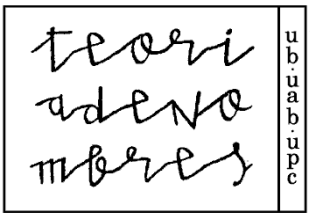
NOTES DEL SEMINARI



COJECTURA DE BIRCH I S.DYER

Barcelona, 2003

5

Notes del Seminari de Teoria de Nombres (UB-UAB-UPC)

COJECTURA DE BIRCH I S.DYER

Edició a cura de

J.Quer

Amb contribucions de

P. Bayer
J. Guàrdia
E. Nart
E. Torres
A. Travesa
M. Vela

J. Quer
Fac. de Matemàtiques
i Informàtica
Univ. Politècnica de Catalunya
Pau Gargallo, 5
08228 Barcelona Espanya

Classificació AMS
Primària:
Secundària:

Barcelona, 2003
Amb suport parcial de MCYT, BFM2000-0627

ISBN: 84-923250-4-6

La conjectura de Birch i Swinnerton-Dyer

ÀNGELA ARENAS[1]

En aquestes notes es tracta d'enunciar el contingut d'aquesta conjectura així com també de fer una breu exposició dels fets més rellevants que s'han produït fins ara.

§1. Origen i desenvolupament de la conjectura

Es considera l'equació polinòmica en dues variables:

$$f(x,y)=0 \qquad (*)$$

amb coeficients racionals. Si $f(x,y)$ és una forma quadràtica, el teorema de Hasse-Minkowski ens assegura que $(*)$ té solucions racionals no trivials si i només si $(*)$ té solucions no trivials a $\mathbb{Q}_p$, per a tot p, inclós $p=\infty$. El teorema de Minkowski-Siegel dóna una expressió quantitativa del resultat precedent. Concretament, Siegel prova que la densitat de punts racionals en una quàdrica n–dimensional es pot expressar en termes de densitats de punts p–àdics i aquests últims valors depenen directament del nombre de solucions de l'equació corresponent mòdul p. De fet per a tot primer p, llevat d'un nombre finit, es té que essencialment aquests valors son $p^{-1}N_p$ on

$$N_p=\operatorname{card}\Big\{(x_1,\ldots,x_n)\in\mathbb{F}_p \mid f(x_1,\ldots,x_n)\equiv 0 \pmod p\Big\}.$$

Si $f(x,y)$ és ara el polinomi que defineix un corba el·líptica $E/\mathbb{Q}$ definida sobre $\mathbb{Q}$, el teorema de Mordell, el qual va ser conjecturat per Poincaré, diu que el grup $E(\mathbb{Q})$ dels punts $\mathbb{Q}$-racionals de E és finit-generat: $E(\mathbb{Q})=$

[1]Conferència impartida el 23 de gener de 1999. Amb el suport parcial de la DGES: PB96–0166.

$\mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$, $r = \text{rang}\,(E(\mathbb{Q}))$, $r \geq 0$. El càlcul del subgrup de torsió és efectiu tan teòricament com a la pràctica. De fet, el subgrup de torsió és un dels 15 grups següents ([Maz1], [Maz2]):

$$E(\mathbb{Q})_{\text{tors}} = \begin{cases} \mathbb{Z}/n\mathbb{Z}, & 1 \leq n \leq 10 \ \text{ ó } \ n = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & 1 \leq n \leq 4\,. \end{cases}$$

En general, pel rang r es poden trobar fites superiors per descens i fites inferiors si es té la sort de trobar solucions independents. El nombre de solucions racionals de $(*)$ és finit si i només si $r = 0$.

Part de la demostració del teorema de Mordell consisteix en provar que existeix una forma quadràtica definida positiva que s'anomena altura (és única)

$$\hat{h} : E(\mathbb{Q}) \otimes \mathbb{R} \longrightarrow \mathbb{R}$$

amb $\hat{h}(P) - \log \text{màx}\{|\text{num}\ x(P)|,\ \text{den}\, x(P)|\}$ afitat, on $P = (x(P),\, y(P))$ és una solució racional de $(*)$. Si

$$N(A) := \text{card}\Big\{P \in \mathbb{Q}^2 \mid f(P) = 0,\ |\text{num}\ x(P)| \leq A\,,\ |\text{den}\ x(P)| \leq A\Big\}\,,$$

aleshores $N(A) \sim C(\log A)^{r/2}$ $(A \to \infty)$ on $r = \text{rang}(E(\mathbb{Q}))$ i $C > 0$ és una constant donada per

$$C = \frac{\pi^{r/2}\ \#\ (E(\mathbb{Q})_{\text{tors}})}{(r/2)!\ \sqrt{R}}$$

on $R = R(E/\mathbb{Q}) = \det\left(\langle P_i, P_j\rangle_E\right)_{1 \leq i,j \leq r}$, on $P_1, \ldots, P_r$ és una base de $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ i $\langle\,,\rangle$ denota l'aparellament de Néron-Tate. $R(E/\mathbb{Q})$ s'anomena el regulador el·líptic de $E/\mathbb{Q}$ i és el volum d'un domini fonamental de la xarxa de $\mathbb{R} \otimes E(\mathbb{Q})$, $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$, calculat utilitzant la forma quadràtica $\hat{h}$. Si $r = 0$, per conveni escrivim $R = 1$.

Exemples (Zagier)

1) $y^2 = 4x^3 - 27,\ r = 0,\ C = \#\,(E(\mathbb{Q})_{\text{tors}}) = 3\,.$

2) $y^2 - y = x^3 - x,\ r = 1,\ \#\,(E(\mathbb{Q})_{\text{tors}}) = 1,\ C = 8.8464916\ldots$

3) $y^2 = 4x^3 - 28x + 25,\ r = 3,\ \#(E(\mathbb{Q})_{\text{tors}}) = 1,\ C = 6.48553546\ldots$

Birch i Swinnerton-Dyer (1963–65) varen formular una conjectura que determina r i en certa manera C. La idea és que una corba el·líptica amb r molt gran (o bé, donat r, amb C molt gran) té un nombre de punts racionals

molt gran i per tant hauria de tenir en promig un nombre relativament gran de solucions mòdul p, quan tots els primers p varien. Més concretament, si

$$N_p = \mathrm{card}\Big\{ P = (x,y) \in \mathbb{F}_p^2 \mid f(x,y) \equiv 0 (\mathrm{mod}\, p) \Big\},$$

la conjectura de Birch i Swinnerton-Dyer (BSD) diu que hauria d'haver una fórmula assimptòtica

$$\prod_{p<t} \frac{N_p + 1}{p} \sim C_1 (\log\ t)^r \quad (t \to \infty)\,.$$

Per a una formulació més precisa de la conjectura de Birch i Swinnerton-Dyer és convenient treballar amb la sèrie L de Hasse-Weil associada a la corba el·líptica. Sigui $E/\mathbb{Q}$ una corba el·líptica i sigui

$$y^2 + a_1 xy + a_3 = x^3 + a_2 x^2 + a_4 x + a_6$$

$a_i \in \mathbb{Z}$, una equació de Wierstrass global-minimal per a $E/\mathbb{Q}$ i denotem per Δ el seu discriminant minimal. Per a cada primer p sigui A_p el nombre de punts de la corba reduïda $\tilde{E}$ mòdul p (cal incloure el punt de l'infinit); i sigui $t_p = 1 + p - A_p$.

La sèrie L associada a $E/\mathbb{Q}$ ve definida pel següent producte d'Euler:

$$L(E/\mathbb{Q}, s) = \prod_{p|\Delta} (1 - t_p\ p^{-s})^{-1} \prod_{p\not|\,\Delta} (1 - t_p\ p^{-s} + p^{1-2s})^{-1},$$

el qual és convergent per a $\mathrm{Re}(s) > 3/2$. Es conjectura que $L(E/\mathbb{Q}, s)$ té continuació analítica a tot el pla complex. És cert per a corbes el·líptiques amb multiplicació complexa i per a corbes el·líptiques modulars. Si aquest és el cas, considerem el desenvolupament de Taylor:

$$L(E/\mathbb{Q}, s) = c_0 + c_1(s-1) + \ldots + c_m (s-1)^m + \ldots$$

al voltant de $s = 1$.

Es defineix el *rang analític* ρ de $E/\mathbb{Q}$ per $\rho := \min\{i \mid c_i \neq 0\}$. És a dir: $\rho = 0 \Leftrightarrow L(E/\mathbb{Q}, 1) \neq 0$ i

$$\rho = m \geq 1 \Leftrightarrow L(E/\mathbb{Q}, 1) = 0,\ L^{(i)}(E/\mathbb{Q}, 1) = 0,\ i < m,\ L^{(m)}(E/\mathbb{Q}, 1) \neq 0\,.$$

La *conjectura de Birch i Swinnerton-Dyer* (cf. [B-Sw1]) diu:

1) $\rho = r$.

2) $c_r = \lim_{s\to 1} \dfrac{L(E/\mathbb{Q},s)}{(s-1)^r} = \dfrac{R(E/\mathbb{Q})}{\left[\#\left(E(\mathbb{Q})_{\text{tors}}\right)\right]^2}\,\Omega\, S$

on $R(E/\mathbb{Q})$ és el regulador el·líptic de $E/\mathbb{Q}$ definit abans; Ω és el producte dels factors de Tamagawa. Més concretament, si $\omega = \frac{dx}{2y+a_1\,x+a_3}$ és la forma diferencial holomorfa associada amb un model global-minimal de $E/\mathbb{Q}$ (que és única llevat del signe) es té

$$\Omega = \Omega_\infty \prod_p \Omega_p\,,$$

amb

$$\Omega_\infty = \int_{E(\mathbb{R})} |\omega|\,,$$

on $E(\mathbb{R})$ és el grup de $\mathbb{R}$-punts racionals de E. $E(\mathbb{R})$ és un grup de Lie real compacte de dimensió 1, amb 1 ó 2 components connexes segons que $\Delta < 0$ ó $\Delta > 0$. De fet, Ω_∞ és el període real positiu de ω si $E(\mathbb{R})$ és connex, o bé és el doble del període real positiu de ω si $E(\mathbb{R})$ té 2 components connexes.

$$\Omega_p := \#\,\left(\frac{E(\mathbb{Q}_p)}{E_0(\mathbb{Q}_p)}\right)$$

és el nombre de components connexes del model de Néron de $E/\mathbb{Q}_p$.

Si E té bona reducció a p, aleshores $\Omega_p = 1$. És possible expressar els factors de Tamagawa Ω_p, via mesures de Haar, com a valors d'integrals p-àdiques molt semblants a la integral arquimediana que defineix Ω_∞.

S és un enter quadrat que se suposa que és l'ordre del grup de Shafarevich-Tate $\text{Ш}(E/\mathbb{Q})$ de la corba el·líptica $E/\mathbb{Q}$. Quan es va formular aquesta conjectura no es coneixia l'existència de cap $\text{Ш}(E/\mathbb{Q})$ finit. $\text{Ш}(E/\mathbb{Q})$ és un grup de torsió i és "fàcil" calcular la seva 2-component i la seva 3-component. Cassels [Ca1] va provar que si $\text{Ш}(E/\mathbb{Q})$ és finit aleshores el seu ordre és un quadrat. Tate prova el mateix resultat per a una corba el·líptica E/K definida sobre un cos de nombres K.

Rubin (1987) és el primer que dóna exemples concrets de corbes el·líptiques $E/\mathbb{Q}$ amb grup de Shafarevich-Tate finit:

$$E/\mathbb{Q} : y^2 = x^3 + 17x,\ \text{Ш}(E/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$
$$E/\mathbb{Q} : y^2 = x^3 - 2^8 3^4 5^2,\ \text{Ш}(E/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

i la conjectura de Birch i Swinnerton-Dyer és certa per a aquestes corbes el·líptiques.

Podem ara escriure la conjectura de Birch i Swinnerton-Dyer sota la forma:
1) $\rho = r$.
2) $\lim_{s\to 1} \dfrac{L(E/\mathbb{Q},s)}{(s-1)^r} = \Omega_\infty \prod_p \Omega_p \dfrac{R(E/\mathbb{Q})\ \#\text{Ш}(E/\mathbb{Q})}{\left[\#\left(E(\mathbb{Q})_{\text{tors}}\right)\right]^2}$.

§2. Fets a favor de la conjectura

(i) Evidència numèrica

En els articles ([B-Sw1], [B-Sw2]) s'estudia la conjectura per a corbes el·líptiques $E_D/\mathbb{Q}$ amb equació: $y^2 = x^3 - Dx$.

Aquestes corbes el·líptiques són amb multiplicació complexa per $\mathbb{Z}[i]$ i en conseqüència

$$L^*(E_D/\mathbb{Q},s) := \Omega_\infty^{-1} \prod_p \Omega_p^{-1}\ L(E_D/\mathbb{Q},s)$$

és essencialment una sèrie L de Hecke i Birch i Swinnerton-Dyer donen una expressió finita de $L^*(E_D/\mathbb{Q},1)$. De fet computen

$$\gamma := \left[\#\left(E(\mathbb{Q})_{\text{tors}}\right)\right]^2\ L^*(E_D/\mathbb{Q},1)\,,$$

per a 1348 valors de D. Per a cada un d'aquests valors tracten de computar el rang del grup de Mordell $E(\mathbb{Q})$, juntament amb l'ordre de $\text{Ш}(2)$ i ho aconsegueixen en prop de 200 casos. Per a aquests casos un hauria de tenir d'acord amb la conjectura (BSD):

- $\gamma = 0$, si $r > 0$
- $\gamma = \#\text{Ш}(E/\mathbb{Q})$, si $r = 0$.

En cadascun dels més de 1000 casos on es calcula r, la màquina va trobar $\gamma = 0$, si $r > 0$; i que γ és un quadrat de manera que la seva 2-component

coincideix amb l'ordre de $Ш(2)$, si $r = 0$. De fet, fins i tot en els casos en què el seu programa no determina el valor de r ni de $Ш(2)$, es té que γ sempre és un quadrat. Concretament, si $r = 0$ els valors que surten per a γ i.e. pel nombre que se suposa és $\#Ш(E/\mathbb{Q})$ són: 1, 4, 9, 16, 25, 36, 49 i 81.

Stephens [Ste] dóna evidència numèrica per a corbes el·líptiques definides per

$$x^3 + y^3 = D\,.$$

Dóna evidència per a centenars de casos amb $r = 0$ o amb $r = 1$, també per a 4 casos amb $r = 2$ i per a un cas amb $r = 3$.

(ii) Consistència per isogènies

Dues corbes el·líptiques $E/\mathbb{Q}$ i $E'/\mathbb{Q}$, $\mathbb{Q}$-isògenes tenen el mateix nombre de punts mòdul p, per a tot p, i, per tant, tenen la mateixa sèrie L. Aleshores, si la conjectura (BSD) és certa, la quantitat

$$\Omega_\infty \prod_p \Omega_p \frac{Ш(E/\mathbb{Q})\ R(E/\mathbb{Q})}{[\,\#E(\mathbb{Q})_{\text{tors}}]^2} \qquad (**)$$

ha d'ésser invariant per isogènies suposant que $\#Ш(E/\mathbb{Q}) < \infty$. Aleshores, Cassels (1965) prova que, per a corbes el·líptiques sobre $\mathbb{Q}$, $(**)$ és un invariant per isogènies.

Els termes del valor $(**)$ un a un no són invariants per isogènies!

(iii) Teorema de Coates-Wiles [Co-W]

Sigui K un cos quadràtic imaginari de discriminant D, amb nombre de classes $h(D)$ igual a 1. Sigui E una corba el·líptica definida sobre F, on F és $\mathbb{Q}$ o bé el propi K, amb multiplicació complexa per K (i.e. $End(E) = \mathcal{O}, \mathcal{O}$ anell d'enters de K).

Aleshores, si $L(E/F, 1) \neq 0$, es té que $E(F)$ és un grup finit.

(iv) Teorema de Greenberg (1983)

Sigui $E/\mathbb{Q}$ una corba el·líptica amb multiplicació complexa. Suposem que $L(E, s)$ té un zero en $s = 1$ amb multiplicitat $\rho \geq 1$. Aleshores $r \geq 1$ o bé el

grup de Shafarevich-Tate conté una còpia del grup divisible $\mathbb{Q}_p/\mathbb{Z}_p$ per a tot primer $p \neq 2, 3$ on E té bona reducció ordinària.

(v) Fòrmula de Gross-Zagier [Gr-Z]

Sigui $E/\mathbb{Q}$ una corba el·líptica modular tal que $L(E/\mathbb{Q}, 1) = 0$. La fòrmula de Gross-Zagier relaciona el valor de $L'(E/\mathbb{Q}, 1)$ amb la altura canònica d'un punt de Heegner $P \in E(\mathbb{Q})$. En particular proven:
1) Si $L(E/\mathbb{Q}, 1) = 0$, aleshores, $L'(E/\mathbb{Q}, 1) \neq 0 \Leftrightarrow P \in E(\mathbb{Q})$ té ordre infinit.
2) Si $L(E/\mathbb{Q}, 1) = 0$ i rang $E(\mathbb{Q}) = 1$, aleshores, $L'(E/\mathbb{Q}, 1)$ és un múltiple racional de $\Omega\ R(E/\mathbb{Q})$ i de vegades es pot provar que és un quadrat.
3) La corba el·líptica $E/\mathbb{Q}$ de conductor 5077 donada per

$$-139y^2 = x^3 + 10x^2 - 20x + 8\,,$$

satisfà $\rho = r = 3$.

El primer que utilitza els "punts de Heegner" per a produir punts racionals en corbes el·líptiques és el propi Heegner (1952) en l'article en el qual prova que el nombre de classes $h(D)$ d'un cos quadràtic imaginari és 1 només per a un nombre finit de D's:

$$D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\,.$$

Birch ([Bi], [Bi-Ste]) dóna un algorisme inspirat en el treball de Heegner per construir punts racionals d'ordre infinit en certes corbes el·líptiques. Birch defineix els punts de Heegner que van ésser extensament estudiats, des del punt de vista numèric, per Birch i Stephens. De fet, ells van conjecturar expressions equivalents a la fòrmula de Gross-Zagier. Baker i Stark proven que $h(D) = 2$ per a un nombre finit de discriminants. Goldfeld (1975) va provar que si existeix una sèrie L amb propietats analítiques apropiades i amb un zero d'ordre suficientment gran en el punt de simetria de la seva equació funcional, aquesta funció L donaria una fita inferior efectiva de $h(D)$. La L-sèrie de la corba el·líptica : $-139y^2 = x^3 + 10x^2 - 20x + 8$, [Bu-Gr-Z] té totes les propietats demanades per Goldfeld.

Amb la qual cosa l'equació $h(D) = n,\ n$ fix té un nombre finit de solucions. La última fita que s'obté és

$$h(D) > C \prod_{p|D} \left(1 - \frac{2}{\sqrt{p}}\right) \log |D|\,,$$

on C és una constant que és computable efectivament.

(vi) Teoremes de Kolyvagin (1988) ([Ko1], [Ko2])

a) Sigui $E/\mathbb{Q}$ una corba el·líptica modular amb $L(E/\mathbb{Q},1)\neq 0$. Aleshores, el grup de Mordell $E(\mathbb{Q})$ és finit i el grup de Shafarevich-Tate $\text{Ш}(E/\mathbb{Q})$ també és finit.

Aquest resultat també està provat per Kato (1977) sense utilitzar el cos quadràtic auxiliar ni punts de Heegner.

b) Sigui $E/\mathbb{Q}$ una corba el·líptica modular. Si $L(E/\mathbb{Q},1)=0$, però $L'(E/\mathbb{Q},1)\neq 0$, aleshores rang $E(\mathbb{Q})=1$ i el grup de Shafarevich-Tate és finit.

Anem a donar una idea de la demostració del segon teorema de Kolyvagin, que consta de tres pasos importants:

1. Lema de no anul·lació.

   Es tria un cos quadràtic imaginari $K/\mathbb{Q}$ de discriminant D amb les següents condicions:

   - Si p és un factor primer del conductor de $E/\mathbb{Q}$, aleshores p descompon en K.
   - La sèrie $L(E/K,s)$ té un zero simple en $s=1$, amb la qual cosa, com que $L(E/K,s)=L(E/\mathbb{Q},s)\ L(E^{(D)}/\mathbb{Q},s)$ on $E^{(D)}/\mathbb{Q}$ és la torçada de $E/\mathbb{Q}$ pel caràcter de K; es té, en particular, $L(E^{(D)}/\mathbb{Q},1)\neq 0$. L'existència de K ve assegurada per un teorema de Waldspurger (1985) sobre la no anul·lació dels valors de les sèries L automorfes torçades.

2. Fórmula de Gross-Zagier.

   A partir de la fórmula de Gross-Zagier pel cas de E/K i P_K punt de Heegner de $E(K)$:

$$L'(E/K,1)=\frac{\iint_{E(\mathbb{C})}\ \omega\wedge\overline{i\omega}}{\sqrt{D}}\ \hat{h}(P_K)\,,$$

es troba que el punt de Heegner $P_K \in E(K)$ és d'ordre infinit, d'on rang $E(K) \geq 1$. Més precisament, estudiant l'acció de la conjugació complexa sobre P_K es veu que en aquest cas, $P_K \in E(\mathbb{Q})/(E(\mathbb{Q})_{\text{tors}})$, d'on rang $(E(\mathbb{Q})) \geq 1$.

3. Descens de Kolyvagin.

   Utilitzant els sistemes d'Euler, Kolyvagin prova que rang $E(K)$ és exactament 1 i que $\text{Ш}(E/K)$ és finit. Per tant, rang $E(\mathbb{Q}) = 1$. Considera la successió exacta

$$0 \longrightarrow \ker\varphi \longrightarrow \text{Ш}(E/\mathbb{Q}) \xrightarrow{\varphi} \text{Ш}(E/K)$$

   i prova que $\ker\varphi \subset H^1\Big(G_{K/\mathbb{Q}}, E(K)\Big)$ on aquest grup de cohomologia és finit. En particular $\text{Ш}(E/\mathbb{Q})$ és finit.

§3. La conjectura de Birch i Swinnerton-Dyer per a varietats abelianes

Sigui A/K una varietat abeliana de dimensió d definida sobre un cos de nombres K. Sigui $\mathcal{O}$ l'anell d'enters de K, $\mathcal{O}_v$ l'anell local en una de les valoracions discretes, i $k(v)$ el cos residual. Suposem que A té bona reducció en v. Sigui G_v un grup de descomposició, posem
$Nv = \ \#k(v)$;
$Fr_v =$ element de Frobenius de G_v, actuant a $A(\overline{k(v)}\,)$.

Sigui N el model de Néron de A sobre $\mathcal{O}$ i sigui N^0 el model de Néron connex. Sigui v finit, escrivim $A_v = N \otimes_{\mathcal{O}} k(v)$, $A_v^0 = N^0 \otimes_{\mathcal{O}} k(v)$. Aleshores A_v és un esquema de grups commutatiu sobre $k(v)$ i A_v^0 és la component connexa de l'origen en A_v. Es defineix

$$c_v(A) = c_v = \Big(A_v(k(v)) : A_v^0(k(v))\Big).$$

Aleshores c_v és un enter, gairebé sempre igual a 1, igual a l'índex del subgrup de punts del cos residual de la component connexa de la fibra especial, en el grup de tots els punts $k(v)$-racionals de tota la fibra del model de Néron. Aleshores, es defineix

$$C_f(A) = \prod_{v \,\text{finit}} c_v\,.$$

Sigui G el grup de Galois $\mathrm{Gal}\,(\overline{\mathbb{Q}}/K)$ i sigui I_v el subgrup d'inèrcia de G_v, que indueix la identitat en l'extensió del cos residual donada per v. Sigui Fr_v l'element de Frobenius de G_v/I_v. Sigui $\ell \in \mathbb{Z}$ un primer, $\ell \neq \mathrm{car}\ k(v)$, i consideri's el mòdul de Tate

$$T_\ell(A) = \varprojlim\ A(\overline{\mathbb{Q}})\ [\ell^n],$$

on $A(\overline{\mathbb{Q}})\ [\ell^n]$ és el nucli de la multiplicació per ℓ^n en el grup de punts algèbrics de A. $T_\ell(A)$ és un $\mathbb{Z}_\ell$-mòdul lliure de rang $2d$. Es defineix el factor local de la L-sèrie en v, per a tot v, incloent els de mala reducció per la fórmula:

$$L_v(A/K,s) := \det\left(id - Nv^{-s}\ Fr_v^{-1} \mid \mathrm{Hom}_{\mathbb{Z}_\ell}\,(T_\ell(A),\mathbb{Z}_\ell)^{I_v}\right)^{-1}.$$

El super índex I_v indica el submòdul dels elements fixos per tots els elements del grup d'inèrcia I_v. Aleshores, es defineix la sèrie L associada a la varietat abeliana A/K pel producte d'Euler:

$$L(A/K,s) = \prod_{v\,\mathrm{finit}}\ L_v(A/K,s)\,,$$

i es conjectura que aquesta funció L té prolongació analítica a tot el pla complex i que satisfà una equació funcional senzilla, (cf. [Gro]).

