TREBALL DE FI DE MÀSTER

Màster en Matemàtica Aplicada

Títol: No anul·lació de funcions L en valors crítics i resultats d'equidistribució en aritmètica

Autor: David Arazo Marin

Director: Victor Rotger Cerdà

Departament: Matemàtica Aplicada II

Convocatòria: Octubre/09

Facultat de Matemàtiques i Estadística

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Índex

Introducció

La teoria de nombres és una de les branques de la matemàtica que més s'ha desenvolupat en els darrers anys. El resultat més famós és segurament l'últim teorema de Fermat. Andrew Wiles va publicar l'any 1995 la demostració del teorema de la modularitat per algunes corbes el·líptiques el que va permetre, utilitzant el teorema de Ribet, demostrar l'últim teorema de Fermat.

Menys coneguda és la conjectura de Sato-Tate, resolta l'any 2006 per Richard Taylor, conjuntament amb altres matemàtics. A més els resultats presentats per Taylor generalitzaven, en cert sentit, el teorema de la modularitat.

Podem interpretar la conjectura de Sato-Tate com un teorema de distribució en l'aritmètica. Els teoremes de distribució en aritmètica es poden interpretar com de la següent manera. Associem a cada nombre primer p un valor x_p en un conjunt X i ens preguntem per la distribució en X dels valors x_p al fer variar p.

Per tal de presentar la conjectura de Sato-Tate és interessant presentar primer altres teoremes de distribució en aritmètica, el teorema de densitat de Dirichlet i la seva generalització com el teorema de Chebotarev. Presentarem i demostrarem aquests dos teoremes tot desenvolupant els conceptes bàsics de la teoria de nombres algebraica.

La conjectura de Sato-Tate és un resultat de distribució en aritmètica sobre corbes el·líptiques. Presentarem aquesta conjectura a partir de la teoria de Serre, la qual ens permet trobar un model comú pel teorema de Chebotarev i la conjectura de Sato-Tate. La demostració de la conjectura de Sato-Tate utilitza tècniques avançades en teoria de nombres, i queda fora de l'abast del treball. Tot i això descriurem un esquema de la demostració deixant de banda les definicions i resultats tècnics.

Utilitzant la teoria de Serre generalitzarem la conjectura de Sato-Tate a corbes de gènere arbitrari, obtenint la conjectura de Sato-Tate generalitzada. La conjectura generalitzada és encara un problema obert i no s'han obtinguts resultats teòrics importants.

A partir de càlculs numèrics es suggereix en [10] una classificació per solucionar la conjectura de Sato-Tate per corbes de gènere 2. Presentarem els resultats obtinguts en [10] i

posteriorment centrarem l'interès en l'estudi d'una corba D amb QM definida en [2]. Els resultats numèrics realitzats per la corba D, amb el suport d'Andrew Sutherland, ens permetran millorar la classificació proposada en [10]. Estudiant les corbes utilitzades en [10] i la corba D proposarem com podem obtenir una classificació més complerta.

Capítol 1

Teoremes de Dirichlet i Chebotarev

El primer objectiu del treball és presentar els teoremes de densitat de Dirichlet i de Chebotarev, tot donant-ne la demostració.

Per fer-ho, introduïm primer les definicions i resultats principals necessaris per poder desenvolupar la teoria, i demostrem el teorema dels nombres primers de Dirichlet. Aquest teorema es pot interpretar com el primer resultat bàsic d'equidistribució, i ens servirà d'esquema inicial. Els resultats exposats es poden consultar a [19].

1.1 Conceptes previs en aritmètica

Direm que un cos K és un cos de nombres si és una extensió finita, i per tant algebraica, de $\mathbb{Q}$. Sigui K un cos de nombres. Definim els enters de K com els elements de K que són arrel d'algun polinomi mònic amb quoficients a $\mathbb{Z}$. El conjunt de tots els enters de K formen un subanell de K, que definim com l'anell d'enters de K i denotem $\mathcal{O}_K$.

Les propietats principals de $\mathcal{O}_K$ es dedueixen a partir del conjunt dels seus ideals. El següent teorema és un dels teoremes centrals ([19, C. 1, Teorema 3.3]).

Teorema 1.1.1. *Sigui K un cos de nombres. Per a tot ideal propi no trivial $\mathfrak{a}$ de $\mathcal{O}_K$ existeix una factorització*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

en ideals primers de $\mathcal{O}_K$, que és única llevat de l'ordre dels factors.

Aquest teorema pot interpretar-se com una forma de factorització única. El conjunt d'ideals de $\mathcal{O}_K$ no té però estructura de grup. Per dotar-lo d'aquesta estructura, ampliem aquest concepte tot definint els *ideals fraccionaris* de K com els $\mathcal{O}_K$-submòduls de K finitament

generats. Equivalentment, $\mathfrak{a}$ és un ideal fraccionari si existeix un element $c \in \mathcal{O}_K$ tal que $c\mathfrak{a} \subseteq \mathcal{O}_K$ és un ideal de $\mathcal{O}_K$.

Definim J_K com el conjunt d'ideals fraccionaris de K. Sovint cometrem un abús de llenguatge i ens referirem als ideals fraccionaris de K simplement com ideals de K. Quan així ho fem, els ideals de $\mathcal{O}_K$ els anomenarem *ideals enters* de K.

D'aquesta manera, obtenim que el conjunt J_K té una estructura natural de grup abelià, on l'invers d'un ideal $\mathfrak{a}$ es defineix com

$$\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \in \mathcal{O}\}.$$

Sigui P_K el subgrup de J_K format pels ideals fraccionaris principals de K, és a dir, els ideals de la forma $(a) = a\mathcal{O}_\mathcal{K}$ on $a \in K^*$. El grup quocient

$$Cl_K = J_K/P_K$$

s'anomena el *grup de classes d'ideals de* K.

Teorema 1.1.2. *[19, C. 1, Teorema 6.3] El grup Cl_K de classes d'ideals d'un cos de nombres K és finit.*

Per tant té sentit definir h_K, el nombre de classes d'ideals de K, com el cardinal de Cl_K.

Definim la norma d'un ideal $\mathfrak{a}$ de $\mathcal{O}_K$ com $\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$, el qual és sempre finit si $\mathfrak{a}$ és un ideal no nul. Per a ideals principals obtenim que $\mathfrak{N}((a)) = |N_{K|\mathbb{Q}}(a)|$. A més es compleix la propietat

$$\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b}).$$

Sigui $L|K$ una extensió finita de grau n. Prenem $\mathfrak{P}$ un ideal primer de $\mathcal{O}_L$. Llavors $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ és un ideal primer de $\mathcal{O}_K$ i direm que $\mathfrak{P}$ està sobre de l'ideal $\mathfrak{p}$ o que $\mathfrak{P}$ divideix a $\mathfrak{p}$, i ho denotarem $\mathfrak{P}|\mathfrak{p}$.

Definim el cos residual de $\mathfrak{p}$ com

$$\kappa(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}.$$

Així, el cos residual de $\mathfrak{P}$ és $\kappa(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$ i $\kappa(\mathfrak{P})$ és un extensió finita de grau f, per algun $f \geq 1$, del cos $\kappa(\mathfrak{p})$. Segons aquestes definicions, obtenim que $\#\kappa(\mathfrak{p}) = \mathfrak{N}(\mathfrak{p})$ i per tant $\mathfrak{N}(\mathfrak{P}) = \mathfrak{N}(\mathfrak{p})^f$.

Per el Teorema 1.1.1 de factorització única anterior, tenim que tot ideal primer $\mathfrak{p}$ de K

descomposa de manera única com

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

on cada $\mathfrak{P}_i$ és un ideal primer de L, coprimer amb la resta de $\mathfrak{P}_j$.

Definició 1.1.3. *L'exponent e_i s'anomena l'*índex de ramificació de $\mathfrak{P}_i$ *i el grau f_i de l'extensió de cossos $\kappa(\mathfrak{P}_i)|\kappa(\mathfrak{p})$ s'anomena* el grau d'inèrcia de $\mathfrak{P}_i$.

Es compleix la següent igualtat fonamental.

Proposició 1.1.4. *[19, C. 1, Prop. 8.2] Sigui $L|K$ una extensió finita de grau n. Mantenint les notacions anteriors, per a tot primer $\mathfrak{p}$ de K es compleix*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Definició 1.1.5. *Sigui $\mathfrak{p}$ un primer de K i sigui L/K una extensió finita de grau n.*

- *Si $r = n$, i per tant $e_i = f_i = 1$, direm que $\mathfrak{p}$ descomposa totalment.*
- *Si $r = 1$, i per tant només hi ha un ideal $\mathfrak{P}$ sobre $\mathfrak{p}$, direm que $\mathfrak{p}$ no descomposa o que és inert.*
- *Direm que $\mathfrak{P}_i$ és no ramificat sobre K si $e_i = 1$. En cas contrari direm que és ramificat, i totalment ramificat si $f_i = 1$. Direm que l'ideal $\mathfrak{p}$ és no ramificat si tots els $\mathfrak{P}_i$ sobre $\mathfrak{p}$ són no ramificats. En cas contrari direm que $\mathfrak{p}$ és ramificat.*

Per la Proposició 8.4 del capítol 1 de [19], sabem que només hi ha un nombre finit de primers de K ramificats en L.

1.1.1 Extensions de Galois

Suposem ara que l'extensió $L|K$ és de Galois.

Definició 1.1.6. *La norma i la traça d'un element $x \in L$ són*

$$N_{L|K}(x) = \prod_{\sigma \in G} \sigma x \quad , \quad Tr_{L|K}(x) = \sum_{\sigma \in G} \sigma x.$$

Sigui $\mathfrak{p}$ un primer de K. El grup de Galois $G = Gal(L|K)$ actua transitivament en el conjunt de primers de L que divideixen $\mathfrak{p}$ (cf. [19, C. 1, Teorema 9.1]).

Per tant, fixat un primer $\mathfrak{P}|\mathfrak{p}$ de L, tots els primers sobre $\mathfrak{p}$ són de la forma $\sigma\mathfrak{P}$. Els primers $\sigma\mathfrak{P}$ s'anomenen els *primers conjugats de* $\mathfrak{P}$. Sota aquestes hipòtesis obtenim doncs

que l'índex de ramificació i el grau d'inèrcia és igual per a tots els primers conjugats i per tant depenen només de $\mathfrak{p}$.

Per tant la igualtat fonamental anterior s'escriu com

$$ref = n$$

on $e = e_i$ i $f = f_i$, per a tot i.

Veiem com actua el grup de Galois sobre els primers de L.

Definició 1.1.7. *Sigui $\mathfrak{P}$ un primer de L. El grup de descomposició de $\mathfrak{P}$ sobre K és el subgrup de G*

$$G_{\mathfrak{P}} = \{\sigma \in G | \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Observem que $G_{\mathfrak{P}}$ no és en general un subgrup normal de G perquè

$$G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}.$$

Si σ recorre les classes laterals de $G/G_{\mathfrak{P}}$, aleshores el conjunt de primers $\{\sigma\mathfrak{P}\}_\sigma$ és el conjunt de primers de L que divideixen $\mathfrak{p}$. És a dir, es compleix $r = (G : G_{\mathfrak{P}})$ i podem escriure la descomposició de $\mathfrak{p}$ com

$$\mathfrak{p} = \prod_{\sigma \in G/G_{\mathfrak{P}}} \sigma\mathfrak{P}^e.$$

Per tant, que $\mathfrak{p}$ descomposi totalment o bé sigui inert, són propietats de l'ideal que es poden llegir en l'índex $(G : G_{\mathfrak{P}})$.

Donat $\sigma \in G_{\mathfrak{p}}$, podem introduir de manera natural l'endomorfisme

$$\begin{array}{rccc} \bar{\sigma}: & \mathcal{O}/\mathfrak{P} & \longrightarrow & \mathcal{O}/\mathfrak{P} \\ & a \bmod \mathfrak{P} & \mapsto & \sigma a \bmod \mathfrak{P} \end{array}$$

Aquesta definició ens permet construir el homomorfisme

$$\begin{array}{rccc} \pi_{\mathfrak{P}}: & G_{\mathfrak{P}} & \longrightarrow & G\left(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})\right) \\ & \sigma & \mapsto & \bar{\sigma} \end{array}$$

Segons [19, C.1, Teorema 9.4], aquesta aplicació és exhaustiva.

Definició 1.1.8. *El grup d'inèrcia $I_{\mathfrak{P}}$ de $\mathfrak{P}$ sobre K és el nucli de $\pi_{\mathfrak{P}}$.*

Per tant $G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong G\left(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})\right)$ i obtenim la successió exacta

$$1 \to I_{\mathfrak{P}} \to G_{\mathfrak{P}} \to G\left(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})\right) \to 1.$$

Segons aquestes definicions, es compleix que $\#I_{\mathfrak{P}} = e$ i $(G_{\mathfrak{P}} : I_{\mathfrak{P}}) = f$.

Per tant, si el primer $\mathfrak{p}$ no és ramificat, $\pi_{\mathfrak{P}}$ indueix un isomorfisme

$$G_{\mathfrak{P}} \simeq G\left(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})\right).$$

El grup $G\left(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})\right)$ és cíclic d'ordre f, generat per l'automorfisme de Frobenius.

Segons l'isomorfisme anterior, podem trobar una única antiimatge $\varphi_{\mathfrak{P}}$ en $G_{\mathfrak{P}}$.

Anomenarem a $\varphi_{\mathfrak{P}}$ el símbol d'Artin o *l'automorfisme de Frobenius de* $\mathfrak{P}$. El denotarem per $\left(\frac{L|K}{\mathfrak{P}}\right)$. Observem que $\left(\frac{L|K}{\mathfrak{P}}\right)$ està caracteritzat com l'únic element $\varphi_{\mathfrak{P}} \in G$ que compleix

$$\varphi_{\mathfrak{P}}(a) \equiv a^{\mathfrak{N}(\mathfrak{p})} \mod \mathfrak{P} \quad \forall a \in \mathcal{O}_L.$$

1.2 Teorema dels nombres primers de Dirichlet

Comencem demostrant el teorema dels nombres primers de Dirichlet, que ens serveix com una primera aproximació als teoremes de densitat posteriors.

Teorema 1.2.1 (Teorema dels nombres primers de Dirichlet)**.** *Siguin a i m dos nombres enters amb $(a, m) = 1$. Llavors existeixen infinits primers p tals que $p \equiv a \mod m$.*

En altres paraules, la classe de a mòdul m conté infinits primers.

La demostració es fonamenta en la teoria de funcions Zeta i L-sèries, que es pot consultar a [19], i introduïm breument a continuació.

Sigui χ un caràcter de Dirichlet mòdul m, és a dir, un homomorfisme

$$\chi : (\mathbb{Z}/m\mathbb{Z})^* \to S^1.$$

Estenem el caràcter χ al grup additiu dels nombres enters $\mathbb{Z}$, tot definint $\chi(n) = \chi(n \mod m)$ si $(n, m) = 1$ i $\chi(n) = 0$ altrament. Quan escrivim χ entendrem que ens referim indistintament, tot cometent un abús de llenguatge, al caràcter de $(\mathbb{Z}/m\mathbb{Z})^*$ o al caràcter de $\mathbb{Z}$.

El caràcter definit per $\chi(\mathbb{Z}/m\mathbb{Z}) = 1$ s'anomena el *caràcter trivial mòdul* m, i el denotarem χ_0 sempre i quan el mòdul m sigui clar en el context.

Definició 1.2.2. *La L-sèrie de Dirichlet associada a un caràcter de Dirichlet* χ *és*

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}},$$

on s *pren valors complexes i el productori és respecte tots els primers* p*.*

Per $\Re(s) > 1$, la sèrie anterior és convergent i defineix una funció holomorfa en aquest domini (cf. [19, C.7, Teorema 1.1].

Segons la notació anterior, prenent $m = 1$, l'únic caràcter mòdul m és el caràcter trivial de $\mathbb{Z}$. En aquest cas, la L-sèrie corresponent és de fet la funció zeta de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}.$$

Presentem a continuació el principi de Mellin. Es tracta d'un procediment clàssic, emprat per estendre la funció zeta de Riemann a una funció meromorfa en tot el pla complex, i que també ens permet estendre altres sèries L, com ara les associades a caràcters de Dirichlet.

A més, aquest resultat també permet calcular els pols de la funció meromorfa resultant.

Considerem una funció contínua $f : \mathbb{R}^+ \to \mathbb{C}$, on $\mathbb{R}^+$ denota el grup multiplicatiu dels nombres reals positius.

Definició 1.2.3. *Definim la transformada de Mellin de* f *com*

$$L(f; s) = \int_0^{\infty} (f(y) - f(\infty))y^s \frac{dy}{y}$$

en cas que $f(\infty) = \lim_{y\to\infty} f(y)$ *i la integral existeixin.*

Teorema 1.2.4 (Principi de Mellin)**.** *Siguin* $f, g : \mathbb{R}^+ \to \mathbb{C}$ *funcions contínues tal que*

$$f(y) = a_0 + O(e^{-cy^\alpha}), \qquad f(y) = b_0 + O(e^{-cy^\alpha}),$$

per $y \to \infty$*, amb* c *i* α *constants positives. Suposem que es compleix*

$$f\left(\frac{1}{y}\right) = Cy^k g(y),$$

per algun real positiu k *i un nombre complex* C*. Llavors es compleix:*

(i) *Les transformades de Mellin* $L(f; s)$ *i* $L(g; s)$ *defineixen funcions holomorfes per* $\Re(s) > k$*.*

A més es poden estendre a funcions holomorfes a $\mathbb{C} \setminus \{0, k\}$.

(ii) *Les transformades de Mellin poden tenir pols simples en* $s = 0$ *i* $s = k$. *Els residus en aquests punts es poden calcular com*

$$\begin{aligned} \operatorname*{Res}_{s=0} L(f;s) &= -a_0, \quad \operatorname*{Res}_{s=k} L(f;s) = Cb_0, \\ \operatorname*{Res}_{s=0} L(g;s) &= -b_0, \quad \operatorname*{Res}_{s=k} L(g;s) = C^{-1}a_0. \end{aligned}$$

Cal remarcar que si el residu en un d'aquests punts és zero llavors la funció és holomorfa en aquest punt.

(iii) *Es satisfà l'equació funcional*

$$L(f;s) = CL(g;k-s)$$

Podem consultar la demostració d'aquest teorema a [19, C. 7].

El teorema 1.2.4 es pot aplicar a les L-sèries de Dirichlet. Per fer-ho, caldria introduir la teoria de funcions theta, que no introduirem en aquest treball per motius d'espai.

Per als nostres objectius, basta comentar aquí que les L-sèries associades a caràcters de Dirichlet es poden expressar com la transformada de Mellin de funcions theta, fet que permet obtenir la seva prolongació al pla complex.

Més precisament, obtenim que les L-sèries associades a un caràcter de Dirichlet no trivial de mòdul $m > 1$ estenen a funcions enteres en tot el pla complex $\mathbb{C}$.

Pel que fa als caràcters trivials, s'obté que les funcions L associades tenen un únic pol simple en $s = 1$, com és el cas per exemple de la funció zeta de Riemann.

El següent resultat, aparentment intranscendent, és el resultat que ens cal per demostrar el Teorema dels nombres primers de Dirichlet.

Proposició 1.2.5. *Per tot caràcter de Dirichlet no trivial* χ *es compleix*

$$L(\chi, 1) \neq 0.$$

Per a demostrar aquest resultat ens cal la següent definició.

Definició 1.2.6. *Sigui* K *un cos de nombres. La L-sèrie de Dedekind de* K *és*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}},$$

on el sumatori varia sobre els ideals enters no trivials de K, *i el productori es realitza sobre els ideals primers de* K.

Utilitzant el principi de Mellin 1.2.4, s'obté de nou que la funció $\zeta_K(s)$ admet una continuació meromorfa a tot el pla complex amb un únic pol simple en $s = 1$. Observem que la funció zeta de Riemann es recupera de nou com la funció zeta de Dedekind de $\mathbb{Q}$.

Segons aquestes definicions, es compleix la següent igualtat entre L-sèries.

Proposició 1.2.7. *Sigui $K = \mathbb{Q}(\mu_m)$ on μ_m és una arrel m-èssima primitiva de la unitat. Llavors*

$$\zeta_K(s) = G(s) \prod_{\chi} L(\chi, s)$$

on el productori és respecte els caràcters de Dirichlet mòdul m i $G(s) = \prod_{\mathfrak{p}|m} (1 - \mathfrak{N}(\mathfrak{p})^{-s})^{-1}$ on $\mathfrak{p}|m$ indica el productori respecte els primers en la factorització de $m\mathcal{O}_K$.

Demostració. Per demostrar aquesta igualtat utilitzem els resultats sobre factorització de primers en cossos ciclotòmics. Fixem un primer p. Descomposem l'ideal (p) com $p = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ i considerem f el grau d'inèrcia de $\mathfrak{p}_i$, és a dir, $\mathfrak{N}(\mathfrak{p}_i) = p^f$. Llavors pels primers sobre p la funció $\zeta_K(s)$ conté els factors

$$\prod_{\mathfrak{p}|p} (1 - \mathfrak{N}(\mathfrak{p})^{-s})^{-1} = (1 - p^{fs})^{-r}.$$

Per altra banda, els factor del productori de les L-sèries de Dirichlet és $\prod_{\chi}(1-\chi(p)p^{-s})^{-1}$. Si $p|m$ llavors $\chi(p) = 0$ i el factor de $\zeta_K(s)$ és un factor de $G(s)$. Suposem doncs $p \nmid m$. Podem comprovar que $\chi(p)$ és una arrel f-èssima de la unitat i que per cada arrel f-èssima $\zeta \in \mu_f$ existeixen r caràcters de Dirichlet mòdul m tal que $\chi(p) = \zeta$. Per tant

$$\prod_{\chi} (1 - \chi(p)p^{-s})^{-1} = \prod_{\zeta \in \mu_f} (1 - \zeta p^{-s})^{-r} = (1 - p^{fs})^{-r}.$$

Fent el productori sobre tots els primers p obtenim la fórmula enunciada. □

Veiem com demostrar la proposició 1.2.5.

Demostració. (Proposició 1.2.5) Clarament $G(s)$ no té cap pol en $s = 1$. A més, de la relació $L(\chi^0, s) = \prod_{p|m}(1 - p^{-s})\zeta(s)$ deduïm que $L(\chi^0, s)$ també té un pol simple a $s = 1$ ja que $\zeta(s)$ en té. Recordem que $\zeta(s)$ i $\zeta_K(s)$ tenen un pol simple a $s = 1$ i que $L(\chi, s)$ són funcions holomorfes en $s = 1$. Per tant, a causa de la proposició 1.2.7, s'ha de complir que $L(\chi, 1) \neq 0$ per tots els caràcters no trivials χ, com volíem veure. □

Aquest resultat, purament analític, és la clau per a demostrar el teorema dels nombres primers de Dirichlet.

Demostració. (Teorema 1.2.1 dels nombres primers de Dirichlet)

Considerem χ un caràcter de Dirichlet mòdul m. Per a $\Re(s) > 1$ podem calcular el logaritme de $L(\chi, s)$ com

$$\log L(\chi, s) = -\sum_p \log(1 - \chi(p)p^{-s}) = \sum_p \sum_{m=1}^{\infty} \frac{\chi(p^m)}{mp^{ms}} = \sum_p \frac{\chi(p)}{p^s} + g_\chi(s)$$

on $g_\chi(s) = \sum_p \sum_{m=2}^{\infty} \frac{\chi(p^m)}{mp^{ms}}$ és holomorfa per $\Re(s) > 1/2$.

Multiplicant per $\chi(a^{-1})$ i sumant per tots els caràcters mòdul m obtenim

$$\sum_\chi \chi(a^{-1}) \log L(\chi, s) = \sum_\chi \sum_p \frac{\chi(a^{-1}p)}{p^s} + g(s) =$$

$$= \sum_{b=1}^{m} \sum_\chi \chi(a^{-1}b) \sum_{p \equiv b(m)} \frac{1}{p^s} + g(s) = \sum_{p \equiv a(m)} \frac{\varphi(m)}{p^s} + g(s)$$

i $g(s) = \sum_\chi \chi(a^{-1}) g_\chi(s)$ és holomorfa per $\Re(s) > 1/2$ ja que totes les $g_\chi(s)$ ho eren. També hem utilitzat que

$$\sum_\chi \chi(a^{-1}b) = \begin{cases} 0 & \text{si } a \not\equiv b \mod p \\ \varphi(m) & \text{si } a \equiv b \mod p \end{cases}$$

Tal i com hem vist a la proposició 1.2.5, $L(\chi, 1) \neq 0$ si $\chi \neq \chi^0$ i per tant $\log L(\chi, 1)$ està fitat per $\chi \neq \chi^0$. Per a χ^0, $\log L(\chi^0, s)$ és no acotat quan $s \to 1$. Per tant, $\sum_\chi \chi(a^{-1}) \log L(\chi, s)$ també és no acotat quan $s \to 1$ i com que $g(s)$ és holomorfa en $s = 1$ obtenim que el sumatori sobre $p \equiv a(m)$ ha de tenir infinits termes. Per tant hi ha infinits primers p complint $p \equiv a(m)$. □

1.3 Teorema de densitat de Dirichlet

El teorema presentat dona una idea de la distribució dels nombres primers mòdul un nombre m. Ens interessa, però, conèixer quina és la distribució dels nombres primers respecte cada classe de congruència mòdul m. És a dir, volem saber quina és la probabilitat que, fixats a i m amb $(a, m) = 1$, un primer p compleixi $p \equiv a \mod m$.

