Francesc Bars Cortina

Determinació de les corbes $X_0(N)$ biel·líptiques

Treball de recerca
sota la direcció del:
Dr. Salvador Comalada i Clara
Bellaterra, Setembre 1997

Índex

Prefaci

Aquest treball sorgeix a partir del seminari de Teoria de Nombres de la Universitat Autònoma de Barcelona impartit el segon quatrimestre del curs acadèmic 1995-1996 sota el títol:

Punts de grau d en corbes algebraiques.

El seminari es centrà en l'estudi de la finitud del conjunt de punts d'una corba algebraica, definits sobre cossos de nombres de grau més petit o igual que d. Per a $d = 2, 3$, es va demostrar que el problema anterior és equivalent a determinar l'existència de morfismes de grau 2, 3 respectivament, de la corba a la recta projectiva o a una corba el·líptica.

El nostre treball consisteix en estudiar la finitud dels conjunts dels punts quadràtics ($d = 2$) a la família de les corbes modulars $X_0(N)$ i, per tant, en determinar quins d'aquests $X_0(N)$ admeten un morfisme de grau 2 a la recta projectiva o a una corba el·líptica.
El primer cas fou resolt completament per Andrew Ogg ([30]). En quant al segon cas, es coneixen fins ara llistes parcials de corbes biel·líptiques com les donades per Marc Hindry ([19]) per a N primer i les de Joan Carles Lario per a $4 \nmid N$ i $9 \nmid N$.

El treball que presentem tanca el problema plantejat i ofereix un estudi aprofundit del grup d'automorfismes de $X_0(N)$ i a la vegada de certs aspectes importants de les parametritzacions modulars.

Voldria agrair l'ajuda inestimable del director del treball de recerca, Salvador Comalada i Clara, per les seves indicacions i ajudes. Igualment voldria agrair al Departament de Matemàtiques de la Universitat Autònoma de Barcelona el seu suport tècnic en la realització d'aquest treball.

Capítol 1

Introducció

Sigui $X_0(N)$ la corba modular corresponent al subgrup $\Gamma_0(N)$ del grup modular, definit per les matrius $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ amb $N|c$.
Andrew Ogg [30] va determinar que hi ha dinou valors de N pels quals la corba modular $X_0(N)$ és hiperel·líptica, és a dir, existeix un morfisme φ de grau 2 a la recta projectiva:

$$\varphi : X_0(N) \to \mathbb{P}^1$$

Això té com a conseqüència l'existència, per a aquests dinou valors de N, d'una involució $\upsilon \in Aut(X_0(N))$ que és única i tal que $X_0(N)/\upsilon \cong \mathbb{P}^1$. El resultats d'Ogg són els següents:

Teorema. *$N = 37$ és l'únic cas en el que $X_0(N)$ és hiperel·líptica amb una involució $\upsilon \notin SL_2(\mathbb{R})$.*

Teorema. *Hi ha exactament divuit valors de N, $N \neq 37$, tals que $X_0(N)$ és hiperel·líptica. Per a $N = 40$ i $N = 48$ la involució hiperel·líptica υ no és del tipus Atkin-Lehner. La resta es llegeix a la següent taula:*

N	υ	N	υ
22	w_{11}	35	w_{35}
23	w_{23}	39	w_{39}
26	w_{26}	41	w_{41}
28	w_7	46	w_{23}
29	w_{29}	47	w_{47}
30	w_{15}	50	w_{50}
31	w_{31}	59	w_{59}
33	w_{11}	71	w_{71}

El cas de $N = 40$ *correspon a la involució* $\upsilon = \begin{pmatrix} -10 & 1 \\ -120 & 10 \end{pmatrix} = w_5 S_2 w_8 S_2 w_8$ *(veure notació capítol 3). El cas* $N = 48$ *correspon a la involució* $\upsilon = \begin{pmatrix} -6 & 1 \\ -48 & 6 \end{pmatrix} = w_3 S_2 w_{16} S_2 w_{16}$.

El nostre treball consisteix en determinar quan la corba modular $X_0(N)$ és biel·líptica, és a dir, hi ha un morfisme de grau dos a una corba el·líptica. Hem obtingut el següent resultat(gènere sempre superior o igual a 2):

Teorema. *Hi ha exactament quaranta-un valors de* N *pels quals la corba modular* $X_0(N)$ *és biel·líptica. A més,* $X_0(N)$ *admet una involució biel·líptica del tipus d'Atkin-Lehner a excepció del cas* $X_0(72) = X_0(2^3 3^2)$. *El llistat d'aquests* N, $N \neq 72$, *és el següent:*

22	*26*	*28*	*30*	*33*	*34*	*35*	*37*	*38*	*39*
40	*42*	*43*	*44*	*45*	*48*	*50*	*51*	*53*	*54*
55	*56*	*60*	*61*	*62*	*63*	*64*	*65*	*69*	*75*
79	*81*	*83*	*89*	*92*	*94*	*95*	*101*	*119*	*131*

Ens adonem del següent fet curiós: per a la corba $X_0(72)$, podem escollir les involucions w_8, w_9 d'Atkin-Lehner de la següent forma:

$$w_8 = \frac{1}{\sqrt{8}} \begin{pmatrix} -8 & 1 \\ -72 & 8 \end{pmatrix} \quad w_9 = \frac{1}{3} \begin{pmatrix} 9 & 1 \\ 72 & 9 \end{pmatrix}$$

a on els coeficients de les matrius són particularment baixos. Aquest fet, diem-ne excepcional, es produirà en general per a qualsevol $X_0(a^b c^d)$ si i sols si l'equació diofantina $a^b - c^d = 1$ té solució. Davant d'aquesta situació i del resultat del teorema ens formulem la següent pregunta: Hi ha alguna possible relació entre corbes biel·líptiques del tipus $X_0(a^b c^d)$ que no admeten cap involució biel·líptica d'Atkin-Lehner i la resolució de la equació diofantina $a^b - c^d = 1$, a, b, c, d nombres naturals amb $b, d \geq 2$, $a, c \neq 1$?
Per a demostrar el teorema anterior s'utilitzen les tècniques de reducció mòdul un primer p, $p \nmid N$, per a reduir-nos a un número finit de casos, que es van estudiant gràcies al coneixement del grup $Aut(X_0(N))$.
El treball conclou amb un plantejament del problema mitjançant parametritzacions modulars i un petit apèndix a on s'ataca via les representacions de les involucions en l'espai cotangent de $X_0(N)$.

Capítol 2

Corbes hiperel·líptiques i biel·líptiques

Considerem C una corba projectiva no singular (és a dir, completa) sobre un cos k algebraicament tancat.

Definició 2.1. *Diem que la corba C és hiperel·líptica si té un g^1_2, és a dir, si existeix un morfisme $\varphi : C \to \mathbb{P}^1$ amb $deg(\varphi) = 2$.*

Sigui $\phi : C \to Jac(C)$ l'aplicació natural i considerem l'objecte $S^2C = C \times C/\mathcal{S}_2$ i l'aplicació

$$\phi^{(2)} : S^2C \to Jac(C)$$

que, donada a nivell de punts, consisteix en $\phi^{(2)}(x_1 + x_2) = \phi(x_1) + \phi(x_2)$, $x_i \in C$ $i = 1, 2$. Si fixem un punt $\mathfrak{U} = \alpha_1 + \alpha_2$ de S^2C:

$$\phi^{(2)^{-1}}(\phi^{(2)}(\mathfrak{U})) = |\mathfrak{U}| = \{divisors\ positius\ K(C) - equivalents\ a\ \mathfrak{U}\} \subset S^2C.$$

Si C és hiperel·líptica això implica l'existència de sistemes lineals de grau 2 no trivials i, per tant, l'aplicació

$$S^2C \to Imag(\phi^{(2)})$$

no és bijectiva.
Observem, però, que en aquest cas S^2C conté la recta projectiva via

$$\mathbb{P}^1 \to S^2C$$

$$x \mapsto \varphi^{-1}(x)$$

Recíprocament, si S^2C conté una recta projectiva llavors C és una corba hiperel·líptica, del fet que el $\mathbb{P}^1$ va a un punt en $Jac(C)$, es a dir, dóna sistemes de grau 2 no trivials ($\phi^{(2)}$ no és injectiva).

Anotem tot seguit alguns resultats sobre corbes hiperel·líptiques, tot observant que si C és hiperel·líptica existeix una involució $\upsilon \in Aut(C)$ anomenada involució hiperel·líptica complint $\varphi = \varphi \circ \upsilon$.

Proposició 2.2. *La projectivització $\varphi' : C \to \mathbb{P}^{g-1}$ donada per $|K_C|$, el divisor canònic de C, és una immersió (és a dir és injectiva i la diferencial també) si i només si C no és hiperel·líptica.*

Proposició 2.3. *Considerem $car(k) = 0$. La involució υ que fa la corba C hiperel·líptica és única. A més, si C és una superfície de Riemann, és del centre del grup d'automorfismes de C.*

Com a conseqüència immediata del Teorema de Riemann-Roch tenim:

Proposició 2.4. *Sigui C una corba no singular sobre un cos k amb $car(k) = 0$. Llavors C és hiperel·líptica si i només si té una involució amb $2g+2$ punts fixos, on g denota el gènere de C.*

Proposició 2.5. *En la situació de la proposició anterior, si υ és la involució hiperel·líptica, l'aplicació que defineix en les diferencials regulars actua com -1. Aquesta propietat caracteritza el fet que C sigui hiperel·líptica.*

Fins ara C denotava una corba no singular definida igual que l'aplicació φ sobre un cos k algebraicament tancat; volem, però, fer un estudi aritmètic de la propietat que una corba sigui hiperel·líptica, és a dir, si C denota una corba hiperel·líptica definida sobre K complint $K \subset k$ cal preguntar-se si φ està definit sobre K.

Proposició 2.6. *Si C hiperel·líptica està definida sobre un cos K de gènere més gran o igual que dos, llavors C és hiperel·líptica sobre K; és a dir*

$$\varphi : C \to \mathbb{P}^1$$

de grau 2 tot definit sobre K.

Demostració. Sigui $\pi : C \to \mathbb{P}^1$ morfisme de grau 2; llavors per a cada $\delta \in Gal(\overline{K}|K)$ obtenim un morfisme també de grau 2; $\pi^\delta : C \to \mathbb{P}^1$.Pel fet de tenir C gènere superior a 1 s'obté que π i π^δ difereixen en un element $\xi_\delta \in Aut(\mathbb{P}^1) = \mathbb{P}GL_2(\overline{K})$: $\pi^\delta = \xi_\delta \circ \pi$. Construïm una aplicació:

$$\xi : Gal(\overline{K}|K) \to \mathbb{P}GL_2(\overline{K})$$

$$\delta \mapsto \xi_\delta$$

Donats $\sigma, \delta \in Gal(\overline{K}|K)$ es té que $\xi_{\sigma\delta} = \xi_\sigma^\delta \circ \xi_\delta$ i, per tant, això ens dóna un cocicle en $H^1(Gal(\overline{K}|K), \mathbb{P}GL_2(\overline{K}))$. Del fet que $H^1(Gal(\overline{K}|K), \mathbb{P}GL_n(\overline{K})) =$

0 (generalització del teorema 90 de Hilbert) podem escriure $\xi_\sigma = \varphi_1^\sigma \circ \varphi_1^{-1}$ amb $\varphi_1 \in Aut(\mathbb{P}^1)$. Finalment l'aplicació

$$\varphi = \varphi_1^{-1} \circ \pi : C \to \mathbb{P}^1$$

està definida sobre K. □

Anem a analitzar la situació quan a S^2C hi tenim una corba el·líptica.

Definició 2.7. *Diem que C és una corba biel·líptica si existeix una aplicació $\varphi : C \to E$ amb $deg(\varphi) = 2$ on E denota una corba el·líptica.*

Observem que, igual que en el cas hiperel·líptic, si C és biel·líptica l'aplicació φ defineix una involució $\upsilon \in Aut(C)$ que anomenarem involució biel·líptica. Ara, però, aquesta involució no és necessàriament única ni té perquè pertànyer al centre de $Aut(C)$.

Proposició 2.8. *Si $C|_k$ ($car(k) = 0$) és una corba no singular que és biel·líptica, llavors la involució biel·líptica té $2g - 2$ punts fixos.*

És clar que si C és una corba biel·líptica llavors S^2C conté una corba el·líptica. Anem a veure un resultat en la direcció recíproca.

Teorema 2.9 (Harris-Silverman,[18]). *Si C_1 és una corba biel·líptica, i si $C_1 \to C$ és una aplicació finita, llavors tenim que C és biel·líptica o hiperel·líptica.*

Demostració. (sketch) Denotem per $\alpha : C_1 \to C$ l'aplicació de grau finit entre C_1 i C i per $\varphi : C_1 \to E$ amb $deg(\varphi) = 2$. Sense pèrdua de generalitat podem suposar que el gènere$(C) \geq 3$. Considerem V, l'espai de les diferencials regulars de C_1 a on la involució donada per φ hi actua com a -1; i considerem $W = \alpha^{*(-1)}(V)$ dins les diferencials regulars de C; es prova que W té codimensió 1 respecte de tot l'espai de diferencials regulars de C del fet següent:

Teorema. *Si υ és una involució biel·líptica d'una corba de gènere g definida sobre k amb $car(k) = 0$, llavors υ actua a les diferencials regulars com a -1, llevat d'un subespai 1-dimensional.*

Considerem llavors l'aplicació donada pel sistema lineal W; anomenem-la φ_W.

$$\varphi_M : C \to \mathbb{P}^{dim_k(W)-1}$$

i denotem $B = \varphi_M(C)$. Es prova que B no és birracionalment equivalent a la corba C (del fet que C_1 era biel·líptica). Si $dim_k(W) = g$ aleshores W és

l'espai de totes les diferencials regulars i, per la proposició 2.2, C és hiperel·líptica. Per tant considerem $dim_k(W) = g - 1$ i $\varphi_M : C \to \mathbb{P}^{g-2}$. Com que φ_M no és birracional entre C i B, la corba E es troba dins del producte fibrat simètric $C *_B C = \frac{C \times_B C \setminus \Delta}{\sigma}$ (que es defineix com la unió de les components irreductibles del producte ordinari, traient la diagonal, mòdul la involució que permuta els factors):

$$E \to C *_B C$$

$$e \mapsto (\varphi_M(e_1), \varphi_M(e_2))$$

on $\varphi(e_i) = e$. Pensant B dins de $C *_B C$ tenim una aplicació no constant de $E \to B$ i, per tant, B té gènere 0 o 1.
Si $deg(\varphi_M) = 2$ s'acaba: B és la corba el·líptica o recta projectiva buscada. Utilitzant el fet que tota corba irreductible no degenerada de $\mathbb{P}^{g-2}$ té com a mínim grau $g - 2$ obtenim:

$$2g - 2 \geq deg(\varphi_M)(g - 2)$$

i de $g \geq 3$ tenim que $deg(\varphi_M) \leq 4$ (Observem que si $g \geq 5$ l'anterior construcció ens dóna directament el resultat). El cas $deg(\varphi_M) = 3$ no es pot donar ja que tindria com a conseqüència que $C *_B C$ és isomorf a C, però C té gènere superior a 2. Pel cas de grau igual a 4 cal veure $\varphi_M : C \to B$ com a un recobriment i considerar-ne el grup de monodromia G, que serà un subgrup de $\mathcal{S}_4$ i examinar totes les possibilitats per a G. En alguns casos es construeix la involució i els altres casos es veu que no es poden donar per comparació de gèneres i l'estudi de ramificacions. □

Teorema 2.10 (Harris-Silverman). *Sigui C una corba projectiva llisa o no singular. Si el producte simètric S^2C conté una corba de gènere 1, llavors C és biel·líptica o hiperel·líptica.*

Demostració. Sigui E la normalitzada de la corba que conté S^2C i sigui $i : E \to S^2C$ l'aplicació natural. Denotem per $\pi : C^2 \to S^2C$ la projecció i per $\overline{C_2} = \pi^*(i_*(E)) \in Div(C^2)$ el pullback del divisor $i(E)$ dins S^2C via π. Llavors tenim una aplicació racional de $\overline{C_2} \to E$ de grau 2, i pel fet de ser π finita, cada component de $\overline{C_2}$ s'aplica exhaustivament a E. Per aquestes consideracions tenim que $\overline{C_2}$ és irreductible; ja que si no ho fos, tota component $\overline{C_{21}}$ tindria gènere 1, d'on C^2 tindria corbes de gènere 1, però això és impossible ja que el gènere de C és com a mínim 2. Denotem per C_2 la normalització de $\overline{C_2}$ i $j : C_2 \to C^2$ l'aplicació natural. Tenim el següent diagrama commutatiu:

$$\begin{array}{ccccc} & C_2 & \to & C^2 & \\ \varphi & \downarrow & & \downarrow & \pi \\ & E & \to & C^{(2)} & \end{array}$$

on $deg(\varphi) = deg(\pi) = 2$ i C_2 és biel·líptica. Anem doncs a aplicar el teorema anterior, on ara C_2 fa el paper de C_1 en la notació del teorema. Considerem per això les aplicacions $\gamma_i = p_i \circ j$, on p_i són les projeccions de C^2 a C $(i = 1, 2)$;

$$\gamma_i : C_2 \to C$$

Només cal veure que no són constants i aplicar directament el teorema 2.9. Per això observem que si en C^2 denotem per σ l'aplicació: $\sigma(x, y) = (y, x)$, aleshores $\sigma(j(C_2)) = j(C_2)$; d'aquí

$$\gamma_1(C_2) = \gamma_2(C_2)$$

Com que j no és constant, $p_1 \circ j$ i $p_2 \circ j$ tampoc ho són perquè $\overline{C_2}$ és irreductible i les aplicacions $p_i|_{\overline{C_2}}$ no són constants. □

Quan la corba C té gènere superior o igual a 9 tenim un resultat totalment anàleg al del cas hiperel·líptic:

Teorema 2.11 (Harris-Silverman). *En la notació i hipòtesis del teorema anterior i si el gènere de C és més gran o igual que 9 llavors C és biel·líptica.*

Per una prova podeu consultar [18] pag 351. Fins ara hem tractat les corbes biel·líptiques de forma totalment algebraica, pensades com a corbes definides sobre un cos k algebraicament tancat. Anem a fer un petit estudi sobre el seu comportament aritmètic.

Teorema 2.12 (Harris-Silverman). *Suposem que C sigui una corba biel·líptica de gènere més gran o igual que 6 i definida sobre K. Llavors existeix una corba el·líptica E definida sobre K i una aplicació $\varphi : C \to E$ de grau 2 també definida sobre K. És a dir, la propietat de ser corba biel·líptica baixa sobre cossos de definició si el gènere de C és prou gran.*

Demostració. Com que C és biel·líptica existeix una corba el·líptica E' definida sobre $\overline{K}$ i una aplicació $\varphi' : C \to E'$ de grau 2 definida sobre $\overline{K}$. Anem a utilitzar cohomologia galoisiana per a baixar-ho. Considerem per a cada $\delta \in Gal(\overline{K}/K)$ l'aplicació ${\varphi'}^{\delta} : C \to {E'}^{\delta}$ també de grau 2 i el producte:

$$\varphi' \times {\varphi'}^{\delta} : C \to E' \times {E'}^{\delta}$$

i denotem per $E'' = \varphi' \times {\varphi'}^{\delta}(C)$ la imatge. Si C fos birracional amb E'' utilitzant [5] VIII.C-1:

$$gènere(C) \leq (deg(\varphi') - 1)(deg({\varphi'}^{\delta} - 1) + (deg(\varphi'))(gènere(E)) + (deg({\varphi'}^{\delta}))(gènere({E'}^{\delta})) = 5$$

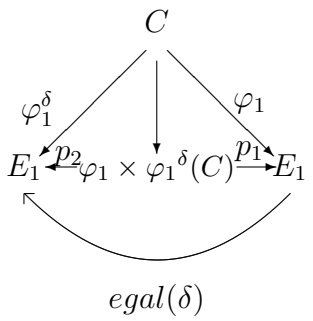
Per tant, podem suposar que C no és birracional amb E''. Considerem la composició següent:

$$C \xrightarrow{\varphi' \times \varphi'^{\delta}} E'' \xrightarrow{proj_1} E'$$

Com que $proj_1 \circ (\varphi' \times \varphi'^{\delta}) = \varphi'$ que té grau 2, E'' és birracionalment equivalent a E'. De manera semblant, considerant $proj_2$ enlloc de $proj_1$ tenim E'' birracionalment equivalent a E'^{δ}. Per tant, per a tot $\delta \in Gal(\overline{K}/K)$, $E' \cong E'^{\delta}$, i així E' és isomorfa sobre $\overline{K}$ a una corba el·líptica E_1 definida sobre K. Canviant E' per aquesta nova corba E_1 i canviant φ' per φ_1, també de grau 2, obtenim

$$\varphi_1 : C \to E_1$$

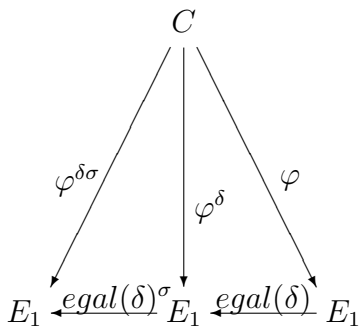
amb C i E_1 definits sobre K. Anem a construir un morfisme de grau 2 de C a una corba el·líptica definit sobre K. Per això per cada $\delta \in Gal(\overline{K}/K)$ considerem $\varphi_1^{\delta} : C \to E_1$. Tenim el següent diagrama commutatiu:



Observem que obtenim una aplicació

$$egal : Gal(\overline{K}/K) \to Aut(E_1)$$

(on $Aut(E_1)$ denota el que alguns llibres denotem per $Isom(E_1)$. No estem exigint que el 0 vagi al 0) que compleix que $\varphi_1^{\delta} = egal(\delta) \circ \varphi$ per a tot $\delta \in Gal(\overline{K}/K)$. Es satisfà, a més, el següent diagrama commutatiu:



d'on obtenim que *egal* ens defineix un 1-cocicle i, per tant, un element de $H^1(Gal(\overline{K}/K), Aut(E_1))$. Recordem el següent resultat sobre twists de corbes el·líptiques:

Teorema. *Sigui $B|_K$ una corba el·líptica. Per a cada twist $B'|_K$ de $B|_K$ elegim un isomorfisme $\phi : B' \to B$ i definim l'aplicació $\xi_\delta = \phi^\delta \circ \phi^{-1} \in Isom(B)$*

1. *ξ és un 1-cocicle. Denotem per $\{\xi\}$ la corresponent classe de cohomologia a $H^1(Gal(\overline{K}/K), Isom(E))$*
2. *La classe de cohomologia $\{\xi\}$ ve determinada per la classe de $K-isomorfisme$ de B', independentment de l'elecció de ϕ. Obtenim una aplicació natural:*

$$Twists(B|_K) \to H^1(Gal(\overline{K}/K), Isom(E))$$

3. *L'aplicació definida en l'apartat anterior és una bijecció, és a dir, els twists de $B|_K$, llevat de $K-isomorfisme$, estan en correspondència bijectiva amb els elements de $H^1(Gal(\overline{K}/K), Isom(B))$.*

Per a una prova de l'anterior resultat un pot consultar [35] cap.12 §2.
En la nostra situació, al nostre *egal* li correspon un twist de E_1 i, per tant, una corba el·líptica E definida sobre K i un isomorfisme definit sobre $\overline{K}$, $\lambda : E \to E_1$ tal que $egal(\delta) = \lambda^\delta \circ \lambda^{-1}$ per a tot $\delta \in Gal(\overline{K}/K)$. Considerem la composició $\varphi = \lambda^{-1} \circ \varphi_1 : C \to E$. φ és una aplicació de grau 2 i observem que

$$(\lambda^{-1} \circ \varphi_1)^\delta = (\lambda^{-1})^\delta \circ egal(\delta) \circ \varphi_1 = (\lambda^{-1})^\delta \circ \lambda^\delta \circ \lambda^{-1} \circ \varphi_1$$

i per tant obtenim $\varphi : C \to E$ tot definit sobre K, tal i com volíem demostrar. □

Si C és una corba complexa no singular i projectiva (és a dir completa), anem a preguntar-nos sobre els seus punts $\mathbb{Q}$-racionals, o millor, els seus punts K-racionals, on K és un cos de nombres. Observem, és clar, que $\#C(\overline{\mathbb{Q}}) = \infty$.

