mu := \frac{1}{\pi}\frac{dz}{\sqrt{4-z^2}},$$

on dz és la mesura de Lebesgue en $[-2,2]$.

Demostració. Considerem α tal que $a_{q^r} = \alpha^r + \overline{\alpha}^r$, de norma $|\alpha| = q^{1/2}$. Aleshores tenim $x_r = \frac{\alpha^r + \overline{\alpha}^r}{q^{r/2}}$ per a tot $r \geq 1$. Sigui $\mathrm{U}(1) := \{u \in \mathbb{C}^\times \mid u\overline{u} = 1\}$. Per a $u = e^{i\theta}$, la mesura de Haar en $\mathrm{U}(1)$ és la mesura uniforme en $\theta \in [-\pi, \pi]$. Amb l'aplicació

$$u \longmapsto z := u + \overline{u} = 2\cos\theta,$$

calculem la mesura de Haar μ en $[-2,2]$, i obtenim $dz = 2\sin\theta d\theta$ i

$$\mu = \frac{1}{\pi}\frac{dz}{\sqrt{4-z^2}}.$$

Els caràcters irreductibles no trivials de $\mathrm{U}(1) \to \mathbb{C}^\times$ són de la forma $\chi_a(u) = u^a$ per a algun $a \in \mathbb{Z}$ diferent de zero. Per a cadascun d'aquests caràcters χ_a tenim

$$\lim_{n\to\infty}\frac{1}{n}\sum_{r=1}^{n}\chi_a(\alpha^r/q^{r/2}) = \lim_{n\to\infty}\frac{1}{n}\sum_{r=1}^{n}(\alpha/q^{1/2})^{ra} =$$

$$= \lim_{n\to\infty}\frac{1}{n}\frac{(\alpha/q^{1/2})^{a(n+1)} - (\alpha/q^{1/2})^a}{(\alpha/q^{1/2})^a - 1} = 0.$$

El fet que E sigui ordinària ens assegura que $\alpha/q^{r/2}$ no és una arrel de la unitat, i per tant el denominador no s'anul·la per a cap $a \in \mathbb{Z}$ diferent de zero. Com a conseqüència del corol·lari 3.27, tenim que $(\alpha/q^{r/2})$ és equidistribuïda en $\mathrm{U}(1)$, i aleshores (x_r) és μ-equidistribuïda. □

3.4 Relació amb equidistribució

Per acabar el capítol, demostrarem un teorema que ens dóna una caracterització de l'equidistribució d'una successió en termes d'extensions holomorfes de certes sèries L.

Siguin G un grup compacte i $X = \mathrm{conj}(G)$ el conjunt de les seves classes de conjugació. Sigui $P = (\mathfrak{p}_1, \mathfrak{p}_2, \ldots)$ una successió de primers $\mathfrak{p}$ de $\Bbbk$ ordenats per norma.

Teorema 3.29. *Siguin $(x_{\mathfrak{p}_i})_{i\geq 1} \subseteq X$ una successió i ρ una representació irreductible de G. Suposem que $L(\rho, s)$ és meromorfa per $\Re(s) \geq 1$ i no s'anul·la ni té cap pol excepte potser en $s = 1$. Aleshores la successió $(x_{\mathfrak{p}_i})_{i\geq 1}$ és μ-equidistribuïda sobre X si i només si per a tota representació irreductible no trivial ρ de G, $L(\rho, s)$ es pot estendre a una funció holomorfa en $\Re(s) \geq 1$ que no s'anul·la en $s = 1$.*

Demostració. Sigui χ el caràcter de la representació ρ. Demostrarem primer el següent resultat:
$L(\rho, s)$ es pot estendre a una funció holomorfa que no s'anul·la en $\Re(s) \geq 1$ si i només si

$$\sum_{N(\mathfrak{p}_i)\leq n} \chi(x_{\mathfrak{p}_i}) = o\Big(\frac{n}{\log n}\Big),\ n \to \infty.$$

Si λ_{ij} són els valors propis de $\rho(x_{\mathfrak{p}_i})$ per a $j = 1, \ldots, n$, podem escriure

$$L(\rho, s) = \prod_{i\geq 1}\prod_{j=1}^{d} \frac{1}{1-\lambda_{ij}N(\mathfrak{p}_i)^{-s}}.$$

La derivada logarítimica de $L(\rho, s)$ és

$$\frac{L'(\rho,s)}{L(\rho,s)} = -\sum_{i\geq 1}\sum_{j=1}^{d}\sum_{m\geq 1} \frac{\lambda_{ij}^m \log(N(\mathfrak{p}_i))}{N(\mathfrak{p}_i)^{ms}} = -\sum_{i\geq 1}\sum_{m\geq 1} \frac{\chi(x_{\mathfrak{p}_i}^m)\log(N(\mathfrak{p}_i))}{N(\mathfrak{p}_i)^{ms}}.$$

Com que $\sum_{i\geq 1}\sum_{m\geq 2} \frac{\log(N(\mathfrak{p}_i))}{|N(\mathfrak{p}_i)^{ms}|}$ convergeix per $\Re(s) > \frac{1}{2}$, podem reescriure la derivada anterior com

$$\frac{L'(\rho,s)}{L(\rho,s)} = F(s)\phi(s),$$

on $\phi(s)$ és una funció holomorfa per $\Re(s) > \frac{1}{2}$ i

$$F(s) = -\sum_{i\geq 1} \frac{\chi(x_{\mathfrak{p}_i})\log(N(\mathfrak{p}_i))}{N(\mathfrak{p}_i)^s}.$$

Per hipòtesis, $L(\rho, s)$ és meromorfa per $\Re(s) \geq 1$, no té pols i no s'anul·la excepte potser un zero en $s = 1$ d'ordre $-c$. Aleshores $\frac{L'(\rho,s)}{L(\rho,s)}$ és meromorfa per $\Re(s) \geq 1$ amb potser un pol simple en $s = 1$ de residu c. Com que $\phi(s)$ és holomorfa per $\Re(s) > \frac{1}{2}$, llavors $F(s)$ també és meromorfa per $\Re(s) \geq 1$ amb com a molt un pol simple en $s = 1$ de residu c.

Necessitarem el teorema de Wiener–Ikehara, que diu que si $F(x)$ és una funció no negativa monòtona decreixent definida per a $x \in \mathbb{R}^+$ per la qual la integral $\int_0^\infty e^{-xs}F(x)dx$ convergeix en el semiplà $\Re(s) > 1$ a una funció analítica en $\Re(s) \geq 1$ excepte per un pol simple a $s = 1$ de residu 1, aleshores

$$\lim_{x\to\infty} e^{-x}F(x) = 1.$$

Si l'apliquem a la funció $F(s)$, obtenim

$$\sum_{N(\mathfrak{p}_i)\leq n} \chi(x_{\mathfrak{p}_i})\log(N(\mathfrak{p}_i)) = cn + o(n),\ n \to \infty.$$

Fent servir el truc de sumació d'Abel arribem a

$$\sum_{N(\mathfrak{p}_i)\leq n} \chi(x_{\mathfrak{p}_i}) = c\frac{n}{\log n} + o\Big(\frac{n}{\log n}\Big),\ n \to \infty$$

i hem provat el resultat desitjat.

Finalment, el teorema es dedueix a partir d'aquest resultat, el corol·lari 3.27 i el teorema dels nombres primers, que ens diu que el nombre de primers $\mathfrak{p}_i$ tals que $N(\mathfrak{p}_i) \leq n$ és $\frac{n}{\log n}$ quan $n \to \infty$. □

Observem que quan G és un grup abelià finit, les representacions irreductibles són precisament els caràcters irreductibles. A la secció 3.1 hem vist que en efecte $L(\chi, s)$ es pot estendre a una funció holomorfa en $\Re(s) \geq 1$ no nul·la en $s = q$, i per tant pel teorema 3.29 tenim l'equidistribució de la successió $(x_{\mathfrak{p}_i})$.