Sigui W_N el $\mathcal{O}$-mòdul projectiu de les diferencials invariants al model de Néron N. Aleshores, $\mathrm{rang}(W_N) = d$ i, per tant, $\wedge^d W_N$ és un $\mathcal{O}$-submòdul de rang 1 de $H^0(A/K,\Omega^d)$. Sigui $\{\omega_1,\ldots,\omega_d\}$ una K-base de $H^0(A/K,\Omega^1)$ i sigui $\eta = \wedge\,\omega_j$. Aleshores

$$\wedge^d\ W_N = \eta\ \mathfrak{a}_\eta \quad \text{en} \quad H^0(A/K,\Omega^d),$$

on $\mathfrak{a}_\eta$ és un ideal fraccionari de K.

Si v és una plaça complexa de K i $\sigma : K \longrightarrow \mathbb{C}$ una immersió que indueix v en K. Sigui $H = H_1(A^\sigma(\mathbb{C}),\mathbb{Z})$ la homologia entera de A^σ. Aleshores, H és un $\mathbb{Z}$-mòdul lliure de rang $2d$. Sigui $\{\gamma_1,\ldots,\gamma_{2d}\}$ una base de H, i definim

$$\begin{aligned} c_v(A,\eta) &= \left|\det\left(\left(\int_{\gamma_i}\omega_j, \int_{\gamma_i}\overline{\omega}_j\right)\right)\right| \\ &= \int_{A(\mathbb{C})}\sqrt{-1}\ \eta\wedge\overline{\eta}\,. \end{aligned}$$

El determinant de la $2d \times 2d$ matriu és diferent de zero i només depèn de η i v.

Si v és una plaça real de K corresponent a l'immersió $\sigma : K \longrightarrow \mathbb{R}$. Sigui H^+ el submòdul de $H_1(A^\sigma(\mathbb{C}), \mathbb{Z})$ que és fix per conjugació complexa. Aleshores, H^+ és lliure de rang d. Sigui $\{\alpha_1, \ldots, \alpha_d\}$ una base i definim

$$\begin{aligned} c_v(A, \eta) &= \left(A^\sigma(\mathbb{R}) : A^\sigma(\mathbb{R})^0\right) \left| \det\left(\left(\int_{\alpha_i} \omega_j\right)\right)\right| \\ &= \int_{A^\sigma(\mathbb{R})} |\eta| \,. \end{aligned}$$

Aquí també el determinant és diferent de zero i només depèn de η i de v.

Sigui d_K el valor absolut del discriminant de K sobre $\mathbb{Q}$. El producte

$$C_\infty(A) = \prod_{v|\infty} c_v(A, \eta)\ N_{K|\mathbb{Q}}\ \mathfrak{a}_\eta / |d_K|^{d/2}$$

és independent de l'elecció de η.

Finalment, es defineix

$$C := C(A) = C_\infty(A) \cdot C_f(A) \,.$$

Aleshores $C(A)$ és un nombre real positiu.

Suposant que $L(A/K, s)$ té continuació analítica a tot el pla complex, es té:

Conjectura de Birch i Swinnerton-Dyer

1. Sigui $r = \operatorname{rang} A(K)$. Aleshores, $L(A/K, s)$ té un zero d'ordre r en $s = 1$.

2. $\dfrac{1}{r!}\ L^{(r)}\,(A/K, 1) = \dfrac{\#\ \text{Ш}\,(A/K)\ R(A/K)\ C(A/K)}{\#\ (A(K)_{\text{tors}})\ \#(A'(K)_{\text{tors}})}$, on $\text{Ш}\,(A/K)$ és el grup de Shafarevich-Tate de la varietat abeliana A, $\text{Ш}\,(A/K) = \ker(H^1(G, A) \longrightarrow \Pi_v\, H^1(G_v, A)\,)$.

Es conjectura que $\text{Ш}\,(A/K)$ és finit; i sota aquesta hipòtesis es té que els grups $\text{Ш}\,(A/K)$ i $\text{Ш}\,(A'/K)$, on A' denota la varietat abeliana dual de A, són duals l'un de l'altre (Cassels-Tate).

$R(A/K)$ s'anomena el regulador de la varietat abeliana A/K i es defineix:

$$R(A/K) = |\det\langle P_i, P'_j\rangle| \,,$$

on $\{P_1, \ldots, P_r\}$ és una base de $A(K)/A(K)_{\text{tors}}$ i $\{P'_1, \ldots, P'_r\}$ és una base de $A'(K)/A'(K)_{\text{tors}}$, i

$$\langle P, P' \rangle := \hat{h}(P, P')\,,$$

és el corresponent aparellament de Néron-Tate.

Observacions. 1) En el cas d'una corba el·líptica $E/\mathbb{Q}$ definida sobre $\mathbb{Q}$ recuperem els resultats del paràgraf anterior.

2) En el denominador del segon apartat de la conjectura (BSD) cal introduir $\#\,[A'(K)_{\text{tors}}]$ per a que tot el valor sigui invariant per isogènies (provat per Tate [Ta]).

3) La conjectura de Birch i Swinnerton-Dyer per a varietats abelianes també es pot donar en termes de nombres de Tamagawa.

Bloch [Bl] conjectura que el nombre de Tamagawa $\tau(A)$ corresponent a una varietat abeliana A/K amb grup de Mordell-Tate $A(K)$ finit és:

$$\tau(A) = \frac{\#\ Pic(A)_{\text{tors}}}{\#\ Ш(A)} \qquad (***)$$

i en l'article esmentat anteriorment prova que si $(***)$ és certa aleshores també la conjectura de Birch i Swinnerton-Dyer ho és.

Bibliografia

[Bi] B.J. Birch, Diophantine analysis and modular functions, *Algebraic Geometry*, Bombay Colloquium, (1968), Oxford University Press, London 1969, 35–42.

[Bi-Ste] B.J. Birch and N.M. Stephens, Computation of Heegner points, *Modular Forms*, R.A. Rankin Ed., Ellis Horwood Ltd., (1984), 13–41.

[B-Sw1] B. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves (I), *J. Reine Angew Math.* **212** (1963), 7–25.

[B-Sw2] B. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves (II), *J. Reine Angew Math.* **218** (1965), 79–108.

[Bl] S. Bloch, A note on Height Pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer Conjecture, *Inv. Math.* **58** (1980), 65–76.

[Bu-Gr-Z] J. Buhler, B. Gross and D. Zagier, On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3, *Math. Comp.* **44** (1985), 473–481.

[Ca1] J.W.S. Cassels, Arithmetic on curves of genus 1 (IV). Proof of the Hauptvermutung, *J. Reine Angew. Math.* **211** (1962), 95–112.

[Ca2] J.W.S. Cassels, Arithmetic on curves of genus 1 (VIII). On the conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math.* **217** (1965), 180–189.

[Co-W] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 223–251.

[Gre] R. Greenberg, On the Birch and Swinnerton-Dyer conjecture, *Invent. Math.* **72** (1983), 241–265.

[Gro] B. Gross, On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication, *Number Theory Related to Fermat's Last Theorem*, Birkhauser (1982), 219–236.

[Gr-Z] B. Gross and D. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986), 225–320.

[Hee] K. Heegner, Diophantische Analysis und Modulfunktionen, *Math. Zeit.* **56** (1952), 227–253.

[Ko1] V.A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and $\text{Ш}(E/\mathbb{Q})$ for a subclass of Weil curves, (Russian) *Izv. Akad. Nauk. Ser. Mat.* **52** (1988) No. 6, 1154–1180; translation in *Math. USSR Izv.* **33** No. 3 (1989), 473–499.

[Ko2] V.A. Kolyvagin, Euler Systems, *The Grothendieck Festschrift*, Vol. II, 435–483, Progr. in Math. **87** Birkhausser, 1990.

[Maz1] B. Mazur, Modular curves and the Eisenstein ideal, *IHES Publ. Math.* **47** (1977), 33–186.

[Maz2] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.

[Sil] J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer, 1986.

[Ste] N.M. Stephens, The diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math.* **231** (1967), 121–162.

[Ta] J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, *Séminaire Bourbaki* 1965–1966, No. 306.

[Wa] J.–L. Waldspurger, Sur les valeurs de certaines fonctions L automorphes en leur centre de symmétrie, *Compos. Math.* **54** No. 2 (1985), 173–242.

Corbes el.líptiques amb multiplicació complexa

Jordi Guàrdia

1 Multiplicació complexa i teoria de cossos de classes

Definició 1 *Sigui E una corba el·líptica definida sobre $\mathbb{C}$. Diem que E té multiplicacions complexes si $\mathrm{End}_{\mathbb{C}}(E) \simeq R$ és un ordre d'un cos de nombres quadràtic imaginari $K/\mathbb{Q}$.*

La xarxa de períodes d'una corba el·líptica amb multiplicacions complexes de R és un R-mòdul projectiu de rang 1. Nosaltres assumirem sempre que $\mathrm{End}_{\mathbb{C}}(E) \simeq \mathcal{O}_K$ és l'anell d'enters de K. En aquest cas, la xarxa de períodes de E és de la forma

$$\Lambda_E = \Omega\mathfrak{a},$$

on $\Omega \in \mathbb{C}$ i $\mathfrak{a}$ és un ideal fraccionari de $\mathrm{Cl}(K)$. Denotarem per $E_{\mathfrak{a}}$ la corba el·líptica $\mathbb{C}/\mathfrak{a}$, i per $j(\mathfrak{a})$ el seu invariant j. Tenim que:

a) La classe de $\mathfrak{a}$ en $\mathrm{Cl}(K)$ determina la classe de $\overline{\mathbb{Q}}$-isomorfisme de la corba el·líptica $\mathbb{C}/\mathfrak{a}$. [1]

b) Si $\sigma \in \mathrm{Aut}(\mathbb{C})$, la corba el·líptica $\mathbb{C}/\sigma\mathfrak{a}$ també té multiplicació complexa per $\mathcal{O}_K$.

Es dedueix d'això que $j(\mathfrak{a})$ és un nombre algebraic. De fet:

Teorema 2

1) El polinomi $f(X) = \prod_{\mathfrak{a} \in\ Cl(K)}(X - j(\mathfrak{a}))$ és irreductible sobre $\mathbb{Q}$.

2) El cos de descomposició del polinomi $f(X)$ sobre K s'obté adjuntant un valor qualsevol $j(\mathfrak{a})$, $\mathfrak{a} \in \mathrm{Cl}(K)$.

[1] Remarquem que es tracta de la classe de $\overline{\mathbb{Q}}$-isomorfisme. Així, per exemple, totes les corbes $Y^2 = X^3 - DX$ tenen multiplicacions complexes de $\mathbb{Z}[i]$, són $\mathbb{Q}(\sqrt{D})$-isomorfes a $Y^2 = X^3 - X$, però l'isomorfisme no es pot definir sobre $\mathbb{Q}$.

3) L'extensió abeliana no ramificada maximal de K (el Hilbert ray class field de K) *és justament aquest cos $H = K(j(\mathfrak{a}))$.*

A més a més, podem assegurar que

Proposició 3 *El mínim cos de definició de la corba el·líptica $\mathbb{C}/\mathfrak{a}$ és $\mathbb{Q}(j(\mathfrak{a}))$. Les multiplicacions complexes d'aquesta corba estan definides sobre el cos $H = K(j(\mathfrak{a}))$.*

2 Incís: Ideles i caràcters

En aquesta secció recordarem les nocions bàsiques referents a les ideles i els caràcters, i fixarem la definició de Grössencharakter. Les referències bàsiques són els llibres [Ne 86], [Ca-Fr 65].

Donat un cos de nombres F, denotarem per J_F el seu grup d'ideals, i per P_F el subgrup dels ideals principals. El grup de classes d'ideals de F és $\mathrm{Cl}(F) := J_F/P_F$.

Definició 4 *L'anell de les adeles de F és*

$$\mathbb{A}_F := \{(x_v)_v \in \prod_v F_v \ | x_v \in \mathcal{O}_v \ q.p.t. \ v\}.$$

El grup de les ideles de F és

$$I_F := \mathbb{A}_F^* = \{(x_v)_v \in \prod_v F_v | x_v \in \mathcal{O}_v^* \ q.p.t. \ v\}$$

Els elements de F^* s'injecten canònicament en I_F mitjançant el morfisme diagonal. El quocient $C_F := I_F/F^*$ s'anomena *grup de classes d'ideles* de F.

Denotarem per S_∞ (resp. S_f) el conjunt de les places arquimedianes (resp. no arquimedianes) de F. Hi ha una aplicació natural del grup d'ideles en el grup d'ideals, donada per:

$$\begin{array}{ccc} I_F & \stackrel{u}{\longrightarrow} & J_F \\ (x_v)_v & \longrightarrow & \prod_{v\in S_f} \mathfrak{p}_v^{v(x_v)}, \end{array}$$

($\mathfrak{p}_v$ primer associat a v).

El nucli d'aquesta aplicació és $I_{F,\infty} := \ker(u) = \prod_{v\in S_\infty} F_v^* \times \prod_{v\in S_f} \mathcal{O}_v^*$, i rep el nom de *grup de les ideles infinites*. Evidentment, $I_F/I_{F,\infty} \simeq J_F$, però a més

Proposició 5

$$I_F/I_{F,\infty}F^* \simeq \mathrm{Cl}(F).$$

El grup de les ideles I_F és pot proveir d'una topologia natural, de forma que esdevé un grup topològic. Només cal prendre com a entorns bàsics de la unitat els conjunts de la forma $\prod_{\mathfrak{p}\in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}$, on S és un conjunt finit de places arquimedianes que F que inclou les places arquimedianes, $W_{\mathfrak{p}}$ és un entorn bàsic de $1 \in F_{\mathfrak{p}}$ i $U_{\mathfrak{p}} = x \in F_{\mathfrak{p}} | v_{\mathfrak{p}}(x) = 0$. En introduir la topologia en el grup de les ideles, podem estudiar la teoria de cossos de classes des del punt de vista analític.

Definició 6 *Un* **Grössencharakter** *de F és un homomorfisme continu*

$$\chi : I_F \longrightarrow \mathbb{C}^*$$

tal que $\chi(F^*) = 1$.

Donat un Grössencharakter , podem considerar els seus components locals, que no són més que les restriccions a cada factor local del productori que defineix el grup d'ideles. Interpretem aquests components com a morfismes sobre el grup d'ideals:

$$\begin{gathered}\chi_v : F_v^* \longrightarrow J_F \\ \chi_v(x) := \chi(1, 1, \ldots, x, 1, \ldots).\end{gathered}$$

En la tesi de Tate (cf. [Ca-Fr 65]) s'estudia com poden ser aquests components locals:

1) En una plaça arquimediana v amb $e_v = [F_v : \mathbb{R}]$ cal que

$$v \in S_\infty \Rightarrow \chi_v(x) = \left(\frac{x}{|x|_v^{e_v}}\right)^n |x|_v^s,$$

per a certs $n \in \mathbb{Z}, s \in \mathbb{C}$.

2) En una plaça finita v el component local corresponent ha de descompondre com

$$\chi_v(x) = \chi_{v,n}(x)|x|_v^s,$$

amb $n \in \mathbb{N}$ $\chi_{v,n} : U_v/(1+\pi^n) \longrightarrow S^1$ un caràcter local.

A partir dels exponents dels components locals dels Grössencharakters es defineix el seu conductor:

Definició 7 *El conductor de χ és* $\mathfrak{f} := \prod_{v\in S_f} \mathfrak{p}_v^{n_v}$.

Usualment, els components locals infinits i els components locals finits d'un Grössencharakter s'agrupen donant lloc a dos morfismes:

$$\begin{gathered}\chi_\infty : I_{F,\infty} \longrightarrow \mathbb{C} \\ \chi_\infty((x_v)_{v\in S_\infty}) = \prod_{v\in S_\infty} \left(\frac{x_v}{|x_v|_v^{e_v}}\right)^{-f_v} |x_v|_v^{s_v},\end{gathered}$$

$$\tilde{\chi} : J_F \longrightarrow \mathbb{C}$$
$$\tilde{\chi} = \chi \circ u,$$

de manera que tenim la descomposició natural

$$\chi(x) = \tilde{\chi}(u(x))\chi_\infty((x_v)_{v\in S_\infty}).$$

Observem que, per als elements $\alpha \in F^*$

$$\chi(\alpha) = 1 \Rightarrow \tilde{\chi}(\alpha\mathcal{O}_F) = \prod_{v\in S_\infty} \left(\frac{\alpha_v}{|\alpha_v|_v^{e_v}}\right)^{f_v} |\alpha_v|_v^{-s_v}.$$

Tenint en compte tot això, veiem que els caràcters d'ordre finit són els que tenen tots els exponents $f_v = 0$ i $s_v = 0$ en les places arquimedianes. En aquest cas, $\chi(I_{F,\infty}) = 1$ i $\mathrm{Im}\chi \subset \mu_\infty$, i χ és un caràcter de Dirichlet. Els caràcters de Dirichlet van lligats a les extensions finites de F. Si volem tractar les extensions infinites de F haurem de considerar els Grössencharakters d'ordre infinit. Weil proposa l'estudi d'un tipus particular de Grössencharakters, que si bé tenen ordre infinit, prenen valors algebraics:

Definició 8 (Weil) *Un Grössencharakter és de tipus A si tots els $s_v \in \mathbb{Q}$. Un Grössencharakter és de tipus A_0 si tots els $s_v \in \mathbb{Z}$, és a dir, si existeixen enters a_v, b_v tals que, per a cada $\alpha \in F^*$:*

$$\tilde{\chi}(\alpha\mathcal{O}_F) = \pm \prod_{v\in S_\infty} \alpha_v^{a_v}\overline{\alpha_v}^{b_v}.$$

Proposició 9

a) Els valors que pren un Grössencharakter de tipus A són algebraics.

b) Els valors que pren un Grössencharakter de tipus A_0 cauen tots dins d'una extensió finita de $\mathbb{Q}$.

A més a més, hom pot definir la sèrie L associada a un Grössencharakter de tipus A_0, que resulta tenir unes propietats immillorables:

Proposició 10 (Hecke, Tate) *La sèrie L dels Grössencharakters de tipus A_0 satisfà una equació funcional, que permet extendre-la a una funció analítica en tot el pla complex.*

3 El treball de Deuring

Sigui v una plaça de F en la qual E té bona reducció. Denotem per $F(v)$ el cos residual, i per E_v la reducció d'E. Mitjançant els mòduls de Tate es prova que els homorfismes de reducció:

$$\begin{aligned} \mathrm{End}_F(E) &\longrightarrow \mathrm{End}_{F(v)}(E_v) \\ \mathrm{End}_F(E) \otimes \mathbb{Q} &\longrightarrow \mathrm{End}_{F(v)}(E_v) \otimes \mathbb{Q} \end{aligned}$$

són injectius. Això dóna lloc a una injecció

$$K \xrightarrow{\theta_v} \mathrm{End}_{F(v)}(E_v) \otimes \mathbb{Q}.$$

L'àlgebra d'endomorfismes $\mathrm{End}_{F(v)}(E_v) \otimes \mathbb{Q}$ pot ser un cos quadràtic imaginari o una àlgebra de quaternions, però en qualsevol cas, el seu centre és justament $\theta_v(K)$. En particular l'endomorfisme de Frobenius π_v pertany a la imatge de θ_v. És a dir:

$$\exists! \quad \alpha_v \in K \mid \theta_v(\alpha_v) = \pi_v.$$

Això ens dóna una correspondència $v \mapsto \alpha_v$ entre les places de F i els elements de K^*. Deuring ([De 53-57]) demostra que aquesta correspondència és un Grössencharakter, la qual cosa permet provar, a posteriori, la conjectura de Hasse-Weil per a les corbes el·líptiques amb multiplicacions complexes d'un cos de nombres quadràtic imaginari:

Teorema 11 *La corba el·líptica $E_{/F}$, amb multiplicacions complexes del cos $K = \mathbb{Q}(\sqrt{-D}) \subset F$ determina un únic caràcter continu:*

$$\psi_E : I_F \longrightarrow K^*,$$

que queda caracteritzat per les propietats següents:

a) Si $a = \{\alpha\}_v$ és una idele principal, $\psi_E(a) = N_{F/K}(\alpha)$.

b) Si $a = \{a_v\}_v$ és una idele tal que $a_v \equiv 1 \pmod{v}$ en totes les places de mala reducció d'E, llavors

$$\psi_E(a) = \prod_{v \text{ de bona reducció}} \alpha_v^{v(a_v)}.$$

c) $\ker(\psi_E)$ és un subgrup obert de I_F.

Els conductors de x i E estan lligats per la relació $N_E = N_{\psi_E}^2$.

Donat un primer racional $\ell \in \mathbb{Z}$, considerem el *twist* ℓ-àdic de ψ_E:

$$\begin{array}{rcl} \chi_\ell : I_F & \longrightarrow & K_\ell^* \\ a & \longrightarrow & \psi_E(a)/N_{F_\ell/K_\ell}(a_\ell). \end{array}$$

Per definició, $\chi_\ell(F^*) = 1$, i com que K_ℓ^* és totalment disconnex, χ_ℓ ha de ser trivial sobre el component connex de la identitat I_F^0 en I_F. A través de l'isomorfisme d'Artin, χ_ℓ defineix un caràcter de $\mathrm{Gal}(\overline{F}/F)^{ab}$, que indueix un caràcter de Galois

$$\chi_\ell : \mathrm{Gal}(\overline{F}/F) \longrightarrow K_\ell^*.$$

Proposició 12 *El caràcter χ_ℓ és el caràcter associat a la representació ℓ-àdica de $\mathrm{Gal}(\overline{F}/F)$ determinada per E.*

En les places infinites, podem fer una construcció anàloga. L'homomorfisme

$$\begin{array}{rcl} \chi_\infty : I_F & \longrightarrow & K_\infty^* \\ a & \longrightarrow & \psi_E(a)/N_{F_\infty/K_\infty}(a_\infty), \end{array}$$

també és trivial sobre F^*. Ell i el seu conjugat complex són dos Grössencharakters de tipus A_0, que denotarem χ_E i $\overline{\chi_E}$.

Teorema 13 (Deuring, [De 53-57]) *$K \subset F$*
1) χ_E i $\overline{\chi_E}$ són dos Grössencharakters de tipus A_0.
2) $L(E/F, s) = L(\chi_E, s)L(\overline{\chi_E}, s)$.
3) Si E està definida sobre $\mathbb{Q}$ llavors, $L(E/\mathbb{Q}, s) = L(\chi_E, s)$ llevat d'un nombre finit de factors d'Euler.
4) Les corbes el·líptiques amb multiplicacions complexes d'un cos quadràtic imaginari satisfan la conjectura de Hasse-Weil.

4 El teorema de Coates-Wiles

Teorema 14 (Coates-Wiles, [Co-Wi 77]) *Sigui K un cos quadràtic imaginari amb nombre de classes $h(K) = 1$. Sigui E una corba el·líptica definida sobre $F = K$ o sobre $F = \mathbb{Q}$, amb multiplicacions complexes de $\mathcal{O}_K$. Si $rgE(F) \geq 1$, llavors la sèrie $L(E/F, s)$ s'anul·la en $s = 1$.*

Aquest teorema pot aplicar-se, en particular, a les corbes el·líptiques $Y^2 = X^3 - DX$ estudiades originalment per Birch i Swinnerton-Dyer.

En realitat, aquest enunciat és una mica restrictiu: només hi ha 9 cossos quadràtics imaginaris amb nombre de classes 1: són els cossos $\mathbb{Q}(\sqrt{-D})$, amb $D \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$. Els propis Coates i Wiles admeten que la restricció $h(K) = 1$ només es deu a raons tècniques, i anuncien que N. Arthaud ha aconseguit superar-la. En [Ar 78-2] apareix el teorema següent:

Teorema 15 *En les mateixes hipòtesis que el teorema anterior, (en particular $h(K) = 1$), si F és una extensió abeliana de K i E és una corba el·líptica* **definida sobre** *F tal que $rgE(F) \geq 1$, llavors la sèrie $L(E/F, s)$ s'anul·la en $s = 1$.*

Arthaud anuncia una segona part del seu article, en la qual prova una generalització del teorema de Coates-Wiles

- Sense la restricció sobre el nombre de classes;

- Per a una extensió abeliana F/K tal que $F(E_{\text{tors}})/K$ sigui abeliana.