Teorema 2.13 (Faltings). *Si el gènere de C és mes gran o igual que 2 i K és un cos de nombres, llavors el nombre de punts K-racionals és finit.*

Per una prova podeu consultar [15].
Per tant, fixat un cos de nombres L sempre el conjunt dels punts L-racionals és finit per una corba llisa C definida sobre un cos de nombres K. Ens plantegem la següent qüestió: fixem un natural d i considerem el conjunt:

$$\Gamma_d(C, L) = \{P \in C(F) | [F : L] \leq d\}$$

on F recorre totes les possibles extensions de grau inferior a d respecte del cos L. Anem a estudiar com és $\#\Gamma_d(C, L)$.

Teorema 2.14 (Abramovich-Harris). *Sigui C corba llisa definida sobre K. Pel cas $d = 2, 3$ i $d = 4$ amb gènere de C diferent de 7, es té:*
$\#\Gamma_d(C, L) = \infty$ per alguna extensió $L|K$ finita si i només si C admet un morfisme $f : C \to \mathbb{P}^1$ o $f : C \to E$ amb $deg(f) \leq d$.

Per la prova de l'anterior resultat podeu consultar [1].
No obstant anem a explicitar un xic l'anterior resultat per a $d = 2$. Per a la prova caldrà utilitzar el celebrat resultat de Faltings

Teorema (Faltings). *Sigui X una subvarietat d'una varietat abeliana definida sobre un cos de nombres K, aleshores existeix un numero finit de punts racionals $P_i \in K$ i subvarietats abelianes $B_i \subset A$ tal que $X(K) = \cup P_i + B_i(K)$.*

Per a una prova de l'anterior resultat veieu [12].

Demostració. (Cas d=2). Veiem que $\#\Gamma_2(C, L) = \infty$ per a tota extensió finita de $K \iff C$ és hiperel·líptica o biel·líptica.
$\Leftarrow$) Es obvi si C és hiperel·líptica. En el cas de ser biel·líptica sols cal observar que per a $E|L$ existeix una extensió finita L' on $\#E(L') = \infty$.
$\Rightarrow$) Si C no és ni hiperel·líptica ni biel·líptica veurem que $\#\Gamma_2(C, L) < \infty$ per a tota extensió finita L de K. Fixem un L. Si $\Gamma_2(C, L) = \emptyset$ ja estem; en cas contrari, sigui $P \in \Gamma_2(C, L)$ i sigui P' el conjugat respecte de la extensió $\overline{L}|L$. Definim

$$\phi^{(2)} : S^2C \to Jac(C)$$

$$q_1 + q_2 \mapsto [q_1 + q_2 - P - P']$$

Per ser C no hiperel·líptica $\phi^{(2)}$ és injectiva , a més, l'aplicació està definida sobre L. Pel teorema de Faltings tenim que $W_2(L) = Im(\phi^{(2)})(L)$ es pot escriure com

$$W_2(L) = \cup P_i + B_i(L)$$

on les B_i són subvarietats abelianes de dimensió menor o igual a 1; però com que C no és biel·líptica ni hiperel·líptica, S^2C no conté ni corbes el·líptiques ni rectes projectives. Així de $S^2C \cong W_2$ tenim $B_i(L) = \emptyset$ i $\#W_2(L) < \infty$. Aleshores podem definir l'aplicació:

$$\Gamma_2(C, L) \to S^2C(L)$$

$$P \mapsto P + P'$$

que és 2 a 1, com a molt, i, per tant, obtenim que $\#\Gamma_2(C, L) < \infty$. □

Quan el gènere de C és més gran o igual a 6, utilitzant els resultats aritmètics obtenim que
$\#\Gamma_2(C, L) < \infty$ per a tota extensió $\iff$ C no és ni hiperel·líptica ni biel·líptica sobre K.
L'anterior resultat ens diu que el nombre de punts quadràtics sempre és finit per a tota corba ni hiperel·líptica ni biel·líptica.

Nota 2.15. *En la prova de l'anterior teorema d'Abramovich-Harris, de l'article [1], es prova que si el gènere de C és ≥ 3 llavors, si $W_2(C)$ conté una corba el·líptica definida sobre L i C no és hiperel·líptica, es pot definir un morfisme de grau 2 sobre L entre C i la corba el·líptica de $W_2(C)$.*

Tenim utilitzant l'anterior nota la següent versió més aritmètica:

Proposició 2.16. *Sigui C llisa definida sobre K de gènere ≥ 3. Llavors $\#\Gamma_2(C, K) = \infty$ si i només si C és hiperel·líptica o biel·líptica sobre K a una corba el·líptica E amb $rank_K(E) > 0$.*

Demostració. $\Leftarrow$) obvi.$\Rightarrow$) Raonant igual que en la prova anterior obtenim una corba el·líptica en $W_2(K)$ amb $rank_K(E) > 0$ i així un morfisme de grau 2 a 1, de C a E, tot definit sobre K. □

Podem aplicar els anteriors resultats a les corbes modulars X_Γ, on Γ és un grup fuchsià de primera espècie. Sigui K el cos de definició d'aquest Γ. Llavors

Corol·lari 2.17. *Si X_Γ no és ni biel·líptica ni hiperel·líptica $\#\Gamma_2(X_\Gamma, L) < \infty$, per a tota L extensió algebraica finita de K.*
A més, si X_Γ és biel·líptica a una corba el·líptica E amb $rank_L(E) = 0$, on L és una extensió finita de K, s'obté també que $\#\Gamma_2(X_\Gamma, L) < \infty$.
En particular, quan $\Gamma = \Gamma_0(N)$ podem prendre $K = \mathbb{Q}$.

Demostració. Sols cal fer notar que pels grups modulars es donen models definits sobre un cos K que està caracteritzat en [37] i en el cas particular indicat es comprova que és $\mathbb{Q}$ (consultar el capítol 7 §3 de l'esmentada referència). □

Capítol 3

El grup d'automorfismes de $X_0(N)$

3.1 El normalitzador de $\Gamma_0(N)$

El fet d'interessar-nos en l'estudi del normalitzador de $\Gamma_0(N)$ en $SL_2(\mathbb{R})$ és degut a que si $\gamma \in SL_2(\mathbb{R})$ hi pertany llavors

$$\gamma\beta_1\tau = \beta_2\gamma\tau$$

on $\beta_1, \beta_2 \in \Gamma_0(N)$ i, per tant, ens defineix un element de $Aut(Y_0(N))$ on $Y_0(N) = \mathbb{H}/\Gamma_0(N)$, que s'estén de manera única a un element de $Aut(X_0(N))$, per l'acció a les puntes de $X_0(N)$.

Denotarem per $Norm(\Gamma_0(N))$ el normalitzador de $\Gamma_0(N)$ en $SL_2(\mathbb{R})$.

El teorema principal d'aquesta secció és el següent:

Teorema 3.1.1 (Newman). *Considerem $N = \sigma^2 q$ amb q lliure de quadrats, $\sigma, q \in \mathbb{N}$. Sigui $\upsilon := \upsilon(N) = (\sigma, \epsilon)$, on $\epsilon = mcd(a-d)$ i a, d són enters recorrent el conjunt $\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0(N)$. Aleshores,*
$M \in Norm(\Gamma_0(N))$ si i només si M és de la següent forma:

$$\sqrt{\delta}\begin{pmatrix} r\Delta & \frac{u}{\upsilon\delta\Delta} \\ \frac{sN}{\upsilon\delta\Delta} & l\Delta \end{pmatrix}$$

amb $r, u, s, l \in \mathbb{Z}$ i $\delta | q$, $\Delta | \frac{\sigma}{\upsilon}$.

Anem a demostrar l'anterior resultat; per això necessitem alguns previs. Es demostra en [28] que si $H \leq SL_2(\mathbb{Z})$ que compleix $\Gamma_0(N) \leq H$ llavors $H = \Gamma_0(M)$ amb $M|N$. Això prova:

Lema 3.1.2. *El normalitzador de* $\Gamma_0(N)$ *en* $SL_2(\mathbb{Z})$ *és* $\Gamma_0(N/\Psi)$.

Anem a fer un estudi del valor de Ψ.

Lema 3.1.3.

$$\Psi = \upsilon(N) = 2^{\mu}3^{w}$$

amb $\mu = min(3, [\frac{1}{2}\upsilon_2(N)])$ *i* $w = min(1, [\frac{1}{2}\upsilon_3(N)])$.

Demostració. Denotem $W = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ i $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, com que $W^{\frac{N}{\Psi}} \in \Gamma_0(\frac{N}{\Psi})$ tenim que $W^{-\frac{N}{\Psi}}TW^{\frac{N}{\Psi}} \in \Gamma_0(N)$, d'on $\frac{N}{\sigma\Psi} \equiv 0(mod\ q)$ i, per tant, $\Psi|\sigma$. Veiem tot seguit que $\upsilon = \upsilon(N)|\Psi$. Efectivament, si denotem un element arbitrari de $\Gamma_0(N)$ per $A = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix}$ es prova que $W^{-\frac{N}{\upsilon(N)}}AW^{\frac{N}{\upsilon(N)}} \in \Gamma_0(N)$ i així $\upsilon(N)|\Psi$. Tot seguit observem que, triant en A $c = 1$ i $d = k$ amb $(k, N) = 1$, de $W^{-\frac{N}{\Psi}}AW^{\frac{N}{\Psi}} \in \Gamma_0(N)$ s'obté que $\Psi|(k^2 - 1)$ i d'aquí es dedueix fàcilment que $\Psi|2^{\mu}3$. En efecte, per a N senar prenem $k = 2$ i per a N parell posem $N = 2^{\upsilon_2(N)}N_1$, triem λ tal que $\lambda N_1 \equiv -1(mod\ 2^{\upsilon_2(N)})$ i prenem $k = \lambda N_1 - 2$.
Finalment un senzill argument utilitzant valoracions ens permet provar que $\Psi = \upsilon(N) = 2^{\mu}3^{\omega}$. Per exemple, quan $N \equiv 0(mod\ 9)$, $3|\sigma$ per a $A \in \Gamma_0(N)$ tenim $ad \equiv 1(mod\ 3)$ on $3|(d - a)$ i, per tant, $3|\Psi$. Els altres casos es desenvolupen de manera semblant. □

Anem a demostrar el teorema.

Demostració. [Teorema] Denotem per $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \iota \end{pmatrix}$ un element del normalitzador. Llavors $MTM^{-1} = \begin{pmatrix} 1 - \alpha\gamma & \alpha^2 \\ -\gamma^2 & 1 + \alpha\gamma \end{pmatrix} \in \Gamma_0(N)$ i

$$M \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} M^{-1} = \begin{pmatrix} 1 + N\beta\iota & -N\beta^2 \\ N\iota^2 & 1 - N\beta\iota \end{pmatrix}$$

Veiem que podem escriure $M = \sqrt{\delta}\begin{pmatrix} R & \frac{U}{\delta\sigma} \\ \frac{S\sigma q}{\delta} & V \end{pmatrix}$, on recordem que $\delta|q$ i $det(M) = 1$. Per a veure això utilitzem les expressions anteriors que permeten posar $\alpha, \beta, \iota, \gamma$ de la següent manera: $\alpha = \underline{u}\sqrt{\frac{q}{\Omega'}}$; $\beta = \frac{u}{\sigma}\sqrt{\frac{q}{t'}}$; $\iota = s\sqrt{\frac{q}{t'}}$ i $\gamma = \sigma q v\sqrt{\frac{\Omega'}{q}}$. De $det(M) = 1$ obtenim que $t' = \Omega'$ i utilitzant, a més, que $\alpha^2 \in \mathbb{Z}$ i $\iota^2 \in \mathbb{Z}$ i que $det(M) = 1$ obtenim que $t'|q$ d'on s'obté el resultat.

Tot seguit observem el següent:
M és del normalitzador si i només si $\forall A \in \Gamma_0(N)$: $MAM^{-1} \in \Gamma_0(N)$, és a

dir, si i només si $(a-d)RU \equiv (a-d)SV \equiv 0(mod\ \sigma)\ \forall A \in \Gamma_0(N)$. Llavors notant $\epsilon = mcd(a-d)$ tenim $RU \equiv SV \equiv 0(mod\ \frac{\sigma}{\upsilon})$ i d'aquí podem escriure $R = r\Delta$, $V = l\Delta$, amb $r, l \in \mathbb{Z}$ i Δ tal que $\Delta|\frac{\sigma}{\upsilon}$. Així podem escriure $\frac{SN}{\sigma\delta} = \frac{sN}{\delta\upsilon\Delta}$ i $\frac{U}{\delta\sigma} = \frac{u}{\delta\Delta\upsilon}$ on $s, u \in \mathbb{Z}$ i obtenim la fórmula per a la matriu M com en l'enunciat del teorema. □

Anem tot seguit a caracteritzar el normalitzador anterior com a grup mitjançant generadors i relacions, és a dir, anem a estudiar el grup quocient $Norm(\Gamma_0(N))/\Gamma_0(N)$.
Abans, però observem que si $M \in Norm(\Gamma_0(N))$ i ϑ_M és l'element dins $Aut(X_0(N))$ que defineix, llavors rM, amb $r \in \mathbb{R}$, defineix el mateix automorfisme. Per tant, el que ens interessa estudiar és el normalitzador en $\mathbb{P}GL_2^+(\mathbb{R})$ que és el mateix que el $\mathbb{P}GL_2^+(\mathbb{Q})$ pel fet de ser $\mathbb{Q}$ dens en $\mathbb{R}$; i és clar que aquest normalitzador mòdul constant coincideix amb el de $SL_2(\mathbb{R})$. Anem doncs a definir els elements que generen les classes laterals $(Norm(\Gamma_0(N)) : \Gamma_0(N))$ i a fer un comentari sobre la seva estructura.

Definició 3.1.4. *Fixem N. Per a cada divisor m' de N amb $(m', N/m') = 1$ es defineix la involució d'Atkin-Lehner $w_{m'}$ com:*

$$w_{m'} = \begin{pmatrix} m'a & b \\ Nc & m'd \end{pmatrix}$$

on $m'ad - \frac{N}{m'}bc = 1$. (Igualment anomenarem involució d'Atkin-Lehner a tota matriu que sigui escalar a la anterior ja que defineix el mateix element en $Aut(X_0(N))$).

Anem a veure que les involucions d'Atkin-Lehner generen tot el grup $Norm(\Gamma_0(N))/\Gamma_0(N)$ pel cas de $\upsilon(N) = 1$, és a dir, pel cas que $4 \nmid N$ i $9 \nmid N$. En efecte, sigui $M \in Norm(\Gamma_0(N))$ i posem $M = \frac{1}{\sqrt{\delta}}\begin{pmatrix} \delta r\Delta & \frac{u}{\Delta} \\ \frac{sN}{\Delta} & \upsilon\Delta\delta \end{pmatrix} = \frac{1}{\Delta\sqrt{\delta}}\begin{pmatrix} \delta r\Delta^2 & u \\ sN & \upsilon\delta\Delta^2 \end{pmatrix}$. Observem que si $(\delta\Delta^2, \frac{N}{\delta\Delta^2}) = 1$, M és la involució d'Atkin-Lehner $w_{\delta\Delta^2}$; però és clar que $(\delta\Delta^2, \frac{N}{\delta\Delta^2}) = 1$ per tenir M determinant 1. Per tant, obtenim que tot element del normalitzador es correspon amb una involució d'Atkin-Lehner. És senzill de comprovar que aquestes involucions d'Atkin-Lehner commuten entre elles i $w_{m'}w_{m''} = w_{m'm''}$ (si $(m', m'') = 1$). Així pel cas $\upsilon(N) = 1$:

$$Norm(\Gamma_0(N))/\Gamma_0(N) \cong \prod_{i=1}^{\pi(N)} \mathbb{Z}/2\mathbb{Z}$$

on $\pi(N) = \{\#primers\ complint\ p|N\}$.
Pel cas de $\upsilon(N) > 1$ apareixen nous elements en $Norm(\Gamma_0(N))$ del fet que $\upsilon(N)$ divideix alguns coeficients de M. Anem a explicitar-ne alguns de concrets.

Definició 3.1.5. *Definim* $S_{\upsilon'} = \begin{pmatrix} 1 & \frac{1}{\upsilon'} \\ 0 & 1 \end{pmatrix}$

A la literatura s'hi troba la següent caracterització del grup quocient $Norm(\Gamma_0(N))/\Gamma_0(N)$, que s'enuncia sense cap prova.

Teorema 3.1.6 (Atkin-Lehner,[4],pag158). *El normalitzador de* $\Gamma_0(N)$ *en* $\mathbb{P}GL_2^+(\mathbb{R})$ *és el producte directe dels grups següents:*

1. $\{w_q\}$ *per cada* q *primer,* $q \geq 5$ $q \mid N$.
2. (a) *Si* $\upsilon_3(N) = 0$, $\{1\}$
   (b) *Si* $\upsilon_3(N) = 1$, $\{w_3\}$
   (c) *Si* $\upsilon_3(N) = 2$, $\{w_9, S_3\}$; *complint* $w_9^2 = S_3^3 = (w_9 S_3)^3 = 1$ *(factor d'ordre 12)*
   (d) *Si* $\upsilon_3(N) \geq 3$; $\{w_{3^{\upsilon_3(N)}}, S_3\}$; *on* $w_{3^{\upsilon_3(N)}}^2 = S_3^3 = 1$ *i* $w_{3^{\upsilon_3(N)}} S_3 w_{3^{\upsilon_3(N)}}$ *commuta amb* S_3 *(factor del grup amb 18 elements)*
3. *Sigui* $\lambda = \upsilon_2(N)$ *i* $\mu = min(3, [\frac{\lambda}{2}])$ *i denotem per* $\upsilon'' = 2^\mu$ *llavors es té:*
   (a) *Si* $\lambda = 0$; $\{1\}$
   (b) *Si* $\lambda = 1$; $\{w_2\}$
   (c) *Si* $\lambda = 2\mu$; $\{w_{2^{\upsilon_2(N)}}, S_{\upsilon''}\}$ *amb les relacions* $w_{2^{\upsilon_2(N)}}^2 = S_{\upsilon''}^{\upsilon''} = (w_{2^{\upsilon_2(N)}} S_{\upsilon''})^3 = 1$, *d'on té ordres 6,24, i 96 per a* $\upsilon = 2, 4, 8$ *respectivament. (Cal fer notar que pel cas 8 les relacions no defineixen totalment aquest factor del grup).*
   (d) *Si* $\lambda > 2\mu$; $\{ w_{2^{\upsilon_2(N)}}, S_{\upsilon''}\}$; $w_{2^{\upsilon_2(N)}}^2 = S_{\upsilon''}^{\upsilon''} = 1$. *A més,* $S_{\upsilon''}$ *commuta amb* $w_{2^{\upsilon_2(N)}} S_{\upsilon''} w_{2^{\upsilon_2(N)}}$ *(factor del grup amb ordre* $2\upsilon''^2$*).*

Teorema 3.1.7. *L'anterior enunciat d'Atkin-Lehner és fals en general.*

Demostració. Considerem la corba modular $X_0(48)$ i suposem veritat l'anterior resultat. Així obtenim que $Norm(\Gamma_0(48))/\Gamma_0(48) \cong \mathbb{Z}/2 \times \mathcal{S}_4$. Com que $Z(\mathcal{S}_4)) = 1$ (centre de $\mathcal{S}_4$), $X_0(48)$ és una corba hiperel·líptica i la involució hiperel·líptica es troba en el seu centre, aquesta hauria de ser del tipus d'Atkin-Lehner, però precisament a [30] es veu que la involució hiperel·líptica no és del tipus d'Atkin-Lehner. □

El problema en $X_0(48)$ recau en el fet que la involució w_3 no commuta amb l'automorfisme S_4 i, per tant, el producte no pot ser directe.