Per fer aquest càlcul necessitem introduir alguns conceptes. Cal observar que el procediment següent manté l'esquema anterior. Comencem definint la densitat de Dirichlet, la qual correspondrà a la probabilitat anterior.

Definició 1.3.1. *Sigui K un cos de nombres. Sigui M un conjunt d'ideals primers de K. La*

densitat de Dirichlet de M és

$$d(M) = \lim_{s\to 1} \frac{\sum_{\mathfrak{p}\in M} \mathfrak{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{-s}},$$

sempre i quan el límit existeixi.

Veiem una manera equivalent de definir aquest límit. Introduïm la següent notació per simplificar el llenguatge. Donades dues funcions meromorfes f i g escriurem $f \sim g$ si $f(s)-g(s)$ és analítica en $s = 1$.

Utilitzant l'expressió

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

obtenim

$$\log \zeta_K(s) = \sum_{\mathfrak{p}} \sum_{m\geq 1} \frac{1}{m\mathfrak{N}(\mathfrak{p})^{ms}} = \sum_{\mathfrak{p}} \frac{1}{\mathfrak{N}(\mathfrak{p})^{s}} + \sum_{\mathfrak{p}} \sum_{m>1} \frac{1}{m\mathfrak{N}(\mathfrak{p})^{ms}}.$$

Podem comprovar que la segona suma defineix una funció analítica en $s = 1$. I de la mateixa manera també podem veure que la funció $\sum_{\deg(\mathfrak{p})>1} \mathfrak{N}(\mathfrak{p})^{-s}$, on la suma varia sobre tots els primers amb grau d'inèrcia sobre $\mathbb{Q}$ superior a 1, també defineix una funció analítica en $s = 1$.

Per tant, segons la notació anterior

$$\log \zeta_K(s) \sim \sum_{\mathfrak{p}} \frac{1}{\mathfrak{N}(\mathfrak{p})^{s}} \sim \sum_{\deg(\mathfrak{p})=1} \frac{1}{\mathfrak{N}(\mathfrak{p})^{s}}.$$

Per altra banda, $\zeta_K(s)$ té un pol simple a $s = 1$. Si R és el residu de $\zeta_K(s)$ en $s = 1$ llavors

$$\zeta_K(s) \sim \frac{R}{1-s}.$$

Manipulant l'expressió anterior

$$\log \zeta_K(s) \sim \log \frac{1}{1-s}$$

i per tant

$$\sum_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{-s} \sim \log \frac{1}{1-s}.$$

En conclusió veiem que

$$d(M) = \lim_{s\to 1} \frac{\sum_{\mathfrak{p}\in M} \mathfrak{N}(\mathfrak{p})^{-s}}{\log \frac{1}{1-s}}.$$

Cal observar que segons el resultat obtingut, la densitat de Dirichlet de M no depèn dels primers de M amb grau d'inèrcia sobre $\mathbb{Q}$ superior a 1.

Hem d'interpretar la densitat de Dirichlet com la probabilitat que un ideal de K pertanyi a M, tot i que aquesta probabilitat correspon a la densitat natural $\delta(M)$.

Definició 1.3.2. *Sigui K un cos de nombres. Sigui M un conjunt d'ideals primers de K. La densitat natural de M és*

$$\delta(M) = \lim_{x\to\infty} \frac{\{\#\mathfrak{p} \in M | \mathfrak{N}(\mathfrak{p}) \leq x\}}{\{\#\mathfrak{p} | \mathfrak{N}(\mathfrak{p}) \leq x\}}.$$

sempre i quan el límit existeixi.

Llavors

Proposició 1.3.3. *L'existència de $\delta(M)$ implica l'existència de $d(M)$ i a més $\delta(M) = d(M)$.*

El recíproc però no és cert en general: es pot comprovar que per alguns conjunts M existeix $d(M)$ però no $\delta(M)$. Per exemple, el conjunt dels primers amb primer dígit en expressió decimal igual a 1 no té densitat natural, però té densitat de Dirichlet igual a $\log_{10} 2$. Per a més informació, es pot consultar [22].

Per presentar el teorema de densitat de Dirichlet, ens calen algunes definicions pròpies de la teoria de classes de cossos. Sigui $\mathfrak{m}$ un ideal enter de K.

Definim $J_K^{\mathfrak{m}}$ com el grup d'ideals fraccionaris coprimers amb $\mathfrak{m}$, i $P_K^{\mathfrak{m}}$ el subgrups d'ideals principals (a) que compleixen $a \equiv 1 \mod \mathfrak{m}$ i a totalment positiu.

Aquí, la congruència anterior cal interpretar-la de la següent manera. Si escrivim $a = b/c$, amb b i c en $\mathcal{O}_K$, llavors $a \equiv 1 \mod \mathfrak{m}$ equival a dir que $b \equiv c \mod \mathfrak{m}$.

D'altra banda, diem que a és totalment positiu si per tota immersió $\sigma : K \hookrightarrow \mathbb{R}$ es compleix $\sigma(a) > 0$.

Teorema 1.3.4 (Teorema de densitat de Dirichlet)**.** *Sigui $H_K^{\mathfrak{m}}$ un subgrup de $J_K^{\mathfrak{m}}$ que conté $P_K^{\mathfrak{m}}$ amb índex finit $h_m = (J_K^{\mathfrak{m}} : H_K^{\mathfrak{m}})$. Sigui $\mathfrak{K}$ una classe de $J_K^{\mathfrak{m}}/H_K^{\mathfrak{m}}$ i $P(\mathfrak{K})$ el conjunt dels primers de K pertanyents a $\mathfrak{K}$. Llavors la densitat de Dirichlet de $P(\mathfrak{K})$ es pot calcular com*

$$d(P(\mathfrak{K})) = \frac{1}{h_{\mathfrak{m}}}.$$

Observem que és suficient demostrar el teorema per a $H_K^{\mathfrak{m}} = P_K^{\mathfrak{m}}$. En efecte, les classes de $J_K^{\mathfrak{m}}/H_K^{\mathfrak{m}}$ consisteixen en unions de classes de $J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$, és a dir, la classe $\mathfrak{K} \in J_K^{\mathfrak{m}}/H_K^{\mathfrak{m}}$ correspon a la unió de les classes $k_1, \ldots, k_r$ de $J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$ on $r = (H_K^{\mathfrak{m}} : P_K^{\mathfrak{m}})$. Denotem per $P(k_i)$ el conjunt dels primers de K pertanyents a k_i. Llavors

$$d(P(\mathfrak{K})) = d\left(P(k_1) \cup \overset{r}{\ldots} \cup P(k_r)\right) = d(P(k_1)) + \overset{r}{\ldots} + d(P(k_r)) =$$
$$= \frac{r}{(J_K^{\mathfrak{m}} : P_K^{\mathfrak{m}})} = \frac{(H_K^{\mathfrak{m}} : P^{\mathfrak{m}})}{(J_K^{\mathfrak{m}} : P_K^{\mathfrak{m}})} = \frac{1}{(J_K^{\mathfrak{m}} : H_K^{\mathfrak{m}})} = h_m.$$

Suposem doncs $H_K^{\mathfrak{m}} = P_K^{\mathfrak{m}}$. Per demostrar el teorema anterior ens basem en l'esquema de la demostració del Teorema 1.2.1 dels nombres primers de Dirichlet. En aquell teorema volíem demostrar que els nombres primers satisfan una certa distribució en el grup $(\mathbb{Z}/m\mathbb{Z})^*$. Per a la demostració consideràvem el cos de les arrels m-èssimes de la unitat, ja que el seu grup de Galois és precisament $(\mathbb{Z}/m\mathbb{Z})^*$. I a partir de la igualtat

$$\zeta_K(s) = G(s) \prod_{\chi \neq \chi^0} L(\chi, s)\zeta(s)$$

deduíem que $L(\chi, 1) \neq 0$ per els caràcters no trivials.

Per a seguir aquest mateix esquema ens cal trobar una extensió de cossos $L|K$ de manera que

$$G(L|K) \cong J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}.$$

La teoria de classes de cossos resol aquesta qüestió i ens permet considerar una extensió abeliana $L|K$ amb la propietat anterior. A més, l'isomorfisme ve donat pel símbol d'Artin. Podem consultar els resultats sobre la teoria de classes de cossos a [19].

De manera natural, podem considerar ara els caràcters $\widetilde{\chi}$ de $J^{\mathfrak{m}}$ induïts pels caràcters χ de $G(L|K)$.

Cal comentar que de fet $\widetilde{\chi}$ és un Größencharakter mòdul m, és a dir, un caràcter del grup de classes d'idèles (tot i que no ens estendrem en detalls sobre aquesta teoria, els resultats sobre Größencharakter poden consultar-se a [19]).

Definició 1.3.5. *La L-sèrie de Hecke associada al caràcter $\widetilde{\chi}$ és*

$$L(\widetilde{\chi}, s) = \sum_{\mathfrak{a}} \frac{\widetilde{\chi}(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \widetilde{\chi}(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}}$$

on el sumatori recorre tots els ideals enters no trivials de K i el productori es restringeix als ideals primers. Aquí, $\widetilde{\chi}(\mathfrak{a}) = 0$ si $(\mathfrak{m}, \mathfrak{a}) \neq 1$.

De nou, aquestes L-sèries es poden estendre a tot el pla complex mitjançant el principi de

Mellin. Com en el cas de les funcions L associades a caràcters de Dirichlet, aquestes funcions L són enteres en tot $\mathbb{C}$ si $\chi \neq \chi^0$.

A continuació veiem el següent resultat, que generalitza la Proposició 1.2.7.

Proposició 1.3.6.

$$\zeta_L(s) = G(s) \prod_{\chi \neq \chi^0} L(\widetilde{\chi}, s)\zeta_K(s)$$

on el producte és respecte els caràcters irreductibles no trivials de $G(L|K)$ i la funció $G(s)$ és un producte finit de factors d'Euler de la forma $(1-\chi(\varphi_{\mathfrak{p}})\mathfrak{N}(\mathfrak{p}^{-s}))^{-1}$ on $\varphi_{\mathfrak{p}}$ és l' automorfisme de Frobenius de $\mathfrak{p}$.

No donarem els detalls d'aquesta demostració. Ens limitem a comentar que per deduir aquesta fórmula cal introduir resultats de la teoria de representació de grups, que donen la descomposició de la representació regular en representacions irreductibles. Tot definint la L-sèrie d'Artin $L(L|K, \chi, s)$ associada a un caràcter χ de $G(L|K)$ de manera completament anàloga a com ho vam fer quan en el cas dels caràcters de Dirichlet, s'arriba a la següent conclusió.

Proposició 1.3.7. *[19, C.10, Cor. 10.5]*

$$\zeta_L(s) = \prod_{\chi \neq \chi^0} L(L|K, \chi, s)\zeta_K(s),$$

on el producte recorre els caràcters irreductibles no trivials de $G(L|K)$.

Finalment, gràcies a [19, C. 10, Teorema 10.6], els factors que conformen $L(L|K, \chi, s)$ coincideixen exactament amb els factors de $L(\widetilde{\chi}, s)$, llevat de productes finits de la forma $(1 - \chi(\varphi_{\mathfrak{p}})\mathfrak{N}(\mathfrak{p}^{-s}))^{-1}$ que no pertanyen a $L(\widetilde{\chi}, s)$. Aquests factors de discrepància són els que defineixen la funció $G(s)$ que apareix en la Proposició 1.3.6 anterior.

De la mateixa manera que la Proposició 1.2.5 ens ha permès demostrar en la secció anterior el Teorema 1.2.1 dels nombres primers de Dirichlet, la Proposició 1.3.8 següent ens permetrà demostrar el Teorema 1.3.4 de densitat de Dirichlet.

Proposició 1.3.8. *Sigui $L|K$ una extensió abeliana. Per a tot caràcter irreductible no trivial χ del grup de Galois $G(L|K)$ es compleix*

$$L(\widetilde{\chi}, 1) \neq 0$$

on $\widetilde{\chi}$ és el caràcter induït a $J^{\mathfrak{m}}$.

Demostració. La demostració és igual a la realitzada per a demostrar 1.2.5. En aquest cas utilitzem 1.3.6. Com que $\zeta_L(s)$ i $\zeta_K(s)$ tenen un pol simple en $s = 1$ i $G(s)$ és holomorfa i no nul·la en $s = 1$, deduïm que $L(\widetilde{\chi}, 1) \neq 0$. □

Demostració. (Teorema 1.3.4 de densitat de Dirichlet.)

Utilitzant els raonaments realitzats per a L-sèries de Dirichlet obtenim

$$\log L(\widetilde{\chi},s)\sim\sum_{\mathfrak{p}}\frac{\widetilde{\chi}(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}=\sum_{\mathfrak{K}'\in J^{\mathfrak{m}}/P^{\mathfrak{m}}}\widetilde{\chi}(\mathfrak{K}')\sum_{\mathfrak{p}\in\mathfrak{K}'}\frac{1}{\mathfrak{N}(\mathfrak{p})^s}.$$

Multiplicant per $\widetilde{\chi}(\mathfrak{K}^{-1})$ i sumant sobre tots els caràcters irreductibles

$$\log\zeta_K(s)+\sum_{\chi\neq\chi^0}\widetilde{\chi}(\mathfrak{K}^{-1})\log L(\widetilde{\chi},s)\sim\sum_{\chi}\sum_{\mathfrak{K}'\in J^{\mathfrak{m}}/P^{\mathfrak{m}}}\widetilde{\chi}(\mathfrak{K}'\mathfrak{K}^{-1})\sum_{\mathfrak{p}\in\mathfrak{K}'}\frac{1}{\mathfrak{N}(\mathfrak{p})^s}.$$

Com que $L(\widetilde{\chi},s)\neq 0$ llavors $\log L(\widetilde{\chi},s)$ és analítica en $s=1$ i per tant

$$\log\zeta_K(s)\sim\log\zeta_K(s)+\sum_{\chi\neq\chi^0}\widetilde{\chi}(\mathfrak{K}^{-1})\log L(\widetilde{\chi},s).$$

Utilitzant el següent resultat

$$\sum_{\chi}\widetilde{\chi}(\mathfrak{K}'\mathfrak{K}^{-1})=\sum_{\chi}\chi(\mathfrak{K}'\mathfrak{K}^{-1})=\begin{cases}0 & \text{si } \mathfrak{K}'\neq\mathfrak{K}\\ h_{\mathfrak{m}} & \text{si } \mathfrak{K}'=\mathfrak{K}\end{cases}$$

podem concloure

$$\log\frac{1}{s-1}\sim\log\zeta_K(s)\sim h_{\mathfrak{m}}\sum_{\mathfrak{p}\in\mathfrak{K}}\frac{1}{\mathfrak{N}(\mathfrak{p})^s}.$$

Com que $\log\frac{1}{s-1}$ té un pol en $s=1$ el resultat anterior és equivalent a

$$\frac{1}{h_{\mathfrak{m}}}\sim\frac{\displaystyle\sum_{\mathfrak{p}\in\mathfrak{K}}\mathfrak{N}(\mathfrak{p})^{-s}}{\log\dfrac{1}{s-1}}.$$

Per tant, $\dfrac{1}{h_{\mathfrak{m}}}$ és la densitat de Dirichlet dels primers de K en $\mathfrak{K}$. □

Per finalitzar veiem la relació amb el teorema de les nombres primers de Dirichlet 1.2.1. Segons les notacions anteriors elegim $K=\mathbb{Q}$, $\mathfrak{m}=(m)$ i $H_K^{\mathfrak{m}}=P_K^{\mathfrak{m}}$. En aquest cas, s'obté $J_K^{\mathfrak{m}}/H_K^{\mathfrak{m}}=(\mathbb{Z}/m\mathbb{Z})^*$ i el teorema anterior es tradueix en dir que la densitat de Dirichlet dels primers congruents amb un nombre a, complint $(a,m)=1$, és $1/\varphi(m)$. Està clar que la densitat de Dirichlet d'un nombre finit de primers és 0 i per tant hi ha un nombre infinit de primers p complint $(a,m)=1$.

Podem comprovar que existeix la densitat natural del conjunt de primers congruents amb

a mòdul m. Per tant $\delta(M) = d(M) = 1/\varphi(m)$, el que ens permet dir que els primers estan distribuïts uniformement en les diverses classes mòdul m. Demostrarem aquest resultat a la secció 2.2.

1.4 Teorema de densitat de Chebotarev

Interpretarem el teorema de densitat de Dirichlet des del punt de vista de la teoria de Galois. Considerem una extensió abeliana finita $L|K$. Per la teoria de classes de cossos existeix $P_K^{\mathfrak{m}} \subseteq H_K^{\mathfrak{m}} \subseteq J_K^{\mathfrak{m}}$ de manera que $G(L|K) \cong J_K^{\mathfrak{m}}/H_K^{\mathfrak{m}}$. Donat un element $\sigma \in G(L|K)$ aquest isomorfisme ens permet calcular la densitat del conjunt $P_{L|K}(\sigma)$ de primers $\mathfrak{p}$ amb $\left(\frac{L|K}{\mathfrak{p}}\right) = \sigma$ a través del teorema de la densitat de Dirichlet. Obtenim així que

$$d(P_{L|K}(\sigma)) = \frac{1}{\#G(L|K)}.$$

Veiem com ampliar el resultat a extensions finites $L|K$ de Galois no abelianes. Fixat un element $\sigma \in G(L|K)$ considerem el conjunt $P_{L|K}(\sigma)$ de tots els primers $\mathfrak{p}$ de K de manera que existeix algun primer $\mathfrak{P}$ de L sobre $\mathfrak{p}$ complint

$$\sigma = \left(\frac{L|K}{\mathfrak{P}}\right).$$

Recordem que $\tau^{-1}\left(\frac{L|K}{\mathfrak{P}}\right)\tau = \left(\frac{L|K}{\tau\mathfrak{P}}\right)$ i per tant $P_{L|K}(\sigma)$ depèn només de $\langle\sigma\rangle$, la classe de conjugació de σ.

El teorema següent ens permet calcular la densitat del conjunt $P_{L|K}(\sigma)$.

Teorema 1.4.1 (Teorema de Chebotarev)**.** *Sigui $L|K$ una extensió de Galois finita amb grup de Galois $G = G(L|K)$. Per tot element $\sigma \in G$ el conjunt $P_{L|K}(\sigma)$ té densitat de Dirichlet i ve donada per*

$$d(P_{L|K}(\sigma)) = \frac{\#\langle\sigma\rangle}{\#G}.$$

Demostració. Per demostrar el teorema ens cal principalment conèixer el comportament de la factorització de primers respecte les extensions de cossos. Considerem primer el cas on G és un grup cíclic generat per σ. Per tant, l'extensió $L|K$ és abeliana i en conseqüència podem elegir un ideal $\mathfrak{m}$, el conductor de $L|K$, i un grup $H^{\mathfrak{m}}$, amb $P_K^{\mathfrak{m}} \subseteq H_K^{\mathfrak{m}} \subseteq J_K^{\mathfrak{m}}$, de manera que

$$J^{\mathfrak{m}}/H^{\mathfrak{m}} \cong G.$$

Segons l'isomorfisme anterior, considerem la classe $\mathfrak{K}$ de $J^{\mathfrak{m}}/H^{\mathfrak{m}}$ corresponent a σ. Per la pròpia definició del conjunt $P_{L|K}(\sigma)$, els elements d'aquest conjunt són precisament els

primers que pertanyen a $\mathfrak{K}$. I utilitzant el teorema de densitat de Dirichlet obtenim que

$$d(P_{L|K}(\sigma)) = d(P(\mathfrak{K})) = \frac{1}{h_{\mathfrak{m}}} = \frac{1}{\#G} = \frac{\#\langle\sigma\rangle}{\#G}.$$

Considerem ara el cas general. Sigui Σ el cos fix de (σ), el subgrup generat per σ. Podem aplicar el raonament anterior a l'extensió $L|\Sigma$. Si f és l'ordre de σ llavors $d(P_{L|\Sigma}(\sigma)) = \frac{1}{f}$. Considerem el conjunt $P'_{L|\Sigma}(\sigma)$ de primers $\mathfrak{q}$ de $P_{L|\Sigma}(\sigma)$ de grau 1 sobre K. Com ja hem discutit anteriorment, es compleix

$$d(P'_{L|\Sigma}(\sigma)) = d(P_{L|\Sigma}(\sigma)) = \frac{1}{f}.$$

A més, per tots els primers $\mathfrak{p}$ de $P_{L|K}(\sigma)$ el grup generat per σ és el grup de descomposició de $\mathfrak{P}$, un primer de L sobre $\mathfrak{p}$. Per la definició de Σ com el cos fix de (σ) obtenim que els primers de $P'_{L|\Sigma}(\sigma)$ estan en bijecció amb el conjunt $\bar{P}(\sigma)$ de primers $\mathfrak{P}$ de L tal que $\mathfrak{P}|\mathfrak{p}$ i $\left(\frac{L|K}{\mathfrak{P}}\right) = \sigma$.

L'aplicació natural entre els primers de Σ i els primers de K permet definir

$$\begin{array}{ccc} \rho : P'_{L|\Sigma}(\sigma) & \to & P_{L|K}(\sigma) \\ \mathfrak{q} & \mapsto & \mathfrak{q} \cap K \end{array}$$

Com que $P'_{L|\Sigma}(\sigma) \cong \bar{P}(\sigma)$ obtenim

$$\rho^{-1}(\mathfrak{p}) \cong \left\{\mathfrak{P} \in \bar{P}(\sigma) \,\middle|\, \mathfrak{P}|\mathfrak{p}\right\}.$$

El conjunt de primers $\mathfrak{P}|\mathfrak{p}$ està en bijecció amb el conjunt $G/G_{\mathfrak{P}}$. A més, si $\mathfrak{P} \in \bar{P}(\sigma)$ llavors $G_{\mathfrak{P}} = (\sigma)$ i donat un element $\tau \in G$ es compleix que $\tau\mathfrak{P} \in \bar{P}(\sigma)$ si i només si $\tau \in Z(\sigma)$. On $Z(\sigma) = \{\tau \in G | \tau\sigma = \sigma\tau\}$ és el centralitzador de σ en G. Per tant,

$$\rho^{-1}(\mathfrak{p}) \cong \left\{\mathfrak{P} \in \bar{P}(\sigma) \,\middle|\, \mathfrak{P}|\mathfrak{p}\right\} \cong Z(\sigma)/(\sigma).$$

Utilitzant aquesta última propietat podem calcular $d(P_{L|K}(\sigma))$ com

$$d(P_{L|K}(\sigma)) = \frac{1}{(Z(\sigma) : (\sigma))} d(P'_{L|\Sigma}(\sigma)) = \frac{f}{\#Z(\sigma)} \frac{1}{f} = \frac{\#\langle\sigma\rangle}{\#G}.$$

□

A partir del teorema de Chebotarev 1.4.1 podem obtenir altres resultats importants sobre extensions de cossos. Per exemple, ens permet caracteritzar les extensions de Galois d'un cos

K a partir de subconjunts de primers de K a partir del corol·lari 13.10 del capítol 13 de [19].

Corol·lari 1.4.2. *Una extensió de Galois $L|K$ està determinada únicament pel conjunt $P(L|K)$ de primers de K que descomponen completament a L.*

Per tant, per classificar totes les extensions de Galois d'un cos K és suficient estudiar els possibles conjunts de primers de la forma $P(L|K)$. Per a extensions abelianes aquesta qüestió la resol la teoria de classes de cossos i és, de fet, un dels objectius principals d'aquesta teoria. Per exemple, si $K = \mathbb{Q}$ i $L = \mathbb{Q}(\mu_m)$ on μ_m és una m-arrel primitiva de la unitat llavors $P(L|K)$ correspon als primers $p \equiv 1 \mod m$. Per a extensions no abelianes no es coneix, en general, una caracterització de $P(L|K)$.

Capítol 2

Teoria de Serre

Per entendre els problemes relacionats amb la equidistribució en aritmètica, és precís formular una teoria que englobi els resultats anteriors i es pugui aplicar en altres àmbits. Per aquest objectiu presentem la teoria introduïda per Serre. Seguirem el desenvolupament realitzat a [23].

Sigui X un espai topològic compacte i $C(X)$ l'espai de Banach de les funcions continues de X a valors complexes segons la norma del suprem:

$$\|f\| = \sup_{x \in X} |f(x)|.$$

Sigui μ una mesura de Radon a X, és a dir, una forma lineal contínua sobre $C(X)$.