Finalment, per connectar aquest teorema amb un resultat ja vist, com a conseqüència recuperem el teorema de Chebotarev enunciat al primer capítol:

Corol·lari 3.30. *Sigui $\mathbb{L}/\Bbbk$ una extensió finita de Galois, $G = \mathrm{Gal}(\mathbb{L}/\Bbbk)$, i sigui P la successió de primers de $\Bbbk$ que no ramifiquen ordenats per norma. Aleshores la successió $(\mathrm{conj}_{\mathbb{L}}(\mathrm{Frob}_{\mathfrak{p}}))_{\mathfrak{p}\in P}$ és equidistribuïda en $\mathrm{conj}(G)$. En particular, es compleix el teorema de Chebotarev (1.12).*

Capítol 4

La conjectura de Sato–Tate

Un cop hem presentat les corbes el·líptiques, les sèries L i l'equidistribució, ens trobem en condicions d'enunciar i demostrar la conjectura de Sato–Tate, distingint els casos CM i no CM. Finalment, reenunciarem el resultat en termes de teoria de grups.

4.1 Multiplicació complexa en corbes el·líptiques

Com hem vist en la secció 2.2, l'anell d'endomorfismes d'una corba el·líptica E pot ser isomorf a

- $\mathbb{Z}$,
- un ordre en un cos quadràtic imaginari, o
- un ordre en una àlgebra de quaternions sobre $\mathbb{Q}$.

Recordem que l'últim cas només pot passar si la corba està definida sobre un cos de característica positiva. En particular, no pot passar sobre $\mathbb{Q}$, que és on ho estudiarem de manera natural.

Quan $\mathrm{End}(E)$ és més gran que $\mathbb{Z}$, direm que la corba té *multiplicació complexa*, o simplement CM. Per entendre bé el que vol dir tenir un anell d'endomorfismes gran, pensarem els punts d'una corba el·líptica sobre $\mathbb{C}$, $E(\mathbb{C})$, com el quocient $\mathbb{C}/\Lambda$, on $\Lambda = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ és un reticle, i e_1, e_2 són una $\mathbb{R}$-base de $\mathbb{C}$. Al capítol 5 veurem amb detall els motius pels quals aquesta identificació té sentit.

Considerem un endomorfisme ψ diferent de la multiplicació per un enter, $\psi : E(\mathbb{C}) \to E(\mathbb{C})$, el qual ens dóna una aplicació holomorfa

$$f : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda.$$

Pel fet de ser holomorfa, és analítica, i en conseqüència la podem representar amb una sèrie de potències convergent

$$f(z) = b_0 + b_1 z + b_2 z^2 + b_3 z^3 + \dots$$

en un entorn del 0. I per ser un homomorfisme, per a dos complexos z_1, z_2 d'un entorn del zero, $f(z_1 + z_2) = f(z_1) + f(z_2)$ en $\mathbb{C}/\Lambda$, o equivalentment,

$$f(z_1 + z_2) - f(z_1) - f(z_2) \in \Lambda.$$

Si f no fos constant, la imatge d'un obert hauria de ser un obert. Tanmateix, Λ no conté cap obert no buit al ser un conjunt discret. De manera que f és constant. Si evaluem en $z_1 = z_2 = 0$, veiem que és $-b_0$. A més, de $f(0) = 0$ podem deduir $b_0 \in \Lambda$, assumir $b_0 = 0$, i concloure

$$f(z_1 + z_2) = f(z_1) + f(z_2)$$

per a tot z_1, z_2 propers a 0.

Si calculem els endomorfismes que compleixen la condició anterior, veiem que són de la forma

$$f(z) = cz,$$

per a una certa $c \in \mathbb{C}$ no arbitrària. Atès que f és una aplicació en el quocient, si prenem dos representants w_1, w_2 de la mateixa classe, han de tenir la mateixa imatge. Així doncs, en $\mathbb{C}/\Lambda$ es compleix

$$f(w_1) = f(w_2) \Leftrightarrow cw_1 = cw_2 \Leftrightarrow c(w_1 - w_2) \in \Lambda.$$

Per tant, el nombre $c \in \mathbb{C}$ ha de satisfer la restricció

$$c\Lambda \subset \Lambda.$$

Quan $c \in \mathbb{Z}$, sempre és certa. D'aquí surt el nom de *multiplicació complexa*, perquè per a que la corba tingui més endomorfismes a part de la multiplicació per un enter, ha d'existir algun $c \in \mathbb{C} \setminus \mathbb{Z}$ que satisfaci la condició anterior, obtenint l'endomorfisme multiplicació per un complex $f(z) = cz$.

Un exemple típic de corba el·líptica amb CM és $E : y^2 = x^3 + x$ sobre $\mathbb{Q}(i)$, amb l'endomorfisme $\psi(x, y) = (-x, iy)$.

De fet, la teoria de la multiplicació complexa es fa servir per construir l'extensió abeliana maximal d'un cos quadràtic imaginari. En [24, Capítol 6], trobem un exemple de com fer-ho per a $\mathbb{Q}(i)$ utilitzant precisament la corba el·líptica $E : y^2 = x^3 + x$.

En aquest capítol veurem que quan una corba el·líptica té CM, la demostració de la conjectura de Sato–Tate és ben coneguda i es pot entendre en termes d'uns certs caràcters i unes funcions L associades. En canvi, si no té CM és força més complicada.

4.2 Sato–Tate per a corbes el·líptiques amb CM

Quan tenim una corba el·líptica definida sobre un cos $\Bbbk$ amb CM, podem distingir dos casos segons si $\Bbbk$ conté el cos de multiplicació complexa o no. En la primera situació, la conjectura de Sato–Tate s'enuncia de la següent manera:

Teorema 4.1 (Conjectura de Sato–Tate per a corbes amb CM sobre $\Bbbk$)**.** *Siguin $\Bbbk$ un cos i $E/\Bbbk$ una corba el·líptica de conductor $\mathfrak{f}$ amb multiplicació complexa sobre $\Bbbk$. Sigui P la successió de primers de $\Bbbk$ que no divideixen $\mathfrak{f}$ ordenats per norma. Sigui $x_\mathfrak{p} := \frac{a_\mathfrak{p}}{N(\mathfrak{p})^{1/2}} \in [-2, 2]$ la traça de l'element de Frobenius de $E_\mathfrak{p}$ normalitzada per a cada $\mathfrak{p} \in P$. La successió $(x_\mathfrak{p})$ està equidistribuïda en $[-2, 2]$ respecte la mesura*

$$\mu_{\mathrm{CM}} := \frac{1}{\pi} \frac{dz}{\sqrt{4 - z^2}}.$$

L'exemple més habitual d'aquesta situació és un cos quadràtic imaginari $\Bbbk$ i una corba el·líptica definida sobre aquest cos quadràtic imaginari pel qual té CM.

Per provar 4.1, neccesitem definir-nos els caràcters de Hecke i la seva funció L associada.

Definició 4.2. Siguin $\mathbb{L}$ un cos de nombres, $\mathcal{O}_\mathbb{L}$ el seu anell d'enters i $I, J, \mathfrak{M} \subset \mathcal{O}_\mathbb{L}$ ideals. Un *caràcter de Hecke mòdul* $\mathfrak{M}$ és una aplicació ψ dels ideals fraccionaris de $\mathcal{O}_\mathbb{L}$ als nombres complexos, és a dir, dels ideals A pels quals existeix $x \in \mathcal{O}_\mathbb{L}$ no nul tal que $xA \subseteq \mathcal{O}_\mathbb{L}$ a $\mathbb{C}$, que satisfà:

(i) $\psi(\mathcal{O}_\mathbb{L}) = 1$,

(ii) $\psi(I) \neq 0$ si i només si no hi ha cap ideal primer que divideixi I i $\mathfrak{M}$,

(iii) $\psi(IJ) = \psi(I)\psi(J)$.

Aquesta definició generalitza el concepte de caràcter de Dirichlet. Anàlogament a com havíem fet a 3.1, podem considerar el conductor d'un caràcter de Hecke, al que denotarem $\mathfrak{f}$. Considerem un caràcter de Dirichlet qualsevol $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$. Prenem $\mathbb{L} = \mathbb{Q}$, $\mathcal{O}_\mathbb{L} = \mathbb{Z}$, i definim $\mathfrak{f} = n\mathbb{Z}$. Tenint en compte que $\mathbb{Z}$ és un domini d'ideals principals, es pot veure que efectivament, el caràcter

$$\begin{aligned} \psi_\chi : \{\text{ideals fraccionaris de } \mathbb{Z}\} &\longrightarrow \mathbb{C} \\ (\alpha) &\longmapsto \chi(|\alpha|), \end{aligned}$$

està ben definit i és un caràcter de Hecke de conductor $\mathfrak{f}$.