Pregunta 3.1.8. *És cert el teorema d'Atkin-Lehner sota la hipòtesi addicional que les involucions d'Atkin-Lehner $w_{p^{v_p(N)}}$ commutin amb S_3, si $(p,3)=1$, i amb $S_{2^{v''}}$ si $(p,2)=1$, sempre i quan S_3 i $S_{2^{v''}}$ tinguin sentit?*

Hem vist que l'anterior resposta és afirmativa quan no tenim automorfismes de la forma $S_{v'}$ per algun v'. És el cas del producte de les involucions d'Atkin-Lehner. Anem a estudiar-ho en certs casos particulars que ens seran de gran interès. En aquests casos la resposta a la pregunta és afirmativa.

Lema 3.1.9. *Si $4|N$ llavors la involució S_2 commuta amb totes les involucions d'Atkin-Lehner w_m amb $(m,2)=1$ i amb tots el altres S_i.*

Demostració. Sol cal observar que si denotem per $w_m = \frac{1}{\sqrt{m}} \begin{pmatrix} mk & 1 \\ Nt & m \end{pmatrix}$ s'obté que

$$w_m S_2 w_m S_2 = \begin{pmatrix} \frac{2mk^2+2Nt+mkNt}{2m} & \frac{(2+2m)(2m+2mk+Nt)}{4m} \\ \frac{Nt(2m+2mk+Nt)}{2m} & m+Nt+\frac{Nt}{m}+\frac{kNt}{2}+\frac{Nt^2}{4m} \end{pmatrix}$$

De $(m,2)=1$ i $4|N$ veiem que l'anterior expressió és de $\Gamma_0(N)$. □

3.1.1 Un estudi per a $\upsilon(N)=2$

Al llarg d'aquesta subsecció considerarem N de la forma $N = 2^{\upsilon_2(N)} \prod p_i^{n_i}$, p_i primers diferents, amb $\upsilon(N)=2$, és a dir $\upsilon_2(N) \leq 3$, i $\upsilon_3(N) \leq 1$.

Proposició 3.1.10. *Sigui $N = 2^{\upsilon_2(N)} \prod_i p_i^{n_i}$ amb p_i primers diferents, amb $\upsilon_2(N) \leq 3$ i $\upsilon_3(N) \leq 1$. Llavors el teorema 3.1.6 és correcte.*

Anem a provar l'anterior resultat.

Lema 3.1.11. *Sigui $u \in Norm(\Gamma_0(N))$ i escrivim-lo:*

$$u = \frac{1}{\sqrt{\delta\Delta^2}} \begin{pmatrix} \Delta^2\delta r & \frac{u}{2} \\ \frac{sN}{2} & l\Delta^2\delta \end{pmatrix}$$

d'acord amb les notacions del teorema 3.1.1(Newman)
Llavors:
si $(\delta,2)=1$,

$$w_{\Delta^2\delta} u = \begin{pmatrix} r' & \frac{u'}{2} \\ \frac{s'N}{2} & v' \end{pmatrix}$$

i si $(\delta, 2) = 2$ *llavors s'obté*

$$w_{\Delta^2 \frac{\delta}{2}} u = \frac{1}{\sqrt{2}} \begin{pmatrix} 2r'' & \frac{u''}{2} \\ \frac{s''N}{2} & 2v'' \end{pmatrix}$$

La prova és una simple comprovació. Anem doncs a estudiar com són tots els elements diferents del tipus

$$a(r', u', s', v') = \begin{pmatrix} r' & \frac{u'}{2} \\ \frac{s'N}{2} & v' \end{pmatrix}$$

$$b(r'', u'', s'', v'') = \frac{1}{\sqrt{2}} \begin{pmatrix} 2r'' & \frac{u''}{2} \\ \frac{s''N}{2} & 2v'' \end{pmatrix}.$$

Notem que b únicament es dona si $N \equiv 0(8)$.

Lema 3.1.12. *Pel cas* $N \equiv 4(mod\ 8)$ *tots els elements del normalitzador que són del tipus* $a(r', u', s', v')$ *corresponen a algun element del grup* $\{S_2, w_4 | S_2^2 = w_4^2 = (w_4 S_2)^3 = 1\}$ *(grup amb 6 elements).*

Demostració. Es desprèn directament de les següents igualtats:

$$a(r', u', s', v') \in \Gamma_0(N) \Leftrightarrow s' \equiv u' \equiv 0(mod\ 2)$$

$$a(r', u', s', v')S_2 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv\ u' \equiv 1\ s' \equiv 0(mod\ 2)$$
$$a(r', u', s', v')w_4 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv 0\ u' \equiv s' \equiv 1(mod\ 2)$$
$$a(r', u', s', v')w_4 S_2 \in \Gamma_0(N) \Leftrightarrow r' \equiv u' \equiv s' \equiv 1\ v' \equiv 0(mod\ 2)$$
$$a(r', u', s', v')S_2 w_4 \in \Gamma_0(N) \Leftrightarrow v' \equiv u' \equiv s' \equiv 1\ r' \equiv 0(mod\ 2)$$
$$a(r', u', s', v')S_2 w_4 S_2 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv s' \equiv 1\ u' \equiv 0(mod\ 2)$$

□

Lema 3.1.13. *Sigui* N *amb* $\upsilon_2(N) = 3$*. Llavors tots els elements de la forma* $a(r', u', s', v')$ *i* $b(r'', u'', s'', v'')$ *corresponen a algun element del grup de 8 elements*

$$\{S_2, w_8 | S_2^2 = w_8^2 = 1, S_2 w_8 S_2 w_8 = w_8 S_2 w_8 S_2\}$$

Demostració. Directament de les següents igualtats:

$$a(r', u', s', v') \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv 1, u' \equiv s' \equiv 0(mod\ 2)$$

$$a(r', u', s', v')S_2 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv u' \equiv 1, s' \equiv 0(mod\ 2)$$

$$a(r',u',s',v')w_8S_2w_8 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv s' \equiv 1, u' \equiv 0(mod\ 2)$$
$$a(r',u',s',v')S_2w_8S_2w_8 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv s' \equiv v' \equiv 1(mod\ 2)$$
$$b(r'',u'',s'',v'')w_8 \in \Gamma_0(N) \Leftrightarrow r'' \equiv v'' \equiv 0, u'' \equiv s'' \equiv 1(mod\ 2)$$
$$b(r'',u'',s'',v'')S_2w_8S_2 \in \Gamma_0(N) \Leftrightarrow r'' \equiv v'' \equiv u'' \equiv s'' \equiv 1(mod\ 2)$$
$$b(r'',u'',s'',v'')S_2w_8 \in \Gamma_0(N) \Leftrightarrow r'' \equiv 0, u'' \equiv s'' \equiv v'' \equiv 1(mod\ 2)$$
$$b(r'',u'',s'',v'')w_8S_2 \in \Gamma_0(N) \Leftrightarrow v'' \equiv 0, u'' \equiv s'' \equiv r'' \equiv 1(mod\ 2)$$

□

Demostració. [Proposició] Sigui doncs $N = 2^{\upsilon_2(N))}\prod_i p_i$, amb els p_i primers diferents. Sigui $u \in Norm(\Gamma_0(N))$. Si $\upsilon_2(N) \leq 1$ ja està vist. Considerem doncs $\upsilon_2(N) = 2$. Llavors, pels lemes 3.1.11 i 3.1.12, $w_\delta u = \alpha$, $\alpha \in \{S_2, w_4 | S_2^2 = w_4^2 = (w_4S_2)^3 = 1$ i d'aquí $u = w_\delta\alpha$. Com que w_δ $((\delta, 2) = 1)$ commuta amb S_2 i les involucions d'Atkin-Lehner commuten també hem acabat. El cas $8||N$ es prova utilitzant el mateix argument que pel cas $4||N$ i els lemes 3.1.11 i 3.1.13. □

3.1.2 Un estudi per a $\upsilon(N) = 3$ i $N \equiv 9(mod\ 27)$

Anem a fer un estudi de la veracitat del teorema 3.1.6 pels N complint $N = 9\prod_i p_i$ amb p_i primers diferents coprimers amb 3, en tota aquesta subsecció.

Proposició 3.1.14. *Sigui N com abans i suposem que algun p_i compleix $p_i \equiv -1(mod\ 3)$. Llavors el grup $Norm(\Gamma_0(N))/\Gamma_0(N)$ no és producte directe dels factors explicitats en el teorema 3.1.6.*

Demostració. Es suficient veure que S_3 no commuta amb w_{p_i} si $p_i \equiv -1(mod\ 3)$. En efecte, si escrivim $w_{p_i} = \frac{1}{\sqrt{p_i}}\begin{pmatrix} p_ik & 1 \\ Nt & p_i \end{pmatrix}$:

$$w_{p_i}S_3w_{p_i}S_3^2 = \frac{1}{p_i}\begin{pmatrix} (p_ik)^2 + Nt(1+\frac{p_ik}{3}) & p_ik(\frac{2p_ik}{3}+1) + (\frac{p_ik}{3}+1)(\frac{2Nt}{3}+p_i) \\ Nt(p_ik) + Nt(\frac{Nt}{3}+p_i) & Nt(\frac{2p_ik}{3}+1) + p_i(\frac{Nt}{3}+p_i)(\frac{2Nt}{3}+p_i) \end{pmatrix}$$

Per què l'anterior expressió sigui de $\Gamma_0(N)$ s'ha de complir que $\frac{2k^2p_i}{3} + \frac{p_ik}{3} \in \mathbb{Z}$ com $p_i \equiv 1\ o\ -1(mod\ 3)$ i així $k \equiv 1(mod\ 3)$. Del fet que $det(w_p) = 1$ tenim que $p_ik \equiv 1(mod\ 3)$ i, per tant, $p_i \equiv 1(mod\ 3)$. □

Nota 3.1.15. *De la prova anterior es desprèn que pels $N = 9\prod_i p_i$, p_i primers diferents $(p_i, 3) = 1$, w_{p_i} commuta amb S_3 si i només si per a cada p_i es compleix $p_i \equiv 1(mod\ 3)$ $(p_i \equiv 1(mod\ 3)\ \forall i)$.*

Proposició 3.1.16. *Pels $N = 9\prod_i p_i = 9q$ amb p_i primers diferents $(p_i, 3) = 1$ i $p_i \equiv 1(mod\ 3)$, el teorema 3.1.6 és vàlid.*

Demostració. Considerem w un element arbitrari de $Norm(\Gamma_0(N))$. Seguint la notació del teorema 2.1.1. tenim $\Delta = 1$ i $v(N) = 3$; llavors

$$w = \frac{1}{\sqrt{\delta}} \begin{pmatrix} \delta r & \frac{u}{3} \\ \frac{Ns}{3} & \delta v \end{pmatrix}$$

on $\delta | \prod_j p_j$. A més,

$$w_\delta w = \begin{pmatrix} r' & \frac{u'}{3} \\ \frac{Nt'}{3} & v' \end{pmatrix} \in Norm(\Gamma_0(N))$$

Denotem per $a(r', u', t', v')$ la matriu que surt de l'anterior expressió. Llavors s'obté:

$$a(r', u', t', v') \in \Gamma_0(N) \Leftrightarrow t' \equiv u' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')w_9 \in \Gamma_0(N) \Leftrightarrow r' \equiv v' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')S_3 \in \Gamma_0(N) \Leftrightarrow r' + u' \equiv t' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')S_3^2 \in \Gamma_0(N) \Leftrightarrow 2r' + u' \equiv t' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')S_3w_9 \in \Gamma_0(N) \Leftrightarrow r' \equiv qt' + v' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')S_3^2w_9 \in \Gamma_0(N) \Leftrightarrow r' \equiv 2qt' + v' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')w_9S_3^2 \in \Gamma_0(N) \Leftrightarrow r' + u' \equiv v' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')w_9S_3 \in \Gamma_0(N) \Leftrightarrow r' + 2u' \equiv v' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')w_9S_3^2w_9 \in \Gamma_0(N) \Leftrightarrow u' \equiv qt' + v' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')S_3^2w_9S_3^2 \in \Gamma_0(N) \Leftrightarrow u' \equiv 2qt' + v' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')S_3^2w_9S_3 \in \Gamma_0(N) \Leftrightarrow r' + u' \equiv 2t'q + v' \equiv 0(mod\ 3)$$

$$a(r', u', t', v')S_3w_9S_3^2 \in \Gamma_0(N) \Leftrightarrow 2r' + u' \equiv qt' + v' \equiv 0(mod\ 3)$$

□

Corol·lari 3.1.17. *Sigui $N = 9q$. Llavors, α s'escriu de la forma $\alpha = w_{q'}\beta$ on $q'|q$ i $\beta \in \{S_3, w_9 | s_3^3 = w_9^2 = (w_9S_3)^3 = 1\}$.*

Demostració. És realment el que es prova en la proposició anterior. □

3.2 El grup $Aut(X_0(N))$

Considerem $X_0(N)$ la corba modular definida sobre $\mathbb{Q}$ ([37] cap 7). Estudiem aquí, però, la corba $X_0(N)(\mathbb{C})$ i el seu grup d'automorfismes que denotem per $Aut(X_0(N))$.
Recordem que si C és una corba de gènere 0 o 1, llavors $\#Aut(C) = \infty$. Per tant, centrem-nos en el cas de gènere més gran que 1. En general, coneixem la següent fita:

$$\#Aut(C) \leq 84(g-1)$$

on $g = gènere(C) \geq 2$.
El resultat més rellevant d'aquesta secció és el següent:

Teorema 3.2.1 (Kenku-Momose,[21]). *Per a les corbes modulars $X_0(N)$ amb gènere més gran o igual que dos es té*

$$Aut(X_0(N)) = Norm(\Gamma_0(N))$$

si $N \neq 37, 63$.

Anem a examinar d'aquest resultat en un cas concret i donar una ullada al cas general. La idea de la prova de l'anterior resultat passa per l'estudi de la $Jac(X_0(N))$.

Lema 3.2.2. *Es té la inclusió natural $Aut(X_0(N)) \subset Aut(Jac(X_0(N)))$*

Anem a fer un estudi del grup $Aut(X_0(N))$ amb N primer.

Teorema 3.2.3 (Ribet,[33]). *Pel cas N primer tot $\upsilon \in End(Jac(X_0(N)))$ està definit sobre $\mathbb{Q}$.*

Estudiem doncs com són els factors $\mathbb{Q}$-simples de $Jac(X_0(N))$. En els resultats que segueixen N no cal que sigui necessàriament un nombre primer. Considerem l'àlgebra de Hecke $\mathbb{Q}[T_m]_{(m,N)=1}$, $\mathbb{Q}$-àlgebra commutativa de dimensió g sobre $\mathbb{Q}$ (veure [37] cap3).

Teorema 3.2.4 (Atkin-Lehner). *$S_2(\Gamma_0(N))$ ve generat per vectors propis respecte de tota l'àlgebra de Hecke $\mathbb{Q}[T_m]_{(m,N)=1}$*

(Per a la prova consulteu [4]).
Si f és una forma nova de $S_2(\Gamma_0(M))$ per algun M i normalitzada (i.e. si escrivim $f = \sum a_n q^n$ amb $a_1 = 1$) anomenem M el nivell de f i denotem per K_f el cos $K_f := \mathbb{Q}(\{a_n\})$ (recordem que nova vol dir que és vector propi dels operadors de Hecke T_p amb $(p, M) = 1$ i, a més, és ortogonal respecte del producte de Petersson al subespai generat per les formes $g \in S_2(\Gamma_0(D))$ amb $D|M$ $D \neq M$ i $g(e\tau)$, on e varia entre els divisors positius de M/D).

Proposició 3.2.5. *El cos K_f és un cos de nombres totalment real.*

En la situació anterior, per a cada immersió $\sigma : K_f \to \mathbb{C}$ posem $\sigma f = \sum a_n^\sigma q^n$ que és una forma nova també normalitzada de $S_2(\Gamma_0(M))$([37], cap 7).
Per a cada f forma cuspidal de pes 2, nova en el nivell que li correspon, denotat per $nivell(f)$, i per a cada divisor positiu d complint $d|\frac{N}{nivell(f)}$ posem $f|_{B_d} = \sum a_n q^{dn} \in S_2(\Gamma_0(N))$, que té com valors propis a_n pels T_n amb $(n, N) = 1$, ([4]).

Lema 3.2.6. *$\{f|_{B_d}\}_{\{f,d_f\}}$ és una base de $S_2(\Gamma_0(N))$ formada per vectors propis de l'àlgebra de Hecke, on f recorre el conjunt de formes normalitzades noves de $nivell(f)|N$ i d_f recorre el conjunt de divisors positius de $N/nivell(f)$. Fem notar que tots els elements del subespai $\{f|_{B_d}\}_d$ amb f fixada tenen els mateixos valors propis.*

Teorema 3.2.7 (Shimura). *Sigui $f \in S_2(\Gamma_0(M))$ nova. Al conjunt $\{\sigma f\}$, on σ recorre totes les immersions de K_f en $\mathbb{C}$, li correspon un factor de la $Jac(X_0(M))$ sobre $\mathbb{Q}$, que denotem per $J_{\sigma f}$.*
A més, si $m(f)$ és el nombre de divisors positius de $N/nivell(f)$ llavors s'obté la següent descomposició de la jacobiana sobre $\mathbb{Q}$ en factors simples:

$$Jac(X_0(N)) \sim_{\mathbb{Q}} \prod_{\{\sigma f\}} J_{\{\sigma f\}}^{m(f)}$$

amb $dim(J_{\{\sigma f\}}) = [K_f : \mathbb{Q}]$ i $K_f = End(J_{\{\sigma f\}}) \otimes \mathbb{Q}$.

(Per a una prova de l'anterior resultat es pot consultar [38] i [37] cap 7.)

Teorema 3.2.8 (Congruència de Eichler-Shimura).

$$End(Jac(X_0(N))) \otimes \mathbb{Q} = \mathbb{Q}[T_m]_{(m,N)=1}$$

Després de les anteriors observacions generals retornem al cas N primer. Pel resultat de Ribet,

$$Aut(X_0(N)) \subset Aut(Jac(X_0(N))) \otimes \mathbb{Q}.$$

$\mathbb{Q}[T_m]_{(m,N)=1}$ és una àlgebra semisimple de dimensió g i $m(f) = 1$, llavors,

$$\mathbb{Q}[T_m]_{(m,N)=1} = K_1 \times \ldots \times K_n$$

on K_i són cossos totalment reals corresponent a σf_i i n és el nombre de factors $\mathbb{Q} - simples$ en els que es parteix $Jac(X_0(N))$. D'aquí s'obté:

$$Aut(X_0(N)) \subset \{\pm 1\} \times \ldots \times \{\pm 1\}$$

Per tant, si $u \in Aut(X_0(N))$ aleshores és d'ordre ≤ 2 i està definit sobre $\mathbb{Q}$. Estudiem a part el cas $N = 37$. $X_0(37)$ té gènere 2 i tenim dues diferencials noves $S_2(\Gamma_0(37))$. Així:

$$Aut(X_0(37)) \subset \{\pm 1\} \times \{\pm 1\}$$

Hi ha una involució $\upsilon \in Aut(X_0(37))$ (consultar [25]) que no és d'Atkin-Lehner, no porta puntes a puntes i és la involució hiperel·líptica de $X_0(37)$ ([30]); per tant

$$Aut(X_0(37)) \cong \frac{\mathbb{Z}}{2} \times \frac{\mathbb{Z}}{2}$$

utilitzant el teorema de Ribet.

Definició 3.2.9. *Anomenem $\upsilon \in Aut(X_0(N))$, amb $\upsilon \notin Norm(X_0(N))$, un element excepcional de $Aut(X_0(N))$.*

Pensem d'ara en endavant N primer, $N \neq 37$. Estudiem com és el grup $Aut(X_0(N))_\infty$; és a dir, els automorfismes que fixen la punta de l'infinit.

Lema 3.2.10. *Si $u \in Aut(X_0(N))_\infty$, llavors $u = id$.*

Demostració. Si $\Omega_{X_0(N)}$ denota l'espai de les diferencials regulars, és clar que l'acció de u en el cotangent té valors propis ± 1. Si tots valen -1 llavors $X_0(N)$ és hiperel·líptica i u la involució hiperel·líptica. Però Ogg (en [30]) va provar que si $X_0(N)$ és hiperel·líptica, $N \neq 37$, llavors $u = w_N$ i, per tant, no fixa la punta de l'infinit.
Escollim doncs dues diferencials $\omega_1, \omega_2 \in \Omega_{X_0(N)}$ complint

$$\omega_1 \circ u = \omega_1 \quad i \quad \omega_2 \circ u = -\omega_2$$

que siguin vectors propis de l'àlgebra de Hecke $\mathbb{Q}[T_m]_{(m,N)=1}$. Llavors si posem $\omega_i = (\sum_{s=1}^{\infty} a_{i,s} q^s) \frac{dq}{q}$ podem prendre, sense pèrdua de generalitat, $a_{1,1} = a_{2,1} = 1$. Considerant $\omega = \omega_1 + \omega_2$ tenim una diferencial que no s'anul·la en ∞ però $\omega \circ u = \omega_1 - \omega_2$ s'anul·la en ∞, en contra de la hipòtesi $u(\infty) = \infty$. Llavors, per força, tots els valors propis són $+1$ i, per tant, $u = id$. □

Teorema 3.2.11 (Mazur). *Si N és primer, $\frac{\mathbb{Z}}{n} \cong Jac(X_0(N))(\mathbb{Q})^{tors}$ i ve generat pel divisor $(0) - (\infty)$, on $n = numerador\left(\frac{N-1}{12}\right)$.*

(Per a la prova consulteu [24].)
Llavors, si $u \in Aut(X_0(N))$, com que es definit sobre $\mathbb{Q}$ actua sobre el divisor $(0) - (\infty)$ i per tant

$$(u(0)) - (u(\infty)) \sim m((0) - (\infty))$$

amb $m \in \mathbb{Z}/n$.