Exemples 2.0.3. *1. Donat $x \in X$ definim la mesura de Dirac associada a x per $\delta_x(f) = f(x)$.*

2. Donada una successió $(x_n)_{n \in \mathbb{N}}$ de punts de X definim les mesures

$$\mu_n = \frac{\delta_{x_1} + \ldots + \delta_{x_n}}{n}.$$

Segons les definicions prèvies, direm que la successió $(x_n)_n$ és μ-equidistribuïda si $\mu_n(f) \to \mu(f)$ quan $n \to \infty$ per tota $f \in C(x)$. Observem que es pot interpretar aquesta convergència com una convergència dèbil de μ_n a μ. Notem també que la propietat $\mu_n(f) \to \mu(f)$ és llegeix com

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

Lema 2.0.4. *Sigui $(\phi_m)_m$ una família de funcions que generen un subespai dens de $C(X)$ i sigui $(x_n)_n$ una successió d'elements de X. Suposem que per tota m la successió $(\mu_n(\phi_m))_n$ té límit. Llavors la successió $(x_n)_n$ està distribuïda respecte una única mesura μ, definida per la propietat $\mu(\phi_m) = \lim_{n \to \infty} \mu_n(\phi_m)$ per tot m.*

Demostració. Basta definir $\mu(f)$ com el límit de la successió $(\mu_n(f))$. La continuïtat i la linealitat en f es segueix de raonaments bàsics d'equicontinuïtat. □

Sigui G un grup topològic compacte. Considerem a partir d'ara que X és l'espai de les classes de conjugació de G. En ser X el quocient de G per l'acció de G en ell mateix donada per conjugació, l'espai X està dotat de manera natural amb una topologia, la topologia quocient, respecte la qual és compacte.

Tota mesura μ de G indueix una mesura sobre X, que també anomenarem μ, cometent un abús de notació.

Proposició 2.0.5. *Una successió $(x_n)_n$ de X està μ-equidistribuïda si i només si per qualsevol caràcter irreductible χ de G es compleix*

$$\lim_{n\to\infty} \mu_n(\chi) = \mu(\chi).$$

Demostració. Segons el teorema de Peter-Weyl el subespai generat pels caràcters irreductibles de G és dens a $C(X)$. Per tant, aplicant el lema 2.0.4 obtenim directament el resultat enunciat. □

Sigui μ la mesura de Haar de G. Es tracta de la única mesura en G tal que

- És invariant pel producte d'elements de G, és a dir,

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

  per tot S mesurable i tot g de G.
- $\mu(G) = 1$.

En aplicar la proposició 2.0.5 a la mesura de Haar de G, obtenim el següent resultat.

Corol·lari 2.0.6. *Sigui μ la mesura de Haar de G. La successió $(x_n)_n$ d'elements de X és μ-equidistribuïda si i només si per a tot caràcter irreductible no trivial χ de G es compleix*

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

Demostració. Per a tot caràcter irreductible no trivial de G es compleix $\mu(\chi) = 0$. En canvi, $\mu(\chi_0) = 1$, on recordem que χ_0 denota el caràcter trivial. Tenint en compte que $\mu_n(\chi_0) = 1 = \mu(\chi_0)$ per a qualsevol successió, el resultat és ara conseqüència directa de la proposició anterior. □

2.1 Funcions L

Sigui G un grup topològic compacte, sigui X el conjunt de les seves classes de conjugació i sigui μ una mesura en G.

Introduïm a continuació una noció general de funció L que ens permetrà generalitzar els teoremes estudiats anteriorment.

Sigui Σ un conjunt finit o numerable i sigui $(x_v)_{v\in\Sigma}$ una família d'elements de X. Sigui $N : \Sigma \longrightarrow \{n \in \mathbb{Z}, n > 1\}$ una aplicació que satisfà la següent condició:

Existeix una constant C tal que, per tot $n \in \mathbb{Z}$, el nombre de $v \in \Sigma$ amb $Nv = n$ està fitat per C.

Aquesta hipòtesi ens permetrà veure que la convergència de les sèries definides per les funcions L que introduirem a continuació és independent de la reordenació de Σ.

En tots els casos on apliquem la teoria de Serre definirem Σ com el conjunt de primers d'un cos de nombres K, i l'aplicació N serà l'aplicació norma. Per tant la hipòtesi anterior serà sempre certa.

Aquesta condició permet disposar els elements v de Σ en una successió $(v_i)_{i\geq 1}$ tal que $N(v_i) \leq N(v_j)$ per tot $i \leq j$. És clar que aquesta ordenació de Σ no té perquè ser única, però en qualsevol cas l'equidistribució de la família $(x_v)_{v\in\Sigma}$ no depèn d'aquesta tria. Així, d'ara en endavant, té sentit parlar de l' equidistribució dels elements de la família $(x_v)_{v\in\Sigma}$ respecte d'una mesura.

Definició 2.1.1. *Donada una representació irreductible ρ de G definim la funció L associada a ρ, $(x_v)_{v\in\Sigma}$ i N com*

$$L(s,\rho) = \prod_{v\in\Sigma} \frac{1}{\det(1-\rho(x_v)(Nv)^{-s})},$$

on s pren valors complexes.

Observem que la definició anterior no depèn dels representants de x_v en G escollits, ja que el determinant és invariant per conjugació.

També podem comprovar que dues representacions equivalents donen lloc a la mateixa funció L, i per tant $L(s,\rho)$ depèn només de $(x_v)_{v\in\Sigma}$, N i del *caràcter de ρ.*

A més, per la representació trivial ρ_0 obtenim $L(s,\rho_0) = \prod(1-(Nv)^{-s})^{-1}$, que només depèn de l'aplicació N i del conjunt Σ.

Fem les següents hipòtesis sobre la família $(x_v)_{v\in\Sigma}$ i l'aplicació N, relatives a la convergència de les funcions L associades a les representacions ρ:

(1) El productori $L(s, \rho_0)$ és convergent per $\Re(s) > 1$ i defineix una funció holomorfa en aquesta regió. A més, es pot estendre a una funció meromorfa en $\Re(s) \geq 1$ sense zeros ni pols, llevat d'un pol simple a $s = 1$.

(2) Si ρ és una representació irreductible no trivial, la funció $L(s, \rho)$ es pot estendre a una funció meromorfa en el conjunt $\Re(s) \geq 1$, sense zeros ni pols en $\{s \in \mathbb{C}, \Re(s) \geq 1, s \neq 1\}$.

Donada una representació irreductible ρ amb caràcter χ, denotem per $-c_\chi$ l'ordre de $L(s, \rho)$ a $s = 1$. És a dir, si $L(s, \rho)$ té un pol, respectivament un zero, d'ordre m a $s = 1$, llavors $c_\chi = m$, respectivament $c_\chi = -m$.

El següent teorema és el central per concloure posteriorment el resultat sobre equidistribució.

Teorema 2.1.2. *Mantenim la notació anterior i suposem les hipòtesis (1) i (2). Llavors per tot caràcter irreductible χ de G es compleix*

$$\sum_{Nv \leqslant n} \chi(x_v) = c_\chi n / \log(n) + o(n/\log(n)).$$

Per demostrar el teorema necessitem el següent resultat sobre sèries de Dirichlet.

Teorema 2.1.3 (Teorema de Wiener-Ikehara)**.** *Sigui $f(s) = \sum_{n \geqslant 1} a_n/n^s$ una sèrie de Dirichlet. Suposem que existeix una sèrie de Dirichlet $F(s) = \sum_{n \geqslant 1} b_n/n^s$ amb coeficients reals tal que:*

(a) *$|a_n| \leq b_n$ per tot n.*

(b) *La sèrie $F(s)$ convergeix per $\Re(s) > 1$.*

(c) *La funció $F(s)$ es pot estendre a una funció meromorfa en $\Re(s) \geq 1$ sense cap pol excepte un pol simple a $s = 1$ amb residu $R > 0$.*

(d) *La funció $f(s)$ es pot estendre a una funció meromorfa en $\Re(s) \geq 1$ sense cap pol excepte un possible pol simple a $s = 1$ amb residu r.*

Llavors

$$\sum_{m \leq n} a_m = rn + o(n).$$

Podem trobar la demostració al capítol 1 de [18].

També ens serà necessari el següent resultat tècnic.

Proposició 2.1.4 (Truc de sumació d'Abel)**.** *Sigui* $\{a_m\}_{m\in\mathbb{N}}$ *una successió de nombres complexes amb* $a_1 = 0$*. Suposem que per tot enter* n

$$f(n) = \sum_{m\leq n} a_m = \alpha n + o(n).$$

Llavors

$$g(n) = \sum_{m\leq n} \frac{a_m}{\log(m)} = \alpha\frac{n}{\log(n)} + o(\frac{n}{\log n}).$$

Demostració. Observem que $a_m = f(m) - f(m-1)$ i per tant

$$\begin{aligned} g(n) &= \sum_{m\leq n} \frac{f(m) - f(m-1)}{\log(m)} = \sum_{m=2}^{n} \frac{f(m)}{\log(m)} + \sum_{m=1}^{n-1} \frac{f(m)}{\log(m+1)} \\ &= \frac{f(n)}{\log(n)} + \sum_{m=2}^{n-1} f(m)\left(\frac{1}{\log(m)} - \frac{1}{\log(m+1)}\right) \end{aligned}$$

El terme $f(n)/\log(n)$ té ordre $\alpha n/\log(n)$, així que només cal veure que el sumatori és $o(n/\log(n))$. Com que $f(n) = \alpha n + o(n)$ podem substituir $f(m)$ per Cm, on C és una constant. A més

$$\frac{1}{\log(m)} - \frac{1}{\log(m+1)} = \frac{\log(1+1/m)}{\log(m)\log(m+1)} < \frac{1/m}{\log(m)^2}$$

Per tant els termes de la suma estan fitats per $C/\log(m)^2$, i és suficient veure que

$$\sum_{m=2}^{n} \frac{1}{\log(m)^2} = o(\frac{n}{\log n}).$$

Dividim la suma anterior com

$$\sum_{2\leq m\leq\sqrt{n}} \frac{1}{\log(m)^2} + \sum_{\sqrt{n}\leq m\leq n} \frac{1}{\log(m)^2}.$$

Llavors és senzill veure que la primera suma està fitada per $\sqrt{n}/\log(2)^2$ i la segona per $n/\log(\sqrt{n})^2 = 4n/\log(n)^2$. Aquests dos termes són $o(n/\log n)$, el que finalitza la demostració. □

Utilitzant els resultats anteriors demostrem el teorema 2.1.2.

Demostració. (Teorema 2.1.2) Cal observar que pel caràcter trivial el resultat del teorema és

$$\sum_{Nv\leqslant n} 1 = n/\log(n) + o(n/\log(n))$$

Fixem una representació irreductible ρ. Per simplificar la notació denotem $L(s,\rho)$ per L i la seva derivada per L'. A més, definim $\lambda_{v,i}$ com el i-èssim valor propi de l'automorfisme $\rho(x_v)$. Calculem la derivada logarítmica de L, és a dir, L'/L. Segons la definició anterior podem fer la següent descomposició

$$L(s,\rho) = \prod_{v\in\Sigma}\prod_i \frac{1}{1-\lambda_{v,i}(Nv)^{-s}}.$$

Aquesta descomposició ens permet calcular la derivada logarítmica com

$$\frac{L'}{L} = -\sum_{v\in\Sigma}\sum_i \frac{\lambda_{v,i}(Nv)^{-s}\log(Nv)}{1-\lambda_{v,i}(Nv)^{-s}} = -\sum_{v\in\Sigma}\sum_i\sum_{m\geqslant 1}\frac{\lambda_{v,i}^m\log(Nv)}{(Nv)^{ms}}.$$

Si intercanviem els dos últims índexs de sumació obtenim

$$-\sum_{v\in\Sigma}\sum_{m\geqslant 1}\frac{\log(Nv)}{(Nv)^{ms}}\sum_i \lambda_{v,i}^m.$$

Les potències m-èssimes dels elements de la classe de x_v pertanyen a una mateixa classe de X, la qual definim com x_v^m. A més, podem comprovar que els valors propis de $\rho(x_v^m)$ són $\lambda_{v,i}^m$ i per tant obtenim que $\chi(x_v^m) = \sum_i \lambda_{v,i}^m$. En conclusió

$$\frac{L'}{L} = -\sum_{v\in\Sigma}\sum_{m\geqslant 1}\frac{\chi(x_v^m)\log(Nv)}{(Nv)^{ms}}.$$

Per les hipòtesis realitzades sobre les funcions L obtenim que L'/L defineix una funció meromorfa a $\Re(s)\geqslant 1$, excepte per un possible pol simple a $s=1$ amb residu c_χ.

Veiem que podem escriure L'/L com

$$\frac{L'}{L} = -\sum_{v\in\Sigma}\frac{\chi(x_v)\log(Nv)}{(Nv)^s} + g(s)$$

on $g(s)$ és holomorfa per $\Re(s) > 1/2$.

Observem que $|\chi(x_v^m)| \leq d$, on d és el grau de la representació ρ. Per tant, denotant

$\sigma = \Re(s)$, és suficient veure que

$$\sum_{v\in\Sigma}\sum_{m\geqslant 2}\frac{\log(Nv)}{(Nv)^{m\sigma}}$$

convergeix per $\sigma > 1/2$.

Podem comprovar que

$$\sum_{v\in\Sigma}\sum_{m\geqslant 2}\frac{\log(Nv)}{(Nv)^{m\sigma}} = \sum_{v\in\Sigma}\log(Nv)\frac{(Nv)^{-\sigma}}{(Nv)^{\sigma}-1} \leq M\sum_{v\in\Sigma}\frac{\log(Nv)}{(Nv)^{2\sigma}}$$

per M prou gran.

A més

$$\sum_{v\in\Sigma}\frac{\log(Nv)}{(Nv)^{2\sigma}} \leq \sum_{v\in\Sigma}\sum_{m\geqslant 1}\frac{\log(Nv)}{(Nv)^{m2\sigma}}$$

i aquesta última sèrie és, excepte el signe, la derivada logarítmica de $L(s,\rho_0)$ en $s = 2\sigma$. Com que $2\sigma > 1$ llavors, per hipòtesi, $L(s,\rho_0)$ és convergent en $s = 2\sigma$.

Així doncs

$$\frac{L'}{L} = -\sum_{v\in\Sigma}\frac{\chi(x_v)\log(Nv)}{(Nv)^s} + g(s)$$

on $g(s)$ és holomorfa per $\Re(s) > 1/2$. Aleshores

$$-\sum_{v\in\Sigma}\frac{\chi(x_v)\log(Nv)}{(Nv)^s}$$

defineix una funció meromorfa a $\Re(s) \geqslant 1$, excepte per un possible pol simple a $s = 1$ amb residu c_χ.

Apliquem el teorema de Wiener-Ikehara 2.1.3 definint

$$f(s) = -\sum_{v\in\Sigma}\frac{\chi(x_v)\log(Nv)}{(Nv)^s},$$

$$F(s) = d\sum_{v\in\Sigma}\frac{\log(Nv)}{(Nv)^s},$$

on d és el grau de ρ. Segons aquesta notació ja hem demostrat que es compleixen les hipòtesis del teorema 2.1.3 i per tant es compleix

$$\sum_{Nv\leq n}\frac{\chi(x_v)}{\log(Nv)} = c_\chi n + o(n).$$

Utilitzant ara el truc de sumació d'Abel 2.1.4 obtenim

$$\sum_{Nv\leq n}\chi(x_v)=c_\chi\frac{n}{\log n}+o(\frac{n}{\log n}).$$

□

Utilitzant els resultats anteriors podem demostrar el següent teorema,

Teorema 2.1.5. *Mantenim la notació anterior i suposem les hipòtesis* (1) *i* (2)*. Llavors la successió* $(x_v)_{v\in\Sigma}$ *està* μ*-equidistribuïda en* X *si i només si per tot caràcter irreductible* χ *de* G *es compleix*

$$\mu(\chi)=c_\chi.$$

Demostració. Per la proposició 2.0.5, és suficient demostrar que $\lim_{n\to\infty}\frac{\mu_n(\chi)}{n}=c_\chi$. És clar que

$$\lim_{n\to\infty}\frac{\mu_n(\chi)}{n}=\lim_{n\to\infty}\frac{\sum_{Nv\leq n}\chi(x_v)}{\sum_{Nv\leq n}1}.$$

Segons el teorema 2.1.2 es compleix

$$\sum_{Nv\leq n}\chi(x_v)=c_\chi\frac{n}{\log n}+o(\frac{n}{\log n}),$$

$$\sum_{Nv\leq n}1=\frac{n}{\log n}+o(\frac{n}{\log n}).$$

I per tant $\lim_{n\to\infty}\frac{\sum_{Nv\leq n}\chi(x_v)}{\sum_{Nv\leq n}1}=c_\chi$. □

Si considerem μ com la mesura de Haar de G obtenim,

Corol·lari 2.1.6. *Sigui* μ *la mesura de Haar de* G*. La successió* $(x_v)_{v\in\Sigma}$ *d'elements de* X *és* μ*-equidistribuïda si i només si es compleix la hipòtesi* (1) *i per tota representació irreductible no trivial* ρ *de* G *la funció* $L(\rho,s)$ *és holomorfa i no nul·la en* $\Re(s)\leq 1$*.*

El resultat és conseqüència directa del teorema 2.1.5 i del corol·lari 2.0.6.

2.2 Aplicació al Teorema de Chebotarev

Com a primera aplicació de la teoria de Serre veurem com podem interpretar el teorema de Chebotarev, per extensions abelianes, a partir de la teoria desenvolupada anteriorment. Recordem que la demostració d'aquest resultat ja utilitza les funcions L, així doncs la presentació que farem no aportarà cap novetat respecte la manera de demostrar el problema sinó respecte la manera de plantejar-lo.

Sigui L una extensió finita d'un cos de nombres K. Definim G com el grup de Galois de l'extensió $L|K$ i Σ com el conjunt de primers de K no ramificats sobre L. Donat $v \in \Sigma$ definim x_v com la classe de conjugació de l'automorfisme de Frobenius de v i Nv com la norma de v.

Per les definicions realitzades prèviament obtenim que donada una representació ρ de G la funció $L(\rho, s)$ és, excepte un número finit de factors, a la L-sèrie d'Artin $L(L|K, \rho, s)$.

Per tal de poder demostrar les hipòtesis del corol·lari 2.1.6 suposem que $L|K$ és abeliana. Com ja hem vist anteriorment, aquestes funcions L defineixen una funció meromorfa en $\Re(s) \geq 1$.

Si ρ és trivial, $L(L|K, \rho, s)$ té un únic pol simple en $s = 1$. Si ρ no és trivial, $L(L|K, \rho, s)$ és una funció holomorfa, que no s'anul·la en $\Re(s) \geq 1$. Podem trobar la demostració d'aquest resultat a [18].

Segons la notació anterior tenim $c_\chi = 0$. Podem doncs aplicar el corol·lari 2.1.6 obtenint que els elements x_v estan equidistribuïts en X respecte la mesura de Haar de G. Per tant es compleix que per tota funció continua f de $C(X)$ es compleix

$$\mu(f) = \lim_{n\to\infty} \frac{\sum_{Nv\leq n} f(x_v)}{\sum_{Nv\leq n} 1}.$$

Com que G és abelià totes les classes de conjugació tenen un sol element, i identifiquem $X = G$. Donat un element $x \in X$ definim la funció

$$\delta_x(y) = \begin{cases} 0 & \text{si } x \neq y \\ 1 & \text{si } x = y \end{cases}$$

Com que G és finit la seva topologia és la discreta i per tant $\delta_x(y) \in C(X)$. Per tant

$$\mu(\delta_x) = \lim_{n\to\infty} \frac{\sum_{Nv\leq n} \delta_x(x_v)}{\sum_{Nv\leq n} 1}.$$

És clar que $\mu(\delta_x) = 1/\#G$ ja que la mesura de Haar d'un grup finit és la mesura uniforme. Aleshores

$$\frac{1}{\#G} = \lim_{n\to\infty} \frac{\#\{v \in \Sigma | Nv \leq n \ i \ x_v = x\}}{\#\{v \in \Sigma | Nv \leq n\}}$$

Observem que el terme de la dreta és la densitat natural del conjunt $P_{L|K}(x)$. Per tant hem demostrat que per tota extensió abeliana finita $L|K$ i $\sigma \in Gal(L|K)$ es compleix $\delta(P_{L|K}(\sigma)) = 1/\#Gal(L|K)$. Utilitzant la proposició 1.3.3 tenim que l'existència de densitat natural implica l'existència de densitat de Dirichlet i que de fet s'obté una igualtat. Per tant també es $d(P_{L|K}(\sigma)) = 1/\#Gal(L|K)$, és a dir, el teorema 1.4.1.

Hem considerat només extensions abelianes, així que és natural preguntar-se que podem dir sobre l'aplicació de la teoria de Serre en extensions no abelianes. En aquest cas ens caldria demostrar que per tota representació no trivial ρ la L-sèrie d'Artin $L(L|K, \rho, s)$ és holomorfa i no nul·la en $\Re(s) \geq 1$. Aquest resultat no està demostrat en tota generalitat i és conegut com la conjectura d'Artin.

Conjectura 2.2.1 (Artin)**.** *Sigui $L|K$ una extensió finita de cossos de nombres. Sigui ρ una representació irreductible no-trivial de $Gal(L|K)$. Llavors la L-sèrie d'Artin $L(L|K, \rho, s)$ estén a una funció entera en $\mathbb{C}$.*

Podem consultar més detalls sobre aquesta conjectura en [14]. Tornarem a parlar posteriorment de la conjectura d'Artin estudiant la conjectura de Langlands 3.5.2.

Capítol 3

La conjectura de Sato-Tate per a corbes el·líptiques

Hem vist fins al moment resultats d'equidistribució en el context de la teoria algebraica de cossos de nombres, tot i que les demostracions depenen de resultats analítics. El següent pas és obtenir resultats d'equidistribució en contextos més geomètrics, recolzant-nos en la teoria de Serre desenvolupada anteriorment.

En aquest sentit estudiarem la conjectura de Sato-Tate, resolta recentment per Richard Taylor et al.

3.1 Preliminars sobre corbes el·líptiques

Dediquem aquesta secció a presentar alguns resultats previs sobre corbes el·líptiques. Els resultats i les demostracions corresponents es poden trobar a [26].

Sigui K un cos de característica diferent de 2 i 3 i sigui $\overline{K}$ una clausura algebraica fixada qualsevol de K.

Definició 3.1.1. *Una corba el·líptica sobre K és una corba algebraica projectiva E/K associada a una equació afí de la forma*

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

on $A, B \in K$ són elements del cos tals que $\Delta(E) = -16(4A^3 + 27B^2) \neq 0$.

La quantitat $\Delta(E)$ s'anomena el discriminant de la corba el·líptica E.

Es pot comprovar que la corba és no singular si i només si $\Delta(E) \neq 0$. El gènere de

tota corba el·líptica és sempre 1. De fet, recíprocament, com a conseqüència del teorema de Riemann-Roch s'obté que tota corba C/K no singular de gènere 1 amb un punt racional sobre K és isomorfa a una corba el·l'iptica donada en forma de Weierstrass com en la definició anterior.

Introduïm també el invariant j d'E, que es defineix a partir dels coeficients de l'equació de Weierstrass d'E com

$$j(E) = 1728(4A)^3/\Delta(E).$$

L'invariant j determina la corba el·líptica E/K llevat d'isomorfisme sobre $\overline{K}$.

Donada una corba el·líptica E/K podem definir una estructura de grup abelià en el conjunt $E(K)$ dels punts racionals d'E sobre K. Això permet dotar al conjunt $End_{\overline{K}}(E)$ dels endomorfismes d'E definits sobre $\overline{K}$ d'estructura d'anell, en general no commutatiu.

Sovint abreujarem $End(E) := End_{\overline{K}}(E)$. Si L/K és una extensió de cossos en $\overline{K}$, denotarem per $End_L(E)$ el subanell d'$End(E)$ format pels endomorfismes d'E definits sobre L. Definim també $End_L^0(E)$ com $End_L(E) \otimes \mathbb{Q}$.

Podem definir per a cada nombre natural m l'endomorfisme $[m]$ com

$$\begin{array}{rccc} [m]: & E(\overline{K}) & \to & E(\overline{K}) \\ & P & \mapsto & mP = P + \overset{m}{\ldots} + P \end{array}$$

I definim $[-m]$ a partir de la suma dels inversos. D'aquesta manera, $\mathbb{Z} \subseteq End(E)$. De fet, el cas general en característica nul·la és $\mathbb{Z} = End(E)$. El següent teorema determina les possibles estructures de l'anell $End(E)$.

Teorema 3.1.2. *L'anell d'endomorfismes d'una corba el·líptica satisfà*

- $End(E) \cong \mathbb{Z}$, *o bé*
- $End(E)$ *és un ordre d'una extensió quadràtica imaginària de* $\mathbb{Q}$, *o bé*
- $End(E)$ *és un ordre d'una àlgebra de quaternions sobre* $\mathbb{Q}$.