Definició 4.3. Sigui ψ un caràcter de Hecke. La *funció L de Hecke associada a* ψ és

$$L(\psi, s) := \prod_{\mathfrak{p} \nmid \mathfrak{f}} \frac{1}{1 - \psi(\mathfrak{p})N(\mathfrak{p})^{-s}}.$$

La noció de funció L de Hecke també estén la de funció L de Dirichlet, vista a la proposició 3.10.

El proper lema ens dóna un resultat d'equidistribució d'una certa successió definida per un caràcter de Hecke, que veurem que serà la successió $(x_\mathfrak{p})$ de l'enunciat del teorema 4.1.

Lema 4.4. *Sigui ψ un caràcter de Hecke de conductor $\mathfrak{f}$. Sigui $(x_\mathfrak{p})$ la successió indexada pels primers $\mathfrak{p} \nmid \mathfrak{f}$ ordenats per norma amb $x_\mathfrak{p} := \frac{\psi(\mathfrak{p})}{|\psi(\mathfrak{p})|} \in \mathrm{U}(1)$. Aleshores $(x_\mathfrak{p})$ està equidistribuïda en* $\mathrm{U}(1)$.

Demostració. Veure [25, Lema 2.15]. □

Tornant a la nostra corba el·líptica $E/\mathbb{k}$ de conductor $\mathfrak{f}$, un resultat clàssic de Deuring (veure [23, Teorema II.10.5]) ens garanteix l'existència d'un caràcter de Hecke adient ψ_E de $\mathbb{k}$ de conductor $\mathfrak{f}$ tal que per a cada $\mathfrak{p} \nmid \mathfrak{f}$ tenim $|\psi_E(\mathfrak{p})| = N(\mathfrak{p})^{1/2}$ i $\psi_E(\mathfrak{p}) + \overline{\psi_E(\mathfrak{p})} = a_\mathfrak{p}$, on

$$a_\mathfrak{p} := \mathrm{tr}(\mathrm{Frob}_\mathfrak{p}) = N(\mathfrak{p}) + 1 - \#E_\mathfrak{p}(\mathbb{F}_\mathfrak{p}) \in \mathbb{Z}.$$

Fent servir això i el lema anterior, podem demostrar la conjectura de Sato–Tate per a corbes amb CM:

Demostració. (Conjectura de Sato–Tate per a corbes amb CM sobre $\mathbb{k}$, 4.1) Pel lema anterior, tenim que la successió $(\frac{\psi_E(\mathfrak{p})}{N(\mathfrak{p})^{1/2}})_{\mathfrak{p} \in P}$ és equidistribuïda en $\mathrm{U}(1)$. En la proposició 3.28, hem vist que l'aplicació $u \mapsto u + \overline{u}$ ens dóna la mesura de Haar μ_{CM} de $\mathrm{U}(1)$ en $[-2, 2]$. Per a cada $\mathfrak{p} \in P$, la imatge de $\frac{\psi_E(\mathfrak{p})}{N(\mathfrak{p})^{1/2}}$ per l'aplicació esmentada és

$$\frac{\psi_E(\mathfrak{p})}{N(\mathfrak{p})^{1/2}} + \frac{\overline{\psi_E(\mathfrak{p})}}{N(\mathfrak{p})^{1/2}} = \frac{a_\mathfrak{p}}{N(\mathfrak{p})^{1/2}} = x_\mathfrak{p}.$$

□

Un cop vista la conjectura quan $\Bbbk$ conté el cos de multiplicació complexa, vegem el cas contrari. Primer de tot, considerem $\Bbbk = \mathbb{Q}$, i sigui $\mathbb{L}$ el cos de CM. Recordem que E_p és la reducció de la corba mòdul p (2.2). Pels primers de $\mathbb{L}$ que no ramifiquen, tenim dues possibilitats:

- Si p és inert, l'àlgebra d'endomorfismes de E_p conté dos cossos quadràtics imaginaris: el corresponent al de multiplicació complexa $\mathbb{L}$, i el generat per l'endomorfisme de Frobenius. Això implica que l'àlgebra d'endomorfismes és una àlgebra de quaternions, i per tant E_p és supersingular. De fet, es pot veure que $a_p = 0$, i per tant $x_p = 0$ (veure [22, Capítol 5]).

- Si $p = \mathfrak{p}\overline{\mathfrak{p}}$, és a dir, descomposa, $E_p \cong E_{\mathfrak{p}}$, i per tant tenim $a_{\mathfrak{p}} = a_p$.

Pel teorema de Chebotarev (1.12), els conjunts de primers inerts i que descomposen tenen tots dos densitat $1/2$. Per tant, la conjectura de Sato–Tate es formula de forma natural sobre $\mathbb{Q}$ de la següent manera:

Teorema 4.5 (Conjectura de Sato–Tate per a corbes amb CM sobre $\mathbb{L}$)**.** *Sigui $E/\mathbb{Q}$ una corba el·líptica de conductor N amb multiplicació complexa sobre un cos $\mathbb{L}$. Sigui P la successió de primers de $\mathbb{Q}$ que no divideixen N ordenats per norma. Sigui $x_p := \frac{a_p}{\sqrt{p}} \in [-2,2]$ la traça de l'element de Frobenius de E_p normalitzada per a cada $p \in P$. La successió (x_p) està equidistribuïda en $[-2,2]$ respecte la mesura*

$$\frac{1}{2}\delta_0 + \frac{1}{2}\mu_{\mathrm{CM}},$$

on δ_0 és la delta de Dirac en el zero i $\mu_{\mathrm{CM}} = \frac{1}{\pi}\frac{dz}{\sqrt{4-z^2}}$.

Si $\Bbbk \neq \mathbb{Q}$ és un cos que no conté $\mathbb{L}$, se segueix el mateix raonament i obtenim el mateix resultat però en $\Bbbk\mathbb{L}$: la meitat dels primers descomposen i la meitat són inerts, i la conjectura de Sato–Tate s'enuncia de forma similar.

4.3 Sato–Tate per a corbes el·líptiques sense CM

Ara volem veure la conjectura de Sato–Tate per a corbes el·líptiques que no tenen multiplicació complexa. Veurem la demostració per a corbes el·líptiques definides sobre $\mathbb{Q}$, tot i que es coneix per a corbes sobre cossos totalment reals, que són cossos de nombres pels quals la imatge de tot capbussament d'ell mateix en $\mathbb{C}$ està inclosa en els reals, i sobre extensions quadràtiques imaginàries de cossos totalment reals. Ara per ara, el cas general és conegut únicament per a cossos de nombres de grau 1 i 2. L'enunciat sobre $\mathbb{Q}$ és el següent:

Teorema 4.6 (Conjectura de Sato–Tate per a corbes sense CM)**.** *Sigui $E/\mathbb{Q}$ una corba el·líptica sense multiplicació complexa, i sigui (x_p) la successió definida per $x_p := \frac{a_p}{\sqrt{p}} \in [-2,2]$. Aleshores*

$$\lim_{N\to\infty} \frac{\#\{p \leq N \mid x_p \in [a,b]\}}{\#\{p \leq N\}} = \frac{1}{2}\int_a^b \sqrt{4-t^2}dt.$$

Primer de tot, sigui

$$G = \mathrm{SU}(2) := \{\begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C}, \alpha\overline{\alpha} + \beta\overline{\beta} = 1\}.$$

Les representacions irreductibles ρ_m de G són les potències m-èsimes de la representació natural donada per la inclusió $\mathrm{SU}(2) \subseteq \mathrm{GL}(2,\mathbb{C})$. El conjunt de les classes de conjugació de G, $X := \mathrm{conj}(G)$, està format per elements que es poden representar com

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix},\ \theta \in [0,\pi].$$

Cada element de $C(X)$ es pot veure com una funció $f(\theta)$ contínua. Considerem la mesura de Haar de G en X

$$\mu := \frac{2}{\pi}\sin^2\theta d\theta,$$

és a dir, per a cada $f \in C(X)$,

$$\mu(f) = \frac{2}{\pi}\int_0^\pi f(\theta)\sin^2\theta d\theta.$$

Si $E/\mathbb{Q}$ és una corba el·líptica sense CM i P la successió de primers p que no divideixen el conductor $\mathfrak{f}$ de E, considerem per a cada p l'element $x_p \in X$ corresponent a $\theta_p \in [0,\pi]$ tal que

$$2\cos\theta_p\sqrt{p} = a_p = p + 1 - \#E_p(\mathbb{F}_p)$$

és la traça del Frobenius de E_p.