Teorema 3.2.12 (Mazur). *En la situació N primer les úniques possibilitats per a m són $m = \pm 1, 0, \pm\frac{1}{3}$.*

(Per a la prova veieu [24].)
Anem a aplicar-ho. $m = 0$ en la nostra situació no es pot donar ja que llavors $(0) - (\infty)$ seria un divisor principal, i el gènere de $X_0(N)$ zero. Si $m = \pm\frac{1}{3}$ llavors $(3, n) = 1$, i de $m^2 = 1$ tenim $1 \equiv 9(mod\ n)$ i es comprova que l'anterior congruència mai es produeix.
Per tant, $m = \pm 1$; si $m = 1$ llavors $(u0) + (\infty) \sim (0) + (u\infty)$ i pel lema podem pensar $u\infty \neq \infty$, d'on s'obté que $X_0(N)$ és hiperel·líptica i $u = w_N$. Si $m = -1$, $(u0) + (0) \sim (\infty) + (u\infty)$. Si $u\infty \neq 0$ llavors és hiperel·líptica i raonant igual que abans arribem a contradicció. Per tant, $u\infty = 0$ i $w_N \circ u \in Aut(X_0(N))_\infty$ d'on, pel lema, $u = w_N$, provant finalment:

Teorema 3.2.13 (Ogg). *Per a N primer, $N \neq 37$, $Aut(X_0(N)) = \{1, w_N\}$.*

Anem a fer l'estudi general. Per a l'estudi del cas N lliure de quadrats es pot consultar [31]. La prova en el cas general es troba en [21] utilitzant tècniques de [11].
El problema principal en el cas general és que no tenim un resultat de Ribet tant bo, i.e., no tot $End(Jac(X_0(N)))$ està definit sobre $\mathbb{Q}$ i per tant la congruència de Eichler-Shimura no és del tot útil.
Construu¨ im una nova descomposició de la jacobiana.

Definició 3.2.14. *Donada $f \in S_2(\Gamma_0(N))$ vector propi de tots els operadors de Hecke $\mathbb{Q}[T_m]_{(m,N)=1}$, s'anomena de multiplicació complexa si existeix un caràcter de Dirichlet λ d'un cos quadràtic imaginari $\mathbb{Q}(\sqrt{-D})$, de discriminant D, amb conductor $\mathfrak{r}$, que satisfà:*

$$\begin{array}{ccc} \lambda((\alpha)) = \alpha, & \alpha \in \mathbb{Q}(\sqrt{-D})^*, & \alpha \equiv 1(mod\ \mathfrak{r}) \\ \lambda((a)) = \left(\frac{-D}{a}\right) a, & a \in \mathbb{Z}, & (a, DNor(\mathfrak{r})) = 1 \end{array}$$

i f s'escriu com $f(z) = \sum_{\mathfrak{U}} \lambda(\mathfrak{U}) exp(2\pi i Nor(\mathfrak{U}) z)$, on $\mathfrak{U} \neq (0)$ recorre el conjunt de tots els ideals enters primers amb $\mathfrak{r}$.

Denotem per $V_C \otimes \mathbb{C}$ l'espai generat per les formes modulars amb multiplicació complexa, i $V_H \otimes \mathbb{C}$ l'espai generat per les formes modulars que no tenen multiplicació complexa; d'aquí obtenim una partició de l'espai cotangent de $Jac(X_0(N))$ i també de la pròpia $Jac(X_0(N))$ ([38])

Teorema 3.2.15 (Shimura). *$Jac(X_0(N)) \sim_{\mathbb{Q}} J_H \times J_C$ on J_H, J_C denoten els factors de la jacobiana que tenen per espais cotangents $V_H \otimes \mathbb{C}$ i $V_C \otimes \mathbb{C}$, respectivament.*
Llavors, $End(Jac(X_0(N)) \otimes \mathbb{Q} = End(J_C) \otimes \mathbb{Q} \times End(J_H) \otimes \mathbb{Q}$

Posem

$$k(N) = \left\{ \begin{array}{cc} \text{la composició dels} & \text{cossos quadràtics} \\ \text{amb discriminant } D & , D^2|N \end{array} \right\}$$

Proposició 3.2.16 (Kenku-Momose). *Tot $End(J_H)$ es definit sobre $k(N)$.*

$g_C = dim(J_C)$ i $g_H = dim(J_H)$

Lema 3.2.17. *Si gènere$(X_0(N)) > 1 + 2g_C$, llavors tot $u \in Aut(X_0(N))$ està definit sobre $k(N)$ i aquesta condició és compleix també si el gènere és superior a 1, per a tot N, $N \neq 2^6, 2^7, 2^8, 2^9, 3^4, 3^3 2, 3^3 2^2, 3^3 2^3$.*

Llavors, via un estudi de l'anell $End(J_C) \otimes \mathbb{Q}$ s'obté

Corol·lari 3.2.18. *Tot $v \in Aut(X_0(N))$ està definit sobre $k(N)$ amb $N \neq 2^8, 2^9, 2^2 3^3, 2^3 3^3$.*

Pel cas $N = 2^8, 2^9$ l'anterior resultat (Corol·lari 3.2.18) s'obté que el cos de definició és $k'(N)$, que denota el cos de classes de $\mathbb{Q}(\sqrt{-1})$ associat a $ker(\xi)$, on ξ és un caràcter del grup d'ideals de $\mathbb{Q}(\sqrt{-1})$ d'ordre 4 que satisfà $\xi((\alpha)) = 1$ si $\alpha \in \mathbb{Q}(\sqrt{-1})^*$ amb $\alpha \equiv 1(mod 8)$ i $\xi((\alpha)) = 1$ si $\alpha \in \mathbb{Z}$, $(\alpha, 2) = 1$; i pel cas $N = 2^2 3^3, 2^3 3^3$ és considera el caràcter $\xi \neq 1$ del grup d'ideals de $\mathbb{Q}(\sqrt{-3})$ complint $\xi((\alpha)) = 1$ si $\alpha \in \mathbb{Q}(\sqrt{-3})^*$ amb $\alpha \equiv 1(mod 6)$ i $\xi((\alpha)) = 1$ si $\alpha \in \mathbb{Z}$, $(\alpha, 6) = 1$. Així, tot $End(J_C)$ està definit a $k'(N)$, cos associat a $ker(\xi)$.
Anem, igual que en el cas N primer, a estudiar el grup $Aut(X_0(N))_\infty$

Lema 3.2.19. *Sigui $u \in Aut(X_0(N))_\infty$, una involució. Llavors $4|N$, u està definida sobre $\mathbb{Q}$ i no és la involució hiperel·líptica . (D'on, en particular, S_2 està definit sobre $\mathbb{Q}$).*

S'obté gràcies a aquest lema i l'estudi de $\mathcal{O}_{X_0(N),\infty}$:

Proposició 3.2.20 (Kenku-Momose). *$Aut(X_0(N))_\infty = Norm(\Gamma_0(N))_\infty$.*

Del fet que $Norm(\Gamma_0(N))$ actua transitivament sobre les puntes $k(N)$-racionals o $k'(N)$-racionals s'obté:

Proposició 3.2.21 (Kenku-Momose). *Sigui C una punta $k(N)$- racional o $k'(N)$-racional, segons correspongui; i $u \in Aut(X_0(N))$ on $u(C)$ n'és també una punta. Llavors $u \in Norm(X_0(N))$.*

Per a estudiar els automorfismes que no envien puntes a puntes, és a dir, els N tal que $Aut(X_0(N))$ conté elements excepcionals, ho farem per mitjà d'uns punts concrets de $Jac(X_0(N))$.
Considerem el divisor $(0)-(\infty)$, que també té ordre finit en el cas general ([23]). Fixem $u \in Aut(X_0(N))$ i considerem el divisor

$$D_l = \alpha_l((0)-(\infty))$$

on $\alpha_l = uT_l - T_l u^{\sigma_l}$, σ_l el Frobenius, $(l,N)=1$ i T_l l'operador de Hecke corresponent.
S'observa que $\alpha_l = 0$ en $Jac(X_0(N))$ d'on $D_l \sim 0$. Llavors, si $u \in Aut(X_0(N))$ i o bé $u(0)$ o bé $u(\infty)$ no és una punta, $D_l \neq 0$.

Proposició 3.2.22 (Kenku-Momose). *Si $N \neq 37, 2^8, 2^9, 2^2 3^3, 2^3 3^3$, $D_l \neq 0$, $l \geq 5$, llavors: $w_N * (D_l) \neq D_l$ i ni $u(0)$ ni $u(\infty)$ són punts fixos per w_N.*

Si denotem per $l(N)$ el primer més petit que divideix N, aleshores de l'anterior proposició i l'estudi de punts fixos w_N en $X_0(N)$ s'obté que $l(N) \leq 19$; provant així

$$Aut(X_0(N)) = Norm(\Gamma_0(N))$$

si $v_p(N) = 0$ per $p = 2,3,5,7,11,13,17,19$. Pels altres casos amb $N \neq 37, 63$ s'utilitzen alguns lemes tècnics i tècniques de reducció [11].
S'obté, a més, el següent resultat:

Teorema 3.2.23.

- *Existeixen exactament dos valors de N tal que el grup $Aut(X_0(N))$ conté elements excepcionals i aquests són $N = 37$ i $N = 63$. En ambdós casos $(Aut(X_0(N)) : Norm(\Gamma_0(N))) = 2$.*
- $Aut(X_0(37)) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.
- $Aut(X_0(63) \cong S_4 \times \mathbb{Z}/2$.

Per a un estudi més exhaustiu de l'anterior resultat es pot consultar [25], pel cas $N = 37$, i [14] pel cas $N = 63$.

3.3 Punts fixos de les involucions d'Atkin-Lehner

Considerem $N = m'm''$, $(m', m'') = 1$ i estudiem la involució d'Atkin-Lehner $w_{m'}$. Anem a veure primer com es comporta respecte de les puntes de $X_0(N)$. Recordem la següent caracterització de les puntes de $X_0(N)$

Proposició 3.3.1. *Les puntes de $X_0(N)$ són de la forma $P = \begin{pmatrix} x \\ d \end{pmatrix}$ on d recorre tots els divisors positius de N i x el podem prendre mòdul $t_d = (d, N/d)$ amb $(x, d) = 1$. Per tant, per a cada d tenim $\varphi(t_d)$ puntes.*

La descomposició $m'm'' = N$ ens dóna una descomposició única de $d = d'd''$ i $t_d = t'_d t''_d$

Proposició 3.3.2. *Sigui $\overline{P} = w_{m'}(P) = \begin{pmatrix} \overline{x} \\ \overline{d} \end{pmatrix}$. Llavors $\overline{d} = d''\frac{N'}{d'}$, $\overline{t} = t$, $\overline{x} \equiv -x (mod\ t')$ i $\overline{x} \equiv x (mod\ t'')$.*

Demostració. Considerem $w_{m'} = \begin{pmatrix} m'u & 1 \\ Ns & m' \end{pmatrix}$ amb $m'u - s\frac{N}{m'} = 1$ llavors tenim

$$w_{m'} \begin{pmatrix} x \\ d \end{pmatrix} = \frac{\frac{m'ux}{d'} + d''}{\frac{m'd''}{d'}(\frac{m''sx}{d''} + d')}$$

Per tant, per veure que $\overline{d} = \frac{m'd''}{d'}$ és suficient veure que $(\frac{m'ux}{d'} + d'', \frac{m''sx}{d''} + d'') = 1$. Multiplicant per x l'expressió de $det(w_{m'}) = 1$ tenim $m'ux + d''d' - m''sx - d'd'' = x$, d'on $(m'ux + d'd'', m''sx + d'd'') \mid x$ i de $(d, x) = 1$ tenim $(m'ux + d''d', m''sx + d'd'') = (\frac{m'ux}{d'} + d'', \frac{m''sx}{d''} + d') = 1$. Es clar que $\overline{t} = t$ pel càlcul de $\overline{d}$.

Denotem per $\alpha = \begin{pmatrix} \frac{m'ux}{d'} + d'' \\ \frac{m'd''}{d'}(\frac{m''sx}{d''} + d') \end{pmatrix}$ i considerem $A \in \Gamma_0(N)$ complint $A\alpha = \begin{pmatrix} \overline{x} \\ \frac{m'd''}{d'} \end{pmatrix}$. Si escrivim $A = \begin{pmatrix} \tilde{a} & \tilde{b} \\ N\tilde{c} & \tilde{d} \end{pmatrix}$ llavors

$$\tilde{c}(\frac{N}{d''}ux + m''d') + \tilde{d}(\frac{m''}{d''}sx + d') = 1 \tag{3.1}$$

on $\overline{x} = \tilde{a}(\frac{m'}{d'}ux + d'') + \tilde{b}(\frac{m'd''}{d'}(\frac{m''}{d''}sx + d'))$. D'aquí, per un càlcul directe mòdul t' i mòdul t'' s'arriba al resultat. □

Proposició 3.3.3 (Ogg). *$w_{m'}$ no té punts fixos ($m' > 1$) a excepció de $m' = 4$ on les puntes amb $d' = 2$ són fixades.*

Demostració. Sigui P una punta fixada per $w_{m'}$. Aleshores $m' = d'^2$, $t' = d'$ i $2x \equiv 0 (mod\ d')$ o $2 \equiv 0 (mod\ d')$. Com que $m' \neq 1$, per força $m' = 4$ i $d' = 2$ i totes aquestes puntes efectivament són fixades. □

Anem a estudiar com es comporten les involucions d'Atkin-Lehner en els punts de $Y_0(N)$. Per això pensem $Y_0(N)$ com l'espai de mòduli que consisteix en les parelles (E, C), on E denota una corba el·líptica i C un subgrup de

E d'ordre exactament N. Diem llavors que dues parelles $(E_1, C_1), (E_2, C_2)$ representen el mateix punt si existeix un isomorfisme $\phi : E_1 \to E_2$ tal que $\phi(C_1) = C_2$.
Anem a estudiar com actuen les involucions d'Atkin-Lehner en (E, C). Podem sempre pensar $(E, C) = (< \omega_1, \omega_2 >, \frac{\omega_2}{N})$ on $\tau = \frac{\omega_1}{\omega_2} \in \mathbb{H}$; llavors

$$w_{m'} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \frac{\omega_2}{m'} \end{pmatrix}$$

amb $\gamma \in \Gamma_0(m'')$. Com que $\gamma \in SL_2(\mathbb{Z})$, $w_{m'}(E) = E/C'$, on C' és el subgrup d'ordre exactament m' determinat per C. Posem $C = C' + C''$. Com que $\gamma \in \Gamma_0(m'')$: $\gamma(C'') = C''$ i, per tant,

$$w_{m'}((E, C)) = (E/C', \frac{E_{m'} + C''}{C'})$$

Així, si $\tau \in \mathbb{H}$ és punt fix per la involució $w_{m'}$ es compleix que $(E, C) \cong (E/C', E_{m'} + C''/C')$, és a dir, hi ha un isomorfisme $\varphi : E \to E/C'$ amb $\varphi(C) = E_{m'} + C''/C'$, o, equivalentment, $\exists \lambda \in End(E)$ amb $ker(\lambda) = C'$ complint:

$$0 \to C' \to E \to E \to 0$$

$\lambda(E_{m'}) = C'$, $\lambda^2 = m' \circ \phi$, $\phi \in Aut(E)$ i $\lambda(C'') = C''$.
Anem a indicar com la expressió anterior permet trobar el nombre de punts fixos de $w_{m'}$ en $Y_0(N)$.
Fixem-nos primer amb la condició que E té un endomorfisme $\sqrt{-m'} \in End(E)$. Això ens diu que E és una corba de multiplicació complexa amb $End(E) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-m'})$. Recordem-ne alguns resultats d'aquestes corbes el·líptiques que es troben en [37] cap 4.4.

Definició 3.3.4. *Sigui K un cos de nombres. Un ordre $\mathcal{O}$ de K és un subanell de K, que conté $\mathbb{Z}$ i és un $\mathbb{Z}$-mòdul lliure de rang $[K : \mathbb{Q}]$. Tot ordre en K està contingut en l'anell dels enters del cos K. Una xarxa en K, és un $\mathbb{Z}$-submòdul de K lliure de rang $[K : \mathbb{Q}]$. Si $\mathfrak{a}$ és una xarxa en K posem $\mathcal{O} = \{f \in F | f\mathfrak{a} \subset \mathfrak{a}\}$. $\mathcal{O}$ és un ordre de K que anomenem l'ordre de $\mathfrak{a}$ i diem que $\mathfrak{a}$ és un $\mathcal{O}$-ideal propi.*

A partir d'ara K denotarà un cos quadràtic imaginari.

Proposició 3.3.5. *Sigui E una corba el·líptica definida sobre $\mathbb{C}$ complint que $End(E) \otimes \mathbb{Q} \cong K$, i $End(E) = \mathcal{O}$, $\mathcal{O}$ un ordre de K. Llavors $E \cong \mathbb{C}/\mathfrak{a}$ on $\mathfrak{a}$ és un $\mathcal{O}$-ideal propi. A més, per a qualsevol $\mathfrak{a}$ $\mathcal{O}$-ideal propi, $End(\mathbb{C}/\mathfrak{a}) \cong \mathcal{O}$. $\mathbb{C}/\mathfrak{a} \cong \mathbb{C}/\mathfrak{b}$ si i només si $\exists \mu \in K$ tal que $\mu\mathfrak{a} = \mathfrak{b}$; d'aquí direm que la classe dels $\mathcal{O}$-ideals propis està unívocament determinada per la classe d'isomorfia de $\mathbb{C}/\mathfrak{a}$.*

Proposició 3.3.6. *Sigui $\mathcal{O}_K$ l'anell d'enters de K i $\mathcal{O}$ un ordre de K. Llavors hi ha un únic enter positiu c complint $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_K$. A més, per a qualsevol $\mathcal{O}$-ideal propi $\mathfrak{a}$, existeix un element $\mu \in K^*$ complint $\mu\mathfrak{a} + c\mathcal{O} = \mathcal{O}$.*

Proposició 3.3.7. *Per a qualsevol ordre $\mathcal{O}$ de K, el nombre de classes dels $\mathcal{O}$-ideals propis és exactament el nombre de classes d'isomorfia de les corbes el·líptiques amb $End(E) \cong \mathcal{O}$.*

Anem a aplicar aquests resultats a la situació en la que ens trobem. Si (E, C) és un punt fix de $w_{m'}$ llavors $\sqrt{-m'} \in End(E)$ i té un nucli cíclic d'ordre m'. Així $\mathbb{Z}[\sqrt{-m'}] \subset End(E) \subset \mathcal{O}_K$ on $K = \mathbb{Q}(\sqrt{-m'})$. Escrivim $m' = m_1 h^2$. Estudiem el cas amb $m_1 \equiv 2, 1(4)$ $m' > 3$. Així tenim: $\mathcal{O}_K = \mathbb{Z}[\sqrt{-m_1}]$, $d(\mathcal{O}) = c^2 d(\mathcal{O}_K) = -c^2 4m_1$, i $\mathcal{O} = \mathbb{Z}[\sqrt{-m_1 c^2}]$, on $c \mid h$. Pel fet que té nucli cíclic d'ordre m' s'ha de complir que $c = h$; i es comprova fàcilment que tot $\mathfrak{a}$ ideal de $\mathcal{O}$ té un subgrup cíclic d'ordre m'. Per tant, s'obté que el nombre de corbes el·líptiques mòdul isomorfisme amb un subgrup cíclic d'ordre m' complint $m_1 \equiv 2, 1(4)$ és igual a $h(-4m')$.
De manera semblant, si denotem per $\vartheta(m')$ = nombre de corbes el·líptiques mòdul isomorfisme amb un subgrup cíclic d'ordre m' per $m' > 3$, s'obté:

$$\vartheta(m') = \begin{cases} h(-m') + h(-4m') & m' \equiv 3(mod\ 4) \\ h(-4m') & altrament \end{cases}$$

Si $m'' = 1$ s'obtenen les fórmules de Fricke [17]; si $m'' > 1$ es compleix $\lambda(C'') = C''$. Això es tradueix en trobar els $n \in \mathbb{Z}$ tal que $\lambda - n$ tingui un subgrup d'ordre m'' en el seu nucli. Si $m' > 3$ i $m'' > 3$ senar es veu que n'hi ha

$$\prod_{p|m''} (1 + \left(\frac{-4m'}{p}\right))$$

Per tant, el nombre de punts fixos de $w_{m'}$ en $Y_0(N)$ és

$$\vartheta(m') \prod_{p|m''} (1 + \left(\frac{-4m'}{p}\right))$$

Per a cada altre cas caldria un estudi particular:

Teorema 3.3.8 (Kluit). *Denotem per $\upsilon(N, m')$ = el nombre de punts fixos en $X_0(N)$ de la involució $w_{m'}$; llavors es té:*

$$m' = 2; \quad \upsilon(2m'', 2) = \prod_{p|m''} (1 + \left(\frac{-1}{p}\right)) + \prod_{p|m''} (1 + \left(\frac{-2}{p}\right))$$

$$m'=3;\quad \upsilon(3m''2^\lambda,3)=\begin{cases} 2\prod_{p|m''}(1+\left(\frac{-3}{p}\right)) & si\ \lambda=0,1,2 \\ 0 & \lambda>2 \end{cases}$$

$$m'=4;\quad \upsilon(4m'',4)=\prod_{p|m''}(1+\left(\frac{-1}{p}\right))+\sum_{d|m''}\varphi((d,m''/d))$$

Per a $m'\geq 5$*:*

1. $N=m'$*;*

$$\upsilon(N,m')=\begin{cases} h(-4m') & m'\not\equiv 3(mod\ 4) \\ h(-4m')+h(-m') & m'\equiv 3(mod\ 4) \end{cases}$$

2. $N=2^\lambda m'$ *amb* $m'\equiv 1(mod\ 4)$

$$\upsilon(N,m')=\begin{cases} h(-4m') & \lambda=1 \\ 0 & \lambda>1 \end{cases}$$

3. $N=2^\lambda m'$ *amb* $m'\equiv -1(mod\ 4)$

$$\upsilon(N,m')=\begin{cases} h(-4m')+3h(-m') & \lambda=1 \\ 2h(-4m')+2h(-m')(1+\left(\frac{-m'}{2}\right)) & \lambda=2 \\ 2(1+\left(\frac{-m'}{2}\right))\upsilon(m',m') & \lambda>2 \end{cases}$$

4. $N=2^\lambda m'u$ *amb* u *senar i* $(m',2^\lambda u)=1$

$$\upsilon(N,m')=\prod_{p|u}(1+\left(\frac{-m'}{p}\right))\upsilon(2^\lambda m',m')$$

Per a un tractament dels punts fixos sense utilitzar l'estructura com espai de mòduli de $Y_0(N)$ es pot consultar [29] i [22].
Observem que els anteriors resultats ens permeten fer un càlcul efectiu, ja que evidentment $\left(\frac{r}{s}\right)$ és computable i $\varphi(s)$ també. Pel càlcul $h(-N)$, si N és lliure de quadrats, disposem d'un algoritme en [10] pag 228, i pel càlcul general podem escriure $-N=-N_0f^2$ i aleshores:

$$h(-N)=\frac{\omega(-N)}{\omega(-N_0)}h(-N_0)f\prod_{p|f}\left(1-\left(\frac{-N_0}{p}\right)p^{-1}\right)$$

on $\omega(D)$ és el nombre d'arrels de la unitat de l'ordre del cos K amb discriminant D. Per a una prova d'aquest resultat es pot consultar [10] pag 228.