A més, la tercera opció es dóna només sobre cossos de característica no nul·la. Aquest resultat és el corol·lari 9.4 del capítol 3 de [26].

Definició 3.1.3. *Sigui E/K una corba el·líptica sobre un cos K de característica* 0. *Diem que E té multiplicació complexa (CM) si $End(E) \neq \mathbb{Z}$, és a dir, si $End(E)$ és un ordre d'una extensió quadràtica imaginària de $\mathbb{Q}$.*

Definim el conjunt dels punts de m-torsió d'E com $Ker[m]$, i ho denotem per $E[m]$. Gràcies a [26, C. 3, Corol·lari 6.4], tenim el següent resultat.

Teorema 3.1.4. • *Si la característica de K és nul·la o coprimera a m es compleix*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

• *Si la característica de K és p llavors es compleix una de les dues opcions següents*

$$E[p^k] \cong \mathbb{Z}/p^k\mathbb{Z} \qquad \textit{per tot } k \geq 1,$$

$$E[p^k] \cong \{0\} \qquad \textit{per tot } k \geq 1.$$

Quan $E[p] \cong \{0\}$ diem que la corba E és supersingular. En cas contrari diem que la corba és ordinària. A més, una corba és supersingular si, i només si, $End(E)$ és un ordre d'una àlgebra de quaternions sobre $\mathbb{Q}$. Això permet veure una relació entre $End(E)$ i els punts de torsió d'E.

Definició 3.1.5. *Sigui E/K una corba el·líptica sobre un cos finit K, de característica p, amb q elements. L'endomorfisme*

$$\begin{array}{rccc} \phi: & E & \to & E \\ & (x,y) & \mapsto & (x^q, y^q) \end{array}$$

és l'endomorfisme de Frobenius d'E.

Es sap que l'endomorfisme de Frobenius s'anul·la per un polinomi $T^2 - aT + q$, per algun $a \in \mathbb{Z}$. Gràcies a aquest resultat, l'enter $a = a(E)$ s'anomena la traça del Frobenius. Es compleix que la corba és supersingular si, i només si, $car(K) \mid a(E)$.

Sigui ara E/K una corba el·líptica definida sobre un cos de nombres K. Sigui $\mathfrak{p}$ un primer de K. Fixem una equació de Weierstrass $y^2 = x^3 + Ax + B$ d'E amb $A, B \in \mathcal{O}_K$ tals que el discriminant d'aquesta equació tingui valoració mínima respecte $\mathfrak{p}$. Sigui $E_{\mathfrak{p}}/k(\mathfrak{p})$ la corba definida per l'equació $y^2 = x^3 + \tilde{A}x + \tilde{B}$, on $\tilde{A} = A \bmod \mathfrak{p}$, $\tilde{B} = B \bmod \mathfrak{p}$.

Definició 3.1.6. • *Si la corba $E_{\mathfrak{p}}$ és no singular, i per tant el·líptica, direm que E té bona reducció en $\mathfrak{p}$. En cas contrari direm que E té mala reducció en $\mathfrak{p}$.*

• *Si $E_{\mathfrak{p}}$ té un node direm que la reducció és multiplicativa. A més, si les pendents de les rectes tangents en el node pertanyen a $\kappa(\mathfrak{p})$ direm que la reducció és multiplicativa split i en cas contrari multiplicativa no split.*

• *Si $E_{\mathfrak{p}}$ té una cúspide direm que la reducció és additiva.*

Fixem un primer $\mathfrak{p}$ on E té bona reducció. Definim

$$N_{\mathfrak{p}}(E) = \#E_{\mathfrak{p}}(\kappa(\mathfrak{p})).$$

Si ϕ és l'endomorfisme de Frobenius de $E_{\mathfrak{p}}$, és clar que $(Id-\phi)$ és l'endomorfisme constant sobre el grup $E_{\mathfrak{p}}(\kappa(\mathfrak{p}))$. Per tant es compleix que $\#Ker(Id-\phi) = N_{\mathfrak{p}}(E)$, i si $a_{\mathfrak{p}}(E)$ és la traça de ϕ obtenim que

$$N_{\mathfrak{p}}(E) = \mathfrak{N}(\mathfrak{p}) + 1 - a_{\mathfrak{p}}(E).$$

Escriurem $N_{\mathfrak{p}}$ i $a_{\mathfrak{p}}$ quan es sobreentengui a quina corba ens referim. El principal resultat sobre els valors $a_{\mathfrak{p}}$ correspon a Hasse, teorema 1.1 del capítol 5 de [26], que permet fitar la seva norma.

Teorema 3.1.7 (Teorema de Hasse)**.** *Sigui E una corba el·líptica definida sobre un cos de q elements. Aleshores*

$$|a_{\mathfrak{p}}| \leq 2\sqrt{q}.$$

La definició anterior d'$a_{\mathfrak{p}}$ és segurament la més intuïtiva, però no és la més útil. Veiem com podem descriure les traces $a_{\mathfrak{p}}$ de manera equivalent.

Definició 3.1.8. *Donat un primer ℓ, definim el mòdul (ℓ-àdic) de Tate com el límit projectiu dels grups $E[\ell^k]$ respecte les aplicacions $[\ell] : E[\ell^{k+1}] \to E[\ell^k]$, és a dir,*

$$T_\ell(E) = \varprojlim_k E[\ell^k].$$

Donat que $E[\ell^k]$ té una estructura natural de $\mathbb{Z}/\ell^k\mathbb{Z}$-mòdul obtenim que $T_\ell(E)$ és de forma natural un $\mathbb{Z}_\ell$-mòdul, és a dir, un mòdul sobre els enters ℓ-àdics. A partir de la classificació anterior dels grups de torsió obtenim directament que quan $\ell \neq car(K)$, es compleix

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

És clar que els endomorfismes de la corba donen lloc a endomorfismes del mòdul de Tate. De la mateixa manera, els elements del grup de Galois $G_K = Gal(\overline{K}|K)$ commuten amb les aplicacions $[\ell]$ i per tant actuen sobre el mòdul de Tate. Obtenim així les representacions

$$\rho_{E,\ell} : G_K \to Aut(T_\ell(E)).$$

del grup de Galois absolut G_K de K.

Elegint una base de $T_\ell(E)$ i considerant l'inclusió $\mathbb{Z}_\ell \subset \mathbb{Q}_\ell$ podem considerar les representacions anteriors com a representacions 2-dimensionals sobre el cos $\mathbb{Q}_\ell$.

Considerem la classe de conjugació $Frob_{\mathfrak{p}}$ en $G_K = G(\overline{K}|K)$ d'algun automorfisme de Frobenius en $\mathfrak{p}$. Si ℓ no divideix $\mathfrak{p}$, llavors la imatge dels elements de $Frob_{\mathfrak{p}}$ per $\rho_{E,\ell}$ no depèn de l'automorfisme de Frobenius triat i pertanyen a una mateixa classe de conjugació de $Aut(T_\ell(E))$. Els elements d'aquesta classe de conjugació tenen un mateix polinomi mínim, i

de fet aquest polinomi és el polinomi mínim de l' automorfisme de Frobenius de la corba $E_{\mathfrak{p}}$. Per tant, les traces d'aquests dos polinomis són iguals i el valor $a_{\mathfrak{p}}(E)$ està determinat a partir de l'estructura de $T_\ell(E)$. És important observar que el polinomi característic de $\rho_{E,\ell}(Frob_{\mathfrak{p}})$ és independent del valor ℓ triat. Aquesta propietat defineix la família $\rho_{E,\ell}$ com una família compatible de representacions en el sentit de Serre (cf. [23]). Aquest concepte és central en la demostració de la conjectura de Sato-Tate.

Coneixent només els valors $a_{\mathfrak{p}}(E)$ d'una corba E podem obtenir informació sobre l'aritmètica de la corba, de manera similar a com els primers d'un cos de nombre K ho fan de l'aritmètica de K. Recordem que per a cossos de nombres aquesta informació queda codificada en les funcions L de K. En el cas de corbes el·líptiques també podem associar a la corba una funció L a partir dels valors $a_{\mathfrak{p}}(E)$. Definirem aquesta funció L com el producte de factors locals associats a cada primer.

Definició 3.1.9. *Sigui E/K una corba el·líptica E sobre un cos finit K de q elements. Definim la funció zeta d'E sobre K com*

$$Z(T,E) = \exp\left(\sum_{n=1}^{\infty} \#E(K_n)\frac{T^n}{n}\right)$$

on K_n/K és l'extensió de K de grau n.

Veiem com simplificar l'expressió anterior. Sigui ϕ l' automorfisme de Frobenius d'E/K. Tal i com hem fet anteriorment, considerem el polinomi característic de ϕ actuant sobre el mòdul de Tate ℓ-èssim, on $\ell \neq q$:

$$\det(T-\phi) = T^2 - aT + q = (T-\alpha)(T-\beta).$$

Aquí, α i β són les arrels complexes conjugades del polinomi. Aquesta descomposició també ens permet veure que $\det(T-\phi^n) = (T-\alpha^n)(T-\beta^n)$. Com que ϕ^n és l' automorfisme de Frobenius de la corba E/K_n obtenim que $\#E(K_n) = 1 + q^n - tr(\phi^n) = 1 + q^n - \alpha^n - \beta^n$. Apliquem aquestes igualtats a $\log Z(T, E(K))$ i obtenim que

$$\begin{aligned}\log Z(T,E) &= \sum_{n=1}^{\infty}(1+q^n-\alpha^n-\beta^n)\frac{T^n}{n} \\ &= -\log(1-T) - \log(1-qT) + \log(1-\alpha T) + \log(1-\beta T).\end{aligned}$$

Per tant es compleix

$$Z(T,E) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} = \frac{1-aT+qT^2}{(1-T)(1-qT)}.$$

A continuació definim la funció L associada a una corba el·líptica E sobre un cos de

nombres K.

Definició 3.1.10. *Si $\mathfrak{p}$ és un primer on E té bona reducció, definim el factor local de la funció L d'E/K com $L_{\mathfrak{p}}(T, E) = 1 - a_{\mathfrak{p}}T + \mathfrak{N}(\mathfrak{p})T^2$.*

Remarquem que, tal i com acabem de veure, es compleix

$$Z(T, E_{\mathfrak{p}}) = \frac{L_{\mathfrak{p}}(T, E)}{(1-T)(1-\mathfrak{N}(\mathfrak{p})T)},$$

fet que justifica la definició anterior.

Els factors $(1-T)(1-\mathfrak{N}(\mathfrak{p})T)$ no donen informació cabdal per als nostres objectius. A més, en la definició posterior de la funció L, es pot comprovar que la funció resultant seria equivalent si utilitzéssim com a factor local $Z(T, E_{\mathfrak{p}})$ enlloc del que hem introduït.

Definició 3.1.11. *Sigui $\mathfrak{p}$ un primer de K on E té mala reducció. El factor local de la funció L d'E/K és*

$$L_{\mathfrak{p}}(T, E) = \begin{cases} 1-T & \text{Si } E \text{ té reducció multiplicativa split en } \mathfrak{p}, \\ 1+T & \text{Si } E \text{ té reducció multiplicativa no split en } \mathfrak{p}, \\ 1 & \text{Si } E \text{ té reducció additiva en } \mathfrak{p}. \end{cases}$$

L'elecció d'aquests factors locals s'explica pel cardinal del conjunt de punts no singulars de la corba reduïda. Si $E_{ns}(\kappa(\mathfrak{p}))$ és el conjunt de punts no singulars de $E_{\mathfrak{p}}(\kappa(\mathfrak{p}))$ obtenim que per a qualsevol primer $\mathfrak{p}$ es compleix la relació $L_{\mathfrak{p}}(1/\mathfrak{N}(\mathfrak{p}), E) = \#E_{ns}(\kappa(\mathfrak{p}))/\mathfrak{N}(\mathfrak{p})$.

Definició 3.1.12. *La funció L associada a la corba el·líptica E definida sobre K és*

$$L(E, s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(\mathfrak{N}(\mathfrak{p})^{-s}, E)^{-1}.$$

Aplicant el Teorema 3.1.7 de Hasse i utilitzant la convergència de les funcions L de Hecke, podem veure que $L(E, s)$ convergeix per tot $\Re(s) > 3/2$. Al voltant d'aquestes funcions L hi ha moltes conjectures. Per exemple, la conjectura de Taniyama-Shimura per corbes el·líptiques sobre $\mathbb{Q}$, de la qual parlarem posteriorment, que va ser resolta recentment per Andrew Wiles. De fet, Wiles va demostrar la conjectura per corbes semiestables, és a dir sense reducció additiva. Aquest resultat va permetre demostrar el famós teorema de Fermat. Posteriorment la conjectura es va demostrar per a totes les corbes el·líptiques $E/\mathbb{Q}$.

3.2 Equidistribució de Frobenii en corbes el·líptiques

Fixem una corba el·líptica E sobre un cos de nombres K. L'objectiu d'aquesta i de les següents seccions és centrar-nos en l'estudi dels possibles valors de $a_{\mathfrak{p}}(E)$ en variar $\mathfrak{p}$ entre els primers de K on E té bona reducció.

Sigui doncs $\mathfrak{p}$ un primer de K on E tingui bona reducció. En aplicar el teorema de Hasse 3.1.7 a la corba reduïda $E_{\mathfrak{p}}$ obtenim que $|a_p| \leq 2\sqrt{\mathfrak{N}(\mathfrak{p})}$. Aquesta fita permet considerar la quantitat

$$a_{\mathfrak{p}}/2\sqrt{\mathfrak{N}(\mathfrak{p})} \in [-1,1]$$

i també l'angle $\theta_{\mathfrak{p}} \in [0,\pi]$ tal que

$$\cos(\theta_{\mathfrak{p}}) = a_{\mathfrak{p}}/2\sqrt{\mathfrak{N}(\mathfrak{p})}.$$

Observem que aquesta definició és equivalent a dir que el polinomi mínim de l'automorfisme de Frobenius de $E_{\mathfrak{p}}$ és $(T - \sqrt{\mathfrak{N}(\mathfrak{p})}e^{i\theta_{\mathfrak{p}}})(T - \sqrt{\mathfrak{N}(\mathfrak{p})}e^{-i\theta_{\mathfrak{p}}})$ amb $\theta_{\mathfrak{p}} \in [0,\pi]$. Si fem variar $\mathfrak{p}$ entre els primers de K on E té bona reducció, obtenim una successió a l'interval $[0,\pi]$. Donat un interval $I \subset [0,\pi]$, podem preguntar-nos per la probabilitat que $\theta_{\mathfrak{p}} \in I$. Definim aquesta probabilitat com

$$P_E(I) = \lim_{x\to\infty} \frac{\#\{\mathfrak{N}(\mathfrak{p}) \leq x | \theta_{\mathfrak{p}} \in I\}}{\#\{\mathfrak{N}(\mathfrak{p}) \leq x\}}.$$

Òbviament, per a poder definir $P_E(I)$ cal que el límit anterior existeixi. Observem que $P_E(I)$ és la densitat natural dels primers $\mathfrak{p}$ tal que $\theta_{\mathfrak{p}} \in I$. Assumint que els límits anteriors existeixen, podem preguntar-nos per l'existència d'alguna mesura μ_E a $[0,\pi]$ tal que

$$\int_I \mu_E = P_E(I).$$

Per tant, entendre com es distribueixen els valors $a_{\mathfrak{p}}$ és equivalent a conèixer la mesura μ_E. En les properes seccions ens dediquem a estudiar aquest problema, amb especial èmfasis en el cas que el cos de definició de la corba és $\mathbb{Q}$.

3.3 Corbes el·líptiques amb CM

Sigui $E/\mathbb{Q}$ una corba el·líptica amb CM i sigui μ_E la mesura associada a E en la secció anterior.

Teorema 3.3.1. *Es té*

$$\mu_E = \frac{1}{2}\mu_{unif} + \frac{1}{2}\delta_{\pi/2},$$

on $\delta_{\pi/2}$ és la mesura associada a la funció delta en el punt $\pi/2$ i μ_{unif} és la mesura uniforme

en $[0, \pi]$.

És a dir, una meitat dels θ_p compleixen $\theta_p = \pi/2$ i l'altre meitat es distribueix uniformement en $[0, \pi]$.

A continuació expliquem la demostració d'aquest resultat. Aquest teorema s'obté a partir dels resultats obtinguts per Max Deuring i Erich Hecke, els quals resumim a continuació.

Sigui doncs una corba el·líptica E sobre $\mathbb{Q}$ amb multiplicació complexa, i sigui $K = End^0(E)$. Com hem vist $K/\mathbb{Q}$ és una extensió quadràtica imaginària. Deuring va demostrar que la L-sèrie associada a E és una L-sèrie de Hecke associada a un Größencharakter ψ de K. De fet, els resultats obtinguts per Deuring són més amplis però no és necessari presentar-los per al nostre cas. Podem consultar els resultats que presentarem a continuació en [27].

El Größencharakter ψ es defineix com un caràcter sobre el grup d'idèles de K i la seva imatge està inclosa en el cos K. Tampoc és oportú definir formalment aquest caràcter, en canvi si descrivim la seva principal propietat. Sigui $\mathfrak{p}$ un primer de $\mathbb{Q}$ on E té bona reducció. Considerem $E_\mathfrak{p}$ com la corba E reduïda mòdul $\mathfrak{p}$ i $\phi_\mathfrak{p}$ l'endomorfisme de Frobenius de $E_\mathfrak{p}$. Segons aquestes definicions es compleix que el diagrama següent commuta

$$\begin{array}{ccc} E & \xrightarrow{[\psi(\mathfrak{p})]} & E \\ \downarrow & & \downarrow \\ E_\mathfrak{p} & \xrightarrow{\phi_\mathfrak{p}} & E_\mathfrak{p} \end{array}$$

on $[\psi(\mathfrak{p})]$ és la isogènia associada a l'element $\psi(\mathfrak{p})$ de K.

Podem comprovar els següents resultats sobre el caràcter ψ. Sigui p un primer on E té bona reducció. Llavors es compleix:

- Si p descomposa a K com $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ llavors $a_p = \psi(\mathfrak{p}) + \psi(\mathfrak{p}')$ i $\psi(\mathfrak{p})\psi(\mathfrak{p}') = p$.
- Si p és inert a K i per tant $p\mathcal{O}_K = \mathfrak{p}$, obtenim la igualtat $a_p = 0$ i $\psi(\mathfrak{p}) = -p$.
- Si p ramifica a K llavors E té mala reducció additiva en p.

Segons aquests resultats obtenim que per als primers on E té bona reducció, $E_\mathfrak{p}$ és

- ordinària si p descomposa a K,
- supersingular si p és inert a K.

Utilitzant el teorema de Chebotarev sabem que la densitat dels primers que són inerts a K és $1/2$. Aquest resultat ens permet concloure que la meitat dels primers compleixen $a_p = 0$, o

equivalentment $\theta_p = \pi/2$. Per veure la distribució uniforme de la resta de primers és necessari veure la igualtat entre les L-sèries d'E i de ψ. Recordem que el factor local de la L-sèrie de ψ en un primer $\mathfrak{p}$ de K és $L_{\mathfrak{p}}(s,\psi) = 1 - \psi(\mathfrak{p})(\mathfrak{N}\mathfrak{p})^{-s}$. Veiem les igualtats entre els factors locals.

- Si p descomposa a K com $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ llavors

$$L_p(s,E) = 1 - a_p p^{-s} + p^{1-2s} = 1 - (\psi(\mathfrak{p}) + \psi(\mathfrak{p}'))p^{-s} + \psi(\mathfrak{p})\psi(\mathfrak{p}')p^{-2s} =$$
$$= (1 - \psi(\mathfrak{p})(\mathfrak{N}\mathfrak{p})^{-s})(1 - \psi(\mathfrak{p}')(\mathfrak{N}\mathfrak{p}')^{-s}) = L_{\mathfrak{p}}(s,\psi)L_{\mathfrak{p}'}(s,\psi)$$

- Si p és inert a K i $p\mathcal{O}_K = \mathfrak{p}$ llavors

$$L_p(s,E) = 1 - a_p p^{-s} + p^{1-2s} = 1 - 0 \cdot p^{-s} - (-p)p^{-2s} =$$
$$= 1 - \psi(\mathfrak{p})p^{-2s} = 1 - \psi(\mathfrak{p})(\mathfrak{N}\mathfrak{p})^{-s} = L_{\mathfrak{p}}(s,\psi)$$

- Si p ramifica a K i per tant $p\mathcal{O}_K = \mathfrak{p}^2$ llavors

$$L_p(s,E) = 1 = L_{\mathfrak{p}}(s,\psi)$$

Obtenim així

Teorema 3.3.2 (Deuring)**.** *Segons les notacions anteriors es compleix*

$$L(E,s) = L(s,\psi)$$

Aquesta igualtat ens permet deduir resultats sobre la L-sèrie d'E a partir de resultats de les L-sèries de Hecke. Això ens permet demostrar que els valors a_p pels primers p on la corba reduïda és ordinària es distribueixen uniformement en $[0,\pi]$. En la secció 5.1 revisarem aquest resultat, interpretant d'una mateixa manera la distribució per totes les corbes, tinguin o no multiplicació complexa.

3.4 Corbes el·líptiques sense CM: la distibució de Sato-Tate

La conjectura de Sato-Tate prediu la solució a aquest problema per a corbes sense multiplicació complexa.

Conjectura 3.4.1 (Sato-Tate)**.** *Sigui K un cos de nombres i sigui E/K una corba el·líptica sense CM. Llavors μ_E té funció de densitat $\frac{2}{\pi}\sin^2(x)$, és a dir, la probabilitat que es compleixi $a \leq \theta_{\mathfrak{p}} \leq b$ és*

$$P_E([a,b]) = \frac{2}{\pi}\int_a^b \sin^2(x)dx.$$

Cal destacar que la distribució és independent de la corba. Aquesta distribució s'anomena la distribució de Sato-Tate. Per ser precisos, hem de dir que la conjectura de Sato-Tate clàssica es va formular per al cas $K = \mathbb{Q}$. Mikio Sato i John Tate, a través de treballs independents, van proposar al voltant del 1960 la conjectura per a corbes el·líptiques sobre el cos $\mathbb{Q}$ dels nombres racionals. Tot i això ens referirem a la conjectura 3.4.1 com la conjectura de Sato-Tate, que generalitza el plantejament clàssic sobre corbes el·líptiques sobre $\mathbb{Q}$.

L'any 2006, Richard Taylor, conjuntament amb altres matemàtics, va publicar una demostració de la conjectura de Sato-Tate per a corbes el·líptiques E/K sobre cossos totalment reals K amb $j(E) \notin \mathcal{O}_K$. Aquesta condició es compleix per exemple quan E té reducció multiplicativa en algun primer de K.

La demostració completa de la conjectura de Sato-Tate queda fora de l'abast d'aquest treball. Tot i així, utilitzant la teoria de Serre podem presentar els procediments per a demostrar el teorema de Taylor. Per a la resta de cossos no es coneix una demostració de la conjectura i representa avui dia un àmbit de recerca en matemàtiques. És interessant consultar [16] per trobar una introducció més lleugera de la demostració de la conjectura de Sato-Tate 3.4.1. I com a resum de la presentació posterior també és útil la presentació realitzada en [21].

Per seguir el procediment realitzat per Taylor és interessant recordar la demostració dels teoremes de Dirichlet i Chebotarev. En ambdós casos definíem funcions L, les funcions L de Dirichlet i de Hecke, associades al conjunt de primers dels quals volíem concloure el resultat d'equidistribució. A partir dels resultats sobre caràcters induïts podíem deduir la no-anul·lació de les funcions L en $s = 1$ i deduir així els resultats enunciats. El procediment per a demostrar la conjectura de Sato-Tate segueix el mateix esquema. En aquest cas, les funcions L vindran definides a partir de certes representacions de grups associades a la corba el·líptica. La part més complicada correspon a demostrar la no-anul·lació d'aquestes funcions L, fet que es demostra tot utilitzant el teorema de Brauer sobre caràcters induïts.

3.5 La demostració de Taylor: una aplicació de la teoria de Serre

Veiem com presentar la conjectura de Sato-Tate a través de la teoria de Serre. Sigui K un cos de nombres. Fixem una corba el·líptica E definida sobre K sense multiplicació complexa. Definim el conjunt Σ com el conjunt de primers de K on E té bona reducció i Nv com la norma de $v \in \Sigma$.

La notació de v per denotar els primers de K pot semblar poc apropiada però cal interpretar aquesta notació a partir de la teoria de valoracions. Podem trobar una descripció d'aquesta teoria a [19].

La definició menys intuïtiva correspon a la del grup topològic compacte G, i cal motivar-la adequadament.

Recordem que la conjectura 3.4.1 de Sato-Tate estudia la distribució dels valors $a_{\mathfrak{p}}(E)$, la traça dels Frobenius de les corbes reduïdes.