Si repassem tot el que hem definit fins ara en aquesta secció, veiem que ens trobem en les condicions del teorema 3.29 amb $G = \mathrm{SU}(2)$, $X = \mathrm{conj}(G)$, $\Bbbk = \mathbb{Q}$, una successió P ordenada per norma, $(x_p) \subset X$, i per a cada enter $m \geq 1$ tenim $\rho_m : G \to \mathrm{GL}(m+1,\mathbb{C})$ amb la seva funció L associada,

$$L(\rho_m, s) := \prod_{p\nmid\mathfrak{f}} \det(1 - \rho_m(x_p)p^{-s})^{-1} = \prod_{p\nmid\mathfrak{f}}\prod_{k=0}^{m}(1 - e^{i(m-2k)\theta_p}p^{-s})^{-1}.$$

Si per a cada $p \nmid \mathfrak{f}$ prenem les arrels del polinomi $T^2 - a_pT + p$, o sigui, $\alpha_p = e^{i\theta_p}\sqrt{p}$ i la conjugada $\overline{\alpha}_p$, i definim

$$L_m^1(s) := \prod_{p\nmid\mathfrak{f}}\prod_{r=0}^{m}(1 - \alpha_p^{m-r}\overline{\alpha}_p^{r}p^{-s})^{-1},$$

aleshores tenim

$$L(\rho_m, s) = L_m^1(s - m/2).$$

Si suposem que $L_m^1(s)$ és holomorfa i diferent de 0 en $\Re(s) \geq 1 + m/2$, tenim que $L(\rho_m, s)$ també. El teorema 3.29 ens diu que (x_p) és μ-equidistribuïda i per tant la conjectura de Sato–Tate és certa. A continuació explicarem, sense entrar en els detalls, com veure que la suposició anterior, anomenada *conjectura de Tate*, és correcta.

Per fer-ho, és necessari parlar de *formes modulars*. Són un tipus de funcions complexes que tenen molt bones propietats, com per exemple, que podem expressar-les en sèries de Fourier de tal manera que els coeficients corresponents estan en bijecció amb un conjunt amb el que portem treballant tot el treball: els nombres a_p, les traces dels endomorfismes de Frobenius. La teoria sobre formes modulars es va començar a desenvolupar al segle XIX, relacionada amb l'estudi de les funcions el·líptiques. Més endavant, es va veure la seva importància en la teoria de nombres, amb la formulació del *teorema de modularitat*, que precisament ens dóna la correspondència esmentada.

Definició 4.7. Una *forma modular de pes* $k \in \mathbb{Z}$ pel grup de matrius 2×2 de determinant 1, $\mathrm{SL}(2,\mathbb{Z})$, és una funció holomorfa $f : \mathbb{H} \to \mathbb{C}$ del semiplà superior complex als complexos tal que satisfà l'equació funcional

$$f(\gamma z) = (cz+d)^k f(z),\ \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

i és holomorfa a l'infinit.

A la definició, entenem que *holomorfa a l'infinit* significa que podem expressar-la amb sèries de Fourier de la forma $f(z) = \sum_{n\geq 0} a_n e^{2\pi i n z}$. Dins les formes modulars hi ha un subespai, el de les formes modulars *cuspidals*, per a les que el primer coeficient de la sèrie de Fourier és $a_0 = 0$, i aquestes són les que es relacionen amb les corbes el·líptiques.

Es poden definir formes modulars sense exigir que l'equació anterior es compleixi per a tota matriu de $\mathrm{SL}(2,\mathbb{Z})$, n'hi ha prou en demanar-ho per a un subgrup. De fet, per demostrar la conjectura de Sato–Tate es fan servir formes modulars definides pel subgrup de matrius

$$\Gamma_0(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid c \equiv 0 \bmod N\}.$$

A més, de forma natural, les formes modulars tenen associades una representació de Galois, i per tant una funció L. Aquest fet és clau per a la nostra demostració.

El teorema de modularitat va ser conjecturat per primera vegada els anys 60, conegut com la *conjectura de Shimura–Taniyama*, i poc temps després, Weil va demostrar que era conseqüència d'una conjectura sobre funcions L de corbes el·líptiques, i va passar a conèixer-se com la *conjectura de Shimura–Taniyama–Weil*. El 1986, Frey va relacionar-la amb el famós últim teorema de Fermat. A partir del seu estudi, Serre i Ribet van acabar de demostrar que l'últim teorema de Fermat era conseqüència de la conjectura (veure [15]). A finals de segle, amb ajuda de Taylor i altres matemàtics, Wiles va demostrar-la per a corbes el·líptiques que no tenen mala reducció additiva, anomenades semiestables, i la va fer servir per provar el teorema de Fermat (veure [27]). El cas general va ser resolt per Breuil, Conrad, Diamond i Taylor l'any 2001. L'enunciat és el següent:

Teorema 4.8 (Teorema de modularitat)**.** *Per a tota corba el·líptica E sobre $\mathbb{Q}$ existeix una forma modular f de pes 2 tal que la sèrie L de E i la sèrie L de f coincideixen.*

Demostració. Veure [2]. □

Equivalentment, existeix una forma modular f tal que, si $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z}$, els coeficients de Fourier són precisament els valors $a_p = \#E(\mathbb{F}_p)$ quan p és un primer de bona reducció per E.

De fet, les sèries L de les que parla el teorema de modularitat, són

$$L(E,s) = L(f,s) = \prod_{p\nmid \mathfrak{f}} (1 - a_p p^{-s} + p^{1-2s})^{-1} = \prod_{p\nmid \mathfrak{f}} \prod_{r=0}^{1} (1 - \alpha_p^{1-r}\overline{\alpha}_p^{r} p^{-s})^{-1} = L_1^1(s),$$

on α_p i $\overline{\alpha}_p$ són les arrels de $T^2 - a_p T + p$.

Gràcies a propietats de les sèries L de les formes modulars, es pot provar que $L_m^1(s)$ és holomorfa i no s'anul·la en $\Re(s) \geq 3/2$. I, en conclusió, la conjectura de Sato–Tate (4.6) és certa.

4.4 Formulació axiomàtica

En seccions anteriors, hem vist que hi ha tres distribucions de Sato-Tate relacionades amb diferents mesures de Haar en $\mathrm{conj}(G)$ per a cert grup compacte $G \subseteq \mathrm{SU}(2)$. Les possibilitats són:

(a) $G = \mathrm{U}(1)$ amb la mesura $\mu(\theta) = \frac{1}{\pi} d\theta$, quan tenim una corba amb CM definida sobre un cos que conté el cos de CM.

(b) $G = N(\mathrm{U}(1))$ amb la mesura $\mu(\theta) = \frac{1}{2\pi} d\theta + \frac{1}{2}\delta_{\pi/2}$, quan tenim una corba amb CM definida sobre un cos que no conté el cos de CM.

(c) $G = \mathrm{SU}(2)$ amb la mesura $\mu(\theta) = \frac{2}{\pi}\sin^2\theta d\theta$, quan tenim una corba que no té CM.

L'objectiu d'aquesta secció és relacionar la corba E amb un grup G de manera que sigui un invariant aritmètic de la corba, sense dependre dels resultats d'equidistribució vistos en el capítol anterior. Volem seguir un procediment similar al del primer capítol, quan a partir d'un polinomi $f \in \mathbb{Z}[x]$ teníem una representació de Galois $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(d, \mathbb{C})$ que ens determinava $G_f \subseteq \mathrm{GL}(d, \mathbb{C})$ i $\mathrm{conj}(G_f)$. Al final acabàvem amb una successió $(\rho_f(\mathrm{Frob}_p))$ que, per Chebotarev, sabem que és equidistribuïda.