Aquest paper però, no ha estat publicat. Se suposa que deu aparèixer a la seva tesi ([Ar 78-1]). Si més no, Rubin ([Ru 81]) el dóna per vàlid.

5 El treball de Rubin

En les mateixes hipòtesis del final de la secció 4, Rubin prova una versió més forta dels resultats anteriors, en la qual fita l'ordre d'anul·lació de la sèrie L.

A partir de la corba el·líptica E definida sobre F, Rubin considera la restricció d'escalars a K, $B = Res_{F/K}(E)$. Com que suposem que $F(E_{\text{tors}})/K$ és una extensió abeliana, resulta que és una K-corba, és a dir, és isògena a totes les seves K-conjugades. Es té que:

Proposició 16 *La varietat abeliana B és isògena sobre K a un producte $\prod_{i=1}^{r} B_i$ de varietats abelianes simples sobre K, de tipus CM, és a dir:*

$$T_i := \text{End}_K(B_i) \oplus_{\mathcal{O}_K} K$$

és un CM-cos i $\dim B_i = [T_i : K]$. En particular $\sum_{i=1}^{r} [T_i : K] = \dim B = [F : K]$.

Sigui M una extensió abeliana de K que conté F, amb grup de Galois $G = \text{Gal}(M/K)$. Notem que G actua sobre

$$B_i(M)_{T_i} = B_i(M) \otimes_{\mathbb{Z}} \mathbb{Q} = B_i(M) \otimes_{\text{End}_{K(B_i)}} T_i.$$

La descomposició en components irreductibles d'aquesta representació permet fitar l'ordre d'anul·lació en $s = 1$ de la sèrie $L(E/M, s)$:

Teorema 17 (Rubin, [Ru 81]) *Sigui $B_i(M)_{T_i} \simeq \oplus_{j=1}^{l} V_j^{m_j}$ la descomposició de $B_i(M)_{T_i}$ en $T_i[G]$-representacions irreductibles. Es té que*

$$ord_{s=1} L(E/M, s) \geq 2 \sum_{j=1}^{l} \deg V_j.$$

Observació 18 *Es pot provar que* $\mathrm{rg}_{\mathcal{O}_K}(E(M) = \dim_{T_i}(B_i(M)_{T_i})$*, de manera que la predicció de la conjectura de Birch i Swinnerton-Dyer és que* $\mathrm{ord}_{s=1}L(E/M,s) = 2\sum_{j=1}^{l} m_j \deg V_j$.

Rubin ha seguit treballant en la versió completa de conjectura. Ha obtingut resultats parcials a partir dels seus treballs en les conjectures principals de la teoria d'Iwasawa ([Ru 91]). Així mateix, en una de les tesis dirigides per ell es demostra:

Proposició 19 (González-Avilés, [Go 97]) *La versió completa de la conjectura de BSD per a les corbes el·líptiques definides sobre* $\mathbb{Q}(\sqrt{-7})$ *amb multiplicacions complexes per aquest cos i amb* $L(E/\mathbb{Q}(\sqrt{-7})) \neq 0$ *és certa.*

Com a conseqüència d'aquest resultat, es prova la versió completa de la conjectura per a una família de corbes el·líptiques:

Corol·lari 20 (González-Avilés, [Go 97]) *Les corbes*

$$E_d : Y^2 = X^3 + 21dX^2 + 11d^2X,$$

que tenen multiplicació complexa per

$$\mathbb{Z}[(1+\sqrt{-7})/2],$$

satisfan la versió completa de la conjectura BSD si $L(E_d/\mathbb{Q}(\sqrt{-7})) \neq 0$.

6 Altres resultats

Greenberg demostra una aproximació al recíproc del teorema de Coates-Wiles, a favor de la conjectura:

Teorema 21 (Greenberg, [Gr 83]) *Sigui* E *una corba el·líptica definida sobre* $\mathbb{Q}$ *amb multiplicacions complexes d'un cos quadràtic imaginari* K*. Si* $L(E/\mathbb{Q},s)$ *té un zero d'ordre senar en* $s = 1$*, llavors o bé* $\mathrm{rg}E(\mathbb{Q}) \geq 1$ *o bé el subgrup p-primari del grup de Tate-Safarevic és infinit per a tots els primers* $p > 3$ *de bona reducció ordinària.*

7 Idees sobre la demostració del teorema de Coates-Wiles

7.1 Cossos de punts de torsió

Sigui p un primer de bona reducció de E, que descompon totalment en K, amb $p = \mathfrak{p}\overline{\mathfrak{p}}$. Denotem per ψ_E el Grössencharakter de E, i sigui $\pi = \psi_E(\mathfrak{p}) \in \mathcal{O}_K = End(E)$.

Per definició, π és l'únic endormorfisme de E que reduït mòdul $\mathfrak{p}$ dóna el Frobenius de $E \pmod{\mathfrak{p}}$. De fet, $[p]_E = [\pi]_E[\overline{\pi}]_E$.

El fet que l'invariant j de la corba el·líptica E sigui un enter algebraic, combinat amb el criteri de Néron-Ogg-Safarevic, permet determinar una extensió en la qual la corba té bona reducció a tot arreu:

Teorema 22 *La corba el·líptica E té bona reducció sobre el cos $F_0 := K(E_\pi)$.*

Utilitzant bé la relació explícita entre les multiplicacions complexes de E i els símbols d'Artin, es prova el següent

Lema 23 *Sigui $\mathfrak{f} = (f) =$ conductor de ψ_E.*
1) $H := K(E_f)$ és l'extensió maximal abeliana no ramificada fora de $\mathfrak{f}$ de K.
2) El conductor de $F_n := K(E_{\pi^{n+1}})/K$ és $\mathfrak{f}_n := \mathfrak{f}\mathfrak{p}^{n+1}$.
3) El Hilbert ray class field *de K mòdul $\mathfrak{f}_n$ és el cos $\mathcal{R}_n := HF_n$, i $H \cap F_n = K$.*

7.2 Unitats el·líptiques

Definició 24 *Sigui $L = \Omega\mathcal{O}_K$ la xarxa de períodes de la funció $\mathfrak{p}$ de Weierstrass de la corba el·líptica E. Donat un ideal enter $\mathfrak{a}$ de K definim:*

$$\mathbf{\Theta}(z, \mathfrak{a}) = \frac{\Delta(L)}{\Delta(\mathfrak{a}^{-1}L)} \prod_{l \in \mathfrak{a}^{-1}L/L} \frac{\Delta(L)}{(\mathfrak{p}(z) - \mathfrak{p}(l))^6},$$

on Δ denota el discriminant, i l'índex del productori recorre un sistema de representants no nuls de $\mathfrak{a}^{-1}L$ mòdul L.

Sigui $S = \{2, 3\} \cup \{$ primers de mala reducció de $E\}$.

Proposició 25 (Roberts, [Ro 73]) *Sigui ρ_n un punt de $\mathfrak{f}_n$-torsió de L.*

a) Si $\mathfrak{a}$ és un ideal enter de K coprimer amb S i amb p, llavors $\mathbf{\Theta}(\rho_n, \mathfrak{a}) \in \mathcal{R}_n$.

b) Si $\mathfrak{b}$ és un ideal enter de K coprimer amb $\mathfrak{f}_n$, llavors

$$\mathbf{\Theta}(\rho_n, \mathfrak{a})^{(\mathfrak{b}, \mathcal{R}_n/K)} = \mathbf{\Theta}(\psi_E(\mathfrak{b})\rho_n, \mathfrak{a}).$$

c) Si $\mathfrak{g} = \prod_j \mathfrak{a}_j^{n_j}$ és un ideal fraccionari de K tal que $\sum_j n_j(N(\mathfrak{a}_j) - 1) = 0$, llavors $\mathbf{\Theta}(\rho_n, \mathfrak{g}) := \prod \mathbf{\Theta}(\rho_n, \mathfrak{a}_j)^{n_j} \in \mathcal{R}_n^*$ (és una **unitat el·líptica***).*

Denotarem per $\mathcal{C}_n$ el subgrup format per les unitats el·líptiques descrites a l'últim apartat de la proposició anterior. Denotarem per C_n el subgrup de F_n format per les normes de $\mathcal{R}_n$ a F_n dels elements de $\mathcal{C}_n$:

$$\mathcal{C}_n := \{\mathbf{\Theta}(\rho_n, \mathfrak{g})\}_{\mathfrak{g}},$$
$$C_n := N_{\mathcal{R}_n/F_n}(\mathcal{C}_n).$$

El grup C_n té un molt bon comportament galoisià. Resumim les seves propietats:

Proposició 26

a) C_n és estable per l'acció de $G_n = \mathrm{Gal}(F_n/K)$, i és independent del punt de $\mathfrak{f}_n$-torsió $\rho_n \in L$ escollit.

b) Els elements de C_n són $\equiv 1 \pmod{\mathfrak{p}_n}$.

c) Per a cada $m \geq n$, $N_{F_m/F_n}(C_m) = C_n$.

Prenem com a ρ_n el valor $\rho := \Omega/f$. Fixem un conjunt B d'ideals enters de K, coprimers amb $\mathfrak{f}_0 = \mathfrak{f}\mathfrak{p}$ de forma que

$$\mathrm{Gal}(\mathcal{R}_0/F_0) = \{(\mathfrak{b}, \mathcal{R}_0/K) | \mathfrak{b} \in B\}.$$

Per a cada ideal enter de K coprimer amb S i $\mathfrak{p}$, considerem la funció

$$\Lambda(z, \mathfrak{a}) := \prod_{\mathfrak{b} \in B} \Theta(z + \psi(\mathfrak{b}), \mathfrak{a}).$$

Després d'una sèrie de càlculs més o menys elementals però llargs es prova que:

Lema 27 *La funció $\Lambda(z, \mathfrak{a})$ és una funció racional de $\mathfrak{p}(z)$ i $\mathfrak{p}'(z)$, amb coeficients en el cos K. A més:*

$$z \frac{d}{dz} \log \Lambda(z, \mathfrak{a}) = \sum_{k=1}^{\infty} c_k(\mathfrak{a}) z^k,$$

on

$$c_k(\mathfrak{a}) = 12(-1)^{k-1} f^k \Omega^{-k} (N(\mathfrak{a}) - \chi_E^k(\mathfrak{a})) L(\overline{\chi_E}^k, k).$$

Corol·lari 28

$$\Omega^{-k} L(\overline{\chi_E}^k, k) \in K.$$

7.3 Càlculs locals

L'estudi del grup formal de Lubin-Tate associat a la corba el·líptica E ens dóna la següent informació local:

Proposició 29 *L'extensió $\phi_n = K_{\mathfrak{p}}(E_{\pi^{n+1}})/K_{\mathfrak{p}}$ és totalment ramificada de grau $p^n(p-1)$.*

Introduïm les notacions següents:

$G_n := \mathrm{Gal}(\phi_n/K_{\mathfrak{p}}) \simeq (\mathcal{O}_K/\pi^{n+1}\mathcal{O}_K)^*$.

$\mathfrak{p}_n :=$ maximal de $\mathcal{O}_{\phi_n} =$ primer de F_n sobre $\mathfrak{p}$.

$$U_n = \{x \in \mathcal{O}_{\phi_n} |\ x \equiv 1 \pmod{\mathfrak{p}_n}\}.$$

$$U'_n = \{x \in U_n |\ N_{\phi_n/K_\mathfrak{p}(x)=1}\}$$

$\overline{C_n}$ =clausura de C_n respecte la topologia $\mathfrak{p}_n$-àdica.

Notem que $\overline{C_n} \subset U'_n$ i que $U'_n/\overline{C_n}$ és un G_n-mòdul. Denotarem per χ el caràcter que dóna l'acció de G_0 en E_π. Identificant el grup de les arrels $(p-1)$-èsimes de la unitat de $\mathbb{Z}_p$, μ_p, amb la seva reducció mòdul p, assumim que χ pren valors en μ_{p-1}:

$$\begin{array}{rcl} \chi : G_0 & \longrightarrow & \mu_{p-1} \subset \mathbb{Z}_p \\ \sigma & \longrightarrow & \chi(\sigma) : \sigma(u) = \chi(\sigma)u \quad \forall u \in E_\pi. \end{array}$$

Donat un $\mathbb{Z}_p[G_0]$-mòdul A, denotarem per $A^{(k)}$ el submòdul d'A on G_0 actua via χ^k. Així tenim una descomposició

$$A = \oplus_{k=1}^{p-1} A^{(k)}.$$

L'estudi d'aquesta descomposició per als $\mathbb{Z}_p[G_0]$-mòduls $U'_n/\overline{C_n}$ és una part bàsica de la demostració del teorema de Coates-Wiles. Per exemple, el mòdul $U'_0/\overline{C_0}$ està relacionat amb els valors mòdul $\mathfrak{p}$ dels valors de les sèries L dels caràcters χ_E^k. Això es demostra utilitzant novament el grup formal de la corba el·líptica.

Definició 30 *Direm que un primer $p \in \mathbb{Z}$ és anormal per a E si $\pi + \overline{\pi} = 1$ (la traça del Frobenius mòdul $\mathfrak{p}$ és 1).*

Teorema 31 *Sigui $p > 5$ un primer no anormal ni de mala reducció, que descompon en K, $p = \mathfrak{p}\overline{\mathfrak{p}}$. Per a $k = 1, \ldots, p-2$:*

$$(U'_0/\overline{C}_0)^{(k)} \neq 0 \Longleftrightarrow \Omega^{-k} L(\overline{\chi}_E^k, k) \equiv 0 \pmod{\mathfrak{p}}.$$

El problema és que els grups $(U'_0/\overline{C}_0)^{(k)}$ no tenen una interpretació galoisiana clara. Jugant amb el grup d'unitats el·líptiques i una mica de teoria d'Iwasawa, Coates i Wiles proven que

Teorema 32 *Per a $k = 1, \ldots, p-2$,*

$$(U'_0/\overline{C}_0)^{(k)} \neq 0 \Longleftrightarrow \exists n > 0 \ t.q.\ (U'_n/\overline{C}_n)^{(k)} \neq 0.$$

Els grups $(U'_n/\overline{C}_n)^{(k)}$ Coates i Wiles sí que els poden tractar des del punt de vista galoisià, atès que ja havien demostrat el resultat següent:

Teorema 33 (Coates-Wiles 76, [Co-Wi 76]) *Sigui M_n la $p-$extensió abeliana maximal no ramificada fora de $\mathfrak{p}_n$ de F_n. Sigui L_n la $p-$extensió abeliana maximal no ramificada de F_n. Finalment, considerem $F_\infty = \cup_{n\geq 0} F_n$ i $E_n := \{x \in \mathcal{O}_{F_n} \mid x \equiv 1 \pmod{\mathfrak{p}_n}\}$, i denotem per $\overline{E_n}$ la clausura de E_n en U_n'.*

L'aplicació d'Artin estableix un isomorfisme de G_n-mòduls

$$\mathrm{Gal}(M_n/L_nF_\infty) \simeq U_n'/\overline{E}_n.$$

La importància d'aquest resultat per a nosaltres rau en el fet que $C_n \subset E_n \subset U_n'$, de manera que si conseguim veure que el quocient $U_n'/\overline{E}_n \neq 0$ tindrem que $U_n'/\overline{C}_n \neq 0$.

7.4 Demostració del teorema de Coates-Wiles

En aquesta secció repassarem la demostració pròpiament dita del teorema de Coates-Wiles. La hipòtesi del teorema és que tenim un punt d'ordre infinit $P \in E(K)$.

Sigui $S' := S \cup \{5\} \cup \{\text{primers anormals per a E}\}$. Escollim un primer $p \notin S'$ que descompongui en K, $p = \mathfrak{p}\overline{\mathfrak{p}}$. Triem un punt $Q_n \in E(\overline{K})$ tal que $\pi^{n+1}(Q_n) = P$ i considerem l'extensió $H_n := F_n(Q_n)$. Tenim que:

Lema 34

1) H_n/F_n és cíclica i $[H_n : F_n] | p^{n+1}$.

2) H_n és no ramificada fora de $\mathfrak{p}_n$.

3) L'acció de G_0 per conjugació sobre $\mathrm{Gal}(H_n/F_n)$ ve donada per

$$x^\sigma = \chi(\sigma)x \quad \forall x \in \mathrm{Gal}(H_n/F_n), \sigma \in G_0. \tag{1}$$

4) $\forall n >> 0$, H_nF_∞/F_∞ és no trivial i ramificada.

L'últim apartat del lema anterior ens diu en particular que, per a n prou gran, l'extensió $H_nL_nF_\infty/L_nF_\infty$ no és trivial. Atès que $H_nL_nF_\infty \subset M_n$, obtenim que el grup de Galois $\mathrm{Gal}(M_n/L_nF_\infty)$ no és trivial, i ara el teorema 33 ens permet afirmar que

$$U_n'/\overline{E_n} \neq 0.$$

Com que coneixem l'acció de G_0 sobre $Gal(H_n/F_n)$ (apartat 3 del lema anterior), podem assegurar més concretament que $(U_n'/\overline{E}_n)^{(1)} \neq 0$. Ja hem dit abans que $C_n \subset E_n$, de manera que

$$(U_n'/\overline{C}_n)^{(1)} \neq 0.$$

Ara el corol·lari 32 ens diu que per a n prou gran

$$(U_0'/\overline{C}_0)^{(1)} \neq 0.$$

Si apliquem el teorema 31 obtenim que

$$\mathfrak{p}|\Omega^{-1}L(\overline{\chi_E}, 1).$$

Tenim aquesta condició de divisibilitat per als primers $p >$ que descomponen en K, són de bona reducció i no anormals per a E. El teorema de la progressió aritmètica de Dirichlet permet provar que hi ha una infinitat de primers que satisfan aquestes condicions, per la qual cosa podem assegurar que

$$L(\overline{\chi_E}, 1) = 0.$$

Això prova el teorema de Coates-Wiles, ja que, tal com hem vist en el teorema 13, si $F = K$ $L(E/F, s) = L_{(\chi_E}, 1)L_{\mathfrak{f}}(\overline{\chi_E}, 1)$ i si $F = \mathbb{Q}$ $L(E/F, s) = L_{(\chi_E}, 1)$ llevat d'un nombre finit de factors d'Euler.

References

[Ar 78-1] Arthaud, N., *Tesis*, Stanford Univ. (1978).

[Ar 78-2] Arthaud, N., On Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication. I, *Compositio Mathematica*, 37, (1978), pàgs. 209-232.

[Ca-Fr 65] Cassesl, J.W.S.; Frhölich, A., *Algebraic Number Theory*, Academic Press (1965)

[Co-Wi 76] Coates, J.; Wiles, A., Kummer's criterion for Hurwitz numbers, *Alg. Number Theory, Kyoto 1976, Japan Soc. for the Promotion of Science, Tokyo* 1977, pàgs. 9-23.

[Co-Wi 77] Coates, J.; Wiles, A., On the Conjecture of Birch and Swinnerton-Dyer, *Inventiones Mathematicae*, 39 (1976), pàgs. 223-251.

[De 53-57] Deuring, M.; *Die Zetafunktion einer algebraischen Kurve von Geschlechte Eins*, I, II, III, IV. Nachr. Akad. Wiss. Göttingen, 1953-57.

[Go 97] Gonzalez-Avilés, C, On the Conjecture of Birch and Swinnerton-Dyer, *Trans. Am. Math. Soc.*, 349 (1997), pàgs. 4181-4200.

[Gr 83] Greenberg, R., On the Birch and Swinnerton-Dyer conjecture, *Inventiones Mathematicae*, 72 (1983), pàgs. 241-265.

[Ne 86] Neukirch, J., *Class field theory*, Grundlehren der Matematischen Wissenschaft, 280 (1986).

[Ro 73] Robert, G., Unités elliptiques, *Bull. Soc. Math. France*, 36, (1973).

[Ru 81] Rubin, K., Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, *Inventiones Mathematicae*, 64 (1981), pàgs. 455-470.

[Ru 91] Rubin, K., The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Inventiones Mathematicae*, 103 (1991), pàgs. 25-68.

[Shi 71] Shimura, G., *Introduction to the arithmetic theory of automorphic functions*, Pub. Math. Soc. Japan, 11 (1981).

Punts de Heegner i derivades de L sèries (Gross-Zagier)

Josep González

Gener, 1999

Índex

1 Introducció

El principal teorema d'aquest article, relacionat amb la conjectura de Birch i Swinnerton-Dyer, proporciona una relació entre les altures de classes de divisors de Heegner de la jacobiana de la corba modular de $X_0(N)$ i els valors de la primera derivada en $s = 1$ de L-sèries de certes formes modulars. Aquest teorema s'aplica després a una corba el·líptica modular E definida sobre $\mathbf{Q}$ tal que la seva L-sèrie té un zero simple, obtenint-se que E té un punt racional d'ordre infinit i una certa expressió de $L'(E, 1)$.

L'article publicat en l'Inventiones té una extensió d'unes 100 pàgines. Un avanç dels resultats obtinguts en aquest article, que van ser publicats en la revista Comptes Rendues, contenen alguns errors que els mateixos autors assenyalen posteriorment en l'article de l'Inventiones. Aquest treball dona resultats relatius a formes parabòliques de pes $2k > 2$ i una bona quantitat de fórmules intermitges que no mencionarem en aquest resum.

2 La corba modular $X_0(N)/\mathbf{C}$

Siguin un enter $N > 1$ i $\Gamma_0(N) = \{\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SL_2(\mathbf{Z}) : C \equiv 0 \pmod{N}\}$. Denotem per $\mathbf{H}$ el semipla superior de Poincaré. La corba $X_0(N)/\mathbf{C}$ és la superfí cie de Riemann compacte que s'obté quan dotem l'espai topològic $\Gamma_0(N)\backslash\mathbf{H} \cup \mathbf{P}^1(\mathbf{Q})$ d'unes cartes locals tals que el cos de les funcions meromorfes $\mathbf{C}(X_0(N)) = \mathbf{C}(j, j_N)$, on j és la funció modular el·lí ptica i $j_N(\tau) = j(N\tau)$. Denotem per $Y_0(N)$ l'obert de $X_0(N)$ que correspon a $\Gamma_0(N)\backslash\mathbf{H}$ i per $\mathcal{F}$ un domini fonamental de $Y_0(N)$. Les puntes són els punts de $\Gamma_0(N)\backslash\mathbf{P}^1(\mathbf{Q})$. Podem descriure els punts de $Y_0(N)(\mathbf{C})$ de les maneres següents:

- Mitjançant els punts $\tau \in \mathcal{F}$.
- Pels parells de coordenades $(j(\tau), j_N(\tau))$ amb $\tau \in \mathcal{F}$. Ull!!, punts diferents de $Y_0(N)$ poden tenir el mateix parell de coordenades, ja que el model obtingut mitjançant el polinomi modular $\Phi_N(X, Y)$ té singularitats.
- **Interpretació de moduli.** Sigui k un subcos de $\mathbf{C}$. Els punts de $Y_0(N)(k)$ s'interpreten de la manera següent:

  $$x \in Y_0(N)(k) \leftrightarrow x = \phi : E \to E',$$

  on E i E' són corbes el·lí ptiques definides sobre k i ϕ una isogènia cí clica de grau N definida sobre k. Notem que $ker\phi$ en $\overline{k}$ és isomorf a $\mathbf{Z}/N\mathbf{Z}$. El lligam amb l'anterior descripció és que $(j(x), j_N(x)) = (j(E), j(E'))$ (també es pot triar la identificació amb el punt $(j(x), j_N(x)) = (j(E'), j(E))$). Les puntes són els punts $x \in X_0(N)$ tals que $j(x) = j_N(x) = \infty$. Ogg va determinar les puntes que són racionals i, en particular, $0, \infty \in X_0(N)(\mathbf{Q})$ per a tot N.
- En els cas complex, les classes de isomorfia de corbes el·lí ptiques complexes venen donades per les superfí cies de Riemann compactes $\mathbf{C}/\Lambda$ on Λ és una ret $\langle\omega_1, \omega_2\rangle$ de $\mathbf{C}$. Agafarem les rets orientades, és a dir $\omega_1/\omega_2 \in \mathbf{H}$. Aleshores, $j(\mathbf{C}/\Lambda) = j(\omega_1/\omega_2)$. Dues corbes el·lí ptiques donades per les rets Λ, Λ' són isògenes (resp. isomorfes) sii existeix $\alpha \in \mathbf{C}^*$ tal que $\alpha\Lambda \subset \Lambda'$ (resp. $\alpha\Lambda = \Lambda'$) i la isogenia (resp. l'isomorfisme) ve donat per:

  $$[\alpha] : \mathbf{C}/\Lambda \to \mathbf{C}/\Lambda', \quad z \mapsto \alpha\, z\,.$$

  Els punts de $Y_0(N)(\mathbf{C})$ poden ser descrits com segueix:

  $$x \in Y_0(N)(\mathbf{C}) \leftrightarrow x = \mathrm{Id} : \mathbf{C}/\Lambda \to \mathbf{C}/\Lambda',$$

  on Id és la identitat i $\Lambda' = \langle\omega_1, \omega_2/N\rangle \subset \Lambda$.