Escrivint $\cos(\theta_{\mathfrak{p}}(E)) = a_{\mathfrak{p}}/2\sqrt{\mathfrak{N}(\mathfrak{p})}$ podríem interpretar aquests valors en l'interval $[0,\pi]$. Per tant podria semblar natural considerar $G = [0,\pi]$, identificar $[0,\pi]$ amb $\mathbb{R}/\pi\mathbb{Z}$, i introduir la família $\{x_v = \theta_v(E)\}$. És senzill comprovar que la mesura de Haar associada al grup topològic $\mathbb{R}/\pi\mathbb{Z}$ és la mesura uniforme. Això ens portaria però a la conclusió que els valors $\theta_{\mathfrak{p}}(E)$ estan equidistribuïts respecte una mesura que no és pas la mesura de Sato-Tate, i que no està d'acord amb els experiments numèrics que fàcilment es poden realitzar. És clar doncs que l'elecció $G = \mathbb{R}/\pi\mathbb{Z}$ no permet demostrar l'equidistribució plantejada.

L'elecció oportuna del grup G és el grup $SU(2)$ de les matrius complexes unitàries de dimensió 2 amb determinant 1. Tots els elements d'una mateixa classe de conjugació de $SU(2)$ tenen el mateix polinomi característic, i de fet les classes de conjugació estan unívocament determinades a partir del polinomi característic dels seus elements. Observem que el polinomi característic d'un element $x \in SU(2)$ és de la forma $T^2 - aT + 1$, on a és la traça del polinomi característic. Per tant, la classe de conjugació de x està determinada a partir d'a. Si factoritzem $T^2 - aT + 1 = (T-\alpha)(T-\beta)$ veiem que $|\alpha| = |\beta| = 1$ i $\bar{\alpha} = \beta$, ja que les matrius són unitàries.

Així doncs $a = \alpha + \bar{\alpha} = 2\Re(\alpha) \in [-2,2]$ i per tant les classes de conjugació de $SU(2)$ estan en bijecció amb el conjunt $[-2,2]$.

Donat $v \in \Sigma$ procedim a definir x_v. La corba E té bona reducció en v, per definició de Σ, i per tant podem considerar el morfisme de Frobenius ϕ de la corba reduïda. Com ja hem vist, $a_v(E)$ és la traça del polinomi característic de ϕ i el teorema 3.1.7 de Hasse implica que

$$|a_v(E)| \leq 2\sqrt{Nv}.$$

Per tant $a_v(E)/\sqrt{Nv} \in [-2,2]$ i definim x_v com la classe de conjugació de G corresponent a $a_v(E)/\sqrt{Nv}$. Observem que el polinomi característic de x_v és $\det(T - \phi/\sqrt{\mathfrak{N}(\mathfrak{p})})$.

Un cop presentada la notació, expliquem a continuació de quina manera la Conjectura 3.4.1 de Sato-Tate és conseqüència del Corol·lari 2.1.6, en cas que les hipòtesis d'aquest enunciat es satisfessin.

Suposem doncs que $(x_v)_{v\in\Sigma}$ està equidistribuït respecte la mesura de Haar $\mu_{SU(2)}$ de $SU(2)$. Com ja hem vist, podem definir una aplicació bijectiva entre les classes de conjugació de $SU(2)$ i $[-2,2]$. Composant amb l'aplicació de $[-2,2]$ a $[0,\pi]$ definida per $x \mapsto \arccos(x/2)$ obtenim una bijecció h entre les classes de conjugació de $SU(2)$ i $[0,\pi]$. Podem doncs consi-

derar la mesura μ de $[0,\pi]$ induïda a partir de la mesura de Haar de $SU(2)$, és a dir,

$$\mu = h_*(\mu_{SU(2)}).$$

És clar que si $(x_v)_{v\in\Sigma}$ està $\mu_{SU(2)}$-equidistribuït llavors $(h(x_v))_{v\in\Sigma}$ està μ-equidistribuït. Podem trobar l'expressió de la mesura $h_*(\mu_S U(2))$ a [9], obtenint que la mesura $h_*(\mu_S U(2))$ és $2/\pi \sin^2(x)dx$. Observem a més que $h(x_v)$ és el valor θ_v presentat a la conjectura 3.4.1 de Sato-Tate i per tant $(\theta_v)_{v\in\Sigma}$ està equidistribuït respecte la mesura de Sato-Tate.

Més concretament, fixem un interval $I \subset [0,\pi]$. Prenem una successió de funcions contínues $(\phi_n)_{n\in\mathbb{Z}}$ amb límit la funció característica de I. Com que $(\theta_v)_{v\in\Sigma}$ està μ-equidistribuït es compleix que

$$\int_{[0,\pi]} \phi_n \mu = \lim_{x\to\infty} \frac{\sum_{Nv\leq x} \phi_n(\theta_v)}{\sum_{Nv\leq x} 1}.$$

Prenent el límit per $n \to \infty$ obtenim que

$$\int_I \mu = \lim_{n\to\infty} \int_{[0,\pi]} \phi_n \mu = \lim_{x\to\infty} \frac{\#\{p \leq x | \theta_p \in I\}}{\#\{p \leq x\}} = P_E(I).$$

I per tant $\frac{2}{\pi}\sin^2(x)dx = \mu = \mu_E$, el que demostra la conjectura de Sato-Tate tal i com l'hem enunciat.

Per tant, per a poder demostrar la conjectura de Sato-Tate utilitzant la teoria de Serre és suficient veure que es compleixen les hipòtesis del corol·lari 2.1.6. Comencem veient que la hipòtesi (1) definida en la teoria de Serre es compleix sempre en el cas que estem tractant, i que de fet només depèn del cos K. Per comprovar la hipòtesi (1) cal veure que la funció L associada al caràcter trivial ρ_0 defineix una funció holomorfa i no nul·la en $\Re(s) \geq 1$, excepte per un pol simple en $s = 1$. Recordem que

$$L(s,\rho_0) = \prod_{v\in\Sigma} \frac{1}{1-(Nv)^{-s}}$$

i com ja hem comentat depèn únicament de Σ i dels valors Nv. Observem que en el nostre cas la funció $L(s,\rho_0)$ és, llevat d'un nombre finit de factors, la funció Zeta de Dedekind $\zeta_K(s)$.

Com ja hem vist quan demostràvem el teorema de Chebotarev, la funció $\zeta_K(s)$ defineix una funció holomorfa i no nul·la en $\Re(s) \geq 1$ excepte per un pol simple en $s = 1$. Per tant, com que $L(s,\rho_0)$ i $\zeta_K(s)$ difereixen d'un nombre finit de factors, tots ells no nuls en $\Re(s) \geq 1$, llavors es compleix la hipòtesi (1).

Obtenim doncs que per demostrar la conjectura de Sato-Tate ens cal demostrar que per

tot caràcter irreductible no trivial ρ de $SU(2)$, la funció

$$L(s,\rho)=\prod_{v\in\Sigma}\frac{1}{\det(1-\rho(x_v)(Nv)^{-s})}$$

estén a una funció holomorfa i no nul·la en $\Re(s)\geq 1$.

Presentem breument alguns resultats sobre representacions de grups, els quals podem consultar a [4].

Sigui ρ una representació 2-dimensional d'un grup G. Donat $n\in\mathbb{N}$ considerem la representació $(n+1)$-dimensional $Symm^n\rho$ definida com la n-èssima potència simètrica de la representació ρ. Veiem com podem interpretar $Symm^n\rho$.

Fixat $g\in G$ tenim $\det(T-\rho(g))=(T-\alpha)(T-\beta)$. És a dir, els valors propis de $\rho(g)$ són $\{\alpha,\beta\}$. Llavors es compleix que els valors propis de $Symm^n\rho(g)$ és el conjunt de valors $\{\alpha^{n-i}\beta^i|0\leq i\leq n\}$.

Considerem la representació 2-dimensional natural r de $SU(2)$. Llavors es compleix que tota representació irreductible de $SU(2)$ és equivalent a $Symm^n r$ per algun n (cf. [4]). Fixat $v\in\Sigma$ ja hem vist que $\det(T-r(x_v))=(T-e^{i\theta_v})(T-e^{-i\theta_v})$. Per tant els valors propis de $Symm^n r(x_v)$ és el conjunt de valors $\{e^{i(n-2i)\theta_v}|0\leq i\leq n\}$. Segons aquestes definicions obtenim que

$$L(s,Symm^n r)=\prod_{v\in\Sigma}\prod_{i=0}^{n}\frac{1}{1-e^{i(n-2i)\theta_v}(Nv)^{-s}}.$$

Fixat ℓ considerem la representació $\rho_{E,\ell}$ i les seves n-èssimes potències simètriques $Symm^n\rho_{E,\ell}$. Recordant que $\det(T-\rho_{E,\ell}(\phi_v))=(T-\sqrt{\mathfrak{N}(v)}e^{i\theta_v})(T-\sqrt{\mathfrak{N}(v)}e^{-i\theta_v})$ definim la L-sèrie associada a la representació $Symm^n\rho_{E,\ell}$

$$L(s,Symm^n\rho_{E,\ell})=\prod_{v\in\Sigma}\prod_{i=0}^{n}\frac{1}{1-\sqrt{\mathfrak{N}v}^n e^{i(n-2i)\theta_v}(\mathfrak{N}v)^{-s}}.$$

Segons aquestes definicions està clar que es compleix la relació

$$L(s,Symm^n r)=L(s-n/2,Symm^n\rho_{E,\ell}).$$

Aquesta igualtat i el fet que totes les representacions irreductibles no trivials de $SU(2)$ siguin de la forma $Symm^n r$ implica que la conjectura de Sato-Tate es pugui deduir a partir de la següent conjectura.

Conjectura 3.5.1 (Tate)**.** *Sigui E/K una corba el·líptica sense CM definida sobre un cos de nombres K. Llavors $L(s,Symm^n\rho_{E,\ell})$ defineix una funció holomorfa i no nul·la en $\Re(s)\geq$*

$1 + n/2$.

Aquesta conjectura va ser plantejada per John Tate en [28]. Per demostrar aquest resultat sobre les funcions $L(s, Symm^n \rho_{E,\ell})$ és necessari introduir les representacions automorfes de $GL_n(\mathbb{A}_F)$, el grup general lineal de grau n sobre l'anell d'adeles d'un cos F.

No entrarem en aquesta teoria ni presentarem les notacions necessàries ja que excedeixen el propòsit de la nostra presentació. Per aquesta raó les definicions i resultats s'han d'interpretar com una guia sense els detalls tècnics dels resultats formals. Deixem pels lectors més avesats en el tema la correcta interpretació dels resultats que presentem. Podem interpretar el concepte de representació automorfa com una generalització de forma modular. Podem consultar les definicions necessàries en [5].

També ens caldria definir les representacions automorfes cuspidals com un anàleg de les formes modulars cuspidals. Donada una representació automorfa cuspidal π de $GL_n(\mathbb{A}_F)$ podem construir la L-sèrie associada $L(s, \pi)$. Es compleix que $L(s, \pi)$ és holomorfa i no nul·la en $\Re(s) \geq (n+1)/2$. Aquesta última propietat és la principal propietat que ens interessa sobre les representacions automorfes, el que justifica que no fem cap introducció a les definicions oportunes.

Donada una representació automorfa podem construir una representació del grup $G_F = G(\overline{F}|F)$. Direm que una representació r de grau n de G_F és automorfa si prové d'alguna representació π de $GL_n(\mathbb{A}_F)$. Si a més π és cuspidal, també direm que r ho és. Llavors es compleix que $L(s, r) = L(s, \pi)$, i per tant si π és cuspidal llavors $L(s, r)$ és holomorfa i no nul·la en $\Re(s) \geq (n + 1)/2$. A més, si r és automorfa llavors també ho són les representacions equivalents a r.

Veiem com podem utilitzar aquest resultat sobre representacions automorfes per demostrar la conjectura de Sato-Tate. Recordem que $Symm^n \rho_{E,\ell}$ és una representació de G_K de grau $n+1$ i per tant té sentit suposar que $Symm^n \rho_{E,\ell}$ prové d'una representació automorfa cuspidal π de $GL_{n+1}(\mathbb{A}_K)$. Llavors $L(s, \pi)$ és holomorfa i no nul·la en $\Re(s) \geq 1 + n/2$ i per tant també ho seria $L(s, Symm^n \rho_{E,\ell})$. Així doncs, si per tot n es té que $Symm^n \rho_{E,\ell}$ és automorfa cuspidal llavors es compleix la conjectura de Tate 3.5.1. Així doncs la conjectura 3.4.1 de Sato-Tate és certa si es compleix:

Conjectura 3.5.2 (Langlands)**.** *Sigui E una corba el·líptica sense CM definida sobre un cos de nombres K. Llavors per tot n la representació $Symm^n \rho_{E,\ell}$ és automorfa cuspidal.*

És interessant donar un context històric a aquesta conjectura per veure la seva transcendència dintre del desenvolupament de les matemàtiques en els últims anys. Observem que la Conjectura 3.5.2 de Langlands és un cas de la conjectura 2.2.1 d'Artin. Aquestes dues conjectures formen part del que és conegut com el programa de Langlands. Podem consultar [5], [14] per més informació sobre el programa de Langlands, incloent la conjectura 3.5.2. Aquest

programa associa representacions automorfes a objectes de la teoria de nombres i de la geometria algebraica, tot obtenint igualtats entre L-sèries com a l'anterior conjectura. Moltes de les conjectures del programa de Langlands encara estan obertes. Per veure l'importància de les conjectures plantejades per aquest programa és suficient comentar que el teorema de Wiles es pot interpretar com un cas particular de la conjectura anterior. De fet, el teorema de Wiles demostra el teorema de modularitat, abans conegut com a conjectura de Taniyama-Shimura, per algunes corbes el·líptiques. Recordem l'enunciat d'aquest teorema.

Teorema 3.5.3 (Teorema de modularitat)**.** *Sigui E una corba el·líptica sobre $\mathbb{Q}$. Llavors existeix una forma modular cuspidal f de $GL_2(\mathbb{A}_{\mathbb{Q}})$ tal que*

$$L(s, f) = L(E, s),$$

on $L(s, f)$ és la L-sèrie associada a f.

Per a corbes amb CM, el teorema de modularitat és el teorema 3.3.2. Per a corbes sense CM, el teorema 3.5.3 és de fet un cas particular de la conjectura 3.5.2, prenent $n = 1$. Això es deu a que les representacions automorfes cuspidals de $GL_2(\mathbb{A}_K)$ les podem interpretar com a formes modulars cuspidals, i $L(s, Symm^1 \rho_{E,\ell})$ com $L(E, s)$. Podem consultar [29] per més informació sobre 3.5.3.

El teorema de Wiles va permetre demostrar el que segurament és un dels teoremes matemàtics més famosos, l'últim teorema de Fermat. Per ser precisos, la demostració de l'últim teorema de Fermat depèn del teorema de Ribet, antigament conegut com la conjectura èpsilon. Segons el teorema de Ribet, si existís un contraexemple del teorema de Fermat podríem construir una corba el·líptica que no compliria el teorema de modularitat.

Podem interpretar la conjectura 3.5.2 com la generalització més natural del teorema 3.5.3. En els últims anys s'ha treball en la demostració de la conjectura 3.5.2, però encara no s'ha demostrat en tota generalitat. Veiem alguns resultats sobre la demostració d'aquesta conjectura.

- Com hem comentat, el cas $n = 1$ és el teorema de modularitat.
- El cas $n = 2$ és pot demostrar a partir del treball de Gelbart-Jacquet (veure [6]).
- Per $n = 3$ va ser demostrat per Kim-Shahidi (veure [12]).
- El cas $n = 4$ va ser comprovat recentment per Kim (veure [13]).
- Per $n \geq 5$ també hi ha alguns resultats, essencialment de Kim, però cap demostració genèrica.

Per tant, per demostrar la conjectura de Sato-Tate 3.4.1, cal buscar un mètode alternatiu a la conjectura 3.5.2. Per aquest propòsit cal considerar el treball realitzat per Richard Taylor.

La primera part d'aquest treball es basa en demostrar una versió més dèbil de la conjectura 3.5.2, i només per cossos totalment reals. Per això ens cal una noció de representació automorfa menys restrictiva.

Donada una representació r de G_K direm que és potencialment automorfa si existeix una extensió de Galois $F|K$ amb F totalment real de manera que $r|_{G_F}$, la restricció de r a G_F, és automorfa. Definim el concepte de potencialment automorfa cuspidal de manera anàloga. Utilitzant aquesta definició, es pot demostrar una versió més dèbil de la conjectura 3.5.2 però que permet demostrar la conjectura de Sato-Tate 3.4.1. El següent teorema és el teorema 4.1 de [7], el qual està presentat en una versió més general.

Teorema 3.5.4 (Taylor)**.** *Sigui E una corba el·líptica sense CM sobre un cos de nombres K totalment real. Suposem a més que E té reducció multiplicativa en algun primer. Llavors $Symm^n\rho_{E,\ell}$ és potencialment automorfa cuspidal per tot n.*

Veiem com deduir la conjectura de Tate 3.5.1 a partir d'aquest teorema. Considerem doncs una extensió de Galois $F|K$ amb F totalment real de manera que $Symm^n\rho_{E,\ell}|_{G_F}$ és automorfa cuspidal. Llavors, segons el resultat de canvi de base de Langlands obtenim que per tot cos intermig $K \subseteq L \subseteq F$ amb $F|L$ resoluble, la restricció de $Symm^n\rho_{E,\ell}$ a G_L també és automorfa cuspidal. Per tant existeix una representació π_L de manera que $Symm^n\rho_{E,\ell}|_{G_L}$ prové de π_L i $L(\pi_L, s) = L(Symm^n\rho_{E,\ell}|_{G_L}, s)$.

Per altra banda, gràcies al teorema de representació de Brauer podem descomposar el caràcter trivial $\mathbf{1}$ de $G(F|K)$ com

$$\mathbf{1} = \sum_{i\in I} n_i Ind_{G(F|F_i)}^{G(F|K)}\chi_i$$

on I és un conjunt finit i per cada $i \in I$ es té $n_i \in \mathbb{Z}$, $K \subseteq F_i \subseteq F$ amb $F|F_i$ resoluble, i χ_i una representació 1-dimensional de $G(F|F_i)$. El caràcter $Ind_{G(F|F_i)}^{G(F|K)}\chi_i$ és el caràcter induït per la inclusió natural de $G(F|F_i)$ en $G(F|K)$. Consultar [4] per trobar la definició de caràcter induït, i també de la suma i producte de representacions que utilitzarem a continuació.

És clar que $L(Symm^n\rho_{E,\ell}, s) = L(Symm^n\rho_{E,\ell}\otimes\mathbf{1}, s)$, ja que la representació $Symm^n\rho_{E,\ell}\otimes\mathbf{1}$ és equivalent a $Symm^n\rho_{E,\ell}$. Utilitzant la descomposició anterior de la representació trivial i sabent que la L-sèrie de la suma de representacions és el producte de les L-sèries de les representacions obtenim que

$$L(Symm^n\rho_{E,\ell}, s) = \prod_i L(Symm^n\rho_{E,\ell}\otimes Ind\chi_i, s)^{n_i}.$$

Observem que la representació $Ind\ \chi_i$ s'ha d'interpretar com a representació de G_K. Utilitzem ara que la L-sèrie dels caràcters és la mateixa que la L-sèrie dels caràcters induïts. Com que el caràcter induït $Ind\ \chi_i$ prové del caràcter χ_i de G_{F_i}, cal restringir $Symm^n\rho_{E,\ell}$ a

G_{F_i}. Per tant es compleix

$$L(Symm^n \rho_{E,\ell} \otimes Ind\ \chi_i, s) = L(Symm^n \rho_{E,\ell}|_{G_{F_i}} \otimes \chi_i, s).$$

Com ja hem comentat, segons el teorema 3.5.4 existeix una representació π_{F_i} de manera que $Symm^n \rho_{E,\ell}|_{G_{F_i}}$ prové de π_{F_i} i $L(\pi_{F_i}, s) = L(Symm^n \rho_{E,\ell}|_{G_{F_i}}, s)$. Per tant, segons els resultats anteriors obtenim

$$L(Symm^n \rho_{E,\ell}, s) = \prod_i L(\pi_{F_i} \otimes \chi_i, s)^{n_i}.$$

Finalment, només cal comprovar que el producte $\pi_{F_i} \otimes \chi_i$ manté les propietats de π_{F_i}. Llavors, com que π_{F_i} és una representació automorfa cuspidal de $GL_{n+1}(\mathbb{A}_{F_i})$, la L-sèrie $L(\pi_{F_i} \otimes \chi_i, s)$ és holomorfa i no nul·la en $\Re(s) \geq 1 + n/2$.

Per tant podem deduir la conjectura 3.4.1 de Sato-Tate utilitzant el teorema 3.5.4. Veiem com demostrar el teorema 3.5.4. El concepte principal per a la demostració és el de família compatible de representacions. Considerem la família de representacions $\{\rho_{E,\ell}\}_\ell$. Anteriorment ja hem comentat que formaven una família compatible de representacions en el sentit de Serre, ja que el polinomi característic de $\rho_{E,\ell}(Frob_\mathfrak{p})$ té coeficients enters, independentment de ℓ. Formalitzem aquest concepte.

Definició 3.5.5. *Sigui K un cos de nombres i $\{\rho_\ell : G_K \to GL_n(\mathbb{Q}_l)\}_\ell$ una família de representacions indexada pels primers de $\mathbb{Z}$. Direm que és una família compatible si per cada primer $\mathfrak{p}$ de K, excepte un nombre finit, existeix un polinomi mònic $P_\mathfrak{p}(x)$ de $\mathbb{Q}[x]$ de manera que el polinomi característic de $\rho_\ell(Frob_\mathfrak{p})$ coincideixi amb $P_\mathfrak{p}(x)$.*

Segons aquesta definició, és clar que $\{\rho_{E,\ell}\}_\ell$ és una família compatible de representacions. També podem comprovar que la família $\{Symm^n \rho_{E,\ell}\}_\ell$ és una família compatible de representacions per a tot n. El resultat principal sobre les famílies compatibles de representacions és el següent.

Teorema 3.5.6. *Considerem una família compatible de representacions. Si una representació de la família és automorfa llavors totes les representacions de la família són automorfes.*

Segons aquest teorema, si $Symm^n \rho_{E,\ell}$ és automorfa per a algun ℓ, llavors també ho són $Symm^n \rho_{E,\ell'}$ per a qualsevol ℓ'. Així doncs, per a demostrar el teorema 3.5.4 ens cal demostrar que $Symm^n \rho_{E,\ell}$ és potencial automorfa cuspidal per algun ℓ.

Per aquest propòsit és necessari introduir el teorema d'aixecament de la modularitat de Taylor, que expliquem a continuació.

Donada una representació $r : G_K \to GL_n(\overline{\mathbb{Q}_l})$ podem construir la representació $\bar{r} : G_K \to GL_n(\overline{\mathbb{F}_\ell})$ projectant sobre el cos residual de $\overline{\mathbb{Q}_l}$. Anomenem a $\bar{r}$ la representació residual de r.

Definició 3.5.7. *Diem que una representació $r_0 : G_K \to GL_n(\overline{\mathbb{F}_\ell})$ és automorfa si existeix una representació automorfa $r : G_K \to GL_n(\overline{\mathbb{Q}_l})$ tal que $\bar{r} = r_0$.*

Així doncs si r és automorfa llavors $\bar{r}$ també és automorfa. En canvi si $\bar{r}$ és automorfa no podem afirmar que r sigui automorfa. Podem preguntar-nos doncs sota quines condicions, si $\bar{r}$ és automorfa llavors també ho és r. Aquest problema és conegut com el problema d'aixecament de la modularitat. El problema d'aixecament de la modularitat és un problema de gran interès avui dia, i és en els últims anys quan s'han obtingut resultats importants. Els teoremes que permeten, sota les hipòtesis necessàries, resoldre el problema d'aixecament de la modularitat són coneguts com teoremes d'aixecament de la modularitat. Les hipòtesis dels teoremes de modularitat poden ser tant sobre les representacions r i $\bar{r}$ com sobre el cos K.

Com a exemple de teorema d'aixecament de la modularitat tenim el teorema d'aixecament de la modularitat de Taylor, el qual podem consultar en [1]. No és possible descriure les hipòtesis d'aquest teorema en la presentació que estem realitzant. Comentem però que el teorema d'aixecament de la modularitat de Taylor considera representacions de G_K amb K totalment real. Per demostrar el teorema 3.5.4 s'utilitza el teorema d'aixecament de la modularitat de Taylor, i per tant és necessari considerar K totalment real en l'enunciat del teorema 3.5.4.

Veiem com podem utilitzar el teorema d'aixecament de la modularitat per a demostrar el teorema 3.5.4. Considerem dues representacions $\rho, r : G_K \to GL_n(\overline{\mathbb{Q}_l})$. Suposem que existeixen dues representacions $\rho', r' : G_K \to GL_n(\overline{\mathbb{Q}_{l'}})$ de manera que

- ρ i ρ' formen part d'una família compatible de representacions.
- r i r' formen part d'una família compatible de representacions.
- $\overline{r'} \cong \overline{\rho'}$, és a dir, $\overline{\rho'}$ és equivalent a $\overline{r'}$.