Ara, el que volem és, a partir d'una corba E sobre un cos de nombres K, trobar un grup $G \subseteq \mathrm{SU}(2)$ que, a través d'una representació de Galois de E, ens proporcioni una aplicació $\mathfrak{p} \to x_{\mathfrak{p}} \in X := \mathrm{conj}(G)$ tal que l'element $x_{\mathfrak{p}}$ es relacioni directament amb la quantitat $a_{\mathfrak{p}}$. Així doncs, la conjectura de Sato–Tate s'enuncia dient que la successió $(x_{\mathfrak{p}})$ està equidistribuïda en X.

Com hem comentat a l'inici de l'apartat, aquest grup G serà un dels tres mencionats anteriorment, i l'anomenarem *grup de Sato–Tate de* E, $\mathrm{ST}(E)$.

Recordem l'apartat 2.4, on hem definit el mòdul de Tate de E, $T_\ell(E) = \varprojlim_n E[\ell^n]$, que ens permetia treballar sobre $\mathbb{Z}_\ell$ a través de la representació $\rho_\ell : G \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}(2, \mathbb{Z}_\ell)$.

Definició 4.9. El *mòdul de Tate racional de* E és

$$V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Amb $V_\ell(E)$, obtenim la imatge de G per ρ_ℓ, $G_\ell \subseteq \mathrm{GL}(2, \mathbb{Q}_\ell)$.

Definició 4.10. El *grup* ℓ*-àdic de monodromia de* E, G_ℓ^{zar}, és la clausura de Zariski de G_ℓ en $\mathrm{GL}(2, \mathbb{Q}_\ell)$.

Considerem ara el subgrup $G_\ell^{1,\mathrm{zar}} \subseteq G_\ell^{\mathrm{zar}}$ imposant la condició $M^t \Omega M = \Omega$, amb $\Omega = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Aquesta condició ens està imposant una *forma simplèctica* en V_ℓ, una aplicació bilinear de mòduls no degenerada alternada, i ens assegura que $G_\ell^{1,\mathrm{zar}}$ és un $\mathbb{Q}_\ell$-subgrup algebraic contingut en el *grup simplèctic* $\mathrm{Sp}(2)$, que són les matrius 2×2 que satisfan aquesta condició. En aquesta dimensió, $\mathrm{Sp}(2) = \mathrm{SL}(2)$, de manera que podríem simplificar la restricció anterior demanant $\det M = 1$. En el proper capítol veurem que, degut a que la inclusió $\mathrm{Sp}(2n) \subset \mathrm{SL}(2n)$ és estricta $\forall n > 1$, en dimensions superiors és necessari expressar-la en termes d'una forma simplèctica.

Sigui $\iota : \mathbb{Q}_\ell \to \mathbb{C}$ un capbussament, i definim $G_{\ell,\iota}^{1,\mathrm{zar}}$ a partir de $G_\ell^{1,\mathrm{zar}}$ fent un canvi de base via ι. Aleshores tenim $G_{\ell,\iota}^{1,\mathrm{zar}}(\mathbb{C}) \subseteq \mathrm{SL}(2)$, que conté un subgrup maximal compacte únic llevat conjugació al que anomenem $H_{\ell,\iota}^{1,\mathrm{zar}}$.

Definició 4.11. El *grup de Sato–Tate de* E, $\mathrm{ST}(E) := H_{\ell,\iota}^{1,\mathrm{zar}} \subseteq \mathrm{SU}(2)$.

És molt important observar que hem aconseguit un grup, $\mathrm{ST}(E)$, que tot i que per construir-lo hem necessitat fer tries com ara el primer ℓ o el capbussament ι, depèn únicament de la corba E.

Per cada primer $\mathfrak{p}$ de bona reducció per E tal que $\mathfrak{p} \nmid \ell$, sigui $M_\mathfrak{p}$ la imatge de $\mathrm{Frob}_\mathfrak{p}$ per

$$\mathrm{Gal}(\overline{K}/K) \xrightarrow{\rho_\ell} G_\ell \hookrightarrow G_\ell^{\mathrm{zar}}(\mathbb{Q}_\ell) \hookrightarrow G_{\ell,\iota}^{\mathrm{zar}}(\mathbb{C}),$$

on l'última inclusió ve donada per ι. Prenem la classe $\overline{M_\mathfrak{p}} = {}^{M_\mathfrak{p}}\!/_{N(\mathfrak{p})^{1/2}}$, una matriu de traça $\frac{a_\mathfrak{p}}{N(\mathfrak{p})^{1/2}} \in [-2,2]$, determinant 1 i valors propis $e^{\pm i\theta_\mathfrak{p}}$. L'angle $\theta_\mathfrak{p}$ ens determina una única classe llevat conjugació en $\mathrm{ST}(E)$, és a dir, un element $x_\mathfrak{p} \in X := \mathrm{conj}(\mathrm{ST}(E))$.

En aquest context, la conjectura de Sato–Tate és equivalent a que $(x_\mathfrak{p})$ estigui equidistribuïda en X. O sigui, l'hem aconseguit enunciar sense tenir en compte si la corba té CM o no, l'única diferència és la mesura per la qual la successió és equidistribuïda. El proper teorema ens indica quin grup de Sato–Tate correspon a cada situació:

Teorema 4.12. *Sigui E una corba el·líptica sobre un cos de nombres $\Bbbk$. Llevat conjugació, tenim:*

$$\mathrm{ST}(E) = \begin{cases} \mathrm{U}(1) & \text{si } E \text{ té CM definida sobre } \Bbbk, \\ N(\mathrm{U}(1)) & \text{si } E \text{ té CM no definida sobre } \Bbbk, \\ \mathrm{SU}(2) & \text{si } E \text{ no té CM}, \end{cases}$$

on $\mathrm{U}(1) \subset \mathrm{SU}(2)$ *mitjançant el capbussament* $u \mapsto \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix}$.

Demostració. Si E té CM definida sobre $\Bbbk$, aleshores G_ℓ és abelià. Això és degut a que l'extensió $\Bbbk(E[\ell^\infty])$ és abeliana (veure [23]). Aquest resultat és com el conegut teorema de Kronecker–Weber, que diu que tota extensió abeliana de $\mathbb{Q}$ està continguda en alguna extensió ciclotòmica, però per a cossos quadràtics imaginaris.

Per tant, el grup G_ℓ està inclòs en un subgrup de Cartan (un subgrup maximal abelià) de $\mathrm{GL}(2,\mathbb{Q}_\ell)$, que en $G_{\ell,\iota}^{\mathrm{zar}}(\mathbb{C})$ és conjugat del grup de matrius diagonals. Aquest fet implica que el grup de Sato–Tate $\mathrm{ST}(E)$ és conjugat de $\mathrm{U}(1)$, el subgrup de matrius diagonals de $\mathrm{SU}(2)$.

Si E té CM no definida sobre $\Bbbk$, aleshores G_ℓ no està contingut en un subgrup de Cartan de $\mathrm{GL}(2,\mathbb{Q}_\ell)$, sinó en el normalitzador. En aquest cas, seguint el raonament anterior, $\mathrm{ST}(E)$ és conjugat del normalitzador $N(\mathrm{U}(1))$ de $\mathrm{U}(1)$ en $\mathrm{SU}(2)$.

Si E no té CM, pel teorema de la imatge oberta de Serre (veure [18] i [20]) tenim que G_ℓ és un subgrup d'índex finit de $\mathrm{GL}(2,\mathbb{Z}_\ell)$. Per tant, $G_\ell^{1,\mathrm{zar}} = \mathrm{SL}(2)$, que implica $\mathrm{ST}(E) = \mathrm{SU}(2)$. □

Capítol 5

Generalització per a varietats abelianes

Per acabar, veurem la conjectura de Sato–Tate per a varietats abelianes. És una generalització natural de tota la teoria presentada fins ara sobre corbes el·líptiques, ja que, en particular, una corba el·líptica és una varietat abeliana de dimensió 1. Finalment, igual que en el capítol anterior, definirem el grup de Sato–Tate d'una varietat abeliana i estudiarem el problema de classificació, que consisteix en trobar els grups que poden aparèixer com a grups de Sato–Tate d'una varietat abeliana.

5.1 Varietats abelianes

Definició 5.1. Una *varietat abeliana* sobre un cos $\Bbbk$ és una varietat algebraica completa A definida sobre $\Bbbk$ juntament amb un punt $\Bbbk$-racional $O \in A(\Bbbk)$ i els morfismes definits sobre $\Bbbk$

$$m : A \times A \longrightarrow A,$$

$$i : A \longrightarrow A,$$

que satisfan les propietats de grup.