3.4 $X_0(N)$ biel·líptiques amb involucions $w_{m'}$

Utilitzem les taules de [42] per a obtenir, pels $N \leq 210$, totes les corbes $X_0(N)$ que són biel·líptiques i admeten una involució d'Atkin-Lehner biel-líptica. Ens centrem en els N amb gènere$(X_0(N)) \geq 2$; per tant descartem els N següents: de $l'1$ fins a 21, 24, 25, 27, 32, 36 i 49.

Lema 3.4.1. *Pels següents N la corba modular $X_0(N)$ és biel·líptica amb les involucions biel·líptiques que s'indiquen en la taula següent, seguint la notació del teorema 3.1.6.*

N	*Involucions biel·líptiques*
22	w_2, w_{22}
26	w_2, w_{13}
28	$w_4, w_{28}, S_2w_4S_2, S_2, w_7S_2, w_7S_2w_4S_2$
30	w_5, w_6, w_{30}
33	w_{33}
34	w_2, w_{17}, w_{34}
35	w_5
37	$w_{37}, \alpha w_{37}$
38	w_{19}, w_{38}
39	w_3
42	w_{14}
43	w_{43}
50	w_2, w_{25}
51	w_{17}, w_{51}
53	w_{53}
55	w_{11}, w_{55}
61	w_{61}
62	w_{31}
65	w_{65}
69	w_{23}
75	w_{75}
79	w_{79}
83	w_{83}
89	w_{89}
94	w_{47}
95	w_{95}
101	w_{101}
119	w_{119}
131	w_{131}

α denota la involució hiperel·líptica de $X_0(37)$.

Demostració. Sols cal notar que si u és una involució biel·líptica té $2g-2$ punts fixos. De la fórmula $gènere(X_0(N)) = 1 + \frac{\psi}{12} - \frac{\upsilon_2}{4} - \frac{\upsilon_3}{3} - \frac{\upsilon_\infty}{2}$ i del fet que totes les involucions són d'Atkin-Lehner ($4 \nmid N$ i $9 \nmid N$) el resultat és un càlcul directe aplicant el teorema 3.3.8. Pels casos $N = 28, 37$ sols cal observar que $X_0(28)$ $X_0(37)$ són corbes de gènere 2 i, per tant, tota involució que no sigui la hiperel·líptica és biel·líptica. □

Igualment, pels casos $4|N$ o $9|N$ obtenim el següent resultat estudiant el nombre de punts fixos de les involucions d'Atkin-Lehner.

Lema 3.4.2. *Pels següents N la corba $X_0(N)$ és biel·líptica.*

N	*involucions*
40	w_{40}
44	w_{11}, w_{44}
45	w_5, w_9, w_{45}
48	w_{48}
54	w_{27}, w_{54}
56	w_7, w_{56}
60	w_{15}
63	w_{63}
64	w_{64}
81	w_{81}
92	w_{23}

Del fet que si $4 \nmid N$ i $9 \nmid N$ totes les involucions són d'Atkin-Lehner i de les taules de [42] obtenim:

Lema 3.4.3. *Pels següents N, $X_0(N)$ no és biel·líptica($g > 1$):*

23	*29*	*31*	*41*	*46*	*47*	*57*	*58*	*59*	*66*
67	*70*	*71*	*73*	*74*	*77*	*78*	*82*	*85*	*86*
87	*91*	*93*	*97*	*98*	*102*	*103*	*105*	*106*	*107*
109	*110*	*111*	*113*	*114*	*115*	*118*	*121*	*122*	*123*
125	*127*	*129*	*130*	*133*	*134*	*137*	*138*	*139*	*141*
142	*143*	*145*	*146*	*147*	*149*	*150*	*151*	*154*	*155*
157	*158*	*159*	*161*	*163*	*165*	*166*	*167*	*169*	*170*
173	*174*	*175*	*177*	*178*	*179*	*181*	*182*	*183*	*185*
186	*187*	*190*	*191*	*193*	*194*	*195*	*197*	*199*	*201*
202	*203*	*205*	*206*	*209*	*210*				

Corol·lari 3.4.4. *Pels N del lema anterior tenim que $X_0(N), X_1(N), X(N)$ no són corbes modulars biel·líptiques, a excepció potser de* 23,29,31,41,46,47,59 *i* 71.

Demostració. Conseqüència immediata del teorema 2.9 i de la caracterització de les corbes $X_0(N)$ hiperel·líptiques [30]. □

Capítol 4

L'estudi via reducció

Suposem que tenim un morfisme

$$\varphi : X_0(N) \to E$$

de grau 2.
Sabem, per [37] §7, que la corba modular $X_0(N)$ està definida sobre $\mathbb{Q}$; a més, podem definir-li un esquema propi i normal sobre $Spec(\mathbb{Z})$ i no singular sobre $Spec(\mathbb{Z}[1/N])$ [20], denotem-lo per $\mathfrak{X}_0(N)$. Llavors, per cada $p \nmid N$, obtenim una corba modular reduïda sobre $\overline{\mathbb{F}}_p$ que denotarem per $X_0(N) \otimes \overline{\mathbb{F}}_p$.
Suposem que φ està definida sobre $\mathbb{Q}$ i E també. Pel teorema 6.1., [36], E té un model de Nerón sobre $Spec(\mathbb{Z}[1/N])$ que el denotem per $\mathfrak{E}$ i, per tant, el morfisme $\varphi : X_0(N) \to E$ puja, per la propietat de models de Nerón, a un $Spec(\mathbb{Z}[1/N]) - morfisme$ de $Spec(\mathbb{Z}[1/N]) - esquemes$

$$\varphi : \mathfrak{X}_0(N) \to \mathfrak{E}$$

on la fibra sobre el punt genèric ens dóna φ i la fibra sobre un primer p amb $p \nmid N$, la reducció de l'aplicació φ sobre $\overline{\mathbb{F}}_p$. Anem a estudiar com són $X_0(N) \otimes \overline{\mathbb{F}}_p$ i $X_0(N) \otimes \overline{\mathbb{F}}_p(\mathbb{F}_{p^2})$ que denota el conjunt de punts sobre $\mathbb{F}_{p^2}$ de la corba reduïda $X_0(N) \otimes \overline{\mathbb{F}}_p$.
Anotem aquí que la corba modular reduïda $X_0(N) \otimes \overline{\mathbb{F}}_p$ és un espai de mòduli en els punts que no són puntes, que ve representat per parelles (E, C) amb E una corba el·líptica sobre $\overline{\mathbb{F}}_p$ i C un subgrup d'ordre exactament N.

Lema 4.1 (Ogg). *Per a tota parella (E, C) de $X_0(N) \otimes \overline{\mathbb{F}}_p$ amb $p \nmid N$ i E una corba supersingular definida sobre $\mathbb{F}_p$ es té llavors que $(E, C) \in X_0(N) \otimes \overline{\mathbb{F}}_p(\mathbb{F}_{p^2})$.*

Per una prova de l'anterior resultat es pot consultar [30].

Lema 4.2 (Harris-Silverman). *Fixat N , denotem per*

$$\upsilon(N) = \#\ dels\ divisors\ primers\ de\ N$$

$$\mu(N) = (SL_2(\mathbb{Z}) : \Gamma_0(N))$$

i per a cada primer p

$$n(p) = \sum_{E/\mathbb{F}_p} \frac{1}{|Aut(E)|}$$

Llavors, si $X_0(N)$ és biel·líptica, tenim:

$$2^{\upsilon(N)} + 2n(p)\mu(N) \leq \#X_0(N) \otimes \overline{\mathbb{F}_p}(\mathbb{F}_{p^2}) \leq min(2(p+1)^2, p^2 + 1 + 2g\grave{e}nere(X_0(N))p)$$

si el gènere és mes gran o igual que 6; i

$$2^{\upsilon(N)} + 2n(p)\mu(N) \leq \#X_0(N) \otimes \overline{\mathbb{F}_p}(\mathbb{F}_{p^2}) \leq p^2 + 10p + 1$$

en altre cas. Sempre i quan en tots els casos es compleixi que $p \nmid N$.

Demostració. Veiem primer que $\#X_0(N) \otimes \overline{\mathbb{F}_p}(\mathbb{F}_{p^2}) \geq 2^{\upsilon(N)} + 2n(p)\mu(N)$. Estudiem possibles punts $\mathbb{F}_{p^2} - racionals$. Totes les puntes unitàries, és a dir, de la forma $1/d$ amb $d|N$ i $1 = (d, N/d)$ estan definides sobre $\mathbb{Q}$ i si $p \nmid N$ definiran punts a $\mathbb{F}_{p^2}$. Com que n'hi ha $2^{\upsilon(N)}$ obtenim així el primer sumand de la part esquerra de la desigualtat. Per a veure l'altre sumand pensem $X_0(N)$ com a espai de mòduli de les parelles (E, C) (consultar [11]) on E és una corba el·líptica i C un subgrup d'ordre N de E. Si $E|_{\mathbb{F}_p}$ és supersingular, pel lema anterior $(E, C) \in X_0(N) \otimes \overline{\mathbb{F}}_p(\mathbb{F}_{p^2})$. Llavors el nombre de subgrups d'ordre N és $\mu(N)$, i si $\phi \in Aut(E)$, (E, C) i $(E, \phi(C))$ representen el mateix punt de $X_0(N)(\mathbb{F}_{p^2})$. Com que $[-1]C = C$, com a mínim hi ha $2\mu(N)/\#Aut(E)$ punts diferents no cuspidals de $X_0(N)(\mathbb{F}_{p^2})$. Sumant respecte de totes les corbes supersingulars sobre $\mathbb{F}_p$ obtenim la desigualtat. Per a provar l'altra desigualtat, pel cas de $g\grave{e}nere(X_0(N)) \leq 5$ tenim l'estimació de Weil que ens diu:

$$\#X_0(N) \otimes \overline{\mathbb{F}_p}(\mathbb{F}_{p^2}) \leq p^2 + 1 + 2pg\grave{e}nere(X_0(N))$$

Pel cas de gènere superior a 5 el morfisme φ el definim sobre $\mathbb{Q}$ i per tant tenim bona reducció ja que $p \nmid N$ d'on obtenim

$$\#X_0(N) \otimes \overline{\mathbb{F}}_p(\mathbb{F}_{p^2}) \leq 2\#E(\mathbb{F}_{p^2})$$

Finalment, $\#E(\mathbb{F}_{p^2}) \leq (p+1)^2$ de la desigualtat $|\#E(\mathbb{F}_q) - (q+1)| \leq 2(q)^{1/2}$ [35]. □

Lema 4.3. *Seguint la notació de l'anterior lema, si $X_0(N)$ és biel·líptica amb gènere més gran o igual que 6 llavors:*

$$2^{\upsilon(N)} + \frac{1}{12}\mu(N) \leq 18 \text{ si } 2 \nmid N$$

$$2^{\upsilon(N)} + \frac{1}{6}\mu(N) \leq 32 \text{ si } 3 \nmid N$$

$$2^{\upsilon(N)} + \frac{1}{3}\mu(N) \leq 72 \text{ si } 5 \nmid N$$

$$2^{\upsilon(N)} + \frac{1}{2}\mu(N) \leq 128 \text{ si } 7 \nmid N$$

$$2^{\upsilon(N)} + \frac{5}{6}\mu(N) \leq 288 \text{ si } 11 \nmid N$$

Pel cas de gènere inferior a 6 les cotes són respectivament 25, 40, 76, 120, 232.

Demostració. És conseqüència immediata del lema anterior, en calcular explícitament el valor de $n(p)$ pels p corresponents; i dels fets teòrics. La fórmula de Deuring i Eichler ens diu que $n'(p) = \frac{p-1}{24}$, on $n'(p)$ recorre el conjunt de corbes supersingulars en característica p. Notem també que tota corba supersingular en característica p està definida sobre $\mathbb{F}_p$, si $p \leq 31$, per tant $n(p) = n'(p)$. □

Lema 4.4. *$X_0(N)$, $X_1(N)$ i $X(N)$ no són biel·líptiques, per a $N \geq 344$.*

Demostració. Utilitzant l'anterior lema amb les estimacions trivials $N \leq \mu(N)$ i $\upsilon(N) \geq 1$ i pensant que l'última corba amb gènere inferior a 6 és $X_0(86)$, obtenim que si $X_0(N)$ és biel·líptica es compleix

$$N \leq 192 \quad 2 \nmid N$$

$$N \leq 180 \quad 3 \nmid N$$

$$N \leq 210 \quad 5 \nmid N$$

$$N \leq 252 \quad 7 \nmid N$$

$$N \leq 343 \quad 11 \nmid N$$

Per tant, suposem que N és divisible per $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Posem $N = N_2 N_3 N_5 N_7 N_{11} M$, on $N_p = p^{n_p} || N$. Com que $X_0(N) \to X_0(N/N_p)$ són finites, si $X_0(N)$ és biel·líptica llavors $X_0(N/N_p)$ és hiperel·líptica o biel·líptica.

Hiperel·líptica no pot ser ja que la última era $X_0(71)$ i $2.3.5.7 > 71$. Aleshores $v(N/N_p) \geq 4$ i

$$2^4 + \frac{1}{12}\frac{N}{N_2} \leq 18$$

d'on $N/N_2 \leq 2 \cdot 12 = 24$, impossible ja que $N_3N_5N_7N_{11}M > 24$. El fet que $X_1(N)$ i $X(N)$ no siguin biel·líptiques ve de l'existència de morfismes de grau finit: $X_1(N) \to X_0(N)$ i $X(N) \to X_0(N)$, i del teorema 2.9. □

Corol·lari 4.5. *$X_0(N)$ no és biel·líptica per $N > 210$, a excepció potser de $X_0(240)$.*

Demostració. Si N no és divisible per 2, 3 o 5 ja hem acabat. Per tant suposem, que $2 \cdot 3 \cdot 5 = 30|N$. Si 7 no divideix N després del 210 l'únic cas que es pot donar és 240. Si 7 divideix, llavors N seria divisible per $2 \cdot 3 \cdot 5 \cdot 7 = 210|N$ i múltiples d'aquest i, com que ha de ser inferior a 344, obtenim el resultat. □

Fem ara un estudi particular de les corbes que ens queden. Ens centrarem explícitament en els $N \leq 210$ que són múltiples de 4 o 9 i en $N = 240$. El motiu va quedar clarament expressat en el capítol anterior, ja que per a $4 \nmid N$ i $9 \nmid N$ existeixen taules dels punts fixos de totes les possibles involucions que podrien fer $X_0(N)$ biel·líptica.
Els casos que estan en la situació anterior i que no admeten involucions biel·líptiques del tipus d'Atkin-Lehner són els següents:

52	68	72	76	80	84	88	96	100	104	108	112	116
120	124	128	132	136	140	144	148	152	156	160	164	168
172	176	180	184	188	192	196	200	204	208	240	90	99
117	126	135	153	162	171	189	198	207				

Utilitzant les fites que apareixen en la demostració del lema 4.4 per a $2 \nmid N$ i $3 \nmid N$ deduïm:

Corol·lari 4.6. *$X_0(N)$ no és biel·líptica per a N =207, 184, 188, 196, 200, 208.*

Del fet que si tenim un morfisme $X_0(N) \to X_0(M)$ finit amb $X_0(N)$ biel·líptica llavors $X_0(M)$ també és biel·líptica o hiperel·líptica obtenim pel lema 3.4.3 del capítol anterior que:

Corol·lari 4.7. *$X_0(N)$ no és biel·líptica per N=116, 132, 140, 148,156, 164, 171, 172, 198, 204, 210.*

Sigui $\mathfrak{X}_0(N)$ el model d'Igusa de $X_0(N)$. Quan reduïm mòdul un primer p amb $p \nmid N$ el nombre de puntes de $X_0(N)$ i $\mathfrak{X}_0(N) \otimes \overline{\mathbb{F}_p}$ no varia.

Proposició 4.8 (Ogg,[32]). *Per a cada $d|N$ tenim $\varphi(t)$ puntes conjugades $\left(\frac{x}{d}\right)$ de $X_0(N)$; on $t=(d,N/d)$ i φ és la φ d'Euler.*

Llavors $\begin{pmatrix} x \\ d \end{pmatrix}$ és una punta $\mathbb{Q}$-racional si t compleix $\varphi(t)=1$. Com que $p \nmid N$, mòdul $\mathbb{F}_p$ aquestes puntes són punts de $\mathfrak{X}_0(N)\otimes\overline{\mathbb{F}}_p(\mathbb{F}_p)$.
Considerem ara les puntes $\begin{pmatrix} x \\ d \end{pmatrix}$ amb $\varphi(t)=2$. Veurem que aquestes puntes reduïdes són punts sobre $\mathbb{F}_{p^2}$. En efecte, siguin $\alpha_1=\begin{pmatrix} x_1 \\ d \end{pmatrix}$, $\alpha_2=\begin{pmatrix} x_2 \\ d \end{pmatrix}$ les dues puntes conjugades. Sigui P una punta $\mathbb{Q}$-racional i considerem el punt de la $Jac(X_0(N))$

$$\alpha_1+\alpha_2-2P.$$

Pel fet de ser $\varphi(t)=2$ tenim que l'anterior està definit sobre $\mathbb{Q}$, fent reducció mòdul p obtenim el divisor

$$\overline{\alpha_1}+\overline{\alpha_2}-\overline{2P}$$

definit sobre $\mathbb{F}_p$. Si considerem l'acció del Frobenius π, de $\mathbb{F}_p$, sobre l'anterior divisor veiem que, per força $\pi(\alpha_1)=\alpha_2$ o α_1, (suposant que la corba modular reduïda no és hiperel·líptica). Aleshores π^2 correspon al Frobenius de $\mathbb{F}_{p^2}$ i $\pi^2(\alpha_i)=\alpha_i$, $i=1,2$, provant que α_i estan definides sobre $\mathbb{F}_{p^2}$; per tant:

Lema 4.9. *Totes les puntes de $X_0(N)$ complint $\varphi(t)\leq 2$ són punts diferents en $\mathfrak{X}_0(N)\otimes\overline{\mathbb{F}_p}(\mathbb{F}_{p^2})$, $p\nmid N$, sempre i quan $X_0(N)$ no sigui hiperel·líptica sobre $\mathbb{F}_p$.*

Nota 4.10. *Observem que el fet que $X_0(N)$ no sigui hiperel·líptica sobre $\overline{\mathbb{F}_p}$, per a molts N, és pot raonar de manera anàloga als arguments anteriors per a corbes biel·líptiques, ja que si tenim*

$$\mathfrak{X}_0(N)\otimes\overline{\mathbb{F}}_p\to\mathbb{P}^1$$

es compleixen unes desigualtats semblants a la del lema 4.3. ([30] pag455) i podem substituir el nombre de puntes definides sobre $\mathbb{F}_{p^2}$, pel nombre de les puntes de $X_0(N)$ definides sobre $\mathbb{Q}$ (millor aproximació que $2^{\upsilon(N)}$). En particular, si $4|N$ o $9|N$, per a tots els $210\geq N\geq 80$ la seva corba reduïda mòdul el primer p més petit, amb $p\nmid N$, corresponent no és hiperel·líptica, [30]. Fem-ne un exemple: N=99. Hi ha 4 puntes sobre $\mathbb{Q}$, per tant, si fos hiperel·líptica sobre $\mathbb{F}_2$ s'hauria de complir la desigualtat $4+\frac{\psi(99)}{12}\leq 10$, [30] pag 455. Com que $4+\frac{\psi(99)}{12}>10$ la corba reduïda mòdul $p=2$ no és hiperel·líptica.