Llavors si r és automorfa també ho és r' gràcies a la proposició 3.5.6. Per tant $\overline{r'}$ també ho és, ja que és la reducció de r'. Com que $\overline{r'} \cong \overline{\rho'}$, llavors $\overline{\rho'}$ també és automorfa. Suposem que podem aplicar un teorema d'aixecament de la modularitat a $\overline{\rho'}$ per obtenir que ρ' és automorfa. Llavors per 3.5.6 obtenim que ρ és automorfa.

Per demostrar el teorema de Taylor 3.5.4 aplicarem successivament l'esquema que acabem de descriure per a diverses representacions. El següent pas de la demostració consisteix a construir una família de representacions que ens permeti aplicar el raonament anterior. Per a aquest propòsit, cal construir una corba el·líptica E' definida sobre una extensió de Galois $F|K$ amb F totalment real. No detallarem la construcció de E' ni de F, però si cal comentar que per a construir la corba E', utilitzem la hipòtesi que E tingui reducció multiplicativa en algun primer de K. A més, una de les propietats que imposem és $\bar{\rho}_{E,\ell} \cong \bar{\rho}_{E',\ell}$. I per tant també $Symm^n \bar{\rho}_{E,\ell} \cong Symm^n \bar{\rho}_{E',\ell}$.

Finalment, cal considerar una extensió de Galois $F'|F$ amb F' totalment real i una família compatible de representacions $\{r_\ell\}_\ell$ de $G_{F'}$ de manera que

- $\overline{r_{\ell'}} \cong Symm^n \bar{\rho}_{E',\ell'}$.
- $\overline{r_{\ell''}} \cong \overline{Ind\ \theta}$ on θ és una representació automorfa de G_M i $M|F'$ és una extensió de grau dos amb M completament imaginari, de fet M és un cos de multiplicació complexa. $Ind\ \theta$ denota la representació induïda a $G_{F'}$.

Per poder demostrar els resultats posteriors, seria necessari imposar més condicions sobre la família $\{r_\ell\}_\ell$ però no és possible introduir-les en el context d'aquesta presentació. Si la família $\{r_\ell\}_\ell$ existeix, llavors podem obtenir que $Symm^n \rho_{E',\ell}$ és automorfa a partir del fet que la representació θ és automorfa.

Com que θ és automorfa sobre M, llavors $Ind\ \theta$ és automorfa sobre F'. Per tant la seva reducció $\overline{Ind\ \theta}$ és automorfa. Si $\overline{Ind\ \theta}$ és automorfa llavors $\overline{r_{\ell''}}$ és automorfa i utilitzant el teorema d'aixecament de la modularitat de Taylor també ho és $r_{\ell''}$. Com que $r_{\ell'}$ pertany a la mateixa família que $r_{\ell''}$, obtenim que $r_{\ell'}$ és automorfa i per tant $\overline{r_{\ell'}}$ també. Per tant $Symm^n \bar{\rho}_{E',\ell'}$ és automorfa i tornant a utilitzar el teorema d'aixecament de la modularitat veiem que $Symm^n \rho_{E',\ell'}$ és automorfa. Llavors $Symm^n \rho_{E',\ell}$ és automorfa i $Symm^n \bar{\rho}_{E',\ell}$ també. Finalment, com que $Symm^n \bar{\rho}_{E,\ell} \cong Symm^n \bar{\rho}_{E',\ell}$, tenim que $Symm^n \bar{\rho}_{E,\ell}$ és automorfa i utilitzant el teorema d'aixecament de la modularitat per darrera vegada concluem que $Symm^n \rho_{E,\ell}$ és automorfa sobre F'.

Veiem un esquema per aclarir com es transmet la propietat de ser representació automorfa. Donades dues representacions r_1 i r_2, escriurem $r_1 \to r_2$ quan podem deduir que r_2 és automorfa a partir que r_1 és automorfa. En cada implicació escriurem

Red: si r_2 és automorfa ja que és la reducció de r_1.

R Eq: si $r_1 \cong r_2$.

FCR: si r_1 i r_2 formen part d'una família compatible de representacions.

TAM: si utilitzem el teorema d'aixecament de la modularitat sobre la representació reduïda r_1 de r_2.

$$Ind\ \theta \xrightarrow{Red} \overline{Ind\ \theta} \xrightarrow{R\ Eq} \overline{r_{\ell''}} \xrightarrow{TAM} r_{\ell''} \xrightarrow{FCR} r_{\ell'} \xrightarrow{Red} \overline{r_{\ell'}} \xrightarrow{R\ Eq}$$

$$\xrightarrow{R\ Eq} Symm^n \bar{\rho}_{E',\ell'} \xrightarrow{TAM} Symm^n \rho_{E',\ell'} \xrightarrow{FCR} Symm^n \rho_{E',\ell} \xrightarrow{Red}$$

$$\xrightarrow{Red} Symm^n \bar{\rho}_{E',\ell} \xrightarrow{R\ Eq} Symm^n \bar{\rho}_{E,\ell} \xrightarrow{TAM} Symm^n \rho_{E,\ell}$$

En resum, com que $Ind\ \theta$ és automorfa sobre F', llavors $Symm^n \rho_{E,\ell}$ també és automorfa sobre F'. Finalment, per a demostrar el teorema 3.5.4 ens cal veure que $Symm^n \rho_{E,\ell}$ és cuspidal sobre F', fet que podem comprovar a partir de la pròpia construcció de les representacions.

L'últim comentari sobre la demostració del teorema 3.5.4 és sobre la construcció de la família compatible de representacions $\{r_\ell\}_\ell$. Per n parell, aquesta família es construeix a partir de les varietats algebraiques

$$s(X_0^{n+1} + \ldots + X_n^{n+1}) = (n+1)tX_0 \cdots X_n$$

on $[X_0 : \ldots : X_n]$ i $[s : t]$ són coordenades homogènies de $\mathbb{P}_n$ i $\mathbb{P}_1$, respectivament. Per ser precisos, hauríem de considerar aquestes varietats com a esquemes sobre $\mathbb{Z}[\frac{1}{n+1}]$.

No detallarem la construcció de la família r_ℓ a partir d'aquestes hipersuperfícies. És suficient comentar que considerant valors de t en cossos F totalment reals i de Galois sobre $\mathbb{Q}$, podem obtenir sistemes compatibles de representacions de G_F a partir de representacions del grup de cohomologia central de la varietat. Observem que per a construir $\{r_\ell\}_\ell$ és necessari que n sigui parell. Per a n senar, podem demostrar el teorema aprofitant aquestes representacions, enunciant els resultats de forma precisa.

Amb aquest últim comentari acabem l'esquema de la demostració de la conjectura de Sato-Tate 3.4.1. Veiem un resum dels passos que hem seguit.

- Utilitzem la teoria de Serre per a demostrar que la conjectura de Sato-Tate depèn de la convergència de les L-sèries obtingudes a partir de la corba.
- Per demostrar la convergència d'aquestes L-sèries veiem que equivalen a les L-sèries d'altres objectes algebraics, seguint el programa de Langlands. En el nostre cas, representacions automorfes cuspidals.
- Per demostrar la igualtat entre L-sèries ens calen, principalment, dos tipus de resultats:
  - Teoremes d'aixecament de la modularitat. En el nostre cas el teorema d'aixecament de la modularitat de Taylor.
  - Construir famílies compatibles de representacions. Per a aquest propòsit es construeixen famílies compatibles a partir dels grups d'homologia de varietats algebraiques. Per exemple, podem pensar en les representacions $\rho_{E,\ell}(E)$ associades a una corba el·líptica E. En aquest cas, només cal observar que $T_\ell(E)$ és el dual del primer grup d'homologia ètale d'E.

Capítol 4

Generalització de la conjectura de Sato-Tate a gèneres superiors

Havent presentat la conjectura de Sato-Tate, és interessant preguntar-se sobre la generalització a corbes algebraiques de gènere superior a 1. Per establir la generalització de la conjectura de Sato-Tate ens calen generalitzar alguns resultats previs sobre corbes el·líptiques. És interessant tenir present com hem procedit en presentar la conjectura de Sato-Tate 3.4.1 per a observar l'analogia del procés que realitzarem a continuació i el realitzat per a corbes el·líptiques.

4.1 Preliminars sobre corbes algebraiques

Generalitzem alguns dels resultats obtinguts per a corbes el·líptiques. Observem que les corbes de gènere superior a 1 no tenen una estructura de grup natural. Tot i així, ens serà necessari associar a la corba un anell d'endomorfismes, el qual ja hem vist que intervé a l'hora de plantejar la conjectura de Sato-Tate.

Sigui doncs C una corba algebraica no singular de gènere g definida sobre un cos K. Considerem la varietat jacobiana de C, la qual denotarem per $Jac(C)$. Podem trobar la definició de varietat Jacobiana a [27] a través de la varietat de Picard, la qual definim a partir dels divisors de C. La Jacobiana de C és una varietat abeliana de dimensió g sobre K, i per tant podem considerar l'anell d'endomorfismes de $Jac(C)$. Abusant de notació escriurem $End(C)$ per a referir-nos a $End(Jac(C))$, i utilitzarem les notacions anàlogues a les utilitzades en el cas de corbes el·líptiques.

Per corbes el·líptiques el teorema 3.1.2 classifica l'estructura de l'anell d'endomorfismes. Aquest resultat es pot generalitzar per a varietats abelianes com el teorema 2.5.7 de [20].

Direm que una varietat abeliana és simple si no és isogena al producte de varietats de di-

mensió inferior. No definirem els conceptes relacionat a la polarització d'una varietat abeliana ja només ens interessarà aplicar el teorema a la Jacobiana d'una corba. La varietat Jacobiana té de forma natural una polarització el que ens permet aplicar el teorema anterior sense necessitat de descriure la polarització. Podem trobar les definicions i els resultats relacionats amb aquest teorema a [17].

Teorema 4.1.1. *Sigui A una varietat abeliana simple de dimensió g definida sobre un cos algebraicament tancat k i L una polarització de A. Sigui $F = End(A) \otimes \mathbb{Q}$ l'àlgebra de divisió associada als endomorfismes de A i K el centre de F. Definim la involució de Rosati $'$ de F a partir de la polarització L i $K_0 = \{f \in K | f = f'\}$. Sigui*

$$e_0 = [K_0 : \mathbb{Q}], \qquad e = [K : \mathbb{Q}], \qquad d^2 = [F : K].$$

Aleshores només es poden donar les següents quatre possibilitats:

Tipus I(e_0): *$F = K = K_0$ és un cos totalment real i la involució és la identitat sobre F, $' = Id_F$. A més es compleix $e_0|g$.*

Tipus II(e_0): *$K = K_0$ és un cos totalment real. F és una àlgebra de quaternions sobre K tal que $\forall \sigma : K \to \mathbb{R}$ morfisme sobre $\mathbb{Q}$ es té*

$$F \otimes_K \mathbb{R}_{(\sigma)} \cong M_2(\mathbb{R})$$

on $\mathbb{R}_{(\sigma)}$ és la K-àlgebra definida via σ i el producte tensorial es refereix al producte de K-àlgebras. A més es compleix $2e_0|g$.

Tipus III(e_0): *$K = K_0$ és un cos totalment real. F és una àlgebra de quaternions sobre K tal que $\forall \sigma : K \to \mathbb{R}$ morfisme sobre $\mathbb{Q}$ es té*

$$F \otimes_K \mathbb{R}_{(\sigma)} \cong \mathcal{H}$$

on $\mathcal{H}$ és la $\mathbb{R}$-àlgebra dels quaternions de Hamilton. A més es compleix $2e_0|g$ si $car(k) = 0$ i $e_0|g$ si $car(k) > 0$.

Tipus IV(e_0,d): *K_0 és un cos totalment real i K és un extensió quadràtica de K_0 totalment imaginària. F és una àlgebra de divisió sobre K. A més es compleix $e_0 d^2|g$ si $car(k) = 0$ i $e_0 d|g$ si $car(k) > 0$.*

Si considerem una varietat definida sobre un cos k no algebraicament tancat llavors l'únic que podem afirmar és que $End_k^0(A)$ és una subàlgebra de $End_{\overline{k}}^0(A)$ i que $End_k(A)$ és un ordre de $End_k^0(A)$. Tot i així, si la varietat A està definida sobre un cos de nombres K llavors existeix una extensió finita $L|K$ de manera que $End_L(A) = End_{\overline{K}}(A)$. Per tant segons aquest

resultat podem considerar que tots els endomorfismes d'A estan definits sobre una extensió finita de K.

Observem que si A és una corba el·líptica sobre un cos de nombres llavors el teorema 4.1.1 implica el teorema 3.1.2 ja que els únics casos possibles són I(1) i IV(1,1). És directe comprovar que el cas I(1) és el cas sense CM i que IV(1,1) és el cas amb CM.

Un cop presentada la classificació de l'anell d'endomorfismes construirem el mòdul de Tate de forma anàloga al cas de corbes el·líptiques. A partir de l'operació de grup en $Jac(C)$, definim el morfisme $[m]$ per tot $m \in \mathbb{Z}$. Donat un primer ℓ diferent de $car(K)$, definim el mòdul Tate ℓ-àdic de $Jac(C)$ com el límit projectiu dels grups $\ker[\ell^k]$ respecte les aplicacions $[\ell] : \ker[\ell^{k+1}] \to \ker[\ell^k]$, és a dir,

$$T_\ell(Jac(C)) = \varprojlim_k \ker[\ell^k].$$

Abusant de notació escriurem $T_\ell(C)$ per a referir-nos al mòdul de Tate de la Jacobiana de C. $T_\ell(C)$ té estructura de $\mathbb{Z}_\ell$-mòdul lliure de rang igual a dues vegades la dimensió de la Jacobiana. A més, podem construir una acció de G_K sobre $T_\ell(C)$ tot fent actuar G_K sobre els elements de $\ker[\ell^k]$. Així doncs obtenim una representació

$$\rho_{C,\ell} : G_K \to Aut(T_\ell(C)).$$

Com ja hem fet per a corbes el·líptiques, si escollim una base de $T_\ell(C)$ podem considerar $\rho_{C,\ell}$ com a morfisme entre G_K i $GL_{2g}(\mathbb{Z}_\ell)$. A més, la inclusió $\mathbb{Z}_\ell \subseteq \mathbb{Q}_\ell$ ens permet interpretar $\rho_{C,\ell}$ com una representació $2g$-dimensional de G_K sobre $\mathbb{Q}_\ell$. Per descriure $\rho_{C,\ell}$, presentem la L-sèrie associada a C.

Definició 4.1.2. *Sigui K és un cos finit de q elements. Sigui C una corba definida sobre K. Definim la funció zeta de C com*

$$Z(T, C) = \exp\left(\sum_{n=1}^{\infty} \#C(K_n)\frac{T^n}{n}\right),$$

on K_n és un cos de q^n elements i $C(K_n)$ denota el conjunt de punts de C amb coordenades a K_n.

Per corbes el·líptiques utilitzàvem el teorema de Hasse 3.1.7 per a deduir els resultats necessaris per a plantejar la conjectura de Sato-Tate 3.4.1. Per corbes de gènere arbitrari l'anàleg al teorema de Hasse és les conjectures de Weil, que van ser demostrades en la seva totalitat per Pierre Deligne.

Teorema 4.1.3 (Conjectures de Weil)**.** *Sigui C una corba algebraica no singular de gènere*

g definida sobre un cos finit K de q elements. Denotem per $Z(T, C)$ la funció zeta de C. Llavors es compleix:

Racionalitat. *Z(T,C) és una funció racional en T, és a dir, és un quocient de polinomis a coeficients racionals.*

Equació funcional. *Sigui E la característica d'Euler de C, és a dir, $E = 2 - 2g$. Llavors es compleix l'equació funcional*

$$Z(\frac{1}{qt}, C) = q^{E/2} t^E Z(T, C).$$

Hipòtesi de Riemann. *Podem escriure*

$$Z(T, C) = \frac{L(T)}{(1 - T)(1 - qT)}$$

on $L(T)$ és un polinomi de grau $2g$ amb coeficients enters. A més es compleix que $L(T) = \prod(1 - \alpha_i T)$ amb $\alpha_i \in \mathbb{C}$ i $|\alpha_i| = \sqrt{q}$.

Tot i que la versió que hem donat de les conjectures de Weil és només per corbes, les conjectures de Weil van ser establertes l'any 1949 per André Weil per a varietats algebraiques. L'any 1974 Pierre Deligne va demostrar la hipòtesi de Riemann per varietats, concloent d'aquesta manera la demostració de les conjectures de Weil. Les conjectures de Weil per corbes el·líptiques es dedueixen a partir del teorema de Hasse 3.1.7, que ja va ser demostrat durant els anys 30. Podem consultar a [8] per la definició i demostració de les conjectures de Weil sobre varietats. La demostració es centra essencialment en resultats sobre la dualitat de Poincaré i el teorema del punt fix de Lefschetz en esquemes.

Suposem ara que K és un cos de nombres. Donat un primer $\mathfrak{p}$ de K definim la corba reduïda $C_\mathfrak{p}$ de manera anàloga al procés realitzat per a corbes el·líptiques. Definim $L_\mathfrak{p}(T)$ com el polinomi $L(T)$ definit en aplicar les conjectures de Weil 4.1.3 a $C_\mathfrak{p}$, és a dir,

$$Z(T, C_\mathfrak{p}) = \frac{L_\mathfrak{p}(T)}{(1 - T)(1 - \mathfrak{N}(\mathfrak{p})T)}.$$

Tal i com obteníem per corbes el·líptiques, els polinomis $L_\mathfrak{p}(T)$ defineixen els factors locals de la L-sèrie de la corba C. I a més obtenim que $L_\mathfrak{p}(T)$ és el polinomi característic de $\rho_{C,\ell}(Frob_\mathfrak{p})$, on $Frob_\mathfrak{p}$ és una classe de conjugació de l' automorfisme de Frobenius de $\mathfrak{p}$ en K.

Definició 4.1.4. *La L-sèrie associada a C és*

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

on els factors locals en els primers de mala reducció es defineixen de forma anàloga a com ho hem fet per a corbes el·líptiques.

4.2 Equidistribució de Frobenii en corbes de gènere superior

A partir de les definicions anteriors generalitzarem la conjectura de Sato-Tate, reformulant alguna de les hipòtesis. Sigui C una corba algebraica no singular de gènere g definida sobre un cos K. Sigui $\mathfrak{p}$ un primer de K on C té bona reducció. Considerem el factor local de la L-sèrie de C. En venir definit a partir de les conjectures de Weil 4.1.3, tenim que $L_{\mathfrak{p}}(T)$ té grau $2g$ i el conjunt de les seves arrels és de la forma $\{\pm\sqrt{\mathfrak{N}(\mathfrak{p})}e^{i\theta_{\mathfrak{p},k}}|1 \leq k \leq g\}$. Considerem el polinomi $\overline{L}_{\mathfrak{p}}(T) = L_{\mathfrak{p}}(\sqrt{\mathfrak{N}(\mathfrak{p})}T)$, el qual té totes les seves arrels unitàries. Per tant el conjunt de les arrels de $\overline{L}_{\mathfrak{p}}(T)$ és $\{\pm e^{i\theta_{\mathfrak{p},k}}|1 \leq k \leq g\}$ amb $\theta_{\mathfrak{p},k} \in [0,\pi]$. Per tal que l'ordre que hem donat a les arrels no intervingui en les definicions posteriors considerarem el conjunt $\{\theta_{\mathfrak{p},k}|1 \leq k \leq g\}$ en $[0,\pi]^g/\mathcal{S}_g$, el quocient de $[0,\pi]^g$ respecte les permutacions de les coordenades.

Fent variar $\mathfrak{p}$ respecte els primers de K on C té bona reducció, obtenim una successió $\{(\theta_{\mathfrak{p},1},\ldots,\theta_{\mathfrak{p},g})\}$ en $[0,\pi]^g/\mathcal{S}_g$. Podem doncs preguntar-nos si aquesta successió està equidistribuïda respecte alguna mesura μ_C de $[0,\pi]^g/\mathcal{S}_g$. Per simplificar la notació, considerarem μ_C com una mesura de $[0,\pi]^g$, invariant per $\mathcal{S}_g$. Observem que si $g = 1$ el plantejament és el mateix que el realitzat per la conjectura de Sato-Tate 3.4.1.

L'objectiu és utilitzar la teoria de Serre per a calcular μ_C. Segons la notació de la teoria de Serre definim Σ com el conjunt de primers de K on C té bona reducció. Per $v \in \Sigma$ definim Nv com la norma de v. Definim el grup G com $USp(2g)$, el grup de les matrius $2g \times 2g$ a coeficients complexes simplèctiques i unitàries. Observem que $USp(2) = SU(2)$ ja que una matriu 2×2 és simplèctica si i només si és unitària.

Veiem com definir x_v. Donat un polinomi amb coeficients reals de grau $2g$ direm que és simplèctic unitari si el conjunt de les seves arrels és de la forma $\{\pm e^{i\theta_1},\ldots,\pm e^{i\theta_g}\}$. Com que tot polinomi queda determinat per les seves arrels obtenim una bijecció entre els polinomis simplèctics unitaris i els conjunts de la forma $\{\pm e^{i\theta_1},\ldots,\pm e^{i\theta_g}\}$, mòdul permutació de les arrels. A més podem veure que els polinomis característics dels elements de $USp(2g)$ són simplèctics unitaris i que de fet tenim una bijecció entre els polinomis simplèctics unitaris i les classes de conjugació de $USp(2g)$.

Definim doncs x_v com la classe de conjugació de $USp(2g)$ associada al polinomi simplèctic unitari $\overline{L}_v(T)$, amb arrels $\{(\pm e^{\theta_{v,1}},\ldots,\pm e^{\theta_{v,g}})\}$. Observem que, donat que $L_v(T)$ és el polinomi característic de $\rho_{C,\ell}(Frob_v)$, obtenim que podem definir x_v a partir del conjunt d'arrels del polinomi $\det(\mathfrak{N}(\mathfrak{p})T - \rho_{C,\ell}(Frob_v))$. Aplicant la teoria de Serre a les definicions anteriors obtenim la següent generalització de la conjectura de Sato-Tate.

Suposem que la successió $(x_v)_{v\in\Sigma}$ està equidistribuïda respecte una mesura μ de $USp(2g)$. Considerem la següent aplicació h entre $USp(2g)$ i $[0,\pi]^g/\mathcal{S}_g$: donat un element x de $USp(2g)$ definim la imatge de x per h a partir de les arrels del seu polinomi característic, $\{\pm e^{i\theta_1},\dots,\pm e^{i\theta_g}\}$, com $h(x)=(\theta_1,\dots,\theta_g)$ en $[0,\pi]^g/\mathcal{S}_g$. Llavors $(h(x_v))_{v\in\Sigma}$ està equidistribuït respecte la mesura $h_*(\mu)$ de $[0,\pi]^g$.

Per tant, segons el plantejament anterior, obtindríem $\mu_C = h_*(\mu)$. Es natural preguntar-se si podem obtenir una expressió explícita de μ_C, tal i com hem vist per a corbes el·líptiques. Per aquest propòsit utilitzem la fórmula d'integració de Weyl. Segons aquesta teoria podem trobar l'expressió explícita de la mesura de Haar d'alguns grups de matrius. Podem trobar aquest resultat a [9], on a més també podem trobar una altra aproximació a la conjectura de Sato-Tate a través del model de matrius aleatòries. No descriurem aquest plantejament per a simplificar el desenvolupament que realitzarem posteriorment.

Per exemple, si $\mu_{USp(2g)}$ és la mesura de Haar de $USp(2g)$, llavors l'expressió de la mesura $h_*(\mu_{USp(2g)})$ de $[0,\pi]^g$ és

$$\frac{1}{g!}\left(\prod_{i<j}(2\cos x_i - 2\cos x_j)\right)^2 \prod_i \left(\frac{2}{\pi}\sin^2 x_i dx_i\right).$$

Observem com per $g=1$ obtenim la distribució de Sato-Tate.

Així doncs podem generalitzar la conjectura de Sato-Tate com

Conjectura 4.2.1. *Sigui C una corba algebraica C de gènere g sobre un cos de nombres K. Llavors la successió $(\theta_{v,1},\dots,\theta_{v,g})_{v\in\Sigma}$ està equidistribuïda en $[0,\pi]^g$ respecte la mesura*

$$\frac{1}{g!}\left(\prod_{i<j}(2\cos x_i - 2\cos x_j)\right)^2 \prod_i \left(\frac{2}{\pi}\sin^2 x_i dx_i\right).$$

És evident que no podem esperar que aquesta conjectura sigui certa en general per a tota C ja que per a corbes el·líptiques E només es compleix si la corba no té multiplicació complexa, és a dir, si $End(E)=\mathbb{Z}$. Podem esperar que per a corbes de gènere arbitrari també calgui imposar alguna restricció sobre C per tal que es compleixi 4.2.1. El més simple és pensar en la restricció $End(C)=\mathbb{Z}$, on recordem que $End(C)$ es refereix a l'anell d'endomorfismes de la Jacobiana de C. Tot i això, la condició segons la qual es presenta actualment la conjectura de Sato-Tate no és $End(C)=\mathbb{Z}$.