La *completesa* en una varietat algebraica és una propietat anàloga a la compacitat en un espai topològic. Significa que per a tota subvarietat $B \subset A$, la projecció $\pi : A \times B \to B$ és una aplicació tancada. De la completesa es prova que la llei de grup és commutativa.

A continuació, estudiarem les varietats abelianes sobre $\mathbb{C}$. El conjunt $A(\mathbb{C})$ té estructura de grup de Lie complex, és una varietat complexa on les operacions de grup són holomorfes. De fet, és un grup de Lie connex compacte. Fent servir les propietats d'aquests grups podrem veure que la llei de grup efectivament és commutativa i que una varietat abeliana sobre $\mathbb{C}$ és un tor complex. Per veure-ho, recordem alguns conceptes sobre àlgebres de Lie i les definicions de reticle i tor complex.

Sigui T un grup de Lie complex amb neutre e. Sigui $V = \mathrm{Lie}(T)$ l'àlgebra de Lie associada a T, que és un espai vectorial de dimensió igual a la dimensió de T com a varietat.

Per a cada vector tangent $v \in V$ hi ha un únic morfisme $\lambda_v : \mathbb{C} \to T$ tal que $\lambda_v(0) = e$ i la seva derivada en zero compleix $(\frac{\partial}{\partial t})_0 \mapsto v$. Definim l'*aplicació exponencial*

$$\begin{aligned} \exp : V &\longrightarrow T \\ v &\longmapsto \lambda_v(1). \end{aligned}$$

Proposició 5.2. *Sigui T un grup de Lie complex connex compacte i considerem $V = \mathrm{Lie}(T)$. Aleshores,*

1. *la llei de grup sobre T és commutativa,*
2. *$\exp : V \to T$ és un morfisme de grups de Lie,*
3. *el morfisme* exp *és exhaustiu, i*
4. *$\ker(\exp)$ és un reticle del $\mathbb{C}$-espai vectorial V i T és un tor complex.*

Recordem que un *reticle* d'un $\mathbb{C}$-espai vectorial V de dimensió g és un subgrup $\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_{2g}$, on $e_1, \ldots, e_{2g} \in V$ són vectors $\mathbb{R}$-linealment independents.

Proposició 5.3. *Un subgrup Λ de V és un reticle de V si i només si Λ és discret i $T = {}^V\!/\!_\Lambda$ és compacte amb la topologia quocient.*

Definim les funcions holomorfes en aquest quocient, donant-li estructura de varietat complexa, de la següent manera: $f : U \to \mathbb{C}$ en $U \subseteq T$ obert és holomorfa si i només si $f \circ \pi$ és holomorfa sobre $\pi^{-1}(U)$, on $\pi : V \to T$ és la projecció canònica. El grup de Lie obtingut s'anomena *tor complex*.

De la proposició anterior es desprèn el que volíem veure:

Corol·lari 5.4. *Sigui A una varietat abeliana sobre $\mathbb{C}$. Aleshores A és un grup abelià i $A(\mathbb{C})$ és un tor complex.*

Una vegada vist que tota varietat abeliana és un tor complex, ens preguntem en quines condicions el recíproc és cert.

Definició 5.5. Una *forma hermítica sobre V* és una aplicació

$$H : V \times V \longrightarrow \mathbb{C}$$

$\mathbb{C}$-bilineal en la primera variable i tal que $H(z, w) = \overline{H(w, z)}$.

Definició 5.6. Una *forma de Riemann respecte un reticle Λ de V* és una forma hermítica $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ tal que $E(\Lambda \times \Lambda) \subset \mathbb{Z}$, on $E = \Im(H) : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$ és la part imaginària de H.

Teorema 5.7. *Un tor complex ${}^V\!/\!_\Lambda$ és una varietat abeliana si i només si existeix una forma de Riemann respecte Λ definida positiva.*

En el cas general, quan considerem una varietat abeliana A sobre un cos qualsevol $\Bbbk$, la condició necessària i suficient es tradueix a que A tingui una *polarització*, un morfisme de A al seu dual A^* exhaustiu i de nucli finit que satisfà una certa simetria.

El primer exemple que veurem de varietat abeliana és el de dimensió 1: les corbes el·líptiques. Considerem un tor complex ${}^{\mathbb{C}}\!/\!_\Lambda$, on $\Lambda = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$, i la *funció el·líptica de Weierstrass* definida com

$$\wp(z; \lambda_1, \lambda_2) := \frac{1}{z^2} + \sum_{(n_1, n_2) \neq (0,0)} \left(\frac{1}{(z + n_1\lambda_1 + n_2\lambda_2)^2} - \frac{1}{(n_1\lambda_1 + n_2\lambda_2)^2} \right).$$

L'aplicació $z \mapsto (1 : \wp(z;\lambda_1,\lambda_2) : \wp'(z;\lambda_1,\lambda_2))$ és una immersió holomorfa de $\mathbb{C}/\Lambda$ a $\mathbb{P}^2(\mathbb{C})$.

El teorema anterior ens assegura que en efecte és una varietat abeliana, ja que existeix una forma de Riemann natural sobre $\mathbb{C}$ respecte Λ, amb $\Im(\frac{\lambda_1}{\lambda_2}) > 0$,

$$H(z_1, z_2) = \frac{z_1 \overline{z}_2}{\lambda_1 \overline{\lambda}_2},$$

que es pot comprovar que és no degenerada.

L'exemple per excel·lència de varietat abeliana ve donat pel que s'anomena la *jacobiana* d'una corba. A una corba C de gènere g li podem associar una varietat abeliana de dimensió g, definida com el grup de classes de divisors de grau zero $\mathrm{Pic}^0(C)$. Per entendre els objectes que apareixen en la definició, cal introduir tot un seguit de conceptes que podem trobar explicats amb detall a [10].

Si C és una corba llisa projectiva sobre els complexos, podem construir la seva jacobiana d'una manera alternativa. En aquest cas, es pot veure que $C(\mathbb{C})$ és una superfície de Riemann compacte. Considerem l'espai vectorial de les 1-formes diferencials holomorfes, que denotem $H^0(C(\mathbb{C}), \Omega^1_C)$, de dimensió g. Aleshores, si $H_1(C(\mathbb{C}), \mathbb{Z})$ és el grup d'homologia singular, isomorf a $\mathbb{Z}^{2g}$, l'aplicació

$$\begin{aligned} H^0(C(\mathbb{C}), \Omega^1_C) \times H_1(C(\mathbb{C}), \mathbb{Z}) &\longrightarrow \mathbb{C} \\ (\omega, \sigma) &\longmapsto \int_\sigma \omega \end{aligned}$$

permet veure $H_1(C(\mathbb{C}), \mathbb{Z}) \cong \mathbb{Z}^{2g}$ com un reticle en el dual $H^0(C(\mathbb{C}), \Omega^1_C)^* \cong \mathbb{C}^g$. Definim la jacobiana de C com el quocient

$$\mathrm{Jac}(C) = {}^{H^0(C(\mathbb{C}), \Omega^1_C)^*}\!/_{H_1(C(\mathbb{C}), \mathbb{Z})},$$

i es pot provar que efectivament és una varietat abeliana.

5.2 La conjectura de Sato–Tate per a varietats abelianes

El nostre objectiu és enunciar una generalització de la conjectura de Sato–Tate per a varietats abelianes. El que farem és reproduir el que hem vist la secció 4.4 i definir el grup de Sato–Tate d'una varietat abeliana.

Sigui A una varietat abeliana sobre un cos $\Bbbk$ de dimensió g. Primer de tot, escollim un primer ℓ i definim el mòdul de Tate

$$T_\ell(A) := \varprojlim_n A[\ell^n],$$

que és un $\mathbb{Z}_\ell$-mòdul lliure de rang $2g$, i el mòdul de Tate racional

$$V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}} \mathbb{Q},$$

un $\mathbb{Q}_\ell$-espai vectorial de dimensió $2g$. A partir de la representació de Galois

$$\rho_\ell : \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \to \mathrm{Aut}(V_\ell(A)) \cong \mathrm{GL}(2g, \mathbb{Q}_\ell),$$

definim G_ℓ com la seva imatge. Prenem G_ℓ^{zar}, la clausura de Zariski de G_ℓ en $\mathrm{GL}(2g, \mathbb{Q}_\ell)$, i imposant la restricció simplèctica $M^t \Omega M = \Omega$ obtenim $G_\ell^{1,\mathrm{zar}}$, un $\mathbb{Q}_\ell$-subgrup algebraic de $\mathrm{Sp}(2g)$. Escollim un capbussament $\iota : \mathbb{Q}_\ell \to \mathbb{C}$ i definim $G_{\ell,\iota}^{1,\mathrm{zar}}$.