3 Involucions i correspondències

Involucions. La involució canónica (**de Fricke o d'Atkin**) w_N ve donada, en les diferents descripcions, per:

- $w_N : X_0(N) \to X_0(N)\,, \tau \mapsto -1/(N\tau) \pmod{\Gamma_0(N)}$.
- $(j(\tau), j_N(\tau)) \mapsto (j_N(\tau), j(\tau))$.
- En la interpretació de moduli: $x = \phi : E \to E' \mapsto w_N(x) = \widehat{\phi} : E' \to E\,.$
- $x = \mathrm{Id} : \mathbf{C}/\langle \omega_1, \omega_2\rangle \to \mathbf{C}/\langle \omega_1, \omega_2/N\rangle \mapsto w_N(x) = [N] : \mathbf{C}/\langle \omega_1, \omega_2/N\rangle \to \mathbf{C}/\langle \omega_1, \omega_2\rangle$.

Pels divisors $d|N$ tals que $(d, N/d) = 1$ tenim les involucions d'Atkin-Lehner w_d:

- $\tau \in \mathcal{F} \mapsto w_d(\tau) = (A\tau + B)/(C\tau + D) \pmod{\Gamma_0(N)}$, amb $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GL_2(\mathbf{Z})$, $det\gamma = d$, $A, D \equiv 0 \pmod{d}$, $C \equiv 0 \pmod{N}$.
- $x = (j(\tau), j_N(\tau)) \mapsto w_d(x) = (j_d(\tau), j_{N/d}(\tau))$.
- Amb la interpretació de moduli:

$$x = \phi : E \to E' \mapsto w_d(x) = \phi_d : E/ker\phi \cap E[d] \to E'/ker\widehat{\phi} \cap E'[d]\,.$$

- $x = \mathrm{Id} : \mathbf{C}/\langle \omega_1, \omega_2\rangle \to \mathbf{C}/\langle \omega_1, \omega_2/N\rangle \mapsto w_d(x) = [N] : \mathbf{C}/\langle \omega_1, \omega_2/d\rangle \to \mathbf{C}/\langle \omega_1/d, \omega_2/N\rangle$.

Designarem per W el grup d'aquestes involucions. Si N té s factors primers diferents, aleshores $|W| = 2^s$ i la llei de composició ve donada per

$$w_d\, w_{d'} = w_{d''}\,, \qquad \text{on } d'' = d\, d'/(d, d')^2\,.$$

Correspondències. Per a cada enter $m \geq 1$ la correspondència de Hecke T_m està definida sobre $X_0(N)$ com segueix:

$$x = \phi : E \to E' \mapsto T_m(x) = \sum_C (x_C)\,, \quad x_C = \phi_C : E/C \to E'/\phi(C)\,,$$

on C recorre tots els subgrups d'ordre m que tallen trivialment a $ker\phi$ i ϕ_C és la isogènia induïda per ϕ entre E/C i $E'/\phi(C)$. El corresponent endomorfisme en la jacobiana de $X_0(N)$, que denotarem per J, està definit sobre $\mathbf{Q}$. Denotem per $\mathbf{T}$ la $\mathbf{Q}$-àlgebra dels operadors de Hecke que és la sub-àlgebra commutativa de $\mathrm{End}_{\mathbf{Q}}(J)$ generada pels T_m.

Obtenció de formes parabòliques de pes 2 a partir de T. Com sempre $S_2(\Gamma_0(N))$ denota el $\mathbf{C}$-espai vectorial de les formes parabòliques de pes 2 per a $\Gamma_0(N)$. Donada una forma $g = \sum_{n\geq 1} b_n q^n \in S_2(\Gamma_0(N))$, posarem $a_1(g) = b_1$. Notem que donada una aplicació $\mathbf{Q}$-lineal $\alpha : \mathbf{T} \to \mathbf{C}$, aleshores la funció $\sum_{m\geq 1} \alpha(T_m)q^m \in S_2(\Gamma_0(N))$. Aquest resultat, que serà utilitzat posteriorment, s'obté a partir del fet que l'aplicació següent:

$$\beta : \mathbf{T} \times S_2(\Gamma_0(N))_{\mathbf{Q}} \to \mathbf{Q}\,, \quad \beta(T, f) = a_1(T(f))\,,$$

és un aparellament perfecte. Aqui $S_2(\Gamma_0(N))_{\mathbf{Q}}$ denota les formes amb desenvolupaments de Fourier racionals (recordem que $\mathbf{C} \otimes S_2(\Gamma_0(N))_{\mathbf{Q}} = S_2(\Gamma_0(N))$. En particular, $\mathbf{T}$ és una $\mathbf{Q}$-àlgebra de dimensió el gènere de $X_0(N)$.

Notem que si k és un subcos de $\mathbf{C}$, aleshores

$$J(k) \simeq Div^0(X_0(N))_k / Divp(X_0(N))_k\,,$$

on:

$$Div^0(X_0(N))_k = \{c \in Div^0 X_0(N) : {}^\sigma c = c \text{ per a tot } \sigma \in \mathrm{Gal}(\overline{k}/k)\}\,,$$

$$Divp(X_0(N))_k = \{c \in Div^0(X_0(N))_k : \exists f \in \mathbf{C}(X_0(N)) \text{ amb } \mathrm{div}\, f = c\}\,.$$

Així , si K és un cos de nombres i H/K és una extensió galoisiana finita amb grup de galois G i $x \in X_0(N)(H)$ aleshores $\sum_{\sigma\in G}({}^\sigma x) - |G|(\infty) \in J(K)$. En el nostre cas K serà un cos quadràtic imaginari i H el seu cos de classes de Hilbert.

4 Corbes el·lí ptiques amb CM i punts de Heegner de $X_0(N)$

Donada una corba el·lí ptica $E/\mathbf{C}$, l'anell $\mathrm{End}(E)$ és $\mathbf{Z}$ o un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K. En aquest darrer cas es diu que E té CM per $\mathcal{O}$, i la condició $\mathbf{Q} \otimes \mathrm{End}(E) = K$ equival al fet que $j(E) = j(\tau)$, amb $\tau \in \mathbf{H}$, implica que $\mathbf{Q}(\tau) = K$ (el rec/'/i proc també és cert). Si E té CM, aleshores $j(E)$ és enter algebraic.

Per a tota c. e. E definida sobre qualsevol cos algebraicament tancat, l'anell $\mathrm{End}(E)$ és un invariant de la classe d'isomorfia de E, mentre que el cos $\mathbf{Q}\otimes\mathrm{End}(E)$ és un invariant de la classe d'isogenia de E. Quan ens limitem a corbes el·lí ptiques complexes, si E té CM pel cos $K = \mathbf{Q} \otimes \mathrm{End}(E)$, aquest cos determina la classe d'isogènia de E (aquest fenomen coincideix amb el que passa quan treballem amb c.e. definides sobre una clausura algebraica d'un cos finit).

Els ordres dels cossos quadràtics queden individualitzats pels seus discriminants. Donem una descripció d'aquesta relació en el cas imaginari. El discriminant d'un ordre d'un cos quàdratic imaginari K és un enter negatiu $D \in \mathbf{Z}$ tal que $D \equiv 0, 1 \pmod 4$. Reciprocament, per a cada enter negatiu $D \in \mathbf{Z}$ tal que

$D \equiv 0, 1 \pmod 4$ existeix un únic ordre $\mathcal{O}$ d'un cos quadràtic que té discrimant D i aquest ordre ve donat per $\mathcal{O} = \langle 1, (D + \sqrt{D})/2 \rangle_{\mathbf{Z}}$. Si D_K denota el discriminant de K, aleshores $D = f^2 D_K$ amb $f \in \mathbf{Z}$; aquest enter $f > 0$ s'anomena el conductor de l'ordre $\mathcal{O}$.

Donat un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K, denotem per $\mathrm{Cl}(\mathcal{O})$ el grup de classes d'ideals fraccionaris invertibles (propis) de $\mathcal{O}$, per $\mathcal{A}_1, \ldots \mathcal{A}_h$ les seves classes i per per $h = h(\mathcal{O})$ el seu cardinal. Siguin $\mathfrak{a}_1, \cdots, \mathfrak{a}_h$ ideals fraccionaris i invertibles de $\mathcal{O}$ tals que $\mathfrak{a}_i \in \mathcal{A}_i$ ($[\mathfrak{a}_i] = \mathcal{A}_i$). Aleshores les classes d'isomorfia de les corbes e
lgem í ptiques

$$\mathbf{C}/\mathfrak{a}_1, \ldots, \mathbf{C}/\mathfrak{a}_h$$

són diferents i descriuen totes les c.e. que tenen CM per $\mathcal{O}$ (en particular tot ordre $\mathcal{O}$ és l'anell d'endomorfismes d'una c.e. amb CM). El cos $H = K(j(\mathfrak{a}_i))$ és el cos de classes de l'anell $\mathcal{O}$, és a dir H és la màxima extensió abeliana de K no ramificada fora de f i tal que $\mathrm{Cl}(\mathcal{O}) \simeq \mathrm{Gal}(H/K)$. En particular, $[H : K] = h$, $\prod_{i=1}^{h}(X - j(\mathfrak{a}_i)) \in \mathbf{Z}[X]$ eś $\mathbf{Q}$-irreductible i i l'isomorfisme $\mathrm{Cl}(\mathcal{O}) \simeq \mathrm{Gal}(H/K)$ que ve donat pel sí mbol d'Artin s'expressa per

$$\mathcal{A} = [\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}) \mapsto \sigma_{\mathcal{A}} \in \mathrm{Gal}(H/K) : H \to H \, , j(\mathfrak{b}) \mapsto j(\overline{\mathfrak{a}}\mathfrak{b}) \, .$$

Punts de Heegner. Un punt $x = \phi : E \to E' \in Y_0(N)$ es diu de Heegner si E i E' tenen CM pel mateix ordre $\mathcal{O}$. Com abans, D denota el discrimant de $\mathcal{O}$. Ens limitem als casos en que $(D, N) = 1$. Tenim que $X_0(N)$ té punts de Heegner d'ordre $\mathcal{O}$ amb $(D, N) = 1$ sii $\exists y \in \mathbf{Z}$ tal que $D \equiv y^2 \pmod{4N}$. El motiu d'aquesta caracterització és el següent:

Si $x = \phi : E \to E'$ és un punt de Heegner, aleshores existeixen dues rets Λ, Λ' de $\mathbf{C}$ que són $\mathcal{O}$-mòduls de rang 1 tals que $E = \mathbf{C}/\Lambda$ i $E' = \mathbf{C}/\Lambda'$. Modificant Λ' per una ret homotetica, podem suposar que $\Lambda \subset \Lambda'$ i que ϕ és la identitat. En aquest cas Λ i Λ' són ideals fraccionaris i propis de $\mathcal{O}$ i $\mathfrak{n} = \Lambda(\Lambda')^{-1}$ és un ideal enter i primitiu ($\mathfrak{n}$ no és divisible per cap natural > 1) que té norma N ($\mathcal{O}/\mathfrak{n} \simeq \mathbf{Z}/NZ$). Aquesta condició equival a que existeixi una forma quadràtica primitiva definida positiva i de discriminant D tal que N es respresentable per aquesta forma quadràtica i, per tant, D és congrüent a un quadrat mòdul $4N$.

En cas d'existir punts de Heegner d'ordre $\mathcal{O}$, aquets punts es descriuen pels parells:

$$(\mathcal{A}, \mathfrak{n}) \quad \text{amb } \mathcal{A} \in \mathrm{Cl}(\mathcal{O}) \text{ i } \mathfrak{n} \text{ és un ideal enter i primitiu de } \mathcal{O} \text{ de norma } N \, .$$

Donat un tal parell, s'agafa $\mathfrak{a} \in \mathcal{A}$ i $x = \mathrm{Id} : \mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1}$ és un punt de Heegner de $X_0(N)$.

El *número* de punts de Heegner relatius a $\mathcal{O}$ és $h.2^s$ (quan n'existeixen), on recordem que s és el nombre de factors primers que divideix N. Aquest fet és degut a que podem triar h classes diferents en $\mathrm{Cl}(\mathcal{O})$ i 2^s ideals enters primitius diferents de norma N (tot primer $p|N$ descompon completament en K).

El grup $\mathrm{Gal}(H/K) \times W$ actua transitivament sobre els punts de Heegner i el seu cardinal coincideix amn el número de punts de Heegner. Posem $G = \mathrm{Gal}(H/K)$ i a continuació describim les accions de la conjugació complexa i de $G \times W$ sobre els punts de Heegner:

- La conjugació complexa: $(\mathcal{A}, \mathfrak{n}) \mapsto (\overline{\mathcal{A}}, \overline{\mathfrak{n}}) = (\overline{\mathcal{A}}, \mathcal{O}\mathfrak{n}^{-1})$.
- El grup G: $\sigma_{\mathcal{A}'} : (\mathcal{A}, \mathfrak{n}) \mapsto (\mathcal{A}\overline{\mathcal{A}'}, \mathfrak{n})$.
- El grup W: $w_d \in W : (\mathcal{A}, \mathfrak{n}) \mapsto (\mathcal{A}[\mathfrak{d}], \mathfrak{n}')$ on $\mathfrak{d}$ és l'ideal mcd de (d) i $\mathfrak{n}$ i $\mathfrak{n}'$ és l'ideal obtingut de $\mathfrak{n}$ canviant els ideals primers que divideixen $\mathfrak{n}$ i (d) pels seus conjugats ($\mathfrak{n}' = \mathfrak{n}\overline{\mathfrak{d}}\mathfrak{d}^{-1}$).

Els punts de Heegner són H-racionals. Fixat un punt de Heegner $x \in X_0(N)$, denotarem per $c, d \in J(H)$ els divisors $c = (x) - (\infty)$, $d = (x) - (0)$. Donat un caràcter $\chi : G \to \mathbf{C}^*$, posem

$$(Div^0 X_0(N)_H)^\chi = \{m \in Div^0 X_0(N)_H \otimes \mathbf{C} : {}^\sigma m = \chi(\sigma)m \text{ per a tot } \sigma \in G\}\,,$$

on el grup G actua només sobre els punts de la corba. Així obtenim que $J(H)^\chi = (Div^0 X_0(N)_H)^\chi / (DivpX_0(N)_H)^\chi$ i que:

$$c_\chi := \sum_G \overline{\chi}(\sigma)^\sigma c \in J(H)^\chi\,.$$

Notació. A partir d'ara, K és un cos quadràtic imaginari de discrimant D amb $(D, N) = 1$ i $D \equiv 1 \pmod 4$, $\mathcal{O}$ denota el seu anell d'enters, $\varepsilon : (\mathbf{Z}/D\mathbf{Z})^* \to \{\pm 1\}$ denota el càracter associat al cos quadràtic K, $u = \#\mathcal{O}^*/2$, H el cos de classes de Hilbert de K, $G = \mathrm{Gal}(H/K)$ i $\chi : G \to \mathbf{C}^*$ un caràcter del grup de classes. Notem que si χ és quadràtic (només agafa els valors ± 1), aleshores χ és un caràcter del gènere i correspon a un caràcter $\chi_{D_1.D_2}$, on $D = D_1.D_2$ i D_1, D_2 són discriminants de cossos quadràtics (un real i l'altre imaginari); l'acció d'aquest caràcter en els ideals enters $\mathfrak{a}$ de $\mathcal{O}$ que són primers amb D ve donada per:

$$\chi_{D_1.D_2}(\mathfrak{a}) = \varepsilon_{D_1}(N(\mathfrak{a}))\varepsilon_{D_2}(N(\mathfrak{a}))\,.$$

5 L-sèries

En aquesta secció no suposem que hi hagin punts de Heegner a $X_0(N)$ d'ordre $\mathcal{O}$. Sigui $S_2(\Gamma_0(N))$ el conjunt de formes parabòliques de pes 2 per a $\Gamma_0(N)$. En $S_2(\Gamma_0(N))$ tenim definit el producte de Petersson:

$$(f, g) = \int\int_{\Gamma_0(N)\backslash \mathbf{H}} f(z)\overline{g(z)}\frac{dxdy}{y^2} \quad z = x + iy\,,$$

on la integral s'efectua en un domini fonamental de $X_0(N)$. EL $\mathbf{C}$-espai vectorial $S_2(\Gamma_0(N)$ s'identifica amb el de les diferencials regulars de $X_0(N)$, mitjançant

$$f \mapsto \omega_f = 2\pi i f(z)dz = q^{-1}f(q)dq\,.$$

Llevat una constant multiplicativa, el producte de Petersson es llegeix en les diferencials regulars de $X_0(N)$:

$$(\omega_1, \omega_2) = \int_{X_0(N)(\mathbf{C})} \omega_1 \wedge \overline{i\omega_2}\,,$$

on $||\omega_f|| = 8\pi^2(f,f)$. Sigui, ara, $f = \sum_{n\geq 1} a_n q^n$ una forma nova de pes 2 per a $\Gamma_0(N)$. Recordem que aleshores $(f,g) = 0$ per a tota forma vella $g \in S_2(\Gamma_0(N))$ i que els operadors $T_m \in \mathbf{T}$, $m \not| N$ operan de manera autoadjunta amb el producte de Petersson.

Com sempre la L-sèrie associada a f és

$$L(f,s) = \sum_{n\geq 1} \frac{a_n}{n^s}\,.$$

La funció $L(f,s)$ convergeix absolutament per a $Re(s) > 3/2$, admet prolongació holomorfa a tot el pla complex i satisfà l'equació funcional:

$$L^*(f,s) := (2\pi)^{-s}\Gamma(s)L(f,s) = -N^{1-s}L^*(f|w_N, 2-s)\,, \qquad \text{per a tot } s \in \mathbf{C}.$$

Si $f|w_N = f$, aleshores $L(f,s)$ té un zero en $s=1$ i si $L(f,s)$ té un zero simple en $s=1$, aleshores $f|w_N = f$.

Fixem $\mathcal{A} \in \mathrm{Cl}_K$. D'una banda, tenim la theta-sèrie:

$$\Theta_{\mathcal{A}}(z) = \frac{1}{2u} + \sum_{\mathfrak{a}\in\mathcal{A}, \mathfrak{a} \text{ enter}} e^{2\pi i z N(\mathfrak{a})} = \sum_{n\geq 0} r_{\mathcal{A}}(n) e^{2\pi i n z}\,,$$

que és una forma modular (no parabòlica) de pes 1 per a $\Gamma_0(|D|)$ i amb caràcter ε. Notem que per a $n \geq 0$, $r_{\mathcal{A}}(n)$ és el nombre d'ideals enters de $\mathcal{A}$ amb norma n.

Posem

$$L_{\mathcal{A}}(f,s) := \sum_{n\geq 1,(n,DN)=1} \varepsilon(n) n^{1-2s} \sum_{n\geq 1} a_n r_{\mathcal{A}}(n) n^{-s}\,.$$

Si f és un vector propi normalitzat de tots els operadors de Hecke i χ un caràcter de classes, posem:

$$L(f,\chi,s) = \sum_{\mathcal{A}\in\mathrm{Cl}_K} \chi(\mathcal{A}) L_{\mathcal{A}}(f,s)\,.$$

Aquesta L-sèrie quan $\chi = \mathrm{Id}$ està relacionada amb la L-sèrie de f mitjançant la igualtat:

$$L(f,s)L_{\varepsilon}(f,s) = L(f,\mathrm{Id},s)\,,$$

on $L_\varepsilon(f,s)=\sum_{n\geq 1}\varepsilon(n)a_n/n^s$.
NOTA: Quan f sigui la L-sèrie d'una c.e modular E definida sobre $\mathbf{Q}$, aleshores $L(f,\mathrm{Id},s)$ serà la L-sèrie de E sobre K.

Els resultats principals estàn continugunts en les següents proposicions.

Proposició 5.1 *Les funcions $L_{\mathcal{A}}(f,s)$ i $L(f,\chi,s)$ tenen prolongació holomorfa a tot el pla complex. Les funció $L(f,s)$ satisfà l'equació funcional*

$$L^*_{\mathcal{A}}(f,s):=(2\pi)^{-2s}N^s|D|^s\Gamma(s)^2L_{\mathcal{A}}(f,s)=-\varepsilon(N)L^*_{\mathcal{A}}(f,2-s)\,.$$

L'equació funcional per a $L(f,\chi,s)$ és idèntica. En particular, si $\varepsilon(N)=1$, aleshores $L_{\mathcal{A}}(f,1)=0$ i $L_{\mathcal{A}}(f,\chi,1)=0$.

Teorema 5.1 *Si $\varepsilon(N)=1$, aleshores existeix una forma modular $\Phi_{\mathcal{A}}(z)=\sum_{m\geq 1}a_{m,\mathcal{A}}q^m\in S_2(\Gamma_0(N))$ tal que:*

1. *$L'_{\mathcal{A}}(f,1)=\frac{8\pi^2}{\sqrt{|D|}}(f,\Phi_{\mathcal{A}})$ per a tota forma nova $f\in S_2(\Gamma_0(N))$.*
2. *Els coeficients $a_{m,\mathcal{A}}$ venen donats per:*

$$-\sum_{1\leq n\leq m|D|/N}\sigma'_{\mathcal{A}}(n)r_{\mathcal{A}}(m|D|-nN)+\frac{h}{u}r_{\mathcal{A}}(m)\left(log\frac{N|D|}{4\pi^2m}-2\gamma+2\frac{L'}{L}(1,\varepsilon)\right)$$

$$+lim_{s\to 0}\left(-2\sum_{n\geq 1}\sigma_{\mathcal{A}}(n)r_{\mathcal{A}}(m|D|+nN)Q_s(1+\frac{2nN}{m|D|})-\frac{h\kappa}{u^2}\sigma_1(m)\frac{1}{s}\right)$$

$$+\frac{h\kappa}{u^2}\left(\sigma_1(m)(log\frac{N}{|D|}+2\sum_{p|N}\frac{logp}{p^2-1}+2+2\frac{\zeta'}{\zeta}(2)-2\frac{L'}{L}(1,\varepsilon))+\sum_{d|m}dlog\frac{m}{d^2}\right)\,,$$

on

- *γ és el factor de Euler*
- *$L(s,\varepsilon)=\sum_{n\geq 1}\frac{\varepsilon(n)}{n^s}$*
- *$Q_s(t)=\int_0^\infty(t+\sqrt{t^2-1}coshu)^{-(s+1)}du$ amb $t>1$, $s>-1$ (Funció de Legendre de segona classe).*
- *$\sigma_1(m)=\sum_{d|m}d$,*
- *$\kappa=-12/N\prod_{p|N}(1+\varepsilon(p)/p)$,*
- *$\sigma_{\mathcal{A}}(n)=\sum_{d|n,d>0}\varepsilon_{\mathcal{A}}(n,d)$,*
- *$\sigma_{\mathcal{A}}=\sum_{d|n,d>0}\varepsilon_{\mathcal{A}}(n,d)log(n(d^2)$,*
- *$\varepsilon_{\mathcal{A}}(n,d)=\begin{cases}0 & si\ (d,n/d,D)\neq 1\\ \varepsilon_{D_1}(d)\varepsilon_{D_2}(\frac{-Nn}{d})\chi_{D_1.D_2}(\mathcal{A}) & altrament,\ |D_2|=(d,D),D_1=\frac{D}{D_2}.\end{cases}$*

NOTA: Quan en $X_0(N)$ existeixen punts de Heegner d'ordre $\mathcal{O}$, aleshores $\varepsilon(p)=1$ per a tot primer $p|N$ i, en particular, $\varepsilon(N)=1$.