Considerem les representacions

$$\rho_{C,\ell}: G_K \to GL_{2g}(\mathbb{Z}_\ell).$$

Segons la topologia de G_K, el conjunt d'automorfismes de Frobenius dels primers de K és dens en G_K. Com que la imatge dels automorfismes de Frobenius té com a polinomi característic un polinomi simplèctic, obtenim que $\rho_{C,\ell}(G_K) \subseteq GSp(2g, \mathbb{Z}_\ell)$, el grup de matrius simplèctiques.

Definició 4.2.2. *Direm que C té imatge de Galois gran si $\rho_{C,\ell}(G_K)$ és dens, respecte la topologia de Zariski, en $GSp(2g, \mathbb{Z}_\ell)$.*

Observem que la definició anterior depèn de ℓ. Però a través dels resultats de Serre [24] sobre representacions l-àdiques, obtenim que la definició anterior és independent de ℓ, és a dir, si $\rho_{C,\ell}(G_K)$ és dens en $GSp(2g, \mathbb{Z}_\ell)$ llavors $\rho_{C,\ell'}(G_K)$ és dens en $GSp(2g, \mathbb{Z}'_\ell)$ per a qualsevol ℓ'.

La propietat que C tingui imatge de Galois gran és la propietat que imposarem per a plantejar la conjectura de Sato-Tate generalitzada. Així doncs és interessant poder determinar quan una corba té o no imatge de Galois gran. Aquest problema representa encara avui dia un problema obert. Es coneixen però alguns resultats que ens permet afirmar que una corba té imatge de Galois gran, i que també ens relacionen aquesta propietat amb $End(C) = \mathbb{Z}$, que havíem considerat inicialment. Tenim que qualsevol de les propietats següents implica que C té imatge de Galois gran:

- C té gènere senar, 2 o 6 i $End(C) = \mathbb{Z}$ (veure [25]).
- C és una corba hiperel·líptica $y^2 = f(x)$ amb $f(x)$ de grau superior a 5 i grup de Galois S_n o A_n (veure [30]).
- C té bona reducció fora d'un conjunt de primers S i la imatge de la reducció mòdul ℓ de $\rho_{E,\ell}$ correspon a $GSp(2g, \mathbb{Z}/\ell\mathbb{Z})$ per algun primer $\ell \geq c(g, S)$. Aquí, $c(g, S)$ és una constant que només depèn de g i S (veure [3],[24]).

Veiem com podem relacionar que una corba tingui imatge de Galois gran amb la conjectura de Sato-Tate. Considerem la següent cadena d'inclusions

$$GSp(2g, \mathbb{Z}_\ell) \to GSp(2g, \mathbb{Q}_\ell) \to GSp(2g, \overline{\mathbb{Q}}_\ell) \to GSp(2g, \mathbb{C}).$$

En l'últim morfisme utilitzem que $\overline{\mathbb{Q}}_\ell$ i $\mathbb{C}$ són isomorfs, i fixem un isomorfisme entre aquests dos cossos.

Denotem $G_\ell = \rho_{C,\ell}(G_K)$. Com que $\rho_{C,\ell}(G_K) \subseteq GSp(2g, \mathbb{Z}_\ell)$, podem prendre la clausura de Zariski de G_ℓ a través de la cadena d'inclusions anterior, obtenint el subgrup $\overline{G}_\ell \subseteq GSp(2g, \mathbb{C})$. Intersectem $\overline{G}_\ell$ amb el grup de matrius unitàries, tot obtenint un grup reductiu R sobre $\mathbb{C}$.

Tot grup reductiu sobre $\mathbb{C}$ té un subgrup compacte maximal, és a dir un grup maximal en el conjunt de subgrups compactes. Elegim doncs un subgrup compacte maximal H de R.

Segons aquestes notacions si G_ℓ és dens, respecte la mesura de Zariski, en $GSp(2g, \mathbb{Z}_\ell)$ llavors $H = USp(2g)$. En general, però, obtenim que H és un subgrup compacte de $USp(2g)$, el qual suposarem infinit.

Observem a més que donada la classe de conjugació $Frob_\mathfrak{p}$ de G_K existeix una única classe de conjugació de H amb polinomi característic $\overline{L}_\mathfrak{p}(T)$. Per tant podem definir x_v com la classe de conjugació en H definida per $\overline{L}_v(T)$, el que ens permet aplicar la teoria de Serre per a demostrar que $\{x_v\}_{v\in\Sigma}$ està equidistribuïda respecte una mesura μ de H.

Suposem que la successió $\{x_v\}_{v\in\Sigma}$ està equidistribuïda respecte la mesura de Haar μ_H de $H \subseteq USp(2g)$. Sigui h l'aplicació definida anteriorment entre $USp(2g)$ i $[0,\pi]^g/\mathcal{S}_g$. Podem considerar de manera natural μ_H com una mesura de $USp(2g)$. Llavors $(h(x_v))_{v\in\Sigma}$ està equidistribuït respecte la mesura $h_*(\mu_H)$ de $[0,\pi]^g$.

Observem que hem definit H com un subgrup compacte maximal, el que determina H llevat de conjugació. Però com que el polinomi característic de dos matrius conjugades és idèntic obtenim que la mesura $h_*(\mu_H)$ no depèn de l'elecció del grup H.

Definició 4.2.3. *Definim, llevat de conjugació, H_C com el grup H definit anteriorment.*

Obtenim així la següent generalització de la conjectura de Sato-Tate.

Conjectura 4.2.4 (Sato-Tate generalitzada)**.** *Sigui C una corba algebraica C de gènere g sobre un cos de nombres K. Llavors existeix un subgrup compacte infinit $H \subseteq USp(2g)$ tal que la successió $(\theta_{v,1}, \ldots, \theta_{v,g})_{v\in\Sigma}$ està equidistribuïda en $[0,\pi]^g$ respecte la mesura $h_*(\mu_H)$. A més la igualtat es compleix si, i només si C té imatge de Galois gran.*

Definició 4.2.5. *Segons la notació de la conjectura direm que C està distribuïda respecte H i que H és un grup de distribució de C.*

Podem conjecturar que H_C és un grup de distribució de la corba C.

La conjectura 4.2.4 segueix oberta. Recordem que de fet el cas $g = 1$ és la conjectura de Sato-Tate, que va ser resolta recentment. Actualment per a resoldre la conjectura 4.2.4 es segueix l'esquema desenvolupat per a resoldre la conjectura de Sato-Tate. Recordem que aquest esquema consisteix en els següents punts:

- Utilitzar la teoria de Serre per a demostrar que la conjectura de Sato-Tate depèn de la convergència de les L-sèries obtingudes a partir de la corba.
- Seguint el programa de Langlands, demostrar la convergència d'aquestes L-sèries, tot veient que equivalen a L-sèries de representacions automorfes.
- Per demostrar la igualtat entre L-sèries calen, principalment, dos tipus de resultats:

- Teoremes d'aixecament de la modularitat.
- Construir famílies compatibles de representacions.

Actualment encara no es té gaire coneixement sobre la conjectura de Sato-Tate generalitzada 4.2.4. En aquest sentit no només ens referim a la demostració de la conjectura en certs casos sinó a altres qüestions com la descripció dels grups de distribució de les corbes o l'expressió explícita de la distribució corresponent a la corba. Recordem a més que la conjectura de Sato-Tate només està demostrada per a corbes definides sobre cossos totalment reals. Per tant la recerca actual sobre la conjectura generalitzada es centra principalment en corbes sobre cossos totalment reals, i en la majoria dels casos considerant corbes sobre $\mathbb{Q}$. A més els principals resultats teòrics corresponen a corbes amb imatge de Galois gran.

Així doncs no presentarem cap altre resultat teòric sobre la conjectura generalitzada 4.2.4. Presentarem però alguns resultats numèrics que reforcen la conjectura. Aquests resultats corresponen a l'article [10] recentment publicat per Kiran S. Kedlaya i Andrew V. Sutherland del Massachusetts Institute of Technology. En aquest article s'estudia la conjectura de Sato-Tate generalitzada 4.2.4 per a corbes sobre $\mathbb{Q}$ de gènere 2, obtenint una classificació dels grups de distribució.

Capítol 5

Corbes de gènere 2

Seguirem el desenvolupament realitzat en [10] presentant els conceptes i resultats principals obtinguts per corbes definides sobre $\mathbb{Q}$ de gènere 2. Abans però de considerar corbes de gènere 2 és interessant tornar a considerar corbes el·líptiques. Recordem que els resultats obtinguts per corbes el·líptiques es dedueixen de dos plantejaments diferents, depenent de si la corba té o no CM. Com a exemple per corbes de gènere superior reinterpretarem els resultats sobre corbes el·líptiques en base de la conjectura 4.2.4.

5.1 Reinterpretació de la conjectura de Sato-Tate per a corbes el·líptiques

Considerem una corba el·líptica $E/\mathbb{Q}$. Segons la conjectura 4.2.4 E està distribuïda respecte $SU(2)$ si, i només si E té imatge de Galois gran. Com ja hem vist, per a $g = 1$ la condició $End(E) = \mathbb{Z}$ implica que E té imatge de Galois gran i per tant obtindríem que la distribució μ_E és la distribució de Sato-Tate si, i només si, E no té CM. Observem que no hem fet referència al fet que la corba E tingui reducció multiplicativa en algun primer, i per tant la conjectura 4.2.4 ampliaria els resultats actuals sobre la conjectura de Sato-Tate.

Suposem doncs que E no té imatge de Galois gran, i per tant E té CM. Com ja hem vist anteriorment a partir del teorema 3.3.2 es compleix $\mu_E = 1/2\mu_{unif} + 1/2\delta_{\pi/2}$. Veiem com podem interpretar aquesta distribució a partir de la mesura de Haar d'un subgrup H de $SU(2)$. Considerem el grup ortogonal $SO(2) \subseteq SU(2)$. Observem que la mesura de Haar $\mu_{SO(2)}$ de $SO(2)$ és la mesura uniforme ja que $SO(2)$ és isomorf a S^1. El normalitzador $N(SO(2))$ de $SO(2)$ té índex 2 sobre $SO(2)$ i per tant la mesura de Haar $\mu_{N(SO(2))}$ de $N(SO(2))$ també és la mesura uniforme. Considerem l'aplicació h entre $SU(2)$ i $[0, \pi]$ definida anteriorment i calculem $h_*(\mu_{N(SO(2))})$. Com que $N(SO(2))$ té dues components connexes, $SO(2)$ i $N(SO(2)) \setminus SO(2)$

es compleix la igualtat

$$h_*(\mu_{N(SO(2))}) = h_*(\mu_{N(SO(2))}|_{SO(2)}) + h_*(\mu_{N(SO(2))}|_{N(SO(2))\setminus SO(2)})$$

on $h_*(\mu_{N(SO(2))}|_{SO(2)})$ i $h_*(\mu_{N(SO(2))}|_{N(SO(2))\setminus SO(2)})$ tenen mesura total $1/2$. Per una banda és clar que $\mu(\mu_{N(SO(2))})|_{SO(2)} = 1/2\mu_{SO(2)}$ i per tant $h_*(\mu_{N(SO(2))})|_{SO(2)}) = 1/2\mu_{unif}$. Per altra banda, tots els elements de $N(SO(2)) \setminus SO(2)$ pertanyen a la mateixa classe de conjugació, ja que tots tenen polinomi característic $T^2 + 1$. Per tant $h(N(SO(2)) \setminus SO(2)) = \pi/2$ i $h_*(\mu_{N(SO(2))})|_{N(SO(2))\setminus SO(2)}) = 1/2\delta_{\pi/2}$. Així doncs $h_*(\mu_{N(SO(2))}) = 1/2\mu_{unif} + 1/2\delta_{\pi/2} = \mu_E$, el que permet assumir que E està distribuïda respecte $N(SO(2))$.

El resultat anterior l'hem deduït únicament acceptant 4.2.4, buscant un grup H que s'ajusti a la conjectura. També hi ha resultats teòrics que ens permeten donar més consistència a la deducció anterior. Per ℓ prou gran es compleix que la imatge de $G_{\mathbb{Q}}$ per la representació reduïda de $\rho_{E,l}$ és el normalitzador d'un subgrup de Cartan propi. Si aquesta propietat es transmet de la representació reduïda a la representació $\rho_{E,l}$ llavors $\rho_{E,l}(G_{\mathbb{Q}})$ és el normalitzador d'un subgrup de Cartan propi i com que el grup H_E el construïm com una clausura de $\rho_{E,l}(G_{\mathbb{Q}})$, té sentit assumir que H_E és el normalitzador d'un subgrup de Cartan propi de $SU(2)$. Els únics subgrups compactes infinits de $SU(2)$ són, llevat de conjugació, $SO(2)$, el normalitzador de $SO(2)$ i $SU(2)$. Així doncs segons les hipòtesis anteriors només es pot donar que H_E sigui conjugat al normalitzador de $SO(2)$.

Observem a més que segons els resultats anteriors $SO(2)$ no és el grup de distribució de cap corba el·líptica. Per tant, a l'hora de descriure els possibles grups per corbes de gènere superior no és suficient en conèixer tots els subgrups compactes infinits de $USp(2g)$ sinó que cal estudiar quins d'ells poden ser el grup de distribució d'alguna corba de gènere g.

5.2 Resultats numèrics

Els resultats per a $g = 1$ ens serveix com a model per a estudiar les corbes de gènere 2. Presentem l'estudi realitzat en [10], el qual consisteix en dos parts principals. En primer terme es calculen les possibles distribucions corresponents a corbes de gènere 2 i posteriorment construïm subgrups de $USp(4)$ que siguin grups de distribució.

5.2.1 Càlcul de la distribució de corbes

Comencem descrivint com obtenir la distribució associada a una corba no singular C de gènere g. Per calcular la mesura associada a C s'utilitzen els polinomis $\overline{L}_p(T)$. Els algoritmes per a realitzar el càlcul d'aquests polinomis es pot consultar en [11]. El més natural per a calcular la mesura μ_C és calcular les arrels de $\overline{L}_p(T)$ fent variar p per obtenir una aproximació de $h_*(\mu_C)$.

Però segons aquest plantejament no està clar com es pot diferenciar diverses distribucions o comprovar que dues successions estan distribuïdes respecte la mateixa mesura. Un mètode molt més efectiu consisteix en considerar les distribucions dels coeficients del polinomi. O més generalment de polinomis simètrics en les arrels de $\overline{L}_p(T)$. Sigui s un polinomi simètric, calculem la successió de moments de la variable aleatòria X definida al avaluar s en els valors propis d'una matriu aleatòria.

Definició 5.2.1. *La successió de moments d'una variable aleatòria X és defineix per*

$$M[X] = (E[X^0], E[X], E[X^2], E[X^3], \ldots)$$

Usant la condició de Carleman ([15] p.126) obtenim que la successió $M[X]$ determina de manera única la distribució de X. Així doncs obtenim el següent resultat, el qual ens permetrà realitzar el càlcul numèric.

Proposició 5.2.2. *Suposem certa la conjectura 4.2.4. Sigui C una corba racional no singular de gènere g. Sigui H un grup de distribució de C. Sigui $s(x_1, \ldots, x_{2g})$ un polinomi simètric real. Considerem s_p com el valor obtingut al avaluar s en les arrels de $\overline{L}_p(T)$ i $\{s_p\}_p$ com la successió dels valors anteriors. Sigui X la variable aleatòria definida avaluant s en les arrels d'una matriu aleatòria de H. Llavors els moments de X existeixen i determinen la distribució de X. A més el límit de la mitjana dels valors s_p^n pels $p \leq N$ on C té bona reducció convergeix a $E[X^n]$ quan $N \to \infty$.*

Es consideren els polinomis simètrics elementals a_k i els polinomis simètrics de Newton s_k amb $2g$ variables. Recordem que el polinomi simètric k-èssim es defineix per

$$s_k(x_1, \ldots, x_{2g}) = \sum_{i=1}^{2g} x_i^n.$$

Observem que el polinomi simètric elemental k-èssim avaluat en les arrels d'un polinomi coincideix, llevat de signe, amb el coeficient k-èssim del polinomi.

Per tal de contrastar les distribucions que obtindrem de corbes i de subgrups de $USp(2g)$ cal conèixer exactament la successió de moments dels polinomis simètrics. Aquest càlcul es pot realitzar per s_k en els subgrups que definirem posteriorment. I utilitzant el càlcul de s_k es pot realitzar el càlcul de a_k. Per a $USp(4)$ obtenim que la successió de moments de s_1 és

$$1, 0, 1, 0, 3, 0, 14, 0, 84, 0, 594, 0, 4719, \ldots$$

Aquesta successió és la successió A138349 de la OEIS, The On-Line Encyclopedia of Integer Sequences.

Si considerem $USp(2g)$ llavors podem calcular, utilitzant diversos resultats tècnics, la

successió de moments associada a s_k. A més també es compleix la següent proposició, la qual limita el volum de càlculs a realitzar.

Proposició 5.2.3. *Per tot $k > 2g$ les successions de moments de s_k són iguals.*

Així doncs és suficient calcular les distribucions s_k per $k \leq 2g+1$. També es pot comprovar que si k és senar llavors $M[s_k](n)$, el moments n-èssim de s_k, és sempre zero per n senar. Els càlculs de la successió de moments es limiten als primers 8 termes de $M[X]$, el qual permet distingir entre distribucions.

A l'hora de realitzar els càlculs també es interessant la següent proposició, segons la qual es pot calcular amb suficient confiança el límit definit en 5.2.2.

Proposició 5.2.4. *Sigui V un espai vectorial finit sobre $\mathbb{C}$. Sigui X la variable aleatòria definida al avaluar un polinomi simètric amb coeficients enters en les arrels d'una matriu aleatòria d'un subgrup compacte de $GL(V)$ distribuït respecte la mesura de Haar. Llavors $E[X^n] \in \mathbb{Z}$ per tots els enters positius n.*

Utilitzant 5.2.2, 5.2.3 i 5.2.4 es pot estudiar numèricament la distribució de s_k i a_k de manera eficient.

A part de les diverses successions de moments també és interessant el càlcul de la probabilitat $z(C)$ que el polinomi $\overline{L}_p(T)$ tingui traça zero. Aquest càlcul es pot aproximar per

$$z(C) = \lim_{N \to \infty} z(C, N)$$

on $z(C, N)$ és la proporció de primers $p \leq N$ tal que $\overline{L}_p(T)$ té traça zero.

Presentem els resultats numèrics per corbes obtinguts a [10]. En primer terme es realitza un estudi per corbes el·líptiques, confirmant els resultats teòrics. A més també es comprova la conjectura per a corbes amb reducció purament additiva, és a dir sense reducció multiplicativa, sense obtenir cap resultat numèric que no s'ajusti a la conjectura 4.2.4.

Posteriorment, tot i que els resultats presentats permeten el càlcul per corbes de gènere arbitrari només és computacionalment efectiu el càlcul per corbes de gènere 2. Així doncs considerarem, a no ser que s'especifiqui d'altra manera, que totes les corbes són corbes sobre $\mathbb{Q}$ no singulars de gènere 2.

Per al càlcul de les distribucions de les corbes es consideren les corbes de la forma

$$y^2 = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$$

amb coeficients enters $f_0, \ldots, f_4$ distribuïts uniformement en l'interval $[-2^{63}+1, 2^{63}-1]$. El resultat d'aquest estudi es que totes les corbes considerades tenen com a distribució la mesura

#	z(C)	M_2	M_4	M_6	M_8	f(x)
1	0	1	3	14	84	x^5+x+1
2	0	2	10	70	588*	$x^5-2x^4+x^3+2x-4$
3	0	2	11	90	888*	$x^5+20x^4-26x^3+20x^2+x$
4	0	2	12	110	1203*	$x^5+4x^4+3x^3-x^2-x$
5	0	4	32	320	3581*	$x^5+7x^3+32x^2+45x+50$
6	1/6	2	12	100	979*	$x^5-5x^3-5x^2-x$
7	1/4	2	12	100	1008*	$x^5+2x^4+2x^2-x$
8	1/4	2	12	110	1257*	$x^5-4x^4-2x^3-4x^2+x$
9	1/2	1	5	35	293*	$x^5-2x^4+11x^3+4x^2+4x$
10	1/2	1	6	55	601*	$x^5-2x^4-3x^3+2x^2+8x$
11	1/2	2	16	160	1789*	x^5+x^3+x
12	1/2	2	18	220	3005*	$x^5-3x^4+19x^3+4x^2+56x-12$
13	1/2	4	48	640	8949*	x^6+1
14	7/12	1	6	50	489*	$x^5-4x^4-3x^3-7x^2-2x-3$
15	7/12	2	18	200	2446*	x^6+2
16	5/8	1	6	50	502*	x^5+x^3+2x
17	5/8	2	18	200	2515*	$x^5-10x^4+50x^2-25x$
18	3/4	1	8	80	894*	x^5-2x^3-x
19	3/4	1	9	100	1222*	x^5-1
20	3/4	1	9	110	1501*	$11x^6+11x^3-4$
21	3/4	2	24	320	4474*	x^5+x
22	13/16	1	9	100	1254*	x^5+3x
23	7/8	1	12	160	2237*	x^5+2x

Taula 5.1: Aquesta taula és la taula 11 de [10]. Pels càlculs s'han utilitzat els primer menors a $N = 2^{26}$. La columna $z(C)$ és la densitat de traces nul·les. El valor M_i és el moment i-èssim de a_1. L'asterisc indica que les aproximacions obtingudes poden no ser els valors correctes. La última columna és un exemple de corba de gènere 2 de la forma $y^2 = f(x)$ amb la distribució corresponent.

de Haar de $USp(4)$, és a dir, tenen imatge de Galois gran. Aquest resultat comprova que triada una corba aleatòriament el més probable es que tingui imatge de Galois gran.

Per obtenir altres distribucions es redueix l'interval on es prenen els coeficients. Es calcula la distribució de totes les corbes de la forma $y^2 = f(x)$ amb $f(x)$ mònic de grau 5 amb coeficients enters en l'interval $[-64, 64]$ i $f(x)$ de grau 6 amb els coeficients enters en l'interval $[-16, 16]$.

A partir dels càlculs realitzats s'obtenen 22 distribucions diferents a la distribució de corbes amb imatge de Galois gran. Per comprovar aquests resultats també es realitza el càlcul per corbes ja considerades en diverses publicacions obtenint que la distribució de totes elles és una de les 23 ja calculades. Els resultats queden resumits en la taula 5.1 on es descriuen els resultats obtinguts en [10].

5.2.2 Càlcul de la distribució de corbes

Un cop calculades les possibles distribucions que es poden obtenir per a corbes de gènere 2 estudiem les successions de moments de la mesura de Haar d'alguns subgrups de $USp(4)$. L'objectiu és trobar per cada distribució de la taula 5.1 un grup compacte infinit amb la mateixa successió de moments.

Veiem com construïm aquests subgrups compactes de $USp(4)$. Recordem que per a corbes el·líptiques la distribució d'una corba el·líptica E està determinada per l'estructura de $End(E)$. És natural doncs esperar que la distribució d'una corba C de gènere 2 també depengui, en major o menor mesura, d'$End(C)$. Si es considera una corba C amb jacobiana igual al producte de dues corbes el·líptiques E_1 i E_2 és natural esperar que la distribució de C depengui de les distribucions de E_1 i E_2.

Suposem que E_1 i E_2 no són isogènies, el qual es pot interpretar com que les distribucions de E_1 i E_2 no estan correlacionades. Llavors té sentit pensar que la distribució de C és el producte de distribucions. Tenint present el concepte anterior construïm els següents grups a partir dels grups de distribució de corbes el·líptiques. Denotem $G_1 = USp(2)$ i $G_2 = N(SO(2))$, els quals són els possibles grups de distribució d'una corba el·líptica.

Definició 5.2.5. *Definim els subgrups $G_1 \times G_1$, $G_1 \times G_2$, $G_2 \times G_1$, i $G_2 \times G_2$ com*

$$G_i \times G_j = \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \middle| \; A \in G_i, \; B \in G_j \right\}.$$

Observem que $G_2 \times G_1$ és conjugat a $G_1 \times G_2$ i per tant defineixen una distribució equivalent. Podem calcular la successió de moments d'aquests grups utilitzant les successions de moments de G_1 i G_2, que podem calcular directament. Obtenim que la successió $M[a_1]$ de G_1 és

$$1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, \ldots$$

on el terme $(2n)$-èssim és el n-èssim nombre de Catalan. (A000108)

També podem veure que $M[a_1]$ de G_2 és

$$1, 0, 1, 0, 3, 0, 10, 0, 35, 0, 126, \ldots$$

on el terme $(2n)$-èssim és $\binom{2n}{n}/2$. (A001700)

Podem calcular la successió $M[a_1]$ de $G_i \times G_j$ com la convolució de les successions de moments $M[a_1]$ de G_i i G_j.