El *grup de Sato–Tate* $\mathrm{ST}(A) \subseteq \mathrm{USp}(2g) := \mathrm{Sp}(2g) \cap \mathrm{U}(2g)$ el definim com el subgrup compacte maximal de $G_{\ell,\iota}^{1,\mathrm{zar}}(\mathbb{C})$, que és únic llevat conjugació.

Per a cada primer de bona reducció $\mathfrak{p} \nmid \ell$, considerem la imatge de l'element de Frobenius $\mathrm{Frob}_\mathfrak{p}$ en $G_{\ell,\iota}^{1,\mathrm{zar}}$ i l'anomenem $M_\mathfrak{p}$. Definim $x_\mathfrak{p} \in \mathrm{conj}(\mathrm{ST}(A))$ com la classe de conjugació de $\overline{M_\mathfrak{p}} := N(\mathfrak{p})^{-1/2} M_\mathfrak{p}$ en $\mathrm{ST}(A)$. L'últim pas és vàlid per dos motius:

1. El grup $G_\ell \subset \mathrm{GL}(2g, \mathbb{Q}_\ell)$ en realitat està contingut en $\mathrm{GSp}(2g, \mathbb{Q}_\ell)$, anomenat *grup de similituds simplèctiques*, definit per la condició $\lambda M^t \Omega M = \Omega$, amb $\Omega = \begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix}$, on $\lambda \in \mathrm{GL}(1)$. Cal remarcar aquest pas ja que per a $g > 1$, la inclusió $\mathrm{GSp}(2g) \subseteq \mathrm{GL}(2g)$ és estricta.

2. $M_\mathfrak{p}$ és diagonalitzable. D'aquesta manera, $\overline{M}_\mathfrak{p}$ també, amb valors propis de valor absolut 1. En conseqüència, $\overline{M}_\mathfrak{p}$ pertany a un subgrup compacte de $G_{\ell,\iota}^{1,\mathrm{zar}}$, que per força serà conjugat d'un subgrup de $\mathrm{ST}(A)$.

Si el gènere és 1, aquesta construcció del grup de Sato–Tate és exactament la mateixa que havíem vist al final del capítol anterior.

Observem que per definir-nos el grup de Sato–Tate hem fet dues tries: el primer ℓ i el capbussament ι. Per a $g \leq 3$ està demostrat que $\mathrm{ST}(A)$ és independent dels ℓ i ι escollits, però és un problema obert en general.

Finalment, podem enunciar la conjectura de Sato–Tate per a varietats abelianes:

Conjectura 5.8. *Sigui A una varietat abeliana sobre un cos de nombres $\Bbbk$, i sigui $\mathrm{ST}(A)$ el seu grup de Sato–Tate. Sigui $(x_\mathfrak{p})$ la successió normalitzada de les classes de conjugació dels elements de Frobenius en $\mathrm{ST}(A)$ dels primers $\mathfrak{p}$ de bona reducció per A ordenats per norma. Aleshores $(x_\mathfrak{p})$ és equidistribuïda respecte la projecció de la mesura de Haar de $\mathrm{ST}(A)$ en $\mathrm{conj}(\mathrm{ST}(A))$.*

5.3 Sato–Tate en teoria de grups

L'objectiu d'aquesta part del capítol és el *problema de classificació del grup de Sato–Tate*: volem determinar quins grups poden ser grups de Sato–Tate per a alguna varietat abeliana A. Per fer-ho, primer ens definirem dos grups algebraics molt relacionats amb $\mathrm{ST}(A)$, el grup de Mumford–Tate i el grup de Hodge, i veurem un seguit de propietats que, sota unes circumstàncies específiques, determinen que un grup pugui ser el grup $\mathrm{ST}(A)$ per a alguna varietat abeliana A.

Per començar, sigui A una varietat abeliana sobre un cos $\Bbbk$, i sigui $\mathbb{C}^g/\Lambda \cong \mathbb{R}^{2g}/\Lambda$ el tor complex corresponent a $A(\mathbb{C})$. Considerem $\Lambda_\mathbb{R} := \Lambda \otimes_\mathbb{Z} \mathbb{R}$, un espai vectorial real de dimensió $2g$ amb *estructura complexa*, és a dir, un morfisme $h : \mathbb{C} \to \mathrm{End}(\Lambda_\mathbb{R})$, i $\Lambda_\mathbb{Q} := \Lambda \otimes_\mathbb{Z} \mathbb{Q}$.

Definició 5.9. El *grup de Mumford–Tate* d'una varietat abeliana A de dimensió g, $\mathrm{MT}(A)$, és el subgrup $\mathbb{Q}$-algebraic més petit G de $\mathrm{GL}(\Lambda_\mathbb{Q})$ pel qual $h(\mathbb{C}^\times) \subseteq G(\mathbb{R})$. El *grup de Hodge* de A, $\mathrm{Hg}(A)$, és la clausura de Zariski de $h(\mathrm{U}(1))$ a $\mathrm{GL}(\Lambda_\mathbb{R})$.

De fet, $\mathrm{Hg}(A) := \mathrm{MT}(A) \cap \mathrm{Sp}(2g)$. Si denotem per G^0 la *component identitat* d'un grup algebraic G, és a dir, la component connexa que conté l'element identitat de G, es pot comprovar el següent:

$$(G_\ell^{\mathrm{zar}})^0 \subseteq \mathrm{MT}(A) \otimes_\mathbb{Q} \mathbb{Q}_\ell, \text{ o equivalentment, } (G_\ell^{1,\mathrm{zar}})^0 \subseteq \mathrm{Hg}(A) \otimes_\mathbb{Q} \mathbb{Q}_\ell.$$

Per a dimensions $g \leq 3$, es coneix que les inclusions són en realitat igualtats (veure [1] i [13]), i de fet, s'espera que també ho siguin per a dimensions més altes:

Conjectura 5.10 (Mumford–Tate)**.** *La inclusió* $(G_\ell^{\mathrm{zar}})^0 \subseteq \mathrm{MT}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ *és una igualtat. Equivalentment, la inclusió* $(G_\ell^{1,\mathrm{zar}})^0 \subseteq \mathrm{Hg}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ *és una igualtat.*

En [21], Serre va descriure un seguit de propietats que, en cas de que la conjectura anterior fos certa, hauria de tenir un grup G per poder ser grup de Sato–Tate. S'anomenen els *axiomes de Sato–Tate*, i si els formulem per a varietats abelianes, són els següents:

(ST1) **Condició de Lie:** G és un subgrup tancat de $\mathrm{USp}(2g)$.

(ST2) **Condició de Hodge:** existeix un subgrup $H \subseteq G$, anomenat un *cercle de Hodge*, que és imatge d'un homomorfisme $\theta : \mathrm{U}(1) \to G^0$ tal que els elements $\theta(u)$ tenen valors propis u i u^{-1} amb multiplicitat g. A més, podem escollir H de manera que els conjugats de H generen un subgrup dens no trivial de G^0.

(ST3) **Condició de racionalitat:** per a cada component C de G i cada caràcter irreductible χ de $\mathrm{GL}(m, \mathbb{C})$, el valor $\int_C \chi\mu$ és enter, on μ és la mesura de Haar de G normalitzada ($\mu(\mathbb{1}_C) = 1$).

Podem treure algunes conclusions interessants d'aquests axiomes si requerim alguna restricció addicional:

1. G és un grup de Lie compacte, per (ST1).
2. G no pot ser un grup finit, ja que per (ST2) ha de contenir un subgrup isomorf a $\mathrm{U}(1)$.
3. Si G és connex, només cal comprovar (ST1) i (ST2) perquè (ST3) sempre se satisfà.
4. Per a dimensions $g > 1$, (ST3) és essencial, però per a $g = 1$ no aporta cap informació.