6 Altures locals i globals

Per a cada plaça v de H, denotem per H_v el completat de H per v i definim l'homomorfisme de valoració $|\ |_v : H_v^* \to \mathbf{R}_+^*$ per:

$$|\alpha|_v = \begin{cases} \alpha\overline{\alpha} = |\alpha|^2 & \text{si } H_v \simeq \mathbf{C} \\ q_v^{-v(\alpha)} & \text{si } H_v \text{ és no arquimedià i } q_v \text{ és l'ordre del cos residual} \end{cases}$$

Per a cada $\alpha \in H^*$ tenim la fòrmula producte: $\prod_v |\alpha|_v = 1$.

La teoria de Néron proporciona un únic sí mbol $\langle a, b\rangle_v$ amb valors a $\mathbf{R}$, que està definit sobre els divisors de grau zero de $X_0(N)$ que són relativament primers entre si i definits sobre H_v. Aquest simbol satisfà les condicions:

- És bilineal,
- simètric,
- continu: $\langle a, \sum_j m_j y_j\rangle$ és contí nua sobre $S\backslash|a|$ (S compacte) amb relació cada y_j,
- $\langle a, b\rangle_v = \sum_x m_x log|f(x)|_v$ quan $a = \sum m_x(x)$ i $b = div(f)$.

Es poden obtenir fòrmules pel sí mbol local utilitzant la teoria del potencial quan v és arquimediana i la teoria d'intersecció quan v no és arquimediana. Si a i b són relativament primers entre si i definits sobre H aleshores es pot definir:

$$\langle a, b\rangle = \sum_v \langle a, b\rangle_v \,,$$

ja que només un numero finit és no nul. El sí mbol depen només de les imatges de a i b en $J(H)$ i defineixen un aparellament a valors reals en $J(H) \otimes \mathbf{R}$. Es denota per $\widehat{h}(a) = \langle a, a\rangle$ que és la altura canònica de Néron-Tate asssociada a la classe del divisor (2Θ). Ja que Θ és simètric i positiu, $\widehat{h}$ és una forma quadràtica definida positiva sobre $J(H) \otimes \mathbf{R}$ i pot ser extessa a una forma hermí tica sobre $J(H) \otimes \mathbf{C}$. Notem que la forma en $J(H)$ només s'anul·la sobre els punts de torsió de $J(H)$.

Suposem, ara, que $x \in X_0(N)$ és punt de Heegner d'ordre $\mathcal{O}$ i fixem $\sigma \in G$. Sigui $\mathcal{A} \in \mathrm{Cl}_K$ tal que via el sí mbol d'Artin proporciona σ. Gross-Zagier calculen el valors dels í mbols $\langle c, T_m{}^\sigma c\rangle_v$ per tal d'identificar la forma $g_\mathcal{A}$ de $S_2(\Gamma_0(N))$ que obtenen a partir de l'aplicació lineal

$$\alpha : \mathbf{T} \to \mathbf{C}\,, \quad \alpha(T_m) = \langle c, T_m{}^\sigma c\rangle\,.$$

Com que $d - c = (0) - (\infty)$ és de torsió, $\langle c, T_m{}^\sigma d\rangle_v = \langle c, T_m{}^\sigma c\rangle_v$. Realitzen el càlcul del sí mbol $\langle c, T_m{}^\sigma d\rangle_v$, per evitar la repetició de ∞ en els dos divisors de l'aparellament. Primer calculen el valor en les places arquimedianes (funcions de

Green) i denoten per $\langle c, T_m{}^\sigma d\rangle_\infty$ la seva suma. Després ho fan en les places no arquimedianes aprupades per primers enters

$$\langle c, T_m{}^\sigma d\rangle_p = \sum_{\mathfrak{p}|p} \langle c, T_m{}^\sigma d\rangle_{\mathfrak{p}} \, .$$

És un pal. Han de distingir quan $r_{\mathcal{A}}(m)$ és zero i diferent de zero, ja que segons sigui un cas o l'altre els divisors de l'aparellament són primers entre si o no. A més, en el cas de les places no arquimedianes, s'ha de distingir quan $\mathfrak{p}$ decompon completament, ramifica o és inert en K.

Aquets càlculs els hi permeten provar que:

$$\langle c, T_m{}^\sigma c\rangle = u^2 a_{m,\mathcal{A}} \quad \text{per a } (m,N)=1.$$

Per tant, $g_{\mathcal{A}}$ i $u^2\Phi_{\mathcal{A}}$ difereixen en una forma vella i tenen el mateix producte de Petersson per a tota forma nova.

D'altre banda, els elements de l'àlgebra $\mathbf{T}$ actuen com endomorfismes lineals de l'espai vectorial $V = \mathbf{C}\otimes J(H)$. La seva acció és autoadjunta respecte $\langle -,-\rangle$, la $\mathbf{Q}$-àlgebra $\mathbf{T}$ està definida sobre $\mathbf{Q}$ i $\mathbf{T}$ conmuta amb l'acció de G. Així , si agafen una base $\{g\}$ de $S_2(\Gamma_0(N)$ amb coeficients reals i que contingui una base de formes noves normalitzades es té que $V = \oplus_g V_g$ (si g és nova el subespai V_g queda determinat per ser l'espai dels vectors propis de tots els T_m amb els mateixos valors propis que g). Per tant, $c_\chi = \sum_g c_{\chi,g}$ amb $c_{\chi,g}\in V_g^\chi$. Finalment, s'obté la proposició següent:

Proposició 6.1

$$L'(f,\chi,1) = \frac{8\pi^2}{hu^2\sqrt{|D|}}\widehat{h}(c_{\chi,f})(f,f) = \frac{||\omega_f||^2}{hu^2\sqrt{D}}\widehat{h}(c_{\chi,f}) = \frac{||\omega_f||^2}{u^2\sqrt{D}}\widehat{h}_K(c_{\chi,f})\,.$$

D'aquesta proposició surten els corol·laris següents:

Corol·lari 6.1 *Si $f\in S_2(\Gamma_0(N))$ és una forma nova i χ un caràcter de classes de K, aleshores $L'(f,\chi,1)\geq 0$.*

Corol·lari 6.2 *Si $f\in S_2(\Gamma_0(N))$ és una forma nova i χ un caràcter de classes de K, aleshores totes les conjugades $L({}^\tau f, {}^\tau\chi, s)$ ($\tau\in Gal(\overline{\mathbf{Q}}/\mathbf{Q})$) tenen un zero simple en $s=1$ o tenen un zero d'ordre ≥ 3.*

El motiu és ben simple $c_{\chi,f}\in J(H)\otimes\mathbf{C}$ s'anul·la si i només s'anul·len els seus conjugats i aquets són els que surten en eles fòrmules.

Corol·lari 6.3 *Si $f\in S_2(\Gamma_0(N))$ és una forma nova i ${}^\tau f$ una conjugada de f, aleshores*

- $ord_{s=1}L(f,1)=0 \Leftrightarrow ord_{s=1}L({}^\tau f,s)=0$,

- $ord_{s=1}L(f,1) = 1 \Leftrightarrow ord_{s=1}L({}^{\tau}f,s) = 1$,
- $ord_{s=1}L(f,1) \geq 2 \Leftrightarrow ord_{s=1}L({}^{\tau}f,s) \geq 2$,
- $ord_{s=1}L(f,1) \geq 3 \Leftrightarrow ord_{s=1}L({}^{\tau}f,s) \geq 3$.

7 Conjectura de Birch i Swinnerton-Dyer

Sigui f la forma nova normalitzatda d'una corba el·líptica modular E definida sobre $\mathbf{Q}$ de conductor N. Sigui $\pi : X_0(N) \to E$ amb $\pi(\infty) = O$ una parametrització modular de E. Sigui ω l'invariant diferencial de E. Sabem que $\pi^*(\omega) = a\,\omega_f$, amb $a \in \mathbf{Z}$ (a es pot agafar > 0) i podem suposar que E és la parametrització forta de Weil, ja que la funció $L(E,s)$ no varia per $\mathbf{Q}$-isogènies i coincideix amb $L(f,s)$ (en aquest cas a és la cosntant de Manin que conjecturalment és 1).

Sigui $x \in X_0(N)$ un punt de Heegner i posem $P_K = \sum_{\sigma\in G}\pi({}^{\sigma}x) \in E(K)$ (la suma és la de E). Si identifiquem $E \simeq Pic^0(E)$, $P \mapsto (P) - (O)$, podem obtenir P_K com imatge d'un punt de $J(H)$ per $\pi_* : J \to Pic^0(E)$. En efectem, notem que $(P_K) - (O) = \pi_*(c_{Id}) = \pi_*(c_{Id,f})$. Es comproba que

$$\widehat{h}(P_K) = \widehat{h}(c_{\mathrm{Id},f})deg(\pi)\,, \quad ||\omega||^2 = a^2||\omega_f||^2/deg(\pi)\,,$$

on les altures en E i J són agafades ara sobre K (notem que $\widehat{h}_H(a) = h\,\widehat{h}_K(a)$). Gross-Zagier diuen que, llevat d'un signe, el punt P_K és independent de l'el·lecció del punt de Heegner x(fixat $\mathcal{O}$). El motiu crec que és el següent. El canvi de un punt de Heegner x per un altre, proporciona un nou divisor $c_{\mathrm{Id},f}$ que pot ser obtingut de l'anterior per alguna $w_d \in W$ i l'acció de w_d en el subespai V_f és la de multiplicar per ± 1 (el valor propi de f per w_d).

Sustituint en la proposició 6.1, s'obté:

Teorema 7.1 $L'(E/K,1) = \frac{||\omega||^2\widehat{h}_K(P_K)}{a^2u^2|D|^{1/2}}$.

Si constrastem aquest teroema amb la conjectura B & S-D per a $L(E/K,1)$, tenim que si $ord_{s=1}L(E/K,s) = 1$, aleshores $rankE(K) \geq 1$ i si $ord_{s=1}L(E/K,s) = rank(E/K) = 1$, aleshores $L'(E/K,1)$ satisfà B & S-D, mòdul quadrats racionals.

Per a la sèrie $L(E/\mathbf{Q},s)$ s'obté:

Teorema 7.2 *Suposem que $L(E,1) = 0$. Aleshores existeix un punt racional $P \in E(\mathbf{Q})$ tal que $L'(E,1) = \alpha\Omega\langle P,P\rangle$ amb $\alpha \in \mathbf{Q}^*$ En particular,*

1. *Si $L'(E,1) \neq 0$, aleshores $E(\mathbf{Q})$ conté un punt d'ordre infinit.*
2. *Si $L'(E,1) \neq 0$ i $rankE(\mathbf{Q}) = 1$, aleshores $L'(E,1) = \alpha\Omega R$ és certa per algun nombre racional α.*

La idea és la següent. Si $L'(E,1) = 0$ és trivial, s'agafa $P = O$. Suposem $L'(E,1) \neq 0$. En aquest cas, degut a l'equació funcional de $L(f,s)$, s'obté que $f|w_N = f$. Per un teorema de Walspurger, podem triar un cos K com els que estem gastant ($(D,N) = 1$, $D \equiv 1 \pmod 4$ i amb existència de punts de Heegner d'ordre $\mathcal{O}$) tal que $L_\varepsilon(s,1) \neq 0$. Tenim que

$$L(f,s)L_\varepsilon(f,s) = L(f,Id,,s)\,, \quad L'(f,1)L_\varepsilon(f,1) = L'(f,Id,1)\,.$$

Si $E : y^2 = x^3 + Ax + B$, aleshores posem $E' : Dy^2 = x^3 + Ax + B$ i tenim que $L_\varepsilon(f,s) = L(E',s)$. Per la teoria de sí mbols modulars de Mazur (Mazur & S-D), es té $L(E',1) = \alpha'\Omega'$, on Ω' és un periode fonamental real de la diferencial $\omega' = \omega/\sqrt{|D|}$ i $\alpha' \in \mathbf{Q}$. D'altre banda,

$$\frac{||\omega||^2}{\sqrt{|D|}} = [E(\mathbf{R}) : E(\mathbf{R})^0].\Omega.\Omega'\,.$$

Per tant,

$$L'(E/\mathbf{Q},1) = \frac{\widehat{h}_K(P_K)[E(\mathbf{R}) : E(\mathbf{R})^0]\Omega}{a^2u^2\alpha'}\,.$$

Gross-Zagier agafen $P = P_K + \overline{P_K} \in E(\mathbf{Q})$ sense justificar que $P \neq O$. Crec que el fet que $f|_{w_N} = f$ implica que $P_K = \overline{P}_K$ i, per tant, $P_K \in E(\mathbf{Q})$. Al aplicar aquestes relacions i el teorema 7.1, s'obté que:

$$L'(E,1) = \alpha\Omega\widehat{h}_{\mathbf{Q}}(P)\,,$$

amb $\alpha \in \mathbf{Q}$ ($\widehat{h}_{\mathbf{Q}}(P) = \widehat{h}_K(P)/2$.

Per concloure, notem que si la conjectura B & S-D és certa i l'ordre de $L(E,s)$ en $s = 1$ és > 1 aleshores els punts de Heegner proporcionen punts de torsió a E i perden la seva utilitat per obtenir punts racionals sense torsió de E.

Varietats abelianes modulars

P. Bayer[1]

Aquesta exposició és introductòria a l'article de Shouwu Zhang **[Zh 98]**, en el qual l'autor estudia la conjectura de Birch i Swinnerton-Dyer en el context de les varietats abelianes associades a formes modulars de Hilbert. Les varietats en qüestió s'obtenen com a quocient de jacobianes de corbes de Shimura, associades a àlgebres de quaternions. Els resultats obtinguts per Zhang generalitzen els que obtingueren Gross-Zagier **[Gr-Za 86]** i Kolyvagin **[Ko 90]**, el seu dia, arran de l'estudi de la conjectura de Birch i Swinnerton-Dyer en el context de les corbes el·líptiques modulars. Les tècniques desenvolupades per Zhang li permeten descriure el comportament aritmètic de certs punts de multiplicació complexa de corbes de Shimura.

§1. Corbes de Shimura

Siguin $\widehat{\mathbb{Z}} = \prod \mathbb{Z}_p$, $\widehat{\mathbb{Q}} = \widehat{\mathbb{Z}} \otimes \mathbb{Q}$, $\widehat{\mathbb{Q}}^\times$, l'anell de les adeles finites enteres, l'anell de les adeles finites racionals, i el grup multiplicatiu de les ideles finites racionals, respectivament. Donat un grup abelià M, denotarem $\widehat{M} = \widehat{\mathbb{Z}} \otimes M$ la seva adelització.

Sigui F un cos de nombres totalment real, de grau $d \geq 1$, i d'anell d'enters $\mathcal{O}_F$. Donada una plaça $\mathfrak{p}$ de F, sigui $F_\mathfrak{p}$ el completat de F en $\mathfrak{p}$ i siguin $\tau_i : F \to \mathbb{R}$ les diferents places reals de F. Denotarem per $\mathbb{A}_F$, respectivament $\mathbb{A}_F^\times$, l'anell d'adeles de F, respectivament el seu grup d'ideles. Notem que $\widehat{F}$ és l'anell de les adeles finites, i que $\widehat{F}^\times$ és el grup de

[1]Conferència impartida el 27 de gener de 1999. Amb el suport parcial de la DGES: PB96-0166.

les ideles finites.

Suposarem donada una àlgebra de quaternions $\mathbf{H}$ de centre F. Per a cada plaça $\mathfrak{p}$ de F, considerem la $F_\mathfrak{p}$-àlgebra $\mathbf{H}_\mathfrak{p} := F_\mathfrak{p} \otimes_F \mathbf{H}$. Recordem que l'àlgebra $\mathbf{H}$ es diu que és ramificada en $\mathfrak{p}$ quan $\mathbf{H}_\mathfrak{p}$ és el cos no commutatiu de rang 4 sobre $F_\mathfrak{p}$; l'àlgebra $\mathbf{H}$ es diu que descompon en $\mathfrak{p}$ quan $\mathbf{H}_\mathfrak{p}$ és l'àlgebra de matrius $\mathbf{M}(2, F_\mathfrak{p})$. Suposarem que $\mathbf{H}$ descompon en una plaça arquimediana τ_1 i que ramifica en la resta d'aquestes places. Considerarem fixat un isomorfisme $\mathbf{H}_{\tau_1} \simeq \mathbf{M}(2, \mathbb{R})$. Recordem que el discriminant reduït de $\mathbf{H}$ coincideix amb el producte de tots els ideals primers de $\mathcal{O}_F$ on $\mathbf{H}$ ramifica. El denotarem per $\mathfrak{d}$.

Començarem per donar una definició del pla complex intrínsecament associada a la F-àlgebra $\mathbf{H}$. Per a tal fi, considerem el tor de dimensió 2 sobre $\mathbb{R}$ obtingut per restricció de Weil del grup multiplicatiu sobre $\mathbb{C}$:

$$\mathbf{S} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\, \mathbf{G}_m.$$

Els seus punts reals són donats per $\mathbf{S}(\mathbb{R}) = (\mathbb{C} \otimes_\mathbb{R} \mathbb{R})^\times = \mathbb{C}^\times$. Considerem el grup algèbric sobre $\mathbb{Q}$ obtingut per restricció d'escalars del grup multiplicatiu $\mathbf{H}^\times$, entès com a grup algèbric sobre F:

$$\mathbf{G} := \mathrm{Res}_{F/\mathbb{Q}}\, \mathbf{H}^\times.$$

Els seus punts reals són donats per:

$$\mathbf{G}(\mathbb{R}) = (\mathbf{H} \otimes_\mathbb{Q} \mathbb{R})^\times = \mathbf{GL}(2, \mathbb{R}) \times (\mathbb{H}^\times)^{d-1},$$

on $\mathbb{H}$ denota el cos dels quaternions de Hamilton.

Si $F = \mathbb{Q}$ i $\mathbf{H} = \mathbf{M}(2, \mathbb{Q})$, aleshores $\mathbf{G}(\mathbb{R}) = \mathbf{GL}(2, \mathbb{R})$. Aquesta és la situació de la qual es parteix en l'estudi de les corbes modulars.

Sigui $\mathbf{T} = \mathrm{Res}_{F/\mathbb{Q}}\, \mathbf{G}_{m,F}$ i designem per $\nu : \mathbf{G} \to \mathbf{T}$ el morfisme de grups algèbrics definit per la norma reduïda. Sigui

$$h : \mathbf{S} \to \mathbf{G}_\mathbb{R} = \mathbb{R} \otimes_\mathbb{Q} \mathbf{G}$$

el morfisme de grups algèbrics del qual prové l'homomorfisme de grups

$$\begin{array}{rccc} h: & \mathbb{C}^\times & \longrightarrow & \mathbf{GL}(2,\mathbb{R}) \times (\mathbb{H}^\times)^{d-1} \\ & x+iy & \mapsto & \left(\begin{bmatrix} x & y \\ -y & x \end{bmatrix}^{-1}, 1, \ldots, 1\right). \end{array}$$

Aleshores, la classe de $\mathbf{G}(\mathbb{R})$-conjugació de h s'identifica amb dues còpies del semiplà superior de Poincaré $\mathcal{H}$ (cf. **[Ca 86]**).

Sigui $\mathfrak{n} \subseteq \mathcal{O}_F$ un ideal no nul. Denotarem per $\mathcal{O}(\mathfrak{d}, \mathfrak{n})$ un ordre de $\mathbf{H}$ de nivell $\mathfrak{n}$, i per $\mathcal{O}_{\mathbf{H}} := \mathcal{O}(\mathfrak{d}, 1)$, un ordre maximal de $\mathbf{H}$ que el contingui:

$$\mathcal{O}(\mathfrak{d}, \mathfrak{n}) \subseteq \mathcal{O}(\mathfrak{d}, 1) = \mathcal{O}_{\mathbf{H}}.$$

El producte $\mathfrak{d}\mathfrak{n}$ coincideix amb el discriminant reduït de $\mathcal{O}(\mathfrak{d}, \mathfrak{n})$. Cal tenir present, però, que els ideals $\mathfrak{d}, \mathfrak{n}$ no individuen ni l'ordre ni la seva classe de conjugació.

Considerem el grup discret aritmètic

$$\Gamma(\mathfrak{d}, \mathfrak{n}) := \mathcal{O}(\mathfrak{d}, \mathfrak{n})^\times,$$

format pels elements invertibles de l'anell $\mathcal{O}(\mathfrak{d}, \mathfrak{n})$. Escriurem $\Gamma = \Gamma(\mathfrak{d}, \mathfrak{n})$, quan convingui. És clar que $\Gamma \subseteq \mathbf{H}^\times$.

Notem que el grup $\mathbf{H}_+$ dels elements de $\mathbf{H}^\times$ de norma reduïda totalment positiva opera en $\mathcal{H}$.

1.1. Teorema. (cf. **[Sh 67]**, **[De 71]**) *Sigui* $\Gamma = \mathcal{O}(\mathfrak{d}, \mathfrak{n})^\times$.

i) El conjunt de classes dobles

$$X(\Gamma)(\mathbb{C}) := \mathbf{H}_+ \backslash \mathcal{H} \times \widehat{\mathbf{H}}^\times / \widehat{F}^\times \widehat{\Gamma} \cup \{\text{puntes}\}$$

s'identifica amb els punts d'una superfície de Riemann compacta.

ii) La corba projectiva associada a $X(\Gamma)(\mathbb{C})$ *posseeix un model canònic,* $X(\Gamma)$*, definit sobre el cos* F*. La corba* $X(\Gamma)$ *és llisa, connexa, però no geomètricament connexa; els seus components connexos geomètrics estan definits sobre certs cossos de classes de* F*.*

iii) Si $J(X(\Gamma))$ *és el subgrup component connex del grup* $\mathrm{Pic}(X(\Gamma))$*, aleshores,*

$$J(X(\Gamma)) = \mathrm{Res}_{\widetilde{F}/F} \mathrm{Pic}^0(X(\Gamma)/\widetilde{F}),$$

on $\widetilde{F}$ *denota l'extensió abeliana de* F *que correspon al subgrup d'ideles* $F_+(\widehat{F}^\times)^2\widehat{\mathcal{O}}_F^\times$*, per mitjà de la teoria de cossos de classes, i* F_+ *és el grup multiplicatiu dels elements de* F *totalment positius.*

La corba $X(\Gamma)$ s'anomena la corba de Shimura associada a Γ. El conjunt de puntes és buit, llevat dels casos $F = \mathbb{Q}$, $\mathfrak{d} = (1)$.

1.2. Observació. La superfície de Riemann $X(\Gamma)(\mathbb{C})$ és unió de superfícies de Riemann compactes i connexes

$$X_i = \mathcal{H}/\Gamma_i \cup \{\text{puntes}\}.$$

Si $\mathcal{O}_i(\mathfrak{d}, \mathfrak{n})$ designen representants de les diferents classes de conjugació d'ordres de $\mathbf{H}$ de nivell $\mathfrak{n}$, aleshores es pot prendre $\Gamma_i = \mathcal{O}_i(\mathfrak{d}, \mathfrak{n})^\times \cap \mathbf{SL}(2, \mathbb{R})$.

1.3. Definició. Sigui $\mathfrak{m} \subseteq \mathcal{O}_F$ un ideal sense factors en comú amb $\mathfrak{d}\mathfrak{n}$. Considerem el subconjunt $\widehat{\mathcal{O}}(\mathfrak{d}, \mathfrak{n})(\mathfrak{m}) \subseteq \widehat{\mathcal{O}}(\mathfrak{d}, \mathfrak{n})$ format pels elements el determinant dels quals genera l'ideal $\widehat{\mathfrak{m}}$. La correspondència de Hecke $T(\mathfrak{m})$ de $X(\Gamma)(\mathbb{C})$ es defineix per

$$T(\mathfrak{m})x = \sum_\gamma [(z, g\gamma)], \quad x \in X(\Gamma)(\mathbb{C}),$$

on $(z, g) \in \mathcal{H} \times \widehat{\mathbf{H}}^\times$ és un representant de x, $[(z, g)]$ és la seva projecció en $X(\Gamma)(\mathbb{C})$, i el sumatori s'estén a totes les classes $\gamma \in \widehat{\mathcal{O}}(\mathfrak{d}, \mathfrak{n})(\mathfrak{m})/\widehat{\Gamma}$.

§2. Interpretació modular de corbes de Shimura

Quan $d = [F : \mathbb{Q}] > 1$, les corbes de Shimura introduïdes a §1 no admeten, en general, cap descripció en termes d'espais de mòduls de varietats abelianes. Per vèncer aquesta dificultat, cal modificar-ne la definició. Per a tal fi, considerarem un grup algèbric, $\mathbf{G}'$, que tindrà el mateix grup derivat que el grup $\mathbf{G} = \mathrm{Res}_{F/\mathbb{Q}} \mathbf{H}^\times$, i un grup aritmètic prou gran, Γ', que també actuarà en el semiplà superior de Poincaré.