Utilitzant, enlloc de $2^{\nu(N)}$, aquesta millor fita pel nombre de les puntes definides sobre $\mathbb{F}_{p^2}$ (puntes de $X_0(N)$ amb $\varphi(t) \leq 2$) obtenim:

Corol·lari 4.11. *$X_0(N)$ no és biel·líptica per a N =80, 84, 96, 99, 100, 104, 108, 112, 117, 120, 124, 126, 128, 135, 136, 144, 152, 153, 160, 162, 168, 176, 180, 189, 192, 240.*

Demostració. Sigui $N = 99$. Observem que

$$\#X_0(99)(\mathbb{F}_4) \geq 8 + \frac{1}{12}\mu(99) \geq 8 + \frac{1}{12}12.4.3 = 8 + 12 = 20$$

però la condició de ser biel·líptica de gènere superior a 6 ens imposa llavors que $\#X_0(99)(\mathbb{F}_4) \leq 18$, per tant, no pot ser biel·líptica. Els altres N es fan semblantment fent reducció segons correspongui $p = 2, 3, 5$ o 7. □

Per a acabar el problema de la determinació de les corbes biel·líptiques falta estudiar unicament els casos següents:

$$N = 52, 68, 72, 76, 88, 90$$

Capítol 5

L'estudi en el cas $4|N$

5.1 Introducció

Per a determinar si les corbes modulars $X_0(N)$, N =52,68,72,76,88 i 90 són biel·líptiques estudiarem totes les possibles involucions a $Aut(X_0(N))$. En aquest capítol ens centrarem en les involucions que apareixen quan $4|N$ i estudiarem exactament totes les involucions quan $4||N$ i $9 \nmid N$ seguint 3.1.6.

5.2 Un estudi sobre la involució S_2

5.2.1 Introducció

Observem que per a les corbes modulars $X_0(N)$ amb $N \equiv 0(mod\ 4)$ tenim la involució

$$S_2 = \begin{pmatrix} 1 & 1/2 \\ 0 & 1 \end{pmatrix}^1$$

Ens interessa especialment l'estudi dels seus punts fixos.

5.2.2 L'estudi com a grup fuchsià de S_2

Considerem el següent subgrup de $GL_2(\mathbb{Q})^+$

$$\Gamma_{4k} = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, c, d \in \mathbb{Z};\ b \in \mathbb{Z}[1/2]; c \equiv 0(mod\ 4k)\ ; ad - bc = 1\}$$

i també considerem, seguint la notació de [4],

$$\Gamma_0(N, k) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{Z};\ b \equiv 0(k);\ c \equiv 0(mod\ N);\ ad - bc = 1\}$$

[1] Un estudi molt semblant és vàlid per a $S_{v''}$ amb $v'' \geq 2$

Nota 5.2.1. *Si $\tau \in \mathbb{H}$ és un punt fix de la involució S_2 de $X_0(4k)$ llavors τ és un punt el·líptic del grup Γ_{4k}, ja que $X_0(4k)$ no té punts el·líptics d'ordre 2.*

Lema 5.2.2. *El grup $\Gamma_0(4k)$ és un subgrup de Γ_{4k} d'índex 2. El grup Γ_{4k} és un grup fuchsià de primera espècie i les seves puntes es corresponen amb $\mathbb{Q} \cup \{\infty\}$.*

Demostració. De $c \equiv 0(mod 4k)$ tenim sempre a, d senars com elements de Γ_{4k}. Per tant, en multiplicar dos elements que no són de $\Gamma_0(4k)$ obtenim un element de $\Gamma_0(4k)$. Això prova que l'índex és 2.
Per a veure que Γ_{4k} és un grup fuchsià cal provar que donats dos punts $\tau, \tau' \in \mathbb{H}$ es tenen entorns U, V en $\mathbb{H}$ de τ i τ' tals que el nombre de $\gamma \in \Gamma_{4k}$ $\gamma U \cap V \neq \emptyset$ és finit. Suposem que això no succeís: $\exists\ \tau, \tau'$ on $\forall U, V$ obert de τ, τ' respectivament hi ha infinits $\gamma \in \Gamma_{4k}$ complint $\gamma U \cap V \neq \emptyset$. Triem entorns U de τ i V de τ' de la següent manera: siguin U' i V' entorns de τ i τ', respectivament, complint que el nombre de $\beta \in \Gamma_0(4k)$ tals que $\beta U' \cap V' \neq \emptyset$ és finit. Igualment siguin U'',V'' entorns de τ i ${\gamma_1}^{-1}\tau'$, respectivament, complint la mateixa condició anterior. Denotem $V''' = {\gamma_1}^{-1}V' \cap V''$, entorn de ${\gamma_1}^{-1}\tau'$, i prenem $V = \gamma_1 V'''$ i $U = U' \cap U''$. Llavors com el nombre de $\alpha \in \Gamma_{4k}$ complint $\alpha U \cap V \neq \emptyset$ és no finit. Despreciant un nombre finit, podem pensar que cada $\alpha \in \Gamma_{4k}$ és de la forma $\alpha_i = \gamma_1 \beta_i$, on $\gamma_1 \in \Gamma_{4k}$ i $\beta_i \in \Gamma_0(4k)$. Com que suposem Γ_{4k} no fuchsià aleshores $\gamma_1 \beta_i U \cap V \neq \emptyset$ i, multiplicant per γ_1^{-1}, $\beta_i U \cap V''' \neq \emptyset$. Això entra en contradicció amb l'elecció de V i U.
Finalment, Γ_{4k} és de primera espècie per ser-ho $\Gamma_0(4k)$. Per a veure que Γ_{4k} té les mateixes puntes que $\Gamma_0(4k)$ és suficient el següent resultat:

Lema 5.2.3. *Siguin Γ, Γ' dos subgrups (de $SL_2(\mathbb{R})$)d'índex finit entre ells i discrets. Aleshores Γ i Γ' tenen el mateix conjunt de puntes.*

Per una prova [37] §3. □

Per tant, l'estudi de la involució S_2 ve lligada a l'estudi de l'anterior grup fuchsià de primera espècie. La determinació dels seus punts el·líptics i els seus punts parabòlics ens permet de calcular el gènere de $\Gamma_{4k}\backslash\overline{\mathbb{H}}$, que no és res més que el gènere de la corba $X_0(N)/S_2$.

Lema 5.2.4. *Sigui $\vartheta(N_2)$ el nombre de punts fixos de $Y_0(N)$ per S_2. Llavors*

$$\vartheta(N_2) \leq 2(\prod_{p|N}(1 + \left(\frac{-1}{p}\right))) \quad si\ N \equiv 4(8)^2$$

[2]Notem que a la pràctica sempre podem determinar exactament aquest valor utilitzant la proposició 5.2.10

$$\vartheta(N_2) = 0 \quad si \ N \equiv 0(8)$$

Demostració. Sigui $\tau \in Y_0(N)$ punt fix de S_2, llavors:

$$\begin{pmatrix} 1 & 1/2 \\ 0 & 1 \end{pmatrix} \tau = \gamma\tau$$

amb $\gamma \in \Gamma_0(N)$, $\gamma \neq id$. De

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix} \tau = \gamma\tau$$

obtenim

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} 2\tau = \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix} \gamma\tau$$

I de

$$\begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix} \gamma = \delta \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix}$$

amb $\delta \in \Gamma_0(4k, 2)$ obtenim

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} 2\tau = \delta 2\tau$$

Per tant, considerant l'aplicació

$$\pi_2 : Y_0(N) \to Y_0(N/2)$$

multiplicar per 2, veiem que 2τ és un punt el·líptic de $\Gamma_0(N/2)$. Com que π_2 té grau 2 i com que $\Gamma_0(M)$ no té punts el·líptics d'ordre 2 si $M \equiv 0(4)$ i quan $M \equiv 2(mod\ 4)$ n'hi ha $\prod_{p|M}(1 + \left(\frac{-1}{p}\right))$, obtenim el resultat amb $M = N/2$. □

Estudiem el comportament a les puntes.

Lema 5.2.5. *Per a $d|N$, sigui $t = (d, N/d)$. Les úniques puntes $P = \begin{pmatrix} x \\ d \end{pmatrix}$ fixes per S_2 són les que compleixen que existeix algun enter k tal que $d = 2tk$ i $\upsilon_2(tk) \geq 1$. És a dir, els d complint $\upsilon_2(d) > [\frac{\upsilon_2(N)}{2}]$.*

Demostració. Sigui $P = \begin{pmatrix} x \\ d \end{pmatrix}$ una punta. Llavors $S_2(P) = \frac{2x+d}{2d}$. Si d és senar la punta no queda fixa; per tant $d \equiv 0(2)$. Escrivim $d = 2d'$. Observem que, a més, s'ha de complir $(x + d', d) = 1$. Si $\upsilon_2(d) = 1$ l'anterior m.c.d. és 2 com a mínim; per tant $\upsilon_2(d) \geq 2$ i llavors és clar, per ser $(x, d) = 1$, que $(x + d', d) = 1$. Per tant, $x + d' \equiv x(mod\ t)$, $t = (d, N/d)$. És a dir, $d' \equiv 0(mod\ t)$. D'aquí que $\exists k \in \mathbb{Z}$ tal que $d = 2tk$, $t = (2tk, N/2tk)$ amb $\upsilon_2(tk) \geq 1$. □

Nota 5.2.6. *L'estudi dels punts fixos per S_2 de $X_0(N)$, com a espai de moduli, requereix una anàlisi del comportament dels automorfismes d'una corba el·líptica sobre els subgrups d'ordre N; ja que si (E, C) és un punt de $X_0(N)$ llavors és senzill de comprovar que $S_2(E) = E$.*

5.2.3 L'estudi efectiu dels punts fixos de S_2

Anem a aplicar els anteriors resultats al cas que ens interessa i que és l'estudi de les corbes modulars en les que no coneixem les seves involucions bielíptiques.
Denotem el *gènere*$(X_0(N))/S_2)$ per g_N llavors:

Corol·lari 5.2.7. *Pel casos $N = 40, 44, 48, 56, 60, 64, 72, 76, 88, 92$ s'obté: $g_{40} = 1$, $g_{44} = 2$, $g_{48} = 1$, $g_{56} = 2$, $g_{60} = 3$, $g_{64} = 1$, $g_{72} = 1$, $g_{76} = 4$, $g_{88} = 4$ i $g_{92} = 5$. Per tant S_2 és una involució biel·líptica pels casos $N = 40, 48$, 64 i 72.*

Demostració. Cas $N \equiv 0(mod\ 8)$. Per la fórmula de Hurwitz tenim

$$2g - 2 = 2(2g_N - 2) + \#\{punts\ fixos\ de\ S_2\}$$

on g denota el gènere de $X_0(N)$. Anem a calcular els punts fixos. Com que $N \equiv 0(8)$ tots els punts fixos es troben en les puntes i, per tant, únicament cal un estudi en cada cas del comportament de S_2 en les puntes. Pel cas $N = 40, 48$ tenim quatre punts fixos, d'on $g_{40} = g_{48} = 1$. Pel cas $N = 56, 88$ un obté 4 puntes fixes, per $N = 64$ s'obtenen 4 puntes fixes i per $N = 72$ se n'obtenen 8.
Cas $N \equiv 4(mod\ 8)$. Sols cal observar que pels anteriors N de l'enunciat del corol·lari $X_0(N/2)$ no té elements parabòlics d'ordre 2 i, per tant, S_2 no té punts fixos en $\mathbb{H}$. Per a calcular els punts fixos únicament és necessari fer un estudi a les puntes. S'obté que el número de puntes fixades és per a $N = 44, 60, 76, 92$: 2,4,2 i 2 respectivament, d'on, novament aplicant la fórmula de Hurwitz, obtenim el resultat. □

Teorema 5.2.8. *Sigui g el gènere de la superfície de Riemann compacta $\Gamma\backslash\overline{\mathbb{H}}$, i sigui m el nombre de puntes no Γ-equivalents i $e_1, \ldots, e_r$ els ordres dels punts el·líptics de Γ no equivalents. Llavors es té:*

$$\frac{1}{2\pi}\int_{\Gamma\backslash\overline{\mathbb{H}}} y^{-2}dxdy = 2g - 2 + m + \sum_{u=1}^{r}(1 - \frac{1}{e_u})$$

Per a la prova consulteu [37] §3.

Corol·lari 5.2.9. *Per a $N = 52, 68$ obtenim $g_{52} = 2$ i $g_{68} = 3$ i, per tant, S_2 no fa a $X_0(N)$ biel·líptica.*

Demostració. Si denotem per $g_0(N)$ el gènere de $X_0(N)$: $g_0(52) = 5$ i $g_0(68) = 7$ i com que

$$\pi_{S_2} : X_0(52) \to X_0(52)/S_2$$

és de grau 2 obtenim

$$2\frac{1}{2\pi}\int_{\overline{\mathbb{H}}/\Gamma_{4k}} y^{-2}dxdy = \frac{1}{2\pi}\int_{\overline{\mathbb{H}}/\Gamma_0(4k)} y^{-2}dxdy$$

Anem doncs a calcular quan val g_{52} i g_{68} utilitzant el teorema 5.2.8 amb $\Gamma = \Gamma_{52}, \Gamma_{68}$:

$$2\frac{1}{2\pi}\int_{\overline{\mathbb{H}}/\Gamma_{52}} y^{-2}dxdy = 2g_0(52) - 2 + 6 + 0 = 14$$

$$2\frac{1}{2\pi}\int_{\overline{\mathbb{H}}/\Gamma_{68}} y^{-2}dxdy = 2g_0(68) - 2 + 6 + 0 = 18$$

Calculem el nombre m de puntes no Γ_{4k}-equivalents, $k = 13, 17$, i en ambdós casos és igual a $m = 4$. Per tant, per a $N = 52$ tenim

$$7 = 2g_{52} - 2 + 4 + \sum_{u=1}^{r}(1 - \frac{1}{e_u})$$

Els punts τ el·líptics han de correspondre necessàriament a punts fixos per S_2 i aquests a punts el·líptics de $\Gamma_0(26)$. Així, com a molt, u recorre de 1 fins a 4 amb $e_u = 2$; per tant, per força, obtenim que $r = 2$ i $g_{52} = 2$.
Pel cas $N = 68$ tenim justament la mateixa situació. $\Gamma_0(34)$ té dos punts el·líptics d'ordre 2 i $9 = 2g_{68} - 2 + 4 + \sum_{u=1}^{r}(1 - \frac{1}{2})$ on r recorre de 1 fins a 4. D'aquí que $r = 2$ i $g_{68} = 3$. □

5.2.4 $X_0(N)/S_2$ és $X_0(N/2)$

Proposició 5.2.10. *La corba $X_0(N)/S_2$ és $X_0(N/2)$ i a més l'aplicació $\pi : X_0(N) \to X_0(N)/S_2$ correspon a multiplicar per 2.*

Demostració. Es clar que la projecció $\pi' : X_0(N) \to X_0(N/2)$ multiplicar per 2, dóna una involució $\upsilon \in Aut(X_0(N))$. Anem a estudiar el comportament a les puntes de υ. Escrivim $N = 2^{\upsilon_2(N)}\prod_1^n p_i^{\upsilon_{p_i}(N)}$. Considerem la involució

υ i una punta de $X_0(N)$ de la forma $\begin{pmatrix} x \\ d \end{pmatrix}$ amb $\upsilon_2(d) > [\frac{\upsilon_2(N)}{2}]$. Veiem primer que és fixa per υ. Com que $\pi'\left(\begin{pmatrix} x \\ d \end{pmatrix}\right) = \begin{pmatrix} x \\ d/2 \end{pmatrix}$ si $\pi'(\begin{pmatrix} x' \\ d' \end{pmatrix}) = \pi'(\begin{pmatrix} x \\ d \end{pmatrix})$ de $\upsilon_2(d) \geq 2$, tenim que, $d = d'$ i $x \equiv x'(mod\ t)$, amb $t = (d/2, N/d)$. Com que $\upsilon_2(d) > [\frac{\upsilon_2(N)}{2}]$, $t = (d, N/d)$ i, per tant, $\begin{pmatrix} x \\ d \end{pmatrix} = \begin{pmatrix} x' \\ d' \end{pmatrix}$ a $X_0(N)$.

Considerem llavors $P = \begin{pmatrix} x \\ d \end{pmatrix}$ punta de $X_0(N)$ amb $\upsilon_2(d) \leq [\frac{\upsilon_2(N)}{2}]$. Per la prova del lema 5.2.5 tenim

$$S_2(\begin{pmatrix} x \\ d \end{pmatrix}) = \frac{2x+d}{2d}.$$

Sigui $k = \upsilon_2(d)$, llavors $S_2(\begin{pmatrix} x \\ d \end{pmatrix}) = \frac{x+2^{k-1}d'}{d}$ on $d' = d/2^k$. Provem que π' envia les dues puntes anteriors a la mateixa punta de $X_0(N/2)$. En efecte, $\pi'(\begin{pmatrix} x \\ d \end{pmatrix}) = \frac{x}{d/2}$ si $k \geq 1$ i $\pi'(\begin{pmatrix} x+2^{k-1}d' \\ d \end{pmatrix}) = \frac{x+2^{k-1}d'}{d/2}$ si $k \geq 1$. Quan $k = 0$ S_2 relaciona les puntes $\begin{pmatrix} x \\ d \end{pmatrix}$ amb $\upsilon_2(d) = 0$ i la punta $\begin{pmatrix} 2x+d \\ 2d \end{pmatrix}$ i és clar que $\pi'(\begin{pmatrix} x \\ d \end{pmatrix}) = \pi'(\begin{pmatrix} 2x+d \\ 2d \end{pmatrix})$ si $k = 0$. Per acavar de provar que υ actua de la mateixa forma que S_2 en aquestes puntes ($k \geq 1$), cal veure que $x \equiv x + 2^{k-1}d'(mod\ t)$, on $t = (\frac{d}{2}, \frac{N/2}{d/2}) = 2^{k-1}d''$ amb $d''|d'$. Això és conseqüència directa de que $k \leq [\frac{\upsilon_2(N)}{2}]$.

Per tant, υ i S_2 actuen de la mateixa manera sobre les puntes de $X_0(N)$ i com que $Norm(\Gamma_0(N))$ actua transitivament sobre les puntes llavors $S_2 = \upsilon$, provant així l'enunciat. □

Recordem el següent resultat:

Teorema 5.2.11 (Schoeneberg). *Sigui X una superfície de Riemann, i P un punt fix d'un automorfisme ω de X, de període $p > 1$. Denotem per g_ω el gènere de X/ω. Si $g_\omega \neq [g/p]$ llavors P és un punt de Weierstrass.*

Corol·lari 5.2.12. *Sigui $X = X_0(N)$ amb $N \equiv 0(mod\ 4)$ llavors tota punta $P = \begin{pmatrix} x \\ d \end{pmatrix}$ amb $\upsilon_2(d) > [\frac{\upsilon_2(N)}{2}]$ és un punt de Weierstrass si el gènere de $X_0(N/2)$ és diferent al nombre $[\frac{gènere(X_0(N))}{2}]$.*

Demostració. Conseqüència immediata del teorema de Shoeneberg i el lema 5.2.5. □

5.3 L'estudi de la involució $w_{2^{\upsilon_2(N)}}S_2w_{2^{\upsilon_2(N)}}$

5.3.1 Introducció

Si $N \equiv 0(mod\ 4)$, $w_{2^{\upsilon_2(N)}}S_2w_{2^{\upsilon_2(N)}}$ és una involució de $X_0(N)$. Estudiem els seus punts fixos per a poder determinar si és una involució biel·líptica pels casos $N = 52, 68, 72, 76, 88$ i també $N = 40, 44, 48, 56, 60, 64, 92$. Denotem en tota aquesta secció $\Upsilon = w_{2^{\upsilon_2(N)}}S_2w_{2^{\upsilon_2(N)}}$.