En general, tenim el següent resultat:

Teorema 5.11. *Llevat conjugació, el nombre de subgrups de* $\mathrm{USp}(2g)$ *que satisfan els axiomes de Sato–Tate és finit per a tota dimensió* $g \geq 1$*.*

Demostració. Veure [7, Remark 3.3]. □

El teorema anterior justifica l'estudi de la classificació de grups de Sato–Tate. Comentarem els casos pels quals es coneix que la conjectura de Mumford–Tate se satisfà: per a $g = 1$, el problema es redueix a l'estudi fet en la secció 4.4; per a $g = 2$, és força més complicat, però està resolt i en veurem sense entrar en detall el resultat; i per a $g = 3$ continua sent un problema obert.

Aleshores, en dimensió $g = 1$, la solució al problema de classificació ve donat pel següent teorema:

Teorema 5.12. *Per a* $g = 1$*, els grups* $\mathrm{U}(1), N(\mathrm{U}(1))$ *i* $\mathrm{SU}(2)$ *són els únics grups (llevat conjugació) que satisfan els axiomes de Sato–Tate.*

Demostració. Suposem que G és un grup de $\mathrm{USp}(2) = \mathrm{SU}(2)$ que satisfà els axiomes de Sato–Tate. Aleshores, G^0 conté un conjugat de $\mathrm{U}(1)$, que ha de ser un grup de Lie compacte connex, sota el capbussament $u \mapsto \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix}$.

Es pot veure que els únics grups de Lie compactes no trivials de $\mathrm{SU}(2)$ són el propi $\mathrm{SU}(2)$ i $\mathrm{U}(1)$. Aleshores, o bé $G^0 = \mathrm{SU}(2)$ i per tant $G = \mathrm{SU}(2)$, o bé G^0 és un conjugat de $\mathrm{U}(1)$. En el darrer cas, com que la component identitat d'un grup de Lie és un subgrup normal d'índex finit, G^0 ha de ser un subgrup normal de G, i $\mathrm{U}(1)$ té índex 2 en el seu normalitzador. Per tant, quan $G^0 = \mathrm{U}(1)$, els únics grups G possibles són $\mathrm{U}(1)$ i $N(\mathrm{U}(1))$. □

Observem que dels tres grups, $N(\mathrm{U}(1))$ i $\mathrm{SU}(2)$ apareixen com a grups de Sato–Tate d'una corba el·líptica sobre $\mathbb{Q}$.

Aquest teorema juntament amb el teorema 4.12 que diu que aquests tres grups són els únics que apareixen com a grup de Sato–Tate d'una corba el·líptica, donen lloc al corol·lari 5.13.

Corol·lari 5.13. *Per a $g = 1$, un grup G satisfà els axiomes de Sato–Tate si i només si és el grup de Sato–Tate d'una corba el·líptica sobre un cos de nombres.*

El resultat en dimensió $g = 2$, que per dificultat no demostrarem, és el següent:

Teorema 5.14. *Per a $g = 2$, existeixen 55 grups (llevat conjugació) que satisfan els axiomes de Sato–Tate en* $\mathrm{USp}(4)$*. Les components connexes possibles per a aquests grups són:*

$$\mathrm{U}(1), \mathrm{SU}(2), \mathrm{U}(1) \times \mathrm{U}(1), \mathrm{U}(1) \times \mathrm{SU}(2), \mathrm{SU}(2) \times \mathrm{SU}(2), \mathrm{USp}(4).$$

El nombre de grups (llevat conjugació) per a cada component connexa és 32, 10, 8, 2, 2, i 1 respectivament.

Demostració. Veure [7, Teorema 3.4]. □

L'anàleg al corol·lari 5.13 però, no es compleix: alguns dels grups que satisfan els axiomes de Sato–Tate no provenen d'una varietat abeliana. En concret, tenim:

Teorema 5.15. *Dels 55 grups del teorema 5.14, només 52 apareixen com a grups de Sato–Tate d'una superfície abeliana sobre un cos de nombres; d'aquests, 34 apareixen com a grups de Sato-Tate d'una superfície abeliana sobre $\mathbb{Q}$.*

Demostració. Veure [7, Teorema 1.5]. □

Tal com havíem comentat, el problema de classificació per a dimensió $g = 3$ continua obert. No obstant, se'n coneixen els casos connexos (veure [25, Taula 2]).

En resum, hem vist quins dels grups que satisfan els axiomes de Sato–Tate poden ser, per a una varietat abeliana A, el grup $\mathrm{ST}(A)$. Per acabar, és natural preguntar-nos l'altra implicació: si $G = \mathrm{ST}(A)$ és el grup de Sato–Tate d'una varietat abeliana A, compleix necessàriament els axiomes de Sato–Tate? S'espera que, en efecte, així sigui, i de fet, està demostrat quan la conjectura de Mumford–Tate se satisfà:

Proposició 5.16. *Sigui A una varietat abeliana de dimensió g sobre un cos de nombres per la qual la conjectura de Mumford–Tate és certa. Aleshores* $\mathrm{ST}(A)$ *satisfà els axiomes de Sato–Tate.*

Demostració. Veure [7, Proposició 3.2]. □

Bibliografia

[1] Grzegorz Banaszak, Kiran S. Kedlaya. *An algebraic Sato–Tate group and Sato–Tate conjecture.* Indiana University Mathematics Journal 64 (2015), 245–274.

[2] Christophe Breuil, Brian Conrad, Fred Diamond, Richard Taylor. *On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises.* Journal of the American Mathematical Society 14 (2001), 783-841.

[3] John W. S. Cassels. *Lectures on Elliptic Curves.* Cambridge University Press (1991).

[4] David A. Cox. *Primes of the form $x^2 + ny^2$.* John Wiley, 1989.

[5] Gerd Faltings. *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Inventiones Mathematicae 73 (1983), 349–350.

[6] Francesc Fité. *Equidistribution, L-functions, and Sato–Tate groups.* Contemporary Mathematics 649 (2015), 63–88.

[7] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, Andrew V. Sutherland. *Sato–Tate distributions and Galois endomorphism modules in genus 2.* Compositio Mathematica 148 (2012), 1390–1442.

[8] Marc Hindry, Marusia Rebolledo, David Roberts. *Variedades abelianas, una introducción.* Academia Nacional de Ciencias (AGRA III), 2018.

[9] Serge Lang. *Introduction to algebraic and abelian functions.* Springer-Verlag, 1982.

[10] James S. Milne. *Arithmetic Geometry*, chapter VII: *Jacobian Varieties.* Springer-Verlag, 1986.

[11] James S. Milne. *Elliptic curves.* BookSurge Publishing, 2006.

[12] James S. Milne. *Algebraic number theory.* 2014.

[13] Ben Moonen, Yuri G. Zarhin. *Hodge classes on abelian varieties of low dimension.* Mathematische Annalen 315 (1999), 711–733.

[14] Jürgen Neukirch. *Class Field Theory.* Springer-Verlag, 1977.

[15] Kenneth A. Ribet. *On modular representations of $(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms.* Inventiones Mathematicae 100 (1990), 431–476.

[16] Christophe Ritzenthaler. *Introduction to elliptic curves.* Université de Rennes I, 2013.

[17] Romyar Sharifi. *Algebraic number theory.* University of California.

[18] Jean-Pierre Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Inventiones Mathematicae 15 (1972), 259–331.

[19] Jean-Pierre Serre. *A course in arithmetic*. Springer-Verlag, 1973.

[20] Jean-Pierre Serre. *Abelian ℓ-adic representations and elliptic curves*. A.K. Peters, 1998.

[21] Jean-Pierre Serre. *Letters to Ken Ribet, 1/1/1981 and 29/1/1981*, Oeuvres – Collected Papers, volume IV. Springer, 2000.

[22] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, 1986.

[23] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, 1994.

[24] Joseph H. Silverman, John T. Tate. *Rational Points on Elliptic Curves*. Springer, 2015.

[25] Andrew V. Sutherland. *Sato–Tate distributions*. Southwest Center for Arithmetic Geometry, 2016.

[26] Yichao Tian. *Lectures on algebraic number theory*. Morningside Center of Mathematics, 2014.

[27] Andrew Wiles. *Modular elliptic curves and Fermat's last theorem*. Annals of Mathematics 141 (1995), 443–551.