Siguin $D < 0$ un nombre racional lliure de quadrats i $F' := F(\sqrt{D})$ l'extensió quadràtica, totalment imaginària, que defineix. Considerem l'àlgebra de quaternions de centre F' que resulta per extensió d'escalars:

$$\mathbf{H}' := F' \otimes_F \mathbf{H}.$$

Sigui $\ell \to \overline{\ell}$ la involució de segona espècie de $\mathbf{H}'$ obtinguda en fer el producte tensorial de la conjugació de F' per la involució canònica de $\mathbf{H}$. La dimensió del $\mathbb{Q}$-espai vectorial V associat a $\mathbf{H}'$ és donada per

$$\dim_{\mathbb{Q}} V = \dim_{F'} \mathbf{H}' \cdot [F' : \mathbb{Q}] = 8d.$$

La multiplicació per l'esquerra dota V d'una estructura d'espai vectorial quaterniònic sobre $\mathbf{H}'$. Sigui $\delta \in \mathbf{H}'$ un element invertible i simètric ($\overline{\delta} = \delta$). En $\mathbf{H}'$, definim una altra involució de segona espècie per la fórmula $\ell^* := \delta^{-1}\overline{\ell}\delta$. D'aquesta manera, el $\mathbb{Q}$-espai vectorial V posseeix una forma bilineal alternada i no degenerada:

$$\psi(v, w) := \mathrm{tr}_{F'/\mathbb{Q}}(\alpha \,\mathrm{tr}_{\mathbf{H}'/F'}(v\delta w^*)),$$

on l'element $\alpha \in F'$ és no nul i imaginari ($\overline{\alpha} = -\alpha$). El parell (V, ψ) esdevé un espai simplèctic sobre $\mathbb{Q}$. A més,

$$\psi(\ell v, w) = \psi(v, \ell^* w), \quad \text{per a tot } \ell \in \mathbf{H}'.$$

Sigui $\mathbf{G}' := \mathbf{Sp}_{2\cdot 4d}(\mathbb{Q}, \psi)$ el grup algèbric sobre $\mathbb{Q}$ de les semblances simplèctiques de (V, ψ). Els punts racionals $\ell \in \mathbf{G}'(\mathbb{Q})$ s'identifiquen amb les matrius

$$\ell = fh \in (F')^\times \times_{F^\times} \mathbf{H}^\times \subseteq (\mathbf{H}')^\times$$

tals que $f\overline{f}\nu(h) =: \mu$ és un nombre racional. Quan això sigui així, tindrem que $\psi(\ell v, \ell w) = \mu\psi(v, w)$.

Siguin $\mathcal{O}_{\mathbf{H}'} \subseteq \mathbf{H}'$ un ordre maximal que contingui $\mathcal{O}_{F'} \times \mathcal{O}(\mathfrak{d}, 1)$, i Γ' un subgrup aritmètic de $\mathcal{O}_{\mathbf{H}'}$, prou gran, que contingui Γ (cf. **[Zh 98]**).

Considerarem el functor $\mathcal{F}_{\Gamma'}$ que associa a un F'–esquema S el conjunt $\mathcal{F}_{\Gamma'}(S)$ format per les classes d'isomorfia d'objectes $A = [A, \rho, \overline{\theta}, \overline{\phi}]$ que satisfan les condicions següents:

- A és S–esquema abelià dotat d'una multiplicació quaterniònica

$$\rho : \mathcal{O}_{\mathbf{H}'} \to \mathrm{End}_S(A).$$

- Per a cada element $\ell \in \mathcal{O}_{\mathbf{H}'}$, se satisfà la igualtat

$$\mathrm{tr}(\rho(\ell) : \mathrm{Lie}(A)) = \mathrm{tr}(\ell : \mathbb{C} \otimes V/F^0(V_{\mathbb{C}})),$$

on el subespai $F^0(V_{\mathbb{C}})$ és relatiu a una estructura de Hodge que prové del morfisme de grups algèbrics $h' : \mathbf{S} \to \mathbf{G}'_{\mathbb{R}}$, deduït de h.

- $\overline{\theta}$ és la classe d'un divisor de A que defineix una polarització

$$\theta : A \to A^{\vee},$$

la involució de Rosati de la qual aplica $\rho(\ell)$ en $\rho(\ell^*)$.

- $\overline{\phi}$ és una Γ'-classe d'isomorfismes ϕ, simplèctics respecte de $\widehat{\psi}$ i $\mathcal{O}_{\mathbf{H}'}$-lineals,

$$\phi : \widehat{\mathbb{Z}} \otimes V \to T(A) := \prod T_\ell(A),$$

on $T_\ell(A)$ denota el mòdul de Tate ℓ-àdic dotat de l'aparellament de Weil.

El teorema següent resumeix resultats obtinguts a **[Sh 67]**, **[Ca 86]** i **[Ka-Ma 85]**.

2.1. Teorema.

i) Sempre que Γ' sigui prou petit, existeix un model canònic $X(\Gamma')$ definit sobre el cos F' que representa grollerament el functor $\mathcal{F}_{\Gamma'}$.

ii) Siguin p un primer tal que $\left(\frac{D}{p}\right) = 1$, $\mathfrak{p}|p$ un primer de $\mathcal{O}_F$, $\mathfrak{p}'|\mathfrak{p}$ un primer de $\mathcal{O}_{F'}$. Existeix un functor $\mathcal{F}_{\Gamma',\mathfrak{p}'}$ definit sobre els $\mathcal{O}_{F'_{\mathfrak{p}'}}$-esquemes $\mathcal{S}_{\mathfrak{p}'}$ que estén naturalment la restricció del functor $\mathcal{F}_{\Gamma'}$ als $F_{\mathfrak{p}'}$-esquemes.

iii) Existeix un model local enter $\mathcal{X}_{\mathfrak{p}'}(\Gamma')$, sobre $\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}'}$, que representa el functor $\mathcal{F}_{\Gamma',\mathfrak{p}'}$. Si Γ' és prou petit respecte de $\mathfrak{p}'$, l'esquema $\mathcal{X}_{\mathfrak{p}'}(\Gamma')$, de dimensió 2, és regular sobre $\operatorname{Spec}\mathcal{O}_{\mathfrak{p}'}$.

iv) Si $\left(\frac{D}{p}\right) = 1$ en un conjunt de primers p prou ampli, la corba de Shimura $X(\Gamma(\mathfrak{d},\mathfrak{n}))$ posseeix un model enter global, $\mathcal{X}(\Gamma)$, que és regular sobre $\operatorname{Spec}\mathcal{O}_F$, *sempre que Γ sigui suficientment petit.*

Siguin K/F una extensió quadràtica totalment imaginària i

$$\varepsilon = \otimes_{\mathfrak{p}} \varepsilon_{\mathfrak{p}} : F^\times \backslash \mathbb{A}_F^\times \to \{\pm 1\}$$

el caràcter, sobre les classes d'ideles de F, que la defineix. Suposarem que se satisfan les hipòtesis següents:

1. L'extensió K/F és ramificada.
2. L'extensió K/F és no ramificada en tots els primers $\mathfrak{p}$ de F de característica residual igual a 2.
3. L'extensió K/F és no ramificada en els primers que divideixen $\mathfrak{d}\mathfrak{n}$.
4. $\varepsilon(\mathfrak{d}\mathfrak{n}) = (-1)^{d-1}$, on $d = [F : \mathbb{Q}]$.
5. Per a tot ideal primer $\mathfrak{p}|\mathfrak{d}\mathfrak{n}$ de F, l'àlgebra de quaternions $\mathbf{H}$ ramifica en $\mathfrak{p}$ si, i només si, $\varepsilon(\mathfrak{p}) = -1$.
6. El grau $d = [F : \mathbb{Q}]$ és senar, o bé $v_{\mathfrak{p}}(\mathfrak{d}\mathfrak{n})$ és senar en algun ideal primer $\mathfrak{p}$ de $\mathcal{O}_F$.
7. Existeix una immersió de F-àlgebres $\lambda : K \hookrightarrow \mathbf{H}$ tal que

$$\lambda(\mathcal{O}_K) \subseteq \mathcal{O}(\mathfrak{d}, \mathfrak{n}),$$

on $\mathcal{O}_K$ és l'anell d'enters de K.

Sigui $\mathcal{N}_K$ l'ideal de $\mathcal{O}_K$ definit per la igualtat

$$\mathcal{O}(\mathfrak{d}, \mathfrak{n}) = \lambda(\mathcal{O}_K) + \mathcal{N}_K \mathcal{O}_{\mathbf{H}}.$$

Sigui $\mathcal{N}$ un ideal de $\mathcal{O}_F$ tal que $\mathcal{N}_K = \prod_{\mathfrak{p}|\mathcal{N}} \mathfrak{p}_K^{v_{\mathfrak{p}}(\mathcal{N})}$, on $\mathfrak{p}_K|\mathfrak{p}$. Sigui $K' = F'K$, i denotem per $\mathcal{N}_{F'}$, respectivament $\mathcal{N}_{K'}$, un aixecament de $\mathcal{N}$, respectivament $\mathcal{N}_K$, a un ideal de $\mathcal{O}_{F'}$, respectivament $\mathcal{O}_{K'}$.

El lema següent precisa la interpretació modular dels punts de les corbes de Shimura, quan se'n considera el model definit sobre el cos F'.

2.2. Lema. *El functor $\mathcal{F}_{\Gamma'}$ és equivalent al functor $\mathcal{F}$ que a cada F'–esquema S li fa correspondre un parell d'objectes $[A, C]$, on A és un esquema abelià sobre S dotat d'una multiplicació per $\mathcal{O}_{\mathbf{H}'}$ (que satisfà totes les propietats esmentades més amunt) i C és un $\mathcal{O}_{K'}$-submòdul de $A[\mathcal{N}_{K'}]$ generat per una base de Drinfeld d'ordre $\mathcal{N}_{F'}$. És a dir,*

$$C = A[\mathcal{N}_{F'}] = \sum_{a \in \mathcal{O}_{\mathbf{H}}/\mathcal{N}} [a\,x].$$

Posarem

$$\mathrm{End}_{\mathcal{O}_{\mathbf{H}'}}([A, C]) := \{\varphi \in \mathrm{End}_{\mathcal{O}_{\mathbf{H}'}}(A) : \varphi(C) \subseteq C\}.$$

2.3. Definició. Siguin $x \in X(\Gamma)(\overline{F}) = X(\Gamma)(\overline{F'})$ i $[A, C]$ un objecte representat per x. Direm que x és un punt de multiplicació complexa per K, en el sentit de Zhang **[Zh 98]**, si, i només si,

$$\mathbb{Q} \otimes \mathrm{End}_{\mathcal{O}_{\mathrm{H}'}}(A) \simeq K'.$$

En aquest cas, existeix un F'-isomorfisme, únic, $\mu : K' \to \mathbb{Q} \otimes \mathrm{End}_{\mathcal{O}_{\mathrm{H}'}}(A)$, tal que $\mathrm{tr}(\mu(a) : \mathrm{Lie}(A)) = 2(a - \overline{a} + \mathrm{tr}_{K/\mathbb{Q}}(a))$, per a tot $a \in K'$. Posarem

$$\mathrm{End}(x) := \{a \in K : \mu(a) \in \mathrm{End}_{\mathcal{O}_{\mathrm{H}'}}([A, C])\}.$$

És clar que $\mathrm{End}(x)$ és un ordre del cos K. L'ideal $\mathfrak{c}$ de $\mathcal{O}_F$ definit per la igualtat

$$\mathrm{End}(x) = \mathcal{O}_{K,\mathfrak{c}} := \mathcal{O}_F + \mathfrak{c}\mathcal{O}_K$$

s'anomena el conductor de x.

2.4. Proposició.

i) En el model canònic de $X(\Gamma)$ sobre F, els punts de multiplicació complexa per K de conductor $\mathfrak{c}$ tenen les seves coordenades en el cos de classes $H_{\mathfrak{c}}$ de K.

ii) Sigui $X_{\mathfrak{c}}$ el subesquema de $X(\Gamma)$ associat als punts de multiplicació complexa per K de conductor $\mathfrak{c}$ (orientats positivament). L'esquema $X_{\mathfrak{c}}$ és definit sobre K i existeix una bijecció

$$X_{\mathfrak{c}}(\mathbb{C}) = X_{\mathfrak{c}}(H_{\mathfrak{c}}) \longleftrightarrow K^{\times} \backslash \widehat{K}^{\times} / \widehat{\mathcal{O}}^{\times}_{K,\mathfrak{c}}.$$

2.5. Definició. Anomenarem punts de Heegner de $X(\Gamma)$, en el sentit de Zhang **[Zh 98]**, els punts de multiplicació complexa per K de conductor $\mathfrak{c} = 1$.

§3. Formes modulars de Hilbert

Aquesta és una secció de contingut analític. Siguin k un enter positiu, $\mathfrak{n} \subseteq \mathcal{O}_F$ un ideal, i $\psi = \otimes \psi_v : F^{\times} \backslash \mathbb{A}_F^{\times} \to \mathbb{C}^{\times}$ un caràcter finit. Suposem

que el conductor de ψ divideix $\mathfrak{n}$ i que $\psi_\tau(-1) = (-1)^{k-1}$, per a tota plaça arquimediana τ del cos F. Considerem el grup de congruència

$$\Gamma_0(\mathfrak{n}) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{GL}(2, \widehat{\mathcal{O}}_F) : c \equiv 0 \pmod{\widehat{\mathfrak{n}}} \right\}.$$

Sigui $\Gamma_\infty \subseteq \prod_{1 \le i \le d} \mathbf{GL}(2, F_{\tau_i})$ el subgrup compacte format per les matrius de la forma

$$r(\theta) = (r(\theta_{\tau_i})) \in \mathbf{GL}(2, \mathbb{R} \otimes_{\mathbb{Q}} F),$$

on, per a $\theta = (\theta_i) \in \mathbb{R}^d$, és

$$r(\theta_i) = \begin{bmatrix} \cos 2\pi\theta_i & \sin 2\pi\theta_i \\ -\sin 2\pi\theta_i & \cos 2\pi\theta_i \end{bmatrix};$$

és a dir,

$$\Gamma_\infty = \prod_{1 \le i \le d} \mathbf{SO}(2, F_{\tau_i}), \quad F_{\tau_i} \simeq \mathbb{R}, \text{ per a tot } i.$$

Denotem per $\mathbf{Z}$ el centre de $\mathbf{GL}(2, -)$, com a grup algèbric. La fórmula

$$\psi\left(\begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} r(\theta) \right) = \psi(z) \cdot \prod_{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}) > 0} \psi_{\mathfrak{p}}(a_{\mathfrak{p}}) \cdot \prod_i e^{2\pi i k \theta_i}$$

permet estendre ψ a un caràcter de $\mathbf{Z}(\mathbb{A}_F)\Gamma_0(\mathfrak{n})\Gamma_\infty$.

3.1. Definició. Una forma modular sobre $F \otimes \mathbf{GL}(2, -)$ de tipus $(\mathfrak{n}, k, \psi)$ és una funció

$$\varphi : \mathbf{GL}(2, \mathbb{A}_F) \to \mathbb{C}$$

que satisfà les condicions següents:

i) $\varphi(\gamma g) = \varphi(g)$, per a tot $\gamma \in \mathbf{GL}(2, F)$.

ii) $\varphi(gk) = \varphi(g)\psi(k)$, per a tot $k \in \mathbf{Z}(\mathbb{A}_F)\Gamma_0(\mathfrak{n})\Gamma_\infty$.

iii) Per a cada plaça arquimediana τ_i és

$$\Delta_i \varphi = \frac{k}{2}\left(1 - \frac{k}{2}\right)\varphi,$$

on Δ_i denota l'operador de Laplace-Beltrami de $\mathbf{GL}(2, F_{\tau_i})$.

iv) La funció φ creix lentament.

Si, a més, satisfà la condició

v)
$$\int_{F\backslash\mathbb{A}_F} \varphi\left(\begin{bmatrix}1 & x\\ 0 & 1\end{bmatrix} g\right) dx = 0\,, \qquad \text{q.p.t. } g \in \mathbf{GL}(2,F),$$

la forma modular φ s'anomena cuspidal.

Denotarem per $\mathcal{A}(\mathfrak{n},k,\psi)$ el $\mathbb{C}$-espai vectorial de les formes modulars de tipus $(\mathfrak{n},k,\psi)$, i per $S(\mathfrak{n},k) = \oplus S(\mathfrak{n},k,\psi)$ el $\mathbb{C}$-espai vectorial de les formes cuspidals. Denotarem per $\psi = 1$ el caràcter trivial.

3.2. Lema. *Sigui $e : F\backslash\mathbb{A}_F \to \mathbb{C}$ el caràcter additiu definit per*

$$e(x) = \exp[2\pi i(\operatorname{tr} x_\infty - \operatorname{tr} x_f)].$$

Tot caràcter additiu complex de $F\backslash\mathbb{A}_F$ és de la forma $x \mapsto e(\xi x)$, per a un cert $\xi \in F$.

Recordem que tenim fixada una immersió $\tau_1 : F \hookrightarrow \mathbb{R}$.

3.3. Proposició. *Donada una forma modular φ sobre $F \otimes \mathbf{GL}(2,-)$, existeix una funció, que denotem per a, definida en el conjunt dels ideals de $\mathcal{O}_F$, tal que*

$$\varphi\left(\begin{bmatrix}y & x\\ 0 & 1\end{bmatrix}\right) = \psi(y)|y|^{k/2} \sum_{\xi \geq 0} a(\xi y_f\, \mathfrak{E}) e(\xi x + \xi y_\infty i),$$

on $y \in \mathbb{A}_F^\times$ és tal que $y_\infty > 0$, $x \in \mathbb{A}_F$, i $\mathfrak{E}$ és l'invers de l'ideal diferent de F:

$$\mathfrak{E}^{-1} = \{x \in F : \operatorname{tr}(x\mathcal{O}_F) \subset \mathbb{Z}\}.$$

3.4. Definició. Suposem que φ és una forma modular cuspidal de caràcter trivial. Atès que tot element del quocient

$$\mathbf{GL}(2,F)\backslash\mathbf{GL}(2,\mathbb{A}_F)/\mathbf{Z}(\mathbb{A}_F)\Gamma_0(\mathfrak{n})\Gamma_\infty$$

admet un representant de la forma $\begin{bmatrix}y & x\\ 0 & 1\end{bmatrix}$, on $y \in \mathbb{A}_F^\times$, $y_\infty > 0$, $x \in \mathbb{A}_F$, la funció a de la proposició anterior determina φ unívocament. Donat un ideal $\mathfrak{m}$ de $\mathcal{O}_F$, direm que $a(\mathfrak{m}) = a(\varphi,\mathfrak{m})$ és el coeficient $\mathfrak{m}$-èsim de φ. Escriurem

$$f = \sum_{\mathfrak{m}} a(\mathfrak{m}) q^{\mathfrak{m}}.$$

3.5. Definició. Sigui $\mathfrak{m} \subseteq \mathcal{O}_F$ un ideal no nul. Considerem el subconjunt de $\mathbf{GL}(2, \widehat{F})$:

$$H(\mathfrak{m}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{M}(2, \widehat{\mathcal{O}}_F) : (d, \mathfrak{n}) = 1,\, c \in \widehat{\mathfrak{n}},\, (ad - bc)\,\widehat{\mathcal{O}}_F = \widehat{\mathfrak{m}} \right\}.$$

En l'espai vectorial complex $S(\mathfrak{n}, k, 1)$ de les formes modulars cuspidals respecte de $\Gamma_0(\mathfrak{n})$, de pes k i caràcter trivial, es defineix l'operador de Hecke $T(\mathfrak{m})$ per la fórmula

$$(T(\mathfrak{m})\varphi)(g) = N(\mathfrak{m})^{k/2-1} \int_{\mathbf{H}(\mathfrak{m})} \varphi(gh) dh\,,$$

on dh és una mesura de Haar del grup localment compacte $\mathbf{GL}(2, \widehat{F})$, normalitzada de manera que el volum de $\Gamma_0(\mathfrak{n})$ sigui igual a 1. Denotem per $\mathbb{T}(\mathfrak{n}, k, 1) \subseteq \mathrm{End}_{\mathbb{C}}(S(\mathfrak{n}, k, 1))$ la subàlgebra generada pels operadors de Hecke $T(\mathfrak{m})$ tals que l'ideal $\mathfrak{m}$ sigui sense factors en comú amb $\mathfrak{n}$. Els coeficients de Fourier de $T(\mathfrak{m})\varphi$ són donats per la fórmula

$$a\,(T(\mathfrak{m})\varphi, \mathfrak{l}) = \sum_{\mathfrak{a} \mid \mathfrak{m}, \mathfrak{l}} N(\mathfrak{a})^{k-1} a(\varphi, \mathfrak{m}\mathfrak{l}/\mathfrak{a}^2)\,.$$

El teorema següent fa palès que en el context de les formes modulars de Hilbert és vàlida la teoria d'Atkin-Lehner.

3.6. Teorema. *Siguin φ_i, $i = 1, 2$, dues formes noves de pes k, de nivells $\mathfrak{n}_1, \mathfrak{n}_2$, respectivament, i de caràcter trivial. Si $a(\varphi_1, \mathfrak{p}) = a(\varphi_2, \mathfrak{p})$ per a quasi tots els ideals primers $\mathfrak{p}$ de $\mathcal{O}_F$, aleshores $\mathfrak{n}_1 = \mathfrak{n}_2$, i $\varphi_1 = \varphi_2$.*

3.7. Corol·lari.

i) L'àlgebra $\mathbb{T}(\mathfrak{n}, k, 1)$ opera fidelment a l'espai

$$S(\mathfrak{n}, k, 1) = \oplus_{\mathfrak{n}' \mid \mathfrak{n}} S^{nou}(\mathfrak{n}', k, 1).$$

ii) Existeix una forma bilineal no degenerada $\mathbb{T}(\mathfrak{n}, k, 1) \otimes_{\mathbb{C}} S(\mathfrak{n}, k, 1) \longrightarrow \mathbb{C}$ tal que

$$(T(\mathfrak{m}), \varphi) = a(\varphi, \mathfrak{m}),$$

per a tot ideal $\mathfrak{m}$ sense factors en comú amb $\mathfrak{n}$.

iii) Per a tota aplicació lineal $\alpha : \mathbb{T}(\mathfrak{n}, k, 1) \to \mathbb{C}$, *existeix una única forma cuspidal* $\varphi \in S(\mathfrak{n}, k, 1)$ *tal que*

$$\alpha(T(\mathfrak{m})) = a(\varphi, \mathfrak{m}),$$

per a tot ideal $\mathfrak{m}$ *sense factors en comú amb* $\mathfrak{n}$.

§4. Varietats abelianes associades a formes modulars de Hilbert

Retornem a la corba de Shimura $X(\Gamma(\mathfrak{d}, \mathfrak{n}))$. Sigui ara $\mathfrak{m} \subseteq \mathcal{O}_F$ un ideal sense factors en comú amb $\mathfrak{d}\mathfrak{n}$. A l'espai vectorial complex de les formes diferencials holomorfes $\Gamma(X(\Gamma)(\mathbb{C}), \Omega^1)$ hi actuen els operadors de Hecke

$$T(\mathfrak{m})\omega := \sum_{\gamma} \gamma^* \omega,$$

on el sumatori s'estén a totes les classes $\gamma \in \widehat{\mathcal{O}}(\mathfrak{d}, \mathfrak{n})(\mathfrak{m})/\widehat{\Gamma}$.

El teorema següent posa de manifest un resultat clau. Relaciona certes formes modulars de Hilbert de pes 2 i caràcter trivial amb diferencials holomorfes sobre les corbes de Shimura.