5.3.2 L'estudi del grup fuchsià $\Gamma_0(4k) \cup \Upsilon\Gamma_0(4k)$

Posem

$$\Upsilon = \frac{1}{2^{\upsilon_2(N)}} \begin{pmatrix} (2^{\upsilon_2(N)}k)^2 + Nt(2^{\upsilon_2(N)-1}k + 2^{\upsilon_2(N)}) & 2^{\upsilon_2(N)}(k + 2^{\upsilon_2(N)-1}k + 2^{\upsilon_2(N)}) \\ Nt2^{\upsilon_2(N)}k + Nt(\frac{N}{2} + 2^{\upsilon_2(N)}) & Nt + 2^{\upsilon_2(N)-1}Nt + 2^{\upsilon_2(N)} \end{pmatrix}$$

amb

$$w_{2^{\upsilon_2(N)}} = \frac{1}{\sqrt{2^{\upsilon_2(N)}}} \begin{pmatrix} 2^{\upsilon_2(N)}k & 1 \\ Nt & 2^{\upsilon_2(N)} \end{pmatrix}.$$

Observem que $\Upsilon \in \Gamma_0(N/2) \setminus \Gamma_0(N)$ i que $X_0(N)/\Upsilon = X_0(N/2)$. Tenim ja coneguts els gèneres dels anteriors grups fuchsians i així obtenim:

Corol·lari 5.3.1. *Sigui g_N el gènere de $X_0(N)/\Upsilon$. Llavors, $g_{40} = 1$, $g_{44} = 2$, $g_{48} = 1$, $g_{52} = 2$, $g_{56} = 2$, $g_{60} = 3$, $g_{64} = 1$, $g_{68} = 3$, $g_{72} = 1$, $g_{76} = 4$, $g_{88} = 4$ i $g_{92} = 5$. Així els únics N tal que la involució Υ és involució biel·líptica són $N = 40, 48, 64$ i 72.*

5.3.3 $X_0(N)/w_{2^{\upsilon_2(N)}}S_2w_{2^{\upsilon_2(N)}}$ és $X_0(N/2)$

Proposició 5.3.2. *La corba $X_0(N)/w_{2^{\upsilon_2(N)}}S_2w_{2^{\upsilon_2(N)}}$ és $X_0(N/2)$ i a més l'aplicació $\pi : X_0(N) \to X_0(N)/w_{2^{\upsilon_2(N)}}S_2w_{2^{\upsilon_2(N)}}$ és la projecció usual.*

Demostració. Sols cal notar que $w_{2^{\upsilon_2(N)}}S_2w_{2^{\upsilon_2(N)}} \in \Gamma_0(N/2) \setminus \Gamma_0(N)$. La involució identifica els elements $\Gamma_0(N/2)$ equivalents, és a dir, és la projecció. □

Lema 5.3.3. *Sigui $N = 2^{\upsilon_2(N)}\prod_i p_i^{n_i}$ amb $\upsilon_2(N) \geq 2$ i suposem $\upsilon_2(N) \equiv 1(mod\ 2)$, llavors si $P = \begin{pmatrix} x \\ d \end{pmatrix}$ és una punta de $X_0(N)$ amb $\upsilon_2(d) \leq [\frac{\upsilon_2(N)}{2}]$ llavors és fixa per la involució $w_{2^{\upsilon_2(N)}}S_2w_{2^{\upsilon_2(N)}}$.*

Demostració. Denotem $P = \begin{pmatrix} x \\ d \end{pmatrix}$ $(x,d) = 1$ on x és un representant invertible mòdul t i $t = (d, N/d)$; denotem per $\pi : X_0(N) \to X_0(N/2)$ la projecció usual. Sigui P amb $\upsilon_2(d) \leq [\frac{\upsilon_2(N)}{2}]$. Notem que $\pi(P) = P$. Sigui $P' = \begin{pmatrix} x' \\ d' \end{pmatrix}$ on $\pi(P') = P$, llavors s'ha de complir que $d = d'$ i $x' \equiv x (mod\, t')$ on $t' = (d, N/2d)$. Però de $\upsilon_2(N) \equiv 1 (mod\ 2)$ tenim $t' = t$, i $P = P'$ a $X_0(N)$. □

Lema 5.3.4. *Sigui $N = 2^{\upsilon_2(N)} \prod_i p_i^{n_i}$ amb $\upsilon_2(N) \geq 2$ i suposem $\upsilon_2(N) \equiv 0 (mod\ 2)$, llavors si $P = \begin{pmatrix} c \\ d \end{pmatrix}$ és una punta de $X_0(N)$ amb $\upsilon_2(d) < [\frac{\upsilon_2(N)}{2}]$ és fixa per la involució $w_{2^{\upsilon_2(N)}} S_2 w_{2^{\upsilon_2(N)}}$.*

Demostració. La prova és la mateixa que en el lema anterior. □

Corol·lari 5.3.5. *Sigui $N = 2^{\upsilon_2(N)} \prod_i p_i$ on p_i són primers diferents i $4|N$, i denotem per $g_0(N)$ el gènere de $X_0(N)$. Si $\upsilon_2(N) \equiv 1 (mod\ 2)$ i es compleix que $g_0(N/2) \neq [g_0(N)/2]$ llavors totes les puntes de $X_0(N)$ són punts de Weierstrass.*

Demostració. Conseqüència immediata de la prova del lema 5.3.3, del teorema de Schoeneberg i del corol·lari 5.2.12 □

Corol·lari 5.3.6. *Sigui $N = 2^{\upsilon_2(N)} \prod_i p_i$ on p_i són primers diferents i $4|N$, i denotem per $g_0(N)$ el gènere de $X_0(N)$. Si $\upsilon_2(N) \equiv 0 (mod\ 2)$ i es compleix que $g_0(N/2) \neq [g_0(N)/2]$ llavors totes les puntes $P = \begin{pmatrix} x \\ d \end{pmatrix}$ de $X_0(N)$, a excepció de les puntes amb $\upsilon_2(d) = [\frac{\upsilon_2(N)}{2}]$, són punts de Weierstrass.*

Demostració. Conseqüència immediata de la prova del lema 5.3.4, del teorema de Schoeneberg i del corol·lari 5.2.12. □

5.4 Breu estudi de $w_r S_2$ i $w_r w_{2^{\upsilon_2(N)}} S_2 w_{2^{\upsilon_2(N)}}$

5.4.1 Introducció

Sigui $X_0(N)$ amb $N \equiv 0 (mod\ 4)$. Aleshores $w_r S_2$ i $w_r w_{2^{\upsilon_2(N)}} S_2 w_{2^{\upsilon_2(N)}}$ són involucions pel fet que S_2 i w_r commuten. Anem a calcular el gènere de $X_0(N)/\Xi_{i,r}$, on $\Xi_{1,r} = w_r S_2$ i $\Xi_{2,r} = w_r w_{2^{\upsilon_2(N)}} S_2 w_{2^{\upsilon_2(N)}}$.

5.4.2 Breu estudi de $\Xi_{1,r}$, $(r,2)=1$

Posant $w_r = \frac{1}{\sqrt{r}} \begin{pmatrix} rk & 1 \\ Nt & r \end{pmatrix}$ tenim que $\Xi_{1,r} = \frac{1}{\sqrt{r}} \begin{pmatrix} rk & \frac{rk}{2}+1 \\ Nt & \frac{Nt}{2}+r \end{pmatrix}$. Escrivint l'anterior expressió de la següent forma:

$$\frac{1}{\sqrt{r}} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} k & rk+2 \\ \frac{Nt}{2r} & \frac{Nt}{2}+r \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$$

veiem que si τ és un punt fix de $\Xi_{1,r}$ llavors es compleix:

$$\frac{1}{\sqrt{r}} \begin{pmatrix} k & rk+2 \\ \frac{Nt}{2r} & \frac{Nt}{2}+r \end{pmatrix} \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \tau = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \gamma\tau$$

on $\gamma \in \Gamma_0(N)$, i d'aquí

$$\frac{1}{\sqrt{r}} \begin{pmatrix} rk & rk+2 \\ \frac{Nt}{2} & \frac{Nt}{2}+r \end{pmatrix} (2\tau) = \delta(2\tau)$$

amb $\delta \in \Gamma_0(N/2,2)$. Observem, però, que la matriu de l'esquerra no és res més que la involució d'Atkin-Lehner w_r de $X_0(N/2)$. Per tant, obtenim

Lema 5.4.1. *Sigui τ un punt fix de $X_0(N)$ per la involució $\Xi_{1,r}$. Llavors 2τ és un punt fix de w_r a $X_0(N/2)$.*

Considerem $X_0(N) \to X_0(N)/S_2$ i sigui τ un punt fix de w_r en $Y_0(N/2)$. τ puja a dos punts en $Y_0(N)$; denotem-los per τ' i $S_2(\tau')$, si τ' no és un punt el·líptic de Γ_N. Considerem w_r involució d'Atkin-Lehner en $X_0(N)$. Volem caracteritzar els $\tau'' \in Y_0(N)$ complint $w_r S_2 \tau'' = \gamma\tau''$, $\gamma \in \Gamma_0(N)$. Observem, però, que si $\tau'' \in Y_0(N)$ és punt fix de w_r tenim

$$w_r\tau'' = \gamma\tau''$$

, $\gamma \in \Gamma_0(90)$. Com que S_2 i w_r són del normalitzador de $\Gamma_0(90)$ i commuten tenim llavors

$$w_r S_2 \tau'' = \gamma' S_2 \tau''$$

, $\gamma' \in \Gamma_0(N)$; seguint el mateix argument que en la prova del lema anterior obtenim

$$w_r 2\tau'' = \delta \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} 2\tau''$$

, $\delta \in \Gamma_0(N/2,2)$. Això prova que els punts fixos de w_r en $X_0(N)$ van a punts fixos de w_r en $X_0(N/2)$ complint $w_r 2\tau'' = \beta 2\tau''$, amb $\beta \in \Gamma_0(N/2) \setminus \Gamma_0(N/2,2)$.

Lema 5.4.2. *El nombre de punts fixos de $w_r S_2$, que denotem per κ, compleix la igualtat següent:*

$$\kappa = 2(\frac{N}{2})_{w_r} - N_{w_r}$$

on M_{w_r} denota el nombre de punts fixos de la involució w_r a $X_0(M)$.

Anem a utilitzar els resultats anteriors pel càlcul del gènere de $X_0(N)/\Xi_{1,r}$.

Corol·lari 5.4.3. *Denotem per $g_{r,N}$ el gènere de $X_0(N)/w_r S_2$. Aleshores es té: $g_{40,5} = 2$, $g_{44,11} = 1$, $g_{48,3} = 2$, $g_{52,13} = 2$, $g_{56,7} = 2$, $g_{60,3} = 4$, $g_{60,5} = 2$, $g_{60,15} = 3$, $g_{68,17} = 2$, $g_{72,9} = 3$, $g_{76,19} = 3$, $g_{88,11}2$ i $g_{92,23} = 4$. Per tant, l'únic valor pel qual aquesta involució és biel·líptica és $N = 44$.*

Demostració. Explicitarem la prova en un cas particular i els altres es fan anàlogament. Considerem $X_0(52)/\Xi_{1,13}$. Per 5.2.8 tenim que

$$\int_{\overline{\mathbb{H}}/(\Gamma:=\Gamma_0(52)\cup\Xi_{1,13}\Gamma_0(52))} y^{-2}dxdy = 2g_{52,13} - 2 + m + \sum_{i=1}^{r} \frac{1}{2}$$

Utilitzant que $(\Gamma : \Gamma_0(52)) = 2$ i aplicant 5.2.8 per a $\Gamma_0(52)$ juntament amb l'anterior igualtat, obtenim

$$7 = 2g_{52,13} - 2 + m + \sum_{i=1}^{r} \frac{1}{2}$$

Un comprova que $w_{13}S_2$ no deixa fixa cap punta, i per tant $m = 3$. Com que els punts fixos de la involució w_{13} en $X_0(26)$ són exactament 2, aquests dos punts pugen a 4 punts ja que la involució w_{13} no té punts fixos en $X_0(52)$, per tant, $7 = 2g_{52,13} - 2 + 3 + 2$ i $g_{52,13} = 2$. □

5.4.3 Breu estudi de $\Xi_{2,r}$

Si τ és un punt fix d l'anterior involució, és equivalentment un punt el·líptic d'ordre 2 del grup fuchsià $\Gamma := \Gamma_0(N) \cup \Xi_{2,r}\Gamma_0(N)$. Sigui $\tau \in Y_0(N)$ un punt fix, és a dir, $\beta w_r \tau = \gamma\tau$, on $\beta = w_{2^{v_2(N)}} S_2 w_{2^{v_2(N)}}$, de $\Gamma_0(N/2) \setminus \Gamma_0(N)$. Multiplicant l'anterior expressió per β a l'esquerra i pensant que $\beta^2 = 1$ tenim $w_r\tau = \delta\tau$, $\delta \in \Gamma_0(N/2) \setminus \Gamma_0(N)$. Això ens diu que τ és un punt fix de w_r a $X_0(N/2)$ (per ser la mateixa involució en $X_0(N)$ i $X_0(N/2)$) i que τ no és un punt fix de w_r a $X_0(N)$ a menys que τ sigui un punt el·líptic de $X_0(N/2)$. En aquest cas aquest punt sols puja a un punt de $X_0(N)$, ja que $X_0(N)$ no té punts el·líptics. Per tant, s'obté el següent lema:

Lema 5.4.4. *El nombre de punts fixos de $w_r w_{2^{v_2(N)}} S_2 w_{2^{v_2(N)}} w_r$, que denotem per κ, compleix la igualtat següent:*

$$\kappa = 2(\frac{N}{2})_{w_r} - N_{w_r}$$

on M_{w_r} denota el nombre de punts fixos de la involució w_r a $X_0(M)$.

Corol·lari 5.4.5. *Denotem per $g_{N,r}$ el gènere de $X_0(N)/\Xi_{2,r}$. Aleshores: $g_{40,5} = 2$, $g_{44,11} = 1$, $g_{48,3} = 2$, $g_{52,13} = 2$, $g_{56,7} = 2$, $g_{60,3} = 4$, $g_{60,5} = 2$, $g_{60,15} = 3$, $g_{68,17} = 2$, $g_{72,9} = 3$ $g_{76,19} = 3$, $g_{88,11} = 2$ i $g_{92,23} = 4$.*
Per tant, l'únic valor pel qual aquesta involució és biel·líptica és $N = 44$.

Demostració. Pels casos $N = 40, 48, (60, 3), 72$ la involució d'Atkin-Lehner corresponent no té cap punt fix en $X_0(N/2)$ i el càlcul del gènere únicament es basa en el nombre de puntes no Γ-equivalents, amb $\Gamma = \Gamma_0(N) \cup \Xi_{2,r}\Gamma_0(N)$. En aplicar 5.2.8 utilitzant les mateixes tècniques que en el corol·lari 5.2.9 s'obté el resultat. Els altres casos es fan semblantment. □

5.5 Resum de resultats $4||N$

Proposició 5.5.1. *Les corbes modulars $X_0(N)$ amb $N = 52$, 68 i 76 no són corbes modulars biel·líptiques.*

Demostració. Tenim que $Aut(X_0(N)) = Norm(\Gamma_0(N)) = \mathbb{Z}/2 \times \mathcal{S}_3$, d'ordre 12, on l'element d'ordre dos del primer factor correspon a w_p $(p, 2) = 1$ i les involucions que vénen del segon factor corresponen a $S_2, w_{2^{v_2(N)}}, w_{2^{v_2(N)}} S_2 w_{2^{v_2(N)}}$. Així, totes les involucions són, pel cas $4||N$ amb $N = 4p$, de la forma $w_p, w_4, w_N, S_2, w_4 S_2 w_4, w_p S_2$ i $w_p w_4 S_2 w_4$. Dels corol·laris 5.2.9, 5.3.1,5.4.3 i 5.4.5 i del fet que les corbes $X_0(N)$ no admeten involucions d'Atkin-Lehner biel·líptiques arribem a la conclusió que $X_0(N)$ no pot ser biel·líptica. □

Corol·lari 5.5.2. *La corba modular $X_0(72)$ és biel·líptica. Dues de les seves involucions biel·líptiques són S_2 i $w_8 S_2 w_8$.*

Demostració. Conseqüència immediata dels lemes 5.2.9 i 5.3.1. □

Corol·lari 5.5.3. *Totes les involucions biel·líptiques de $X_0(44)$ són $w_{11}S_2$, w_{11}, w_{44}, $w_{11}w_4S_2w_4$.*
L'única involució biel·líptica de $X_0(60)$ és w_{15}.
L'única involució biel·líptica de $X_0(92)$ és w_{23}

Demostració. Conseqüència dels lemes i corol·laris 5.2.9,5.3.1,5.4.3,5.4.5 i 3.4.2. □

Nota 5.5.4. *El fet que la involució de $X_0(60)$ i $X_0(92)$ sigui única prové del següent resultat:*

Teorema 5.5.5 (Desigualtat de Castelnuovo-Severi). *Si X és una superfície de Riemann de gènere g i admet una involució T. Denotem per g_T el gènere de X/T. Llavors si $g > 4g_T + 1$, T és única.*

Com a referència es pot consultar [2](pàg 51).

Capítol 6

L'estudi en el cas $8|N$

6.1 Introducció

Hem estudiat en el capítol anterior totes les involucions de $X_0(N)$ en el cas $N = 4\prod p^{n(p)}$ amb $(p^{n(p)}, 9) \leq 3$ i $(p, 2) = 1$. Anem a estudiar ara les involucions que apareixen quan $N = 8\prod p^{n(p)}$, p primers senars diferents i $(p^{n(p)}, 9) \leq 3$. De l'estructura de $Norm(\Gamma_0(N))$ cal reduir-nos a estudiar el grup

$$\prod \frac{\mathbb{Z}}{2\mathbb{Z}} \times \{S_2, w_8; S_2^2 = w_8^2 = 1, S_2 w_8 S_2 w_8 = w_8 S_2 w_8 S_2\}$$

Considerem primer el factor del grup $\{S_2, w_8\}$. La resta de les involucions consistirà en aquestes multiplicades per les involucions d'Atkin-Lehner, pel fet de ser el producte directe. Fent els càlculs pertinents obtenim que totes les involucions en aquest cas són:

$$\begin{array}{ccc} w_s & S_2 & w_8 S_2 w_8 \\ S_2 w_8 S_2 w_8 & w_s S_2 \ (s,2)=1 & w_s w_8 S_2 w_8 \ (s,2)=1 \\ w_s S_2 w_8 S_2, \ (s,2)=1 & w_s S_2 w_8 S_2 w_8, \ (s,2)=1 & S_2 w_8 S_2 \\ & w_8 & w_s w_8 \end{array}$$

On s recorre els divisors positius de N complint $1 = (s, N/s)$, $(s, 2) = 1$.
Les involucions w_s, w_8 ja han estat tractades en el capítol 3 i les involucions $w_8 S_2 w_8$, S_2, $w_s S_2$, $(s, 2) = 1$, i $w_s w_8 S_2 w_8$, $(s, 2) = 1$, en el capítol anterior. Per tant anem a centrar-nos en les altres 4 involucions ens falta estudiar. Pensem bàsicament en el cas $N = 88$, per a poder decidir si la corba modular $X_0(88)$ és biel·líptica, però també en $N = 56$ per a poder determinar totes les involucions biel·líptiques. El cas $N = 40$ el tractarem apart en un apèndix. Observem que les anteriors involucions també ho són per $X_0(72)$, per tant també tractarem aquest cas.

6.2 L'estudi de $S_2 w_8 S_2$

Estudiem els punts fixos a $Y_0(N)$ de l'anterior involució. Donem una fita del seu nombre:

Lema 6.2.1. *El nombre de punts fixos de la involució $S_2 w_8 S_2$ a $Y_0(N)$ és fitat per*

$$4\upsilon(2, N/4)$$

on $\upsilon(2, N/4)$ és el nombre de punts fixos de la involució d'Atkin-Lehner w_2 de $X_0(N/4)$.

Demostració. De $w_8 = \frac{1}{\sqrt{2}} \begin{pmatrix} 4k & 1/2 \\ 4tu & 4 \end{pmatrix}$ tenim

$$S_2 w_8 S_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 2(2k+tu) & \frac{5+4k+2tu}{2} \\ 4tu & 2(2+tu) \end{pmatrix}$$

i la següent igualtat

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 2(2k+tu) & 5+4k+2tu \\ 2tu & 2(2+tu) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix} \tau = \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix} \gamma\tau = \delta 2\tau$$

on $\gamma \in \Gamma_0(N)$ i $\delta \in \Gamma_0(N/2, 2)$. Observem que en l'anterior expressió la matriu de l'esquerra correspon a la involució d'Atkin-Lehner w_2 de $X_0(N/4)$. □

Corol·lari 6.2.2. *Si denotem per g_N el gènere de la corba $X_0(N)/S_2 w_8 S_2$, aleshores: $g_{56} = 3$ i $g_{88} \geq 2$*

Demostració. Pel cas $N = 56$ observem que el nombre de punts fixos de w_2 en $X_0(14)$ és zero. Així, per 5.2.8 i el fet que la involució defineix un morfisme de grau 2 de $X_0(N)$:

$$8 = 2g_{56} - 2 + m$$

on m són les puntes no Γ-equivalents i $\Gamma = \Gamma_0(56) \cup S_2 w_8 S_2 \Gamma_0(56)$. Un càlcul dóna $m = 4$ i d'aquí $g_{56} = 3$.
Pel cas $N = 88$ tenim que w_2 té dos punts fixos a $X_0(22)$ i com que l'extensió és de grau 4:

$$12 \leq 2g_{88} - 2 + m + 4$$

Un càlcul senzill dóna $m = 4$, d'on $g_{88} > 1$. □

Lema 6.2.3. *El nombre de punts fixos de la involució $S_2 w_8 S_2$ en $Y_0(N)$ és igual al nombre de punts fixos de w_8 en $Y_0(N)$.*

Demostració. Si τ és un punt fix de $S_2w_8S_2$ per ser S_2 del normalitzador de $\Gamma_0(N)$ es compleix

$$w_8S_2\tau = \gamma S_2\tau.$$

Posant $\tau' = S_2\tau$ obtenim que τ' és un punt fix de w_8 en $Y_0(N)$. Com que S_2 és una involució de $X_0(N)$ obtenim el resultat. □

Corol·lari 6.2.4. *Seguint la notació del corol·lari anterior tenim $g_{88} = 4$ i $g_{72} = 2$.*

Demostració. La prova és la mateixa que en l'anterior corol·lari, però en aquesta situació coneixem tots els punts el·líptics d'ordre 2 que apareixen en el grup fuchsià $\Gamma_0(N) \cup S_2w_8S_2\Gamma_0(N)$. □

6.3 Estudi de la involució $S_2w_8S_2w_8$

Denotem per $w_8 = \frac{1}{\sqrt{2}}\begin{pmatrix} 4k & 1/2 \\ 4tu & 4 \end{pmatrix}$. Aleshores podem escriure

$$S_2w_8S_2w_8 = \begin{pmatrix} 8k^2 + 5tu + 8ktu + 2tu^2 & 5 + 5k + \frac{5tu}{2} \\ 4tu(2 + 2k + tu) & 8 + 5tu \end{pmatrix}$$

Lema 6.3.1. *Una fita pel nombre de punts fixos a $Y_0(N)$ de $S_2w_8S_2w_8$ és:*

$$4(\upsilon(2) + \upsilon(3))$$

on $\upsilon(i)$ és el nombre de punts el·líptics d'ordre i de $X_0(N/4)$.

Demostració. De $S_2w_8S_2w_8\tau = \gamma\tau$, $\gamma \in \Gamma_0(N)$ tenim:

$$\begin{pmatrix} 8k^2 + 5tu + 8ktu + 2tu^2 & 10 + 10k + 5tu \\ 2tu(2 + 2k + tu) & 8 + 5tu \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix}\tau = \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix}\gamma\tau$$

i d'aquí

$$\begin{pmatrix} 8k^2 + 5tu + 8ktu + 2tu^2 & 10 + 10k + 5tu \\ 2tu(2 + 2k + tu) & 8 + 5tu \end{pmatrix} 2\tau = \delta 2\tau$$

amb $\delta \in \Gamma_0(N/2, 2)$. Per ser $(tu, 2) = 1$, la matriu de l'esquerra és de $\Gamma_0(N/4)\backslash\Gamma_0(N/2)$. Per tant, 2τ és un punt el·líptic de $\Gamma_0(N/4)$ i això conclou la demostració. □

Corol·lari 6.3.2. *Sigui g_N el gènere de $X_0(N)/S_2w_8S_2w_8$, llavors $g_{56} = 3$, $g_{88} = 5$ i $g_{72} = 3$.*

Demostració. La prova es anàloga al corol·lari de la secció anterior. □

6.4 L'estudi de $w_s S_2 w_8 S_2$

Considerem w_s amb $(s,2)=1$.