Definició 5.2.6. *El terme k-èssim de la convolució de dues successions $\{a_n\}_{n\in}$ i $\{b_m\}_{m\in}$ és*

$$\sum_{t=1}^{i} \binom{i}{t} a_k b_{t-k}.$$

En la següent taula es calculen els primers moments parells de a_1 dels grups $G_i \times G_j$. Els moments senars són sempre 0.

$G_i \times G_j$	M_2	M_4	M_6	M_8	M_{10}
$G_1 \times G_1$	2	10	70	588	5544
$G_1 \times G_2$	2	11	90	889	9723
$G_2 \times G_2$	2	12	110	1260	16002

És senzill calcular el nombre de component connexes i la proporció d'elements amb traça nul·la de $G_i \times G_j$ a partir dels resultats coneguts sobre G_i i G_j.

Per construir altres subgrups compactes de $USp(4)$ considerem una corba C de manera que la seva jacobiana sigui el producte de dues corbes isogènies E_1 i E_2. Per exemple podem considerar E_2 isomorfa a E_1.

Definició 5.2.7. *Segons la notació anterior definim*

$$H_i = \left\{ \left. \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \right| A \in G_i \right\}.$$

I si E_2 sigui un twist de E_1, podem consultar [26] per la definició de twist d'una corba el·líptica, considerem els següents grups.

Definició 5.2.8.

$$H_i^- = \left\{ \left. \begin{pmatrix} A & 0 \\ 0 & -A \end{pmatrix} \right| A \in G_i \right\}.$$

Aquesta última construcció es pot generalitzar per a obtenir altres grups. Sigui $G = G_1$ (respectivament G_2) un subgrup compacte de $USp(2)$. Sigui G^* el subgrup de $U(2)$, el grup de matrius unitàries, obtingut al estendre G per escalars i prenent el subgrup format pels elements que tenen com a determinant una arrel k-èssima de la unitat, on k és un enter positiu fixat. De fet només considerarem arrels de la unitat definides sobre extensions quadràtiques de $\mathbb{Q}$, i per tant $k \in \{1, 2, 3, 4, 6\}$.

Donat $A \in G^*$ definim $\overline{A}$ com la conjugada complexa de A. Considerem la matriu

$$M_A = \begin{pmatrix} A & 0 \\ 0 & \overline{A} \end{pmatrix}.$$

M_A és unitària simplèctica, és a dir, $M_A \in USp(4)$. Definim H com el grup de matrius M_A amb $A \in G^*$. Podem comprovar que, com a grup topològic, H té k (resp. $2k$) components connexes i que H és compacte. A més la component connexa de la identitat és isomorfa a $USp(2)$ (resp. $SO(2)$).

Tot element $A \in G^*$ es pot escriure com $\omega^j A_0$ amb $A_0 \in G$, ω una arrel primitiva $2k$-èssima de la unitat i $1 \leq j \leq k$. Utilitzant que $tr(A_0) = tr(\overline{A}_0)$ obtenim

$$tr(M_A) = tr(A) + tr(\overline{A}) = \omega^j tr(A_0) + \omega^{-j} tr(\overline{A}_0) = (\omega^j + \omega^{-j}) tr(A_0).$$

Per tant podem calcular la successió de moments de M_A utilitzant

$$E[tr(M_A)^n] = \left(\frac{1}{k} \sum_{j=1}^{k} (\omega^j + \omega^{-j})^n \right) E[tr(A_0)^n]$$

on $E[tr(M_A)^n]$ és l'esperança sobre H i $E[tr(A_0)^n]$ sobre G.

El terme $E[tr(A_0)^n]$ és el terme n-èssim de la successió de moment $M[a_1]$ de G que ja hem calculat anteriorment. Suposant n parell podem calcular el terme entre parèntesis directament com

$$2^n, \qquad 2^n/2, \qquad (2^n+2)/3, \qquad (2^n + 2^{n/2+1})/4, \qquad (2^n + 2 \cdot 3^{n/2} + 2)/6,$$

per $k = 1, 2, 3, 4, 6$ respectivament.

Podem calcular $z(H)$, la proporció d'elements de H amb traça nul·la, obtenint que per k senar $z(H)$ és 0 (resp. 1/2) i per k parell $z(H)$ és $1/k$ (resp. 1/k+1/2).

Definició 5.2.9. *Segons la construcció anterior definim H_i^k com el grup H construït anteriorment considerant $G = G_i$ i k.*

D'aquesta manera obtenim 10 subgrups compactes propis de $USp(4)$ amb distribucions diferents. Així doncs, considerant els productes directes i el grup total obtenim 14 distribucions diferents. Recordem però que en el càlcul de les distribucions de corbes de gènere 2 es distingeixen 23 distribucions diferents i per tant ens cal considerar més grups. Per analogia al cas de corbes el·líptiques considerem

Definició 5.2.10. *Definim $J(H_i^k)$ com el grup generat per H_i^k i*

$$J = \begin{pmatrix} 0 & iId \\ -iId & 0 \end{pmatrix}.$$

H té índex 2 en $J(H)$ i tots els elements que no són de H tenen traça nul·la. Per tant la successió de moments de $M[a_1]$ de $J(H)$ és la meitat de la successió $M[a_1]$ de H. Aquestes

construccions ens permet definir 10 subgrups compactes més. Podem comprovar però que les distribucions de H_i^2 i $J(H_i^1)$ són iguals, i per tant no considerarem $J(H_i^1)$. Obtenim així 22 distribucions diferents.

Com que H_i^1 és exactament H_i i les distribucions de H_i^2 és igual a la de H_i^-, tot i que aquests dos subgrups no són conjugats, utilitzarem H_i i H_i^- envers de H_i^1 i H_i^2, respectivament.

Finalment definim $J(G_1 \times G_1)$ i $J(G_2 \times G_2)$ de forma anàloga. El grup $J(G_2 \times G_2)$ és el normalitzador de $SO(2) \times SO(2)$ en $USp(4)$ i té 8 components connexes. Considerem llavors un subgrup K de $J(G_2 \times G_2)$ d'índex 2 no conjugat de $(G_2 \times G_2)$. Observem que K està determinat per les propietat que la component connexa de la identitat és $SO(2) \times SO(2)$ i que el grup de components és cíclic d'ordre 4.

Podem veure el càlcul de la successió de moments i de $z(H)$ pels grups definits anteriorment en la taula 5.2. Contrastant amb els resultats de la taula 5.1 podem comprovar que com les distribucions dels grups construïts són les distribucions obtingudes per a corbes. Els únics dos grups que segons aquests càlculs no són grups de distribució de cap corba són $J(H_2^6)$ i $J(G_2 \times G_2)$. En [10] es descriuen possibles raonaments teòrics per a explicar aquest fet.

Els resultats presentats permet conjecturar que si C és una corba amb distribució número n de la taula 5.1 llavors C està distribuïda respecte el grup H número n de la taula 5.2. Aquesta conclusió es reforça a partir del càlcul de la successió $M[a_2]$, obtenint una igualtat entre els primers valors de les successió de moments de la corba i del grup H. A més també es realitzen els càlculs restringits a cada una de les components connexes dels grups i també s'aproxima la dimensió d de la taula 5.2 a partir de la corba. En tots aquests càlculs els resultats numèrics coincideixen amb els resultats teòrics esperats. Podem trobar tots aquests càlculs en [10].

Els resultats presentats permeten plantejar la següent conjectura, descrivint la conjectura 4.2.4 per a corbes de gènere 2.

Conjectura 5.2.11 (Kedlaya-Sutherland)**.** *Sigui C una corba algebraica no singular sobre $\mathbb{Q}$ de gènere 2. Llavors la successió $(\theta_{v,1}, \ldots, \theta_{v,g})_{v \in \Sigma}$ està equidistribuïda en $[0, \pi]^g$ respecte la mesura $h_*(\mu_H)$ d'un dels 23 subgrups H llistats a la taula 5.2. Per la majoria de corbes aquest grup és $USp(4)$.*

A més, en [10] els autors també conjecturen que donada una corba C, el grup de distribució de la taula 5.2 és H_C.

#	H	d	$c(H)$	$z(H)$	M_2	M_4	M_6	M_8	M_{10}
1	$USp(4)$	10	1	0	1	3	14	84	594
2	$G_1 \times G_1$	6	1	0	2	10	70	588	5544
3	$G_1 \times G_2$	4	2	0	2	11	90	889	9723
4	H_1^3	3	3	0	2	12	110	1204	14364
5	H_1	3	1	0	4	32	320	3584	43008
6	H_1^6	3	6	1/6	2	12	100	980	10584
7	H_1^4	3	4	1/4	2	12	100	1008	11424
8	$G_2 \times G_2$	2	4	1/4	2	12	110	1260	16002
9	$J(G_1 \times G_1)$	6	2	1/2	1	5	35	294	2772
10	$J(H_1^3)$	3	6	1/2	1	6	55	602	7182
11	H_1^-	3	2	1/2	2	16	160	1792	21504
12	H_2^3	1	6	1/2	2	18	220	3010	43092
13	H_2	1	2	1/2	4	48	640	8960	129024
14	$J(H_1^6)$	3	12	7/12	1	6	50	490	5292
15	H_2^6	1	12	7/12	2	18	200	2450	31752
16	$J(H_1^4)$	3	8	5/8	1	6	50	504	5712
17	H_2^4	1	8	5/8	2	18	200	2520	34272
18	$J(H_1^-)$	3	4	3/4	1	8	80	896	10752
19	K	2	4	3/4	1	9	100	1225	15876
20	$J(H_2^3)$	1	12	3/4	1	9	110	1505	21546
21	H_2^-	1	4	3/4	2	24	320	4480	64512
22	$J(H_2^4)$	1	16	13/16	1	9	100	1260	17136
23	$J(H_2^-)$	1	8	7/8	1	12	160	2240	32256
*	$J(G_2 \times G_2)$	2	8	5/8	1	6	55	630	8001
*	$J(H_2^6)$	1	24	19/24	1	9	100	1225	15876

Taula 5.2: Aquesta taula és la taula 13 de [10]. Per cada grup H s'indica la distribució # segons la taula 5.1, la dimensió real d, i el nombre de components connexes $c(H)$. La columna $z(H)$ és la proporció de traces nul·les en H. El valor M_i és el moment i-èssim de a_1. Els dos últims grups són els únics que no són grups de distribució de cap corba.

5.3 Dependència de l'anell d'endomorfismes

La conjectura 5.2.11 particularitza la conjectura 4.2.4 per corbes de gènere 2 descrivint la mesura μ_C associada a la corba C com $h_*(\mu_H)$, per algun grup H de la taula 5.2. És natural preguntar-se com podem determinar aquest grup H. Els càlculs realitzats en [10] permeten donar una primera aproximació a partir de l'estructura de l'anell d'endomorfismes. Per presentar els resultats revisem el teorema de classificació 4.1.1 per corbes de gènere 2.

Sigui C una corba de gènere 2 amb Jacobiana simple. A partir de 4.1.1 podem obtenir la següent classificació d'$End^0(C)$:

Tipus I: La restricció $e_0|g$ implica que només es pot donar $e_0 = 1$ o 2. Aquests dos casos són possibles. El Tipus I(1) és el cas trivial i s'obté $End(C) = \mathbb{Z}$, també direm que la corba té ZM. En el Tipus I(2) obtenim que $End^0(C)$ és una extensió quadràtica real de $\mathbb{Q}$ i direm que la corba té RM.

Tipus II: La restricció $2e_0|g$ implica que només es pot donar el Tipus II(1). Aquest cas pot donar-se i $End^0(C)$ és una àlgebra de quaternions sobre $\mathbb{Q}$, direm que la corba té QM.

Tipus III: Només és possible el Tipus III(1), tot i això no pot existir cap corba de manera que la seva Jacobiana sigui del Tipus III(1). Aquest resultat és un teorema no trivial, el qual no exposarem.

Tipus IV: La restricció $e_0d^2|g$ implica que només es pot donar $d = 1$ i $e_0 = 1$ o 2. D'aquests dos casos només es dona el Tipus IV(2,1). En aquest cas $End^0(C)$ és un cos quàrtic de multiplicació complexa i direm que la corba té CM.

Recordem que donada una extensió finita K de $\mathbb{Q}$ l'únic que podem dir sobre $End^0_K(C)$ és que és una subàlgebra de $End^0(C)$.

En [10] els autors especulen, basats en els resultats numèrics obtinguts sobre una gran varietat de corbes, les següents relacions entre l'estructura de la Jacobiana i la distribució de la corba:

- Totes les distribucions, excepte la #1 i la #19, es poden donar per a corbes amb jacobiana no simple. Per a corbes amb jacobiana simple només poden donar-se les distribucions #1, #2, #11 i #19 tal i com descrivim a continuació.
- La distribució #1 es dona només per a corbes amb ZM, és a dir, per a corbes amb imatge de Galois gran.
- Per a corbes amb RM només es pot donar la distribució #2. Aquesta distribució també es dona per a corbes tal que la jacobiana descomposi com el producte de dues corbes el·líptiques sense CM no isogènies.

- Per a corbes amb QM només es pot donar la distribució #11. Aquesta distribució també es dona per a corbes amb jacobiana isogènia al producte d'una corba el·líptiques sense CM i un twist de la corba.
- La distribució #19 es dona només per a corbes amb CM.

Així doncs, per a corbes amb Jacobiana simple, tenim una possible descripció de la distribució de la corba. Observem però que totes les corbes C amb QM considerades en [10] compleixen

- $End^0_L(C) = End^0_{\mathbb{Q}}(C)$ on L és una extensió quadràtica de $\mathbb{Q}$.
- $End^0_{\mathbb{Q}}(C)$ és una extensió quadràtica de $\mathbb{Q}$.

No totes les corbes QM tenen les propietats anteriors i per tal d'ampliar l'estudi realitzat en [10] és interessant considerar la corba D definida en del teorema 2.1 de [2] per

$$y^2 = \left(x^2 + \frac{7}{2}\right)\left(\frac{83}{30}x^4 + 14x^3 - \frac{1519}{30}x^2 + 49x - \frac{1813}{120}\right).$$

Segons es demostra en [2], D és una corba no singular de gènere 2 amb les següent propietats:

- $End^0_L(D) = End^0_{\mathbb{Q}}(D)$ on $L = \mathbb{Q}(\sqrt{-6}, \sqrt{-14})$.
- $End^0_{\mathbb{Q}(\sqrt{-14})}(D) = \mathbb{Q}(\sqrt{2})$.
- $End^0_{\mathbb{Q}(\sqrt{21})}(D) = \mathbb{Q}(\sqrt{3})$.
- $End^0_{\mathbb{Q}(\sqrt{-6})}(D) = \mathbb{Q}(\sqrt{-6})$.
- $End_{\mathbb{Q}}(D) = \mathbb{Z}$.

L'estructura dels endomorfismes de D i la de les corbes amb QM de [10] és doncs clarament diferent. Estudiem la distribució de D, que segons la classificació anterior ha de ser #11. El càlcul de la distribució necessita d'algorismes específics per tal de poder realitzar els càlculs de manera efectiva. Per aquest motiu agraïm el suport d'Andrew V. Sutherland, membre del departament de matemàtiques del Massachusetts Institute of Technology, per realitzar els càlculs necessaris utilitzant els algorismes desenvolupats en [11].

Per tal de poder realitzar els càlculs es considera el següent model amb coeficients enters de D,

$$y^2 = 9960x^6 + 50400x^5 - 147420x^4 + 352800x^3 - 692370x^2 + 617400x - 190365$$

N	$z(D)$	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
2^{10}	0.804	0.089	0.917	0.709	7.264	6.066	69.299	53.936	722.786
2^{11}	0.787	0.052	0.857	0.306	6.492	1.762	62.840	3.097	682.179
2^{12}	0.779	0.073	0.879	0.458	7.035	3.962	72.702	40.477	851.647
2^{13}	0.765	0.001	0.945	-0.175	7.706	-2.730	79.503	-38.333	922.307
2^{14}	0.763	0.009	0.931	-0.146	7.398	-2.425	73.681	-33.492	820.732
2^{15}	0.759	0.006	0.947	-0.042	7.595	-0.790	76.167	-11.106	854.168
2^{16}	0.760	0.004	0.947	-0.082	7.543	-1.236	75.315	-16.240	841.787
2^{17}	0.755	-0.003	0.966	-0.102	7.658	-1.396	76.253	-18.158	852.224
2^{18}	0.753	-0.001	0.966	-0.055	7.577	-0.765	74.810	-10.095	831.420
2^{19}	0.752	-0.007	0.990	-0.090	7.850	-1.085	77.963	-13.901	869.332
2^{20}	0.752	-0.005	0.995	-0.070	7.916	-0.843	78.681	-10.417	876.966
2^{21}	0.752	-0.002	0.998	-0.042	7.963	-0.553	79.336	-7.304	885.108
2^{22}	0.751	-0.002	0.999	-0.028	7.967	-0.354	79.293	-4.455	883.291
2^{23}	0.751	-0.002	0.998	-0.020	7.976	-0.257	79.559	-3.397	887.934

Taula 5.3: Per cada valor N es calcula una aproximació de $z(D)$ i el valor del moment i-èssim M_i pels primers menors a N on la corba té bona reducció.

obtingut a partir de $(x, y) \to (x, y/60)$. Els resultats numèrics es resumeixen en la taula 5.3.

Comparant aquests resultats amb la taula 5.2 podem assumir que la corba D segueix la distribució #18. En la figura 5.1 es pot observar la diferència entre les distribucions #11 i #18.

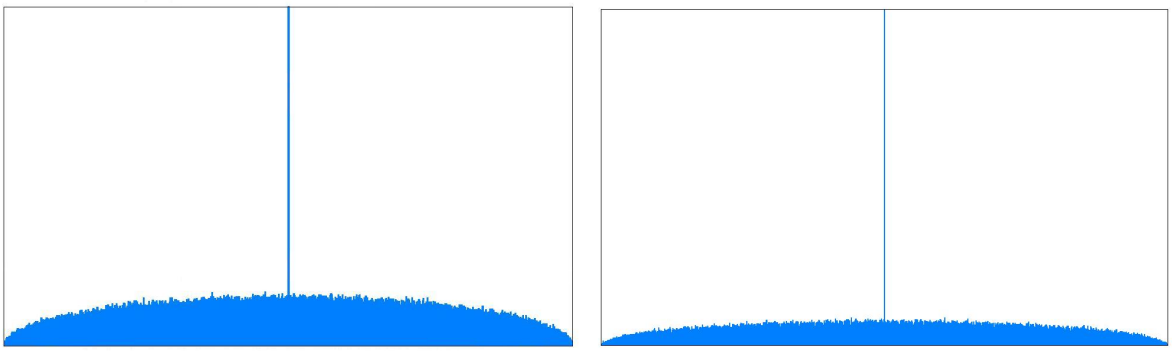

Figura 5.1: Comparació entre les distribucions #11 i #18. A l'esquerra veiem una aproximació de la distribució #11 utilitzant la corba $y^2 = x^5 + x^3 + x$ i a la dreta una aproximació de la distribució #18 utilitzant la corba D. En ambdós casos els resultats són pels primers menors a $N = 2^{23}$.

Per tant les corbes amb QM no tenen una mateixa distribució μ. Així doncs no podem esperar trobar una classificació de les distribucions associades a les corbes de gènere 2 considerant únicament l'estructura de $End^0_{\mathbb{Q}}(C)$ sinó que cal considerar també $End^0_K(C)$ per extensions finites $K|\mathbb{Q}$.

Capítol 6

Conclusions

L'estudi anterior ens permet refinar la classificació proposada en [10]. Tot i així, per tal de poder extreure conclusions més sòlides seria necessari realitzar un estudi més ampli considerant altres corbes amb QM.

Per una banda podem plantejar un estudi un estudi numèric per a obtenir més informació sobre la distribució de les corbes de gènere 2. Seria necessari doncs considerar corbes de manera que l'estructura dels endomorfismes tingui propietats similars a la corba D definida anteriorment.

També podríem plantejar un estudi teòric, amb l'objectiu d'explicar perquè cal considerar $End_K^0(C)$, per extensions finites $K|\mathbb{Q}$, per descriure la distribució de la corba C.

Bibliografia

[1] L. Clozel, M. Harris, R. Taylor, *Automorphy for Some l-adic Lifts of Automorphic Mod l Galois Representations,* Publications Mathématiques de L'IHÉS, vol. 108, 2008.

[2] L. V. Dieulefait, V. Rotger, *On Abelian surfaces with potential quaternionic multiplication,* Bull. Belgian Math. Soc., vol. 12, núm 4, pp. 617-624, 2005.

[3] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. [Finiteness theorems for abelian varieties over number fields],* , Inventiones Mathematicae, vol. 73, núm. 3, pp. 349-366, MR 718935 (85g:11026a) revisat per James Milne, 1983.

[4] W. Fulton, J. Harris, *Representation theory: a first course,* Graduate Texts in Mathematics, vol.129, Springer, 1991.

[5] S. Gelbart, *An elementary introduction to the Langlands program,* Bull. American Maht. Soc., vol. 10, núm. 2, 1984.

[6] S. Gelbart, H. Jacquet, *A relation between automorphic representations of GL(2) and GL(3),* Ann. Sci. École Norm. Sup., vol. 11, pp. 471-552, 1978.

[7] M. Harris, N. Shepherd-Barron, R. Taylor, *Ihara's lemma and potential automorphy,* Preprint, 2006.

[8] R. Hartshorne, *Algebraic geometry,* Graduate Texts in Mathematics, vol.52, 1997.

[9] N.M. Katz, P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy,* American Mathematical Society, 1999.

[10] K.S. Kedlaya, A.V. Sutherland, *Hyperelliptic Curves, L-polynomials, and Random Matrices,* Arithmetic, Geometry, Cryptography and Coding Theory, American Mathematical Society, 1997.

[11] K.S. Kedlaya, A.V. Sutherland, *Computing L-series of hyperelliptic curves,* Algorithmic Number Theory Symposium-ANTS VIII, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 312-326.

[12] H. Kim, F. Shahidi, *Functorial products for $GL(2) \times GL(3)$ and the symmetric cube for $GL(2)$,* , Annals of Math., vol. 155, pp. 837-893, 2002.

[13] H. Kim, *Functoriality for the exterior square of GL_4 and the symmetric fourth power of GL_2,* Jounal Amer. Math. Soc., vol. 16, pp. 139-183, 2003.

[14] A.W. Knapp, *Introduction to the Langlands program,* Proceedings of Symposia in Pure Mathematics, vol. 61, pp. 245-302, 1997.

[15] P. Koosis, *The logarithmic integral: Volume I,* Cambridge University Press, 1998.

[16] B. Mazur, *Finding meaning in error terms,* Bull. Amer. Math. Soc., vol.45, núm 1, pp. 185-228, 2008.

[17] D. Mumford, *Abelian varieties,* 2nd Edition, Oxford University Press, Oxford, 1974.

[18] M.R. Murty, V.K. Murty, *Non-vanishing of L-functions and applications,* Progress in Mathematics, vol.157, Birkhäuser, 1997.

[19] J. Neurkirch, *Algebraic Number Theory,* Grundlehren der mathematischen Wissenschaften, vol.322, Springer-Verlag, 1999.

[20] V. Rotger, *Introducció a les varietat abelianes,* Notes del seminari de teoria de nombres 14è any, Collbató, pp. 27-42, 2000.

[21] M. Schein, *Modularity lifting theorems and the proof of the Sato-Tate conjecture,* Notes for the Hebrew University Number Theory Seminar.

[22] J.P. Serre, *A course in arithmetic,* Graduate texts in mathematics, vol.7, Springer, 1996.

[23] J.P. Serre, *Abelian l-Adic Representations and Elliptic Curves,* segona edició, Addison-Wesley, Redwood City, 1989.

[24] J.P. Serre, *Groupes linéaires modulo p et points d'ordre fini des variétés abéliennes,* Collège de France course notes by Eva Bayer-Fluckiger, 1986. http://alg-geo.epfl.ch/ bayer/files/Serre-cours.pdf.

[25] J.P. Serre, *Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques,* Proceedings of Symposia in Pure Mathematics, vol. 55, pp. 377-400, 1994.

[26] J.H. Silverman, *The arithmetic of elliptic curves,* GMT 106, Springer-Verlag 1986.

[27] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves,* GTM 151, Springer-Verlag, 1995.

[28] J. Tate, *Algebraic cycles and poles of zeta functions,* Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963) ed. O. F. G. Schilling, Harper & Row, pp. 93-110, New York, 1965.

[29] A.J. Wiles, *Modular elliptic curves and Fermat's Last Theorem,* Annals of Math., vol. 141., pp 443-551, 1995.

[30] Y.G. Zarhin, *Hyperelliptic jacobians with complex multiplication,* Mathematical Research Letters, vol. 7, núm. 1, pp. 123-132, 2000.