4.1. Teorema. *Sigui* $\varphi \in S(\mathfrak{d}\mathfrak{n}, 2, 1)$ *una forma nova. Aleshores, existeix una forma diferencial holomorfa* $\omega \in \Gamma(X(\Gamma)(\mathbb{C}), \Omega^1)$, *única llevat de productes per escalars i vector propi dels operadors de Hecke, tal que* φ *i* ω *comparteixen els mateixos valors propis sota l'acció dels respectius operadors de Hecke* $T(\mathfrak{m})$, *per a* $\mathfrak{m}$ *i* $\mathfrak{d}\mathfrak{n}$ *ideals de* $\mathcal{O}_F$ *sense factors en comú.*

Demostració. El punt més delicat de la demostració prové de la teoria de les formes noves sobre $X(\Gamma)$. La demostració donada a **[Zh 98]** utilitza fets específics de la teoria de Jacquet-Langlands (cf. **[Ba-Tr 97]**), i un teorema de Waldspurger **[Wa 91]**. Zhang agraeix en aquest punt l'ajut de Jacquet. □

Sigui $\mathcal{X}(\Gamma)$ el model regular de la corba de Shimura que hem considerat a § 2. L'operador de Hecke $T(\mathfrak{m})$ proporciona una correspondència

sobre $\mathcal{X}(\Gamma)$; per tant, té sentit considerar-ne la reducció en les places de $\mathcal{O}_F$. El teorema següent ens diu que en les corbes de Shimura són vàlides les congruències d'Eichler-Shimura.

4.2. Teorema. ([**Sh 67**]) *Sigui $\mathfrak{p} \nmid \mathfrak{d}\mathfrak{n}$ un ideal primer de $\mathcal{O}_F$. Siguin $\mathrm{Frob}_\mathfrak{p}$ la correspondència de Frobenius de la fibra especial $\mathcal{X}(\Gamma)_\mathfrak{p}$ i $\mathrm{Frob}_\mathfrak{p}^*$ la seva dual. Aleshores,*

$$T(\mathfrak{p})_{/\mathfrak{p}} = \mathrm{Frob}_\mathfrak{p} + \mathrm{Frob}_\mathfrak{p}^*,$$

on $T(\mathfrak{p})_{/\mathfrak{p}}$ denota la reducció mod $\mathfrak{p}$ *de $T(\mathfrak{p})$.*

A partir dels dos teoremes anteriors es demostra el teorema que segueix:

4.3. Teorema. *Sigui $f = \sum a(\mathfrak{m})q^\mathfrak{m}$ una forma modular de Hilbert respecte del grup $\Gamma_0(\mathfrak{d}\mathfrak{n})$. Suposem que f és de pes 2, de caràcter trivial, i nova. Sigui $\mathcal{O}_f$ la $\mathbb{Z}$-àlgebra, de rang finit, generada pels coeficients $a(\mathfrak{m})$ de f quan els ideals $\mathfrak{m}$ i $\mathfrak{d}\mathfrak{n}$ no tenen factors en comú. Aleshores,*

i) Existeix una varietat abeliana A_f definida sobre el cos F, de dimensió $[\mathcal{O}_f : \mathbb{Z}]$, tal que

$$L(A_f, s) \sim \prod_{\sigma : \mathcal{O}_f \hookrightarrow \mathbb{C}} L(f^\sigma, s).$$

Aquí, el signe $\sim$ indica que la igualtat entre les dues funcions L és llevat de factors d'Euler sobre els divisors primers de $\mathfrak{d}\mathfrak{n}$.

ii) La varietat abeliana A_f s'obté com a quocient de la varietat jacobiana $J(X(\Gamma))$ d'una corba de Shimura $X(\Gamma)$ associada a un grup d'unitats $\Gamma = \mathcal{O}(\mathfrak{d}, \mathfrak{n})^\times$ d'un ordre de nivell $\mathfrak{n}$ contingut en l'àlgebra de quaternions sobre F de discriminant $\mathfrak{d}$. Aquesta àlgebra de quaternions és no ramificada en una plaça arquimediana i ramificada en la resta de places arquimedianes.

Demostració. Sigui $\mathbb{T}$ la $\mathbb{Q}$-subàlgebra de $\mathrm{End}_\mathbb{Q}(J(X(\Gamma)))$ generada pels operadors de Hecke $T(\mathfrak{m})$, per a $\mathfrak{m}$ i $\mathfrak{d}\mathfrak{n}$ sense factors en comú. L'àlgebra $\mathbb{T}$ opera fidelment a $H^1(J(X(\Gamma)), \mathbb{Z})$. Aquesta representació de l'àlgebra de Hecke permet associar a cada $T(\mathfrak{m})$ el seu polinomi característic, que és mònic i de coeficients enters.

Com en el cas modular, la varietat A_f es construeix de manera que el seu espai cotangent en el zero és donat per

$$\mathrm{Lie}(A_f)^\vee = \sum_{\sigma:\mathcal{O}_f\hookrightarrow\mathbb{C}} \mathbb{C} f^\sigma .$$

En tot primer $\mathfrak{p}\nmid\mathfrak{d}\mathfrak{n}$, la varietat A_f és de bona reducció.

La congruència d'Eichler-Shimura proporciona la descripció següent de la funció zeta local de A_f:

$$Z_\mathfrak{p}(t) := \det(1 - t\,\mathrm{Frob}_\mathfrak{p} \mid H^1(A_f, \mathbb{Q}_\ell)) = N_{\mathcal{O}_f/\mathbb{Z}}(1 - a(\mathfrak{p})t + N(\mathfrak{p})t^2).$$

□

§5. Divisors de Heegner-Arakelov

Abans que res, ens cal definir una aplicació d'Abel-Jacobi:

$$\phi : X(\Gamma) \to \mathbb{Q}\otimes J(X(\Gamma)).$$

Per a tal fi, escrivim $X(\Gamma)(\mathbb{C}) = \cup X_i$, on X_i són superfícies de Riemann compactes i connexes. Considerem el divisor de $\mathbb{Q}\otimes\mathrm{Pic}(X_i)$ donat per

$$\xi_i := \left([\Omega^1_{X_i}] + \sum_{p\in X_i} (1 - \frac{1}{u_p})[p] + [\text{puntes}] \right) / \frac{1}{2\pi}\int_{X_i} \frac{dx\,dy}{y^2}.$$

En la fórmula anterior, per a cada punt $p\in X_i$, u_p denota l'ordre de grup d'isotropia sota l'acció de Γ d'una antiimatge de p en $\mathcal{H}$. L'aplicació ϕ considerada per Zhang associa a cada punt $x\in X_i$ la classe del divisor $x - \xi_i$.

5.1. Definició. Recordem que $[K:F]=2$, K és un cos totalment imaginari i disposem d'una immersió $K\hookrightarrow\mathbf{H}$. Sigui H_1 el cos de classes de Hilbert del cos K. Sigui $x\in X(\Gamma)(H_1)$ un punt de Heegner amb multiplicació complexa per K. Considerem la classe del divisor

$$\zeta := \frac{1}{u_x}\sum_{\sigma\in\mathrm{Gal}(H_1/K)} \phi(x^\sigma) \in (\mathbb{Q}\otimes J(X(\Gamma))(K).$$

Per a cada forma nova $f \in S(\mathfrak{d}\mathfrak{n}, 2, 1)$, denotarem per ζ_f la imatge de ζ per la projecció

$$\mathbb{Q} \otimes J(X(\Gamma)) \to \mathbb{Q} \otimes A_f \, .$$

5.2. Lema. *Donat un punt $x \in J(X(\Gamma(\mathfrak{d}, \mathfrak{n})))(\overline{F})$, existeix una única forma $f_x \in \sum_{\mathfrak{d}'\mathfrak{n}'|\mathfrak{d}\mathfrak{n}} S^{\mathrm{nou}}(\mathfrak{d}'\mathfrak{n}', 2, 1)$ tal que el valor $\langle x, T(\mathfrak{m})x\rangle$, que correspon a l'aparellament de Néron-Tate associat a les altures, és el coeficient $\mathfrak{m}$-èsim del desenvolupament de Fourier de f_x a l'infinit, per a tot ideal $\mathfrak{m} \subseteq \mathcal{O}_F$ sense factors en comú amb $\mathfrak{d}\mathfrak{n}$.*

En particular, si $\zeta \in \mathbb{Q} \otimes J(X(\Gamma))(K)$ és un divisor de Heegner, la suma formal

$$\sum_{\mathfrak{m}} \langle \zeta, T(\mathfrak{m})\zeta\rangle q^{\mathfrak{m}}$$

és part del desenvolupament d'una forma modular cuspidal de pes 2, nivell un divisor de $\mathfrak{d}\mathfrak{n}$, i caràcter trivial. Denotarem aquesta forma per $\Psi = \Psi_\zeta$.

Tot seguit ens limitarem a descriure l'estratègia seguida per Zhang en el càlcul de la forma $\Psi_\zeta \in S^{nou}(\mathfrak{d}'\mathfrak{n}', 2, 1)$. Els passos són els següents:

• Cal disposar d'un model $\mathcal{X}(\widetilde{\Gamma})$, regular sobre $\operatorname{Spec} \mathcal{O}_F$, que garanteixi que l'esquema $\mathcal{O}_K \otimes \mathcal{X}(\widetilde{\Gamma})$ és, també, regular. Siguin

$$\pi : K \otimes \mathcal{X}(\widetilde{\Gamma}) \to K \otimes \mathcal{X}(\Gamma)$$

la projecció corresponent i $\widetilde{\zeta}$ la antiimatge de ζ en aquest model. Aleshores,

$$\langle \zeta, T(\mathfrak{m})\zeta\rangle = \langle \widetilde{\zeta}, T(\mathfrak{m})\widetilde{\zeta}\rangle / \deg \pi \, .$$

• Cal reconvertir el valor de l'aparellament de Néron-Tate $\langle \widetilde{\zeta}, T(\mathfrak{m})\widetilde{\zeta}\rangle$ en una intersecció d'Arakelov de divisors aritmètics sobre $\mathcal{O}_K \otimes \mathcal{X}(\widetilde{\Gamma})$. Més concretament

$$\langle \widetilde{\zeta}, T(\mathfrak{m})\widetilde{\zeta}\rangle = -(\widehat{\zeta}, T(\mathfrak{m})\widehat{\zeta}) \, ,$$

on el darrer parèntesi correspon a una intersecció aritmètica, i $\widehat{\zeta}$ denota un divisor aritmètic de $\mathcal{O}_K \otimes \mathcal{X}(\widetilde{\Gamma})$, que té curvatura zero en la superfície de Riemann $X(\widetilde{\Gamma})(\mathbb{C})$, i que té grau zero en cada component irreductible de les fibres especials del model $\mathcal{O}_K \otimes \mathcal{X}(\widetilde{\Gamma})$.

- A fi de calcular $T(\mathfrak{m})\widehat{\zeta}$, cal reescriure, de manera convenient,

$$\widehat{\zeta} = \widehat{\eta} - h\widehat{\xi} + Z$$

i aprendre a calcular l'efecte dels operadors de Hecke en cada sumand. El divisor $\widehat{\eta}$ prové dels punts de Heegner; el divisor $\widehat{\xi}$ prové del divisor canònic; h és un nombre de classes escaient; Z és un divisor vertical que s'ajusta de manera que el divisor $\widehat{\zeta}$ sigui de grau zero en cada fibra especial de $\mathcal{O}_K \otimes \mathcal{X}(\widetilde{\Gamma})$.

Començarem per explicar com s'obté el divisor $\widehat{\eta}$. Donat un ideal $\mathfrak{c} \in \mathcal{O}_F$, sigui

$$\eta_{\mathfrak{c}} := \frac{1}{u_{\mathfrak{c}}} \sum_x x,$$

on $u_{\mathfrak{c}}$ denota el nombre d'elements de $\mathcal{O}_{\mathfrak{c}}^{\times}/\mathcal{O}_F^{\times}$ i el sumatori s'estén a tots els punts de multiplicació complexa per K de conductor $\mathfrak{c}$ (convenientment orientats). Siguin $\eta = \eta_1$ i $\widetilde{\eta}$ la seva antiimatge a $K \otimes X(\widetilde{\Gamma})$. Denotem per $\overline{\eta}$ la clausura de Zariski de $\widetilde{\eta}$ a $\mathcal{O}_K \otimes \mathcal{X}(\widetilde{\Gamma})$. Per a cada plaça arquimediana τ de F, considerem la superfície de Riemann compacta $X_\tau(\Gamma)(\mathbb{C})$. Sigui $d\mu$ la forma de volum sobre $X_K(\widetilde{\Gamma})(\mathbb{C})$ tal que cadascun dels seus components irreductibles $\widetilde{X}_i$ té volum 1 i tal que la seva antiimatge a $\mathcal{H}$ és proporcional a la mètrica $dxdy/y^2$. A $X_\tau(\Gamma)(\mathbb{C})$, considerem la funció de Green g definida per:

$$\frac{\partial\overline{\partial}}{\pi i} g = \delta_\eta - \deg(\widetilde{\eta}|_{\widetilde{X}_i}) d\mu.$$

Aleshores, $\widehat{\eta} := (\overline{\eta}, g)$.

Sigui ξ la classe en $\mathbb{Q} \otimes \mathrm{Pic}(X(\Gamma))$ que en cada component geomètricament connex hi té el component ξ_i. Sigui $\widetilde{\xi}$ la antiimatge de ξ a $X_K(\widetilde{\Gamma})$. Aleshores, $\widetilde{\xi}$ és la classe del fibrat $\Omega^1_{X(\widetilde{\Gamma})}(\text{puntes})$. Escollim F' com abans. Sigui $\mathcal{X}'(\widetilde{\Gamma})$ un model enter de la corba de Shimura sobre $\mathcal{O}_{F'}$. Canviant, si cal, el subgrup $\widetilde{\Gamma}$ per un altre de més petit, es pot suposar que sobre $\mathcal{X}'(\widetilde{\Gamma})$ hi és definida una varietat abeliana universal $\mathcal{A}$. Considerem el fibrat de línia $\omega = \det(\mathrm{Lie}\,\mathcal{A})^\vee$. La teoria de Kodaira-Spencer permet afirmar que el fibrat $[\omega]/\deg\omega$ coincideix amb el fibrat canònic, $\widetilde{\xi}'$, definit, com abans, sobre la fibra genèrica. Donat un punt $x \in X_\tau(\Gamma)(\mathbb{C})$ que representi una varietat abeliana A, i donada una secció $\alpha \in \omega = \Gamma(A, \Omega_A^{4g})$, es té que

$$\|\alpha\|^2 = (-i)^{g^2} \int_A \alpha \wedge \overline{\alpha}.$$

Es defineix $\widehat{\xi} := (\omega, \|\cdot\|)/\deg\omega$. Aleshores, $\widehat{\eta} - h\widehat{\xi}$ és de curvatura zero.

Un cop metritzats els divisors de Heegner, es pot procedir al càlcul de la forma $\Psi = \Psi_\zeta$. El càlcul dels coeficients de Ψ és la part més difícil de tot el treball; ocupa unes 30 pàgines de l'article de Zhang [**98**].

Ens limitarem a descriure les funcions que intervenen en el càlcul de les interseccions arquimedianes $\langle \zeta, T(\mathfrak{m})\zeta\rangle_\tau$. Sigui $\widetilde{X}_i = \cup_j \widetilde{X}_{i,j}$ la part de $X(\widetilde{\Gamma})$ que es projecta en X_i. Donat un nombre complex $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$, considerem la funció de Legendre

$$Q_{s-1}(u) = \int_0^\infty (u + \sqrt{u^2-1}\cosh t)^s\, dt.$$

Sigui

$$G_s(z,w) = -Q_{s-1}\left(1 + \frac{|z-w|^2}{2\,\mathrm{Im}\, z\,\mathrm{Im}\, w}\right).$$

Aleshores, la funció definida en $\widetilde{X}_{i,j} \times \widetilde{X}_{i,j}\backslash\text{diagonal}$

$$g_{s,i}(z,w) = \sum_\gamma G_s(z, \gamma\omega)$$

és convergent i té un pol simple a $s = 1$ de residu $1/\chi_{i,j}$, on $\chi_{i,j}$ denota la característica d'Euler-Poincaré del component connex $\widetilde{X}_{i,j}$. El càlcul de $\langle \zeta, T(\mathfrak{m})\zeta\rangle_\tau$ utilitza, en cada component $\widetilde{X}_{i,j}$, la funció

$$g_{i,j}(z,w) := \lim_{s\to 1}\left(g_{s,i}(z,w) - \frac{1}{s(s-1)\chi_{i,j}}\right).$$

En les fibres no arquimedianes, el càlcul de $\langle \zeta, T(\mathfrak{m})\zeta\rangle_v$ es basa en la teoria de Honda-Tate.

§6. L-sèries

Els resultats d'aquesta secció són tots de natura analítica. Siguin, com abans, K/F una extensió quadràtica totalment imaginària, ε el caràcter que la defineix, i $\mathfrak{f}$ el conductor de K/F. Sigui $f \in S(\mathfrak{n}, 2, 1)$ una forma nova. Per canvi de base, es defineix la funció $L_K(f,s)$ per la fórmula:

$$L_K(f,s) = L(f,s)L_\varepsilon(f,s).$$

Per a tot ideal $\mathfrak{n} \subseteq \mathcal{O}_F$, sigui $\psi(\mathfrak{n}) := [\Gamma_0(1) : \Gamma_0(\mathfrak{n})]$. Considerem, com d'habitud,

$$\Lambda_K(f,s) := \left[\frac{\Gamma(s)}{(2\pi)^s}\right]^{2d} N(\mathfrak{f}_\mathfrak{n}\mathfrak{E}^2) L_K(f,s).$$

El teorema següent conté el resultat més important.

6.1. Teorema. ([**Zh 98**]) *Suposem que $\varepsilon(\mathfrak{n}) = (-1)^{d-1}$ i sigui $f \in S(\mathfrak{n},2,1)$ una forma nova.*

i) La funció Λ_K admet una prolongació analítica a tot el pla complex i satisfà l'equació funcional

$$\Lambda_K(f,s) = \varepsilon(\mathfrak{n})(-1)^d \Lambda_K(f,2-s).$$

ii) El valor de la seva derivada en el punt $s=1$ és donat per

$$L'_K(f,1) = \frac{(8\pi^2)^d}{d_F d_K^{1/2}}\, \psi(\mathfrak{n})\, (f,\Phi),$$

on $\Phi \in S(\mathfrak{n},2,1)$, $(-,-)$ denota el producte escalar de Petersson, i d_F, d_K denoten el discriminant de F, K, respectivament.

Demostració. Per donar una idea sobre la demostració del teorema, caldrà que parlem una mica de sèries d'Eisenstein i del mètode de Rankin-Selberg.

Començarem per observar que tota adele $g \in \mathbf{GL}(2,\mathbb{A}_F)$ descompon en la forma

$$g = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} k r(\theta), \quad k \in \Gamma_0(1), \quad r(\theta) \in \Gamma_\infty.$$

Per a cada divisor $\mathfrak{n}'|\mathfrak{n}$, considerem

$$H_s^{\mathfrak{n}'} := \begin{cases} |ad^{-1}|^{s+1/2} \varepsilon(a)\varepsilon(k) e(\theta), & k \in \Gamma_0(\mathfrak{f}_{\mathfrak{n}'}), \\ 0, & \text{altrament.} \end{cases}$$

A partir de l'expressió anterior, formem la sèrie:

$$E_s^{\mathfrak{n}'}(g) := L(2s+1,\varepsilon) \sum_{\gamma \in \mathbf{B}(F)\backslash \mathbf{GL}(2,F)} H_s^{\mathfrak{n}'}(\gamma g), \qquad \mathrm{Re}(s) \geq 1,$$

on $\mathbf{B}$ denota el subgrup de Borel. La sèrie anterior és absolutament convergent per a $\mathrm{Re}(s) > 1$; defineix una sèrie d'Eisenstein no holomorfa de nivell $\mathfrak{fn}'$, pes 1, i caràcter ε. La sèrie

$$\theta := \frac{\sqrt{N(\mathfrak{f}\mathfrak{E})}}{(2\pi)^d} E_0(g), \qquad \mathrm{Re}(z) > -1,$$

és holomorfa. Si escrivim $\theta = \sum \sigma(\mathfrak{m}) q^{\mathfrak{m}}$, els coeficients de Fourier són donats per

$$\sigma(\mathfrak{m}) = \begin{cases} L(1,\varepsilon), & \text{si } \mathfrak{m} = 0, \\ \dfrac{(2\pi)^d}{\sqrt{N(\mathfrak{f}\mathfrak{E})}} R(\mathfrak{m}), & \text{si } \mathfrak{m} \neq 0, \end{cases}$$

on $R(\mathfrak{m})$ denota el nombre d'ideals de $\mathcal{O}_K$ de norma $\mathfrak{m}$.

Càlculs semblants a d'altres realitzats per Rankin-Selberg i Gross-Zagier proporcionen la fórmula

$$L_K(f, 1+s) = \left[\frac{(4\pi)^{s+1}}{\Gamma(s+1)}\right]^g \frac{\psi(\mathfrak{f}\mathfrak{n})}{N(\mathfrak{E})^{s+3/2}} (f, \theta E_s^{\mathfrak{n}}).$$

A partir de la fórmula anterior, i si treballem una mica més, podrem obtenir una fórmula per a $L_K'(f,1)$. Considerem

$$E_{s,\mathfrak{n}} := N(\mathfrak{n})^{1/2+s} \sum_{\mathfrak{a}|\mathfrak{n}} \frac{\varepsilon(\mathfrak{a})}{N(\mathfrak{a})^{1+2s}} E_s^{\mathfrak{n}/\mathfrak{a}},$$

i les funcions

$$\Phi_s^{\mathfrak{n}'}(g) := (E_0 E_{s,\mathfrak{n}})(g\gamma_{\mathfrak{n}'}), \quad \mathfrak{n}'|\mathfrak{f},$$

on $\gamma_{\mathfrak{n}'} = (1, \ldots, \begin{pmatrix} 0 & -1 \\ \pi_v & 0 \end{pmatrix}, \ldots, 1) \in \mathbf{GL}(2, \mathbb{A}_F)$ té components no trivials exactament a les places que divideixen $\mathfrak{n}'$. En prendre en consideració les sèries

$$\Phi_s(g) := \frac{1}{2^{\#\{v|\mathfrak{f}\}}} \sum_{\gamma \in \Gamma_0(\mathfrak{n})/\Gamma_0(\mathfrak{n}\mathfrak{f})} \sum_{\mathfrak{n}'|\mathfrak{f}} N(\mathfrak{n}')^s \Phi_s^{\mathfrak{n}'},$$

$$\widetilde{\Phi} := \frac{N(\mathfrak{f}\mathfrak{E})}{(2\pi)^{2d}} \frac{1}{\sqrt{N(\mathfrak{n})}} \frac{\partial}{\partial s}_{|s=0} \Phi_s,$$

s'obté la fórmula

$$L_K'(f,1) = \frac{(8\pi^2)^d \psi(\mathfrak{n})}{N(\mathfrak{E}^2) N(\mathfrak{f})^{1/2}} (f, \widetilde{\Phi}).$$

La forma $\widetilde{\Phi}$ no és una forma modular de Hilbert holomorfa. Per projecció holomorfa en resulta una forma cuspidal holomorfa $\Phi \in S(\mathfrak{n}, 2, 1)$. Atès que la diferència $\widetilde{\Phi} - \Phi$ s'expressa com a suma de sèries d'Eisenstein i altres funcions ortogonals a f, es té que

$$(f, \widetilde{\Phi}) = (f, \Phi),$$

amb la qual cosa conclou la demostració del teorema. □

§7. El teorema de Zhang

Recordem que $\mathfrak{n}, \mathfrak{d}$ són ideals de $\mathcal{O}_F$, i que $f \in S^{nou}(\mathfrak{dn}, 2, 1)$ és una forma nova tal que la varietat A_f és de dimensió g. La varietat A_f és quocient de $J(X(\Gamma(\mathfrak{d}, \mathfrak{n})))$. Recordem, també, que la forma $\Psi \sim \sum \langle \zeta, T(\mathfrak{m})\zeta \rangle q^{\mathfrak{m}}$ és la forma cuspidal de Hilbert definida a partir d'interseccions d'Arakelov associades al divisor de Heegner ζ, que és un punt de multiplicació complexa per K. La forma Φ és la forma cuspidal de Hilbert obtinguda pel mètode de Rankin-Selberg, i és la que intervé en la fórmula de $L'_K(f, 1)$.