Lema 6.4.1. *El nombre de punts fixos de $w_s S_2 w_8 S_2$ a $Y_0(N)$ ve fitat per $4v(s2, N/4)$ on $v(s2, N/4)$ denota el nombre de punts fixos de la involució d'Atkin-Lehner w_{s2} a $X_0(N/4)$.*

Demostració. Si escrivim $N = 8t$,

$$w_s = \frac{1}{\sqrt{s}} \begin{pmatrix} si & 1 \\ 8tq & s \end{pmatrix} \quad i \quad S_2 w_8 S_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 2(2k+tu) & 2k+tu+\frac{5}{2} \\ 4tu & 2(2+tu) \end{pmatrix}$$

obtenim

$$w_s S_2 w_8 S_2 = \tfrac{1}{\sqrt{2s}} \begin{pmatrix} 2(2ksi+2tu+situ) & \frac{8+5si+4ksi+4tu+2situ}{2} \\ 4(8ktq+stu+4tqtu) & 2(2s+10tq+8ktq+stu+4tqtu) \end{pmatrix}$$

i d'aquí:

$$\begin{pmatrix} 2(2ksi+2tu+situ) & 8+5si+4ksi+4tu+2situ \\ 2(8ktq+stu+4tqtu) & 2(2s+10tq+8ktq+stu+4tqtu) \end{pmatrix} 2\tau = \delta 2\tau$$

amb $\delta \in \Gamma_0(N/2, 2)$. L'expressió de l'esquerra correspon a la involució w_{2s} de $X_0(N/4)$. □

Corol·lari 6.4.2. *Denotem per $g_{N,s}$ el gènere de $X_0(N)/w_s S_2 w_8 S_2$. Llavors $g_{88,11} \geq 3$.*

Demostració. w_{22} té 2 punts fixos a $X_0(22)$, per tant,

$$12 \leq 2g_{88,11} - 2 + m + 4$$

En aquest cas $m = 4$, d'on obtenim $g_{88,11} \geq 3$. □

Lema 6.4.3. *El nombre de punts fixos de la involució $w_s S_2 w_8 S_2$ a $Y_0(N)$ és igual al nombre de punts fixos de la involució $w_s w_8$ a $Y_0(N)$.*

Demostració. Notem que si τ és un punt fix de la involució en $Y_0(N)$, pel fet que S_2 commuta amb w_s i és del normalitzador de $\Gamma_0(N)$ tenim

$$w_s w_8 S_2 \tau = \gamma S_2 \tau$$

amb $\gamma \in \Gamma_0(N)$. Posant $\tau' = S_2\tau$, obtenim que τ' és un punt fix en $Y_0(N)$ de la involució $w_s w_8$. Desfent el canvi obtenim el resultat. □

Corol·lari 6.4.4. *En la notació del corol·lari anterior tenim: $g_{88,11} = 4$, $g_{72,9} = 2$ i $g_{56,7} = 1$.*

Demostració. La prova és la mateixa que en el lema anterior, però en aquest cas coneixem els punts fixos de la involució. □

6.5 La involució $w_s S_2 w_8 S_2 w_8$

Lema 6.5.1. *El nombre de punts fixos de la involució $w_s S_2 w_8 S_2 w_8$ a $Y_0(N)$ és igual al nombre de punts fixos de la involució $w_s S_2$ a $Y_0(N/2)$ i que no són fixos per la involució $w_s S_2$ a $Y_0(N)$.*

Demostració. Com que S_2 i w_s commuten tenim que si $\tau \in Y_0(N)$ és un punt fix de la involució $w_s S_2 w_8 S_2 w_8$ compleix

$$w_s S_2 \tau = \gamma w_8 S_2 w_8 \tau$$

amb $\gamma \in \Gamma_0(N)$. Observem que S_2 i w_s són tant involucions de $X_0(N)$ com de $X_0(N/2)$. Llavors, fent la projecció, τ és un punt fix de la involució $w_s S_2$ en $Y_0(N/2)$. Com que puja a dos punts en $Y_0(N)$, ($X_0(N/2)$ no té punts el·líptics) no ha de ser punt fix per la involució $w_s S_2$. □

Corol·lari 6.5.2. *Denotem per g_N el gènere de $X_0(N)/w_s S_2 w_8 S_2 w_8$. Llavors $g_{56} = 3$, $g_{72} = 1$ i $g_{88} = 5$.*

Demostració. Fem el cas $N = 88$, els altres dos casos es fan de la mateixa manera. Un obté que el nombre de punts fixos de $w_{11} S_2$ en $Y_0(44)$ és 6, i el nombre de punts fixos de $w_{11} S_2$ en $Y_0(88)$ 12. Per tant, a $Y_0(88)$ no hi tenim punts fixos per la involució $w_s S_2 w_8 S_2 w_8$, la qual tampoc deixa cap punta de $X_0(88)$ fixa. Així

$$12 = 2g_{88} - 2 + 4$$

i d'aquí $g_{88} = 5$. □

6.6 Conclusió en el cas $8||N$

Proposició 6.6.1. *La corba modular $X_0(88)$ no és biel·líptica*

Demostració. Totes les seves involucions han estat estudiades en aquest capítol i en l'anterior. En tots els casos el quocient per les involucions té gènere superior a dos. □

Corol·lari 6.6.2. *Totes les involucions biel·líptiques de $X_0(56)$ són w_7, w_{56} i $w_7 S_2 w_8 S_2$.*

Capítol 7

La corba modular $X_0(90)$

Anem a estudiar totes les involucions de $X_0(90)$ per si n'hi ha alguna de biel·líptica. Sigui $\upsilon \in Aut(X_0(90)) = Norm(\Gamma_0(90))$ una involució i denotem per g el gènere de la corba $X_0(90)/\upsilon$. Com que el gènere de $X_0(90)$ és 11 i té 16 puntes obtenim:

$$18 = 2g - 2 + m + \sum_{i=1}^{r} \frac{1}{2}$$

on m denota el nombre de les puntes no $(\Gamma_0(90) \cup \upsilon\Gamma_0(90))$-equivalents i r el nombre de punts el·líptics del grup fuchsià $\Gamma_0(90) \cup \upsilon\Gamma_0(90)$, que també es correspon amb el nombre de punts fixos en $Y_0(90)$ de la involució υ.

Lema 7.1. *Totes les involucions de $X_0(90)$, llevat les del tipus d'Atkin-Lehner que ja coneixem, són les següents* [1]*:*

$S_3 w_9 S_3^2 = \begin{pmatrix} -13 & -\frac{22}{3} \\ -30 & -17 \end{pmatrix}$	$S_3^2 w_9 S_3 = \begin{pmatrix} -23 & -\frac{16}{3} \\ -30 & -7 \end{pmatrix}$
$w_{10} S_3 w_9 S_3^2 = \begin{pmatrix} 2075\sqrt{10} & \frac{35123}{3\sqrt{10}} \\ 10689\sqrt{10} & 6031\sqrt{10} \end{pmatrix}$	$w_{10} S_3^2 w_9 S_3 = \begin{pmatrix} 3595\sqrt{10} & \frac{25013}{3\sqrt{10}} \\ 18519\sqrt{10} & 4295\sqrt{10} \end{pmatrix}$
$w_5 S_3 = \begin{pmatrix} -7\sqrt{5} & -\frac{32}{3\sqrt{5}} \\ -36\sqrt{5} & -11\sqrt{5} \end{pmatrix}$	$w_5 S_3^2 = \begin{pmatrix} -7\sqrt{5} & -\frac{67}{3\sqrt{5}} \\ -36\sqrt{5} & -23\sqrt{5} \end{pmatrix}$

[1] Nota: Importa l'ordre en el que anotem les involucions

$w_5w_9S_3w_9 = \begin{pmatrix} -143\sqrt{5} & \frac{74}{\sqrt{5}} \\ -744\sqrt{5} & 77\sqrt{5} \end{pmatrix}$	$w_5w_9S_3^2w_9 = \begin{pmatrix} -293\sqrt{5} & \frac{149}{\sqrt{5}} \\ -1524\sqrt{5} & 155\sqrt{5} \end{pmatrix}$
$w_2S_3 = \begin{pmatrix} 23\sqrt{2} & \frac{49}{3\sqrt{2}} \\ 45\sqrt{2} & 16\sqrt{2} \end{pmatrix}$	$w_2S_3^2 = \begin{pmatrix} 23\sqrt{2} & \frac{95}{3\sqrt{2}} \\ 45\sqrt{2} & 31\sqrt{2} \end{pmatrix}$
$w_2w_9S_3w_9 = \begin{pmatrix} 817\sqrt{2} & -\frac{169}{\sqrt{2}} \\ 1605\sqrt{2} & -166\sqrt{2} \end{pmatrix}$	$w_2w_9S_3^2w_9 = \begin{pmatrix} 1657\sqrt{2} & -\frac{337}{\sqrt{2}} \\ 3255\sqrt{2} & -331\sqrt{2} \end{pmatrix}$

Demostració. Hem vist, pel corol·lari 3.1.17, que tot element es pot escriure com $w_\delta\alpha$ on $\delta = 1, 2, 5$ *o* 10 i $\alpha \in \{w_9, S_3 | w_9^2 = S_3^3 = (w_9S_3)^3 = 1\}$. Escrivint-los tots i calculant quins tenen el seu quadrat en $\Gamma_0(90)$ s'obté l'enunciat. □

Lema 7.2. *Les involucions $S_3w_9S_3^2$ i $S_3^2w_9S_3$ no són biel·líptiques.*

Demostració. Fem la prova en el cas $S_3w_9S_3^2$. L'altre cas és exactament anàlog. Escrivim:

$$S_3w_9S_3^2 = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} -13 & -22 \\ -10 & -17 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$$

Si $\tau \in Y_0(90)$ és un punt fix per la involució $S_3w_9S_3^2$ llavors

$$\begin{pmatrix} -13 & -22 \\ -10 & -17 \end{pmatrix} 3\tau = \delta 3\tau \tag{7.1}$$

amb $\delta \in \Gamma_0(30, 3)$. Considerem $\theta : X_0(90) \to X_0(30)$ que sigui multiplicar per 3, i $proj : X_0(30) \to X_0(10)$. Observem que si τ és un punt fix a $Y_0(90)$ de $S_3w_9S_3^2$ es correspon, via $proj \circ \theta$, amb un dels dos punts el·líptics de $X_0(10)$ per la igualat 7.1; anomenem aquests dos punts τ_1, τ_2. Anem a fer un estudi del nombre d'elements que poden pujar τ_1, τ_2 a punts de $X_0(90)$ via el morfisme $proj \circ \theta$. Com $X_0(30)$ no té punts el·líptics i els dos punts el·líptics de $X_0(10)$ són d'ordre 2 $\#proj^{-1}(\tau_i) \leq 3$ per $i = 1, 2$, per tant, $\#(proj \circ \theta)^{-1}(\tau_i) \leq 9$ per $i = 1, 2$. D'aquí s'obté que el nombre màxim de punts $\tau \in Y_0(90)$ fixos per la involució $S_3w_9S_3^2$ és 18. Igualment, un càlcul directe prova que el nombre de puntes $\Gamma_0(90) \cup S_3w_9S_3^2\Gamma_0(90)$-no equivalents és 8. Si g és el gènere de $X_0(90)/S_3w_9S_3^2$, aplicant 5.2.8 s'obté:

$$18 \leq 2g - 2 + 8 + 9$$

i per tant $g \geq 2$ d'on la involució no és biel·líptica. □

Lema 7.3. *Les involucions w_2S_3, $w_2S_3^2$, $w_2w_9S_3w_9$ i $w_2w_9S_3^2w_9$ no són involucions biel·líptiques.*

Demostració. Considerem

$$w_2S_3^2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 46 & \frac{95}{3} \\ 90 & 62 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 46 & 95 \\ 30 & 62 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$$

Si $\tau \in Y_0(90)$ punt fix per la involució $w_2S_3^2$ llavors

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 46 & 95 \\ 30 & 62 \end{pmatrix} 3\tau = \delta 3\tau$$

i $\tau' = 3\tau = \theta(\tau)$, ($\theta : X_0(90) \to X_0(30)$ multiplicar per 3), és un punt fix de la involució d'Atkin-Lehner w_2 de $X_0(30)$ que no té cap punt fix. Per tant obtenim que $w_2S_3^2$ no té punts fixos en $Y_0(90)$. Així si g és el gènere de $X_0(90)/w_2S_3^2$ obtenim utilitzant 5.2.8:

$$18 = 2g - 2 + m$$

on m és el nombre de puntes del grup fuchsià $\Gamma_0(90) \cup w_2S_3^2\Gamma_0(90)$, menor que el nombre de puntes del grup fuchsià $\Gamma_0(90)$, que és 16, i d'aquí obtenim $g \geq 2$. Així la involució $w_2S_3^2$ no és biel·líptica. Demostració anàloga pels casos restants. □

Lema 7.4. *Les involucions w_5S_3, $w_5S_3^2$, $w_5w_9S_3w_9$ i $w_5w_9S_3^2w_9$ no són involucions biel·líptiques.*

Demostració. Considerem w_5S_3.
Escrivim

$$w_5S_3 = \frac{1}{\sqrt{5}}\begin{pmatrix} -35 & -\frac{32}{3} \\ -180 & -55 \end{pmatrix} = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} -35 & -32 \\ -60 & -55 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$$

Si $\tau \in Y_0(90)$ és un punt fix de w_5S_3 tenim

$$\frac{1}{\sqrt{5}}\begin{pmatrix} -35 & -32 \\ -60 & -55 \end{pmatrix} 3\tau = \delta 3\tau$$

on $\delta \in \Gamma_0(30, 3)$. Per tant, $\tau' = 3\tau$ és un dels 4 punts fixos de la involució w_5 en $X_0(30)$. Com que $X_0(90) \to X_0(30)$ té grau 3 com a molt el nombre de punts fixos de la involució w_5S_3 en $Y_0(90)$ és 12. Com que la involució no deixa cap punta fixa obtenim, si $g = gènere(X_0(90)/w_5S_3)$, utilitzant 5.2.8:

$$18 \leq 2g - 2 + 8 + 6$$

i d'aquí $g \geq 2$.
Les altres involucions es tracten exactament igual, observant que totes les involucions del lema no deixen cap punta de $X_0(90)$ fixa. □

Lema 7.5. *Les involucions $w_{10}S_3w_9S_3^2$ i $w_{10}S_3^2w_9S_3$ no són biel·líptiques.*

Demostració. Denotem per $i = w_{10}$ $i' = w_{10}S_3w_9S_3^2$ o $w_{10}S_3^2w_9S_3$. Llavors si $\tau \in Y_0(N)$ és un punt fix de la involució i compleix

$$\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} w_{10}^{10}3\tau = \gamma\tau \quad \gamma \in \Gamma_0(90)$$

i també

$$w_{10}^{10}3\tau = \delta 3\tau, \ \delta \in \Gamma_0(30,3) \tag{7.2}$$

on w_{10}^{10} és la involució d'Atkin-Lehner en $X_0(10)$. Per tant es correspon amb algun dels dos punts fixos de la involució w_{10} en $Y_0(10)$ via el morfisme $X_0(90) \to X_0(10)$ (multiplicar per 3). Anem a fer un estudi més profund del nombre de punts que pot pujar complint la condició anterior. Observem, altre cop treballant en $Y_0(90)$, que els punts fixos τ de la involució i compleixen

$$w_{10}\tau = \gamma i'\tau$$

, amb $\gamma \in \Gamma_0(90)$, pel fet que w_{10} i i' commuten i són del $Norm(\Gamma_0(90))$. D'aquí, quan $i' = S_3w_9S_3^2$ escrivint $\gamma = \begin{pmatrix} a & b \\ 90c & d \end{pmatrix}$ obtenim:

$$\frac{1}{\sqrt{10}}\begin{pmatrix} 10k & 1 \\ 90t & 10 \end{pmatrix}\tau = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} a & 3b \\ 30c & d \end{pmatrix}\begin{pmatrix} -13 & -22 \\ -10 & -17 \end{pmatrix}3\tau \tag{7.3}$$

Del fet que $\begin{pmatrix} -13 & -22 \\ -10 & -17 \end{pmatrix} = \beta\begin{pmatrix} 1 & 1 \\ 10 & 11 \end{pmatrix}$, $\beta \in \Gamma_0(30)$ tenim

$$w_{10}^{30}3\tau = \frac{1}{\sqrt{10}}\begin{pmatrix} 10k & 3 \\ 30t & 10 \end{pmatrix}3\tau = \beta'\begin{pmatrix} 1 & 1 \\ 10 & 11 \end{pmatrix}3\tau \tag{7.4}$$

$\beta' \in \Gamma_0(30)$. Raonant de manera anàloga per a $i' = S_3^2w_9S_3$ és compleix:

$$w_{10}^{30}3\tau = \frac{1}{\sqrt{10}}\begin{pmatrix} 10k & 3 \\ 30t & 10 \end{pmatrix}3\tau = \beta''\begin{pmatrix} 3 & 2 \\ 10 & 7 \end{pmatrix}3\tau \tag{7.5}$$

$\beta'' \in \Gamma_0(30)$. Llavors la condició que han de complir els punts $\tau' = 3\tau$ en $Y_0(30)$ que pugen a punts fixos per la involució i en $Y_0(90)$ via el morfisme multiplicar per 3 ve donada per les igualtats 7.4 o 7.5, segons correspongui.

Provem que el nombre de punts en $Y_0(30)$ complint la condició 7.4,7.5 és fitat per 6. En efecte, sigui τ_1 un dels dos punts fixos de w_{10} en $Y_0(10)$ (podem suposar-ho no el·líptic), que puja a 4 punts en $Y_0(30)$: $\tau_{1,1}$,$\tau_{1,2}$,$\tau_{1,3}$ i

$\tau_{1,4}$ on $\tau_{1,i} = \gamma_i \tau_{1,1}$ on $\Gamma_0(10) = \cup_{i=1}^4 \Gamma_0(30)\gamma_i$ amb $\gamma_1 = id$, $\gamma_2 = \begin{pmatrix} 1 & 1 \\ 10 & 11 \end{pmatrix}$, $\gamma_3 = \begin{pmatrix} -1 & -1 \\ 10 & 9 \end{pmatrix}$ i $\gamma_4 = \begin{pmatrix} 3 & 2 \\ 10 & 7 \end{pmatrix}$. La condició 7.5,7.4 no la compleixen tots aquests 4 punts de $Y_0(30)$. En efecte, si tots ho complissin tindriem el següent:
En el cas $i = w_{10}S_3w_9S_3^2$, $w_{10}^{30}\tau_{1,j} = \beta\gamma_2\tau_{1,j}$, $\beta \in \Gamma_0(30)$. Com que w_{10}^{30} no té punts fixos a $X_0(30)$ llavors $w_{10}^{30}\tau_{1,1} = \beta\gamma_2\tau_{1,1} = \beta\tau_{1,2}$ i $w_{10}^{30}\tau_{1,2} = \beta_1\gamma_2\tau_{1,2} = \beta'''\tau_{1,1}$ amb $\beta, \beta_1, \beta''' \in \Gamma_0(30)$ i, per tant, $\gamma_2^2 \in \Gamma_0(30)$. Com que $w_{10}^{30}\tau_{1,3} = \tau_{1,4}$ aleshores $\gamma_2\gamma_3\gamma_4^{-1} \in \Gamma_0(30)$. Això entra en contradicció amb el fet que τ_1 no és el·líptic.
En el cas $i = w_{10}S_3^2w_9S_3$, llavors $w_{10}^{30}\tau_{1,1} = \beta\gamma_4\tau_{1,1}$ i raonant igual que abans tenim $\gamma_4^2 \in \Gamma_0(30)$, en contradicció també amb la hipòtesi de ser τ_1 no el·líptic.

Tenim ara que com a molt hi ha 18 punts en $Y_0(90)$ fixos per la involució i, llavors si $g = gènere(X_0(90)/i)$ i notant que la involució i no deixa cap punta fixa de $X_0(90)$ tenim:

$$18 \leq 2g - 2 + 8 + 9$$

i d'aquí $g > 1$. □

Tots els lemes anteriors proven:

Proposició 7.6. *La corba modular $X_0(90)$ no és biel·líptica.*

Capítol 8

L'estudi via parametritzacions

8.1 Introducció del problema via parametritzacions

El nostre problema consisteix en trobar els N pels quals existeix

$$\varphi : X_0(N) \to E$$

amb $deg(\varphi) = 2$.

Definició 8.1.1. *Sigui E una corba el·líptica. Un morfisme φ de $X_0(N) \to E$ de grau finit s'anomena una parametrització modular de la corba el·líptica E.*

Ens interessa determinar les corbes el·líptiques que admeten una parametrització modular de grau 2 i determinar els N corresponents. Hem demostrat en el capítol 2 que si tenim una corba bieł.líptica amb gènere superior o igual a 6 definida sobre un cos de nombres K, podem definir la parametrització també sobre K. Com que $X_0(N)$ està definida sobre $\mathbb{Q}$, pels N suficientment grans E i φ també estan definits sobre $\mathbb{Q}$ si $X_0(N)$ és biel·líptica . Ens centrarem en parametritzacions modulars on φ i E estan definits sobre $\mathbb{Q}$ i les anomenarem parametritzacions modulars sobre $\mathbb{Q}$. Via aquest estudi i utilitzant el resultat 2.16 es caracteritzaran dins de les corbes modulars $X_0(N)$ quines tenen un nombre no finit de punts quadràtics sobre $\mathbb{Q}$.

8.2 Parametritzacions modulars via sup.Riemann

Considerem una parametrització modular

$$\varphi : X_0(N)(\mathbb{C}) \to E(\mathbb{C})$$

en tota aquesta secció. Tenim un isomorfisme de varietats complexes i, més encara, de grups de Lie entre E i $\mathbb{C}/\Lambda$, on Λ és una xarxa en $