7.1. Teorema. *Per a tota forma nova f respecte de $\Gamma_0(\mathfrak{dn})$, de pes 2, i caràcter trivial, se satisfà la igualtat*

$$L'_K(f, 1) = \frac{(8\pi^2)^d}{d_F d_K^{1/2}} \psi(\mathfrak{dn})(f, f)\langle \zeta_f, \zeta_f \rangle.$$

Demostració. El càlcul explícit dels coeficients de la forma

$$\Phi = \sum a(\mathfrak{m}) q^{\mathfrak{m}} \in S(\mathfrak{dn}, 2, 1)$$

i posterior comparació amb els coeficients de la forma $\Psi \in S(\mathfrak{dn}, 2, 1)$ proporciona una congruència

$$\Phi \equiv \Psi \pmod{\Sigma},$$

on Σ denota el subespai de formes velles. Per tant,

$$L'_K(f, 1) = \frac{(8\pi^2)^d}{d_F \sqrt{d_K}} \psi(\mathfrak{dn})(f, \Psi).$$

La fórmula de l'enunciat s'obté a partir d'aquesta sense dificultat. □

El resultat principal del treball que comentem és el

7.2. Teorema. ([**Zh 98**]) *Si $L(A_f/F,s)$ no s'anul·la en $s=1$, o bé té en aquest punt un zero d'ordre g, aleshores:*

i) $\operatorname{rg} A_f(F) = \operatorname{ord}_{s=1} L(A_f/F,s)$.

ii) El grup de Tate-Shafarevich de A_f és finit.

Demostració. La demostració del teorema quan la funció $L(A_f/F,s)$ no s'anul·la en $s=1$ és similar a la del cas el·líptic; n'ometrem el detall. D'altra banda, el mateix argument que l'esgrimit a [**Gr-Za 86**] fa palesa l'equivalència de la condició $\operatorname{ord}_{s=1} L(A_f/F,s) = g$ amb les condicions $\operatorname{ord}_{s=1} L(f^\sigma,s) = 1$, per a tota immersió $\sigma : \mathcal{O}_f \hookrightarrow \mathbb{C}$. Per tant, sota la hipòtesi de zero d'ordre g, i escollint prou bé el cos K, la fórmula del teorema anterior implica que $\langle \zeta_{f^\sigma}, \zeta_{f^\sigma}\rangle \neq 0$, per a tot σ. Més concretament, cal triar el cos K de manera que $\operatorname{ord}_{s=1} L_K(f,s) = 1$ (cf. [**Wa 91**]). Aleshores,

$$\det(\langle \zeta_{f^{\sigma_i}}, \zeta_{f^{\sigma_j}}\rangle) = \prod_i \langle \zeta_{f^{\sigma_i}}, \zeta_{f^{\sigma_i}}\rangle \neq 0.$$

Veiem, doncs, que

$$\operatorname{rg} A_f(F) \geq g = \dim A_f.$$

Per acabar la demostració de i) i provar ii), Zhang suposa el lector familiaritzat amb el mètode emprat per Kolyvagin per provar la finitud del grup de Tate-Shafarevich en altres situacions. Zhang es limita a dir-nos com cal prendre un cert sistema d'Euler-Kolyvagin de punts de multiplicació complexa. Es consideren ideals $\mathfrak{m} \in \mathcal{O}_F$, lliures de quadrats i sense factors en comú amb $\mathfrak{nf}$. Se suposa que cada divisor primer $\mathfrak{l}$ de $\mathfrak{m}$ és inert en K. Sigui $H_\mathfrak{m}$ el cos de classes de K de l'anell de conductor $\mathfrak{m}$. Per a cada $\mathfrak{m}'$ s'escull un punt de multiplicació complexa $x_{\mathfrak{m}'}$ tal que $x_{\mathfrak{m}'}$ s'inclogui en $T(\mathfrak{l})x_\mathfrak{m}$ si $\mathfrak{m}' = \mathfrak{lm}$. Sigui $u_\mathfrak{c}$ el cardinal del grup $\mathcal{O}_\mathfrak{c}^\times/\mathcal{O}_F^\times$. Aleshores, se satisfà la identitat

$$\frac{1}{u_\mathfrak{m}} T(\mathfrak{l}) x_\mathfrak{m} = \frac{1}{u_{\mathfrak{ml}}} \sum_{\sigma \in \operatorname{Gal}(H_{\mathfrak{ml}}/H_\mathfrak{m})} x_{\mathfrak{ml}}^\sigma,$$

amb la qual cosa $(x_\mathfrak{m})$ és un sistema d'Euler-Kolyvagin. □

Bibliografia

[Ba-Tr 97] Bayer, P; Travesa, A. (eds.): *Representacions modulars de* $\mathbf{GL}(2)$, Notes del Seminari de Teoria de Nombres (UB-UAB-UPC), 1997. ISBN: 84-923250-2-X.

[Ca 86] Carayol, H.: Sur la mauvaise réduction des courbes de Shimura, *Comp. Math.* **59** (1986), 151–230.

[De 71] Deligne, P.: Travaux de Shimura, en el llibre *Séminaire Bourbaki, 23 année*, Lecture Notes in Maths., n. 244, Springer, 1971, pp. 123–165.

[Gr-Za 86] Gross, B.; D. Zagier: Heegner points and derivatives of L-series, *Inventiones math.* **84** (1986), 225–320.

[Ja-La 70] Jacquet, H.; Langlands, R. P.: *Automorphic forms on* $\mathbf{GL}_2$, LNM, n. 114, Springer, 1970.

[Ka-Ma 85] Katz, N.; Mazur, B.: *Arithmetic moduli of elliptic curves*, Ann. Math. Studies, 1985.

[Ko 90] Kolyvagin, V. A.: Euler systems, en el llibre *The Grothendieck Festschrift*, Progress in Math., Birkhauser, 1990.

[Ko-Lo 92] Kolyvagin, V. A.; Logachev, D. Yu.: Finiteness of Ш over totally real fields, *Math. USSR Izvestiya* **39** (1992), 829–853.

[Sh 67] Shimura, G.: Construction of class fields and zeta function of algebraic curves, *Ann. Math.* **85** (1967), 58–159.

[Wa 91] Waldspurger, J. L.: Correspondences de Shimura et quaternions, *Forum Math.* **3** (1991), 219–307.

[Zh 98] Zhang, S.: Heights of Heegner points on Shimura curves, prepublicació (1998), 1–82.

Conjectura de Birch i Swinnerton-Dyer p-àdica.

Primera part: Enunciat

Conjectura de Birch i Swinnerton-Dyer:

Sigui $E/\mathbb{Q}$ una corba el·líptica. Aleshores

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = r$$

$$L^{(r)} = |Ш(E/\mathbb{Q})| \cdot \frac{R(E/\mathbb{Q})}{|E(\mathbb{Q})_{\mathrm{tors}}|^2} \cdot (\prod_{\ell} \Omega_\ell) \cdot \Omega_\infty$$

Conjectura de Birch i Swinnerton-Dyer p-àdica:
(Mazur-Tate-Teitelbaum, Inv. Math. 86)

Siguin $E/\mathbb{Q}$ una corba el·líptica modular i p un primer de reducció ordinària. Aleshores

$$\mathrm{ord}_{s=1} L_p(E/\mathbb{Q}, s) = r' := \begin{cases} r+1, & \text{mult. split,} \\ r, & \text{altrament.} \end{cases}$$

$$L_p^{(r')} = |Ш(E/\mathbb{Q})| \cdot \frac{R_p(E/\mathbb{Q})}{|E(\mathbb{Q})_{\mathrm{tors}}|^2} \cdot (\prod_{\ell} m_\ell) \cdot \begin{cases} \mathcal{L}_p(E/\mathbb{Q}_p), & \text{mult. split,} \\ (1-\frac{1}{\alpha})^2, & \text{bona,} \\ 2, & \text{mult. no split.} \end{cases}$$

- Si $E(\mathbb{Q})$ és finit i p no té reducció multiplicativa split és equivalent (per construcció de L_p) a la conjectura genèrica.

- Si $E(\mathbb{Q})$ és finit i p té reducció multiplicativa split és equivalent a la conjectura genèrica (Greenberg-Stevens, Inv. Math. 93).

- Resultats per corbes amb multiplicació complexa: Rubin, Inv. Math. 92

- Generalitzacions a corbes modulars considerant $L(E/K, s)$ amb K quadràtic à la Gross-Zagier-Kolyvagin (Perrin-Riou, Inv. Math. 87, Bertolini-Darmon, Inv. Math. 96 i 98)

Nous invariants:

En el cas de reducció multiplicativa split sigui $q = q(j_E) \in \mathbb{Q}_p$, amb

$$j = q^{-1} + 744 + 196884q + \dots$$

el període multiplicatiu p-àdic tal que (Tate)

$$E(\mathbb{Q}_p) \simeq \mathbb{Q}_p^*/q^{\mathbb{Z}}$$

Es defineix

$$\mathcal{L}_p = \frac{\log_p(q)}{\operatorname{ord}_p q}$$

En el cas de bona reducció $\alpha \in \mathbb{Q}_p$ és l'arrel amb $\operatorname{ord}_p(\alpha) = 0$ del polinomi

$$X^2 - a_p X + p, \qquad a_p = 1 + p - N_p.$$

Altures p-àdiques

Siguin x, y coordenades d'un model minimal global, $\omega = dx/(2y + a_1x + a_3)$ i $t = -x/y$. Existeix una única funció parell $\sigma^2 \in t^2(1 + t\mathbb{Z}_p[[t]])$ tal que

$$-\frac{d}{w}(\frac{d}{w}\log\sigma^2) = 2x + \alpha, \quad \alpha \in \mathbb{Z}_p$$

De fet, aquesta equació permet calcular de manera recurrent els seus coeficients (Mazur-Tate).

L'aplicació

$$h_p(P) = \log_p \frac{\sigma^2(P)}{\operatorname{den} x(P)}, \qquad P \in E(\mathbb{Q}) \cap E_1(\mathbb{Q}_p)$$

extén a una forma quadràtica h_p sobre $E(\mathbb{Q}) \otimes \mathbb{Q}_p$.

El regulador és el seu determinant sobre una base de $E(\mathbb{Q})$ mòdul torsió.

Segona part: L-sèries p-àdiques de formes modulars

Sigui $T = \lim_{\leftarrow} T_n$ (finits). Per exemple

$$\mathbb{Z}_{p,M} = \varprojlim(\mathbb{Z}/p^n M\mathbb{Z}) = \varprojlim(1/p^n M)\mathbb{Z}/\mathbb{Z} \simeq (\mathbb{Z}/M\mathbb{Z}) \times \mathbb{Z}_p$$

que té per base d'entorns de x les boles $D(x,n) = x + p^n M\mathbb{Z}_{p,M}$, o també

$$\mathbb{Z}^*_{p,M} = \varprojlim(\mathbb{Z}/p^n M\mathbb{Z})^* \simeq (\mathbb{Z}/M\mathbb{Z})^* \times \mathbb{Z}^*_p$$

Una *distribució* a T amb valors a un grup abelià V és (defs. equiv.)

- una família $\mu_n : T_n \to V$ compatible: $\mu_n(x) = \sum_{y \mapsto x} \mu_{n+1}(y)$
- una aplicació μ : {oberts compactes} $\to V$ additiva
- un morfisme de grups $\mathrm{Step}(T, \mathbb{Z}) \to V$, $f \mapsto \int_T f\, d\mu$

Exemple: distribucions de Dirac per $x \in T$

$$\delta_x(U) = \begin{cases} 1, & x \in U \\ 0, & x \notin U. \end{cases}$$

Exemple: distribucions de Bernoulli a $\mathbb{Z}_{p,M}$

$$\mu_{B,k}(a + p^n M\mathbb{Z}_{p,M}) = p^{n(k-1)} B_k(a/p^n M), \qquad a \in \mathbb{Z}, \quad 1 \leqslant a < p^n M,$$

on B_k és el k-èsim polinomi de Bernoulli determinat per la identitat

$$\frac{te^{xt}}{e^t - 1} = \left(\sum_{k=0}^{\infty} B_k \frac{t^k}{k!}\right)\left(\sum_{k=0}^{\infty} \frac{(xt)^k}{k!}\right) = \sum_{k=0}^{\infty} B_k(x)\frac{t^k}{k!}.$$

(o pel fet que la fórmula anterior és una distribució per algun p)

Per $k = 0$ es té la distribució de Haar

$$\mu_{\text{Haar}}(a + p^n M\mathbb{Z}_{p,M}) = p^{-n}.$$

Considerem *distribucions p-àdiques*: V és un K-espai de Banach de dimensió finita amb $[K:\mathbb{Q}_p]<\infty$ o bé $K=\mathbb{C}_p$ i denotem $\mathcal{O}$ l'anell d'enters de K.

Una *mesura p-àdica* és una distribució p-àdica fitada:

$$\mu(U)\leqslant B<\infty, \quad \text{per tot obert compacte } U.$$

Teorema 1 *Sigui μ una mesura p-àdica. Per tota funció contínua $f\in \mathcal{C}(T,K)$ la integral definida com a límit de sumes de Riemann*

$$\int_T f\,d\mu=\lim_{n\to\infty}\sum_{x\in D(x,n)} f(x)\mu(D(x,n))$$

està bén definida; és a dir, el límit existeix i no depen dels punts escollits.

L'aplicació $f\mapsto \int_T f\,d\mu : \mathcal{C}(X,K)\to V$ és un homomorfisme fitat d'espais de Banach (amb $|\int_T f\,d\mu|\leqslant B\|f\|$ on $B=\sup\{\mu(U)\}$ és el suprem de la mesura dels oberts compactes) i tot homomorfisme fitat com aquest és la integració per alguna mesura p-àdica.

Un *caracter p-àdic mòdul M* és un morfisme continu $\chi : \mathbb{Z}_{p,M}^* \to \mathbb{C}_p^*$. Els caracters de Dirichlet $\psi : \mathbb{Z}/p^n M\mathbb{Z} \to \mathbb{C}_p^*$ proporcionen caracters p-àdics.

$$X = \mathrm{Hom}(\mathbb{Z}_{p,M}^*, \mathbb{C}_p^*)$$

Es té la descomposició

$$\mathbb{Z}_{p,M}^* \simeq (\mathbb{Z}/M\mathbb{Z}) \times \mathbb{Z}_p^* \simeq (\mathbb{Z}/qM\mathbb{Z})^* \times (1 + q\mathbb{Z}_p), \qquad q = 4 \text{ o } p$$

La projecció $x \mapsto \langle x \rangle \in 1 + q\mathbb{Z}_p$ és un caracter. Si $s \in \mathcal{O}$ es defineix el caracter

$$\chi_s(x) = \langle x \rangle^s = \exp(s \log_p \langle x \rangle) = \sum_{r=0}^{\infty} \frac{s^r}{r!} (\log_p \langle x \rangle)^r$$

Sigui μ una mesura p-àdica a $\mathbb{Z}_{p,M}^*$. La seva *L-sèrie p-àdica* (o transformada de Mellin p-àdica) és defineix com

$$L_p(\mu, \chi) = \int_{\mathbb{Z}_{p,M}^*} \chi \, d\mu, \qquad \chi \in X$$

i, per $s \in \mathcal{O}$, es defineix

$$L_p(\mu, \chi, s) = L_p(\mu, \chi\chi_s) = \int_{\mathbb{Z}_{p,M}^*} \chi \langle x \rangle^s \, d\mu$$

Com que, topològicament, $1+q\mathbb{Z}_p \simeq \mathbb{Z}_p$ i $\mathrm{Hom}(1+q\mathbb{Z}_p, \mathbb{C}_p^*)$ pot identificar-se amb la bola $U = \{z \in \mathbb{C}_p \mid \mathrm{ord}(z-1) > 0\}$, X té una estructura analítica.

Teorema 2 *La funció L p-àdica associada a una distribució és localment analítica*

$$L_p(\mu, \chi, s) = \sum_{n=0}^{\infty} c_n s^n, \quad c_n \in \mathbb{C}_p.$$

Si ψ és un caracter de Dirichlet de conductor $p^n M$,

$$L_p(\mu, \psi, s) = \sum_{r=0}^{\infty} \frac{s^r}{r!} \sum_{a \mod p^n M} \psi(a) \int_{D(a,n)} \log_p \langle x \rangle^r \, d\mu$$

A més, la funció L p-àdica queda completament determinada pels seus valors en els caracters d'ordre finit (caracters de Dirichlet). L'objectiu és interpolar els valors especials de les torçades d'una L-serie per caracters de Dirichlet:

$$L_p(\psi) = c_\psi L(\psi, 1).$$

Sigui S_2 el $\mathbb{C}$-espai vectorial de les formes parabòliques de pes 2 per subgrups de congruència. Les matrius de $\mathrm{GL}_2(\mathbb{Q})^+$ hi operen vía

$$f|_A(z) = \frac{\det A}{(cz+d)^2} f(\frac{az+b}{cz+d}), \qquad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Sigui $S_2(N) = \oplus_\varepsilon S_2(N, \varepsilon)$. Si $f \in S_2(N)$ es defineix el símbol modular

$$\lambda_f(r) = 2\pi \int_0^\infty f(r+it)\, dt, \qquad r \in \mathbb{Q}/\mathbb{Z}$$

que és $\mathbb{C}$-lineal respecte la f i compleix la identitat

$$\lambda_{f|_A}(r) = \lambda_f(Ar) - \lambda_f(A\infty).$$

El mòdul dels valors L_f és el sub-$\mathbb{Z}$-mòdul de $\mathbb{C}$ generat pels $\lambda_f(r)$, que és finitament generat.

Si $f(z) = \sum a_n q^n \in S_2(N)$,

$$L(f,s) = a_n n^{-s} = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it) t^s \frac{dt}{t}.$$

En particular, per $s = 1$,

$$L(f,1) = 2\pi \int_0^\infty f(it)\, dt = \lambda_f(0).$$

Per tot caracter de Dirichlet $\psi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$,

$$(f \otimes \psi)(z) = \sum a_n \psi(n) q^n = \frac{1}{\tau(\overline{\psi})} \sum_{a \mod m} \overline{\psi}(a) f(z + \frac{a}{m})$$

i els valors especials de la L-sèrie corresponent venen donats per

$$L(f \otimes \psi, 1) = \frac{\tau(\psi)}{m} \sum_{a \mod m} \lambda_f(\frac{a}{m}).$$

L'espai $S_2(N,\varepsilon)$ és tancat per l'acció de l'àlgebra generada pels operadors de Hecke

$$T_p = \sum_{i=0}^{p-1} \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} + \varepsilon(p) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

Proposició 1 *Si $f \in S_2(N,\varepsilon)$, per tot primer p*

$$\lambda_{f|T_p} = \sum_{i=0}^{p-1} \lambda_f(\frac{r+i}{p}) + \varepsilon(p)\lambda_f(pr)$$

Corol·lari 1 *Sigui $f \in S_2(N,\varepsilon)$ un vector propi per T_p de valor propi a_p. Si α és una arrel no nul·la del polinomi $X^2 - a_pX + \varepsilon(p)p$ aleshores*

$$\mu_{f,\alpha}(D(a,n)) = \frac{\lambda_f(a/p^nM)}{\alpha^n} - \varepsilon(p)\frac{\lambda_f(a/p^{n-1}M)}{\alpha^{n+1}}$$

és una distribució p-àdica a $\mathbb{Z}_{p,M}^*$ que pren valors a $V_f = \mathbb{C}_p \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}}L_f$. En cas que $\mathrm{ord}_p(\alpha) = 0$ és una mesura p-àdica.

La L-sèrie p-àdica associada a la forma modular f és la funció localment analítica definida per caracters p-àdics de conductor M com

$$L_p(f,\chi) = \int_{\mathbb{Z}_{p,M}^*} \chi \, d\mu_{f,\alpha}$$

Observació: Considerant mesures no fitades però "admisibles" s'aconsegueix una teoria d'integració per funcions localment analítiques a $\mathbb{Z}_{p,M}^*$ i definir L-sèries.

Per tota forma parabòlica de pes $k \geqslant 2$ per $\Gamma_1(N)$ vector propi de T_p amb valor propi a_p i arrel α de $X^2 - a_p X + \varepsilon(p)p^{k-1}$ admisible (o sigui, amb $\operatorname{ord}\alpha < k-1$) es generalitza la construcció anterior obtenint-se una distribució admisible i una L-sèrie p-àdica (Manin-Vishik, Amice-Velu, Mazur-Tate-Teitelbaum).

Per tot caracter de Dirichlet ψ de conductor m es defineix el *multiplicador p-àdic*

$$e_p(\psi) = \frac{1}{\alpha^n}\left(1 - \frac{\overline{\psi}(p)\varepsilon(p)}{\alpha}\right)\left(1 - \frac{\psi(p)}{\alpha}\right)$$

Aleshores

$$L_p(f,\psi,0) = L_p(f,\psi) = e_p(\psi)\frac{p^n M}{\tau(\overline{\psi})}\lambda_{f\otimes\overline{\psi}}(0) = e_p(\psi)\frac{p^n M}{\tau(\overline{\psi})}L(f\otimes\overline{\psi},1)$$

És a dir, la L-sèrie p-àdica interpola valors especials de les L-sèries de f torçades per caracters de Dirichlet. El multiplicador p-àdic intervé en l'anul·lació.

Conjectura 1

$$\operatorname{ord}_{s=0} L_p(f,\psi,s) = \begin{cases} \operatorname{ord}_{s=1} L(f\otimes\overline{\psi},s), & e_p(\psi)\neq 0, \\ 1+\operatorname{ord}_{s=1} L(f\otimes\overline{\psi},s), & e_p(\psi)=0. \end{cases}$$

Sigui $E/\mathbb{Q}$ una corba el·líptica modular amb forma modular associada f. Sigui

$$\Lambda = \{\int_\gamma \omega \,|\, \gamma \in H_1(E(\mathbb{C}),\mathbb{Z})\} \subseteq \mathbb{Z}\Omega_E^+ + \mathbb{Z}i\Omega_E^-$$

la ret de períodes de Néron, amb $\Omega_E^+ = \frac{1}{2}\int_{E(\mathbb{R})}\omega$. Gràcies al Teorema de Manin-Drinfeld (els divisors amb suport a les puntes són de torsió),

$$\lambda_f(r) = 2\pi\int_0^\infty f(r+it)\,dt = c\int_\gamma \omega = [r]^+\Omega_E^+ + [r]^- i\Omega_E^-$$

amb $[r] = [r]^+$ i $[r]^-$ racionals.

Sigui p un primer de reducció ordinària. L'aplicació $r \mapsto [r] : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}$ és un símbol modular $\mathbb{Q} \subset \mathbb{Q}_p$-valorat, se li asocia per tant una mesura $\mathbb{Q}_p$-valorada μ_E i li correspon una L-sèrie p-àdica

$$L_p(E/\mathbb{Q},s) = \int_{\mathbb{Z}_p^*}\langle x\rangle^s\, d\mu_E \in \mathbb{Q}_p[[s]]$$

Perquè el punt crític sigui $s = 1$ es pot fer un desplaçament i definir $L_p(E/\mathbb{Q},s)$ com la integral de la funció $\langle x\rangle^{s-1}$.

Tercera part: La conjectura refinada

(formulació: Mazur-Tate 88, resultats: Darmon 91-93...)

Sigui $E/\mathbb{Q}$ una corba el·líptica modular de rang r i S un producte de primers de bona reducció ordinària. Sigui $G_S = (\mathbb{Z}/S\mathbb{Z})^*/\{\pm 1\}$. Si R és un anell sigui $I_S \subset R[G_S]$ l'ideal d'augmentació. Considerem G dins de I_S/I_S^2 via $\sigma_a \mapsto \sigma_a - 1$.

L'*element modular* és

$$\theta_S = \sum_{\sigma_a \in G} \left(\sum_{T|S} \mu(S/T) \left[\frac{aT'}{T} \right] \right) \sigma_a \in \mathbb{Z}[G], \qquad T' = (S/T)^{-1} \pmod{T}.$$

Tot caracter de Dirichlet parell ψ de conductor $f \mid S$ s'extén a un morfisme d'anells $\mathbb{Z}[G_S] \to \mathbb{C}^*$ i es té

$$\psi(\theta_S) = c\frac{S}{f}\tau'(\psi)\frac{L(E/\mathbb{Q}, \overline{\psi}, 1)}{2\Omega_E^+}.$$

Sigui

$$0 \longrightarrow E_S(\mathbb{Q}) \longrightarrow E(\mathbb{Q}) \longrightarrow \oplus_{p|S} E(\mathbb{F}_p) \times E/E_0 \longrightarrow J_S \longrightarrow 0$$

Mazur-Tate defineixen un aparellament

$$\langle\ ,\ \rangle_S : E(\mathbb{Q}) \times E_S(\mathbb{Q}) \to G_S$$

i un regulador $R_S(E/\mathbb{Q}) \in I_S^r/I_S^{r+1}$

La *conjectura refinada* de Mazur-Tate (versió simplificada de Darmon) és

$$\theta_S \in I_S^r$$

$$\tilde{\theta}_S = c \cdot |Ш(E/\mathbb{Q})| R_S(E/\mathbb{Q}) J_S \in I_S^r/I_S^{r+1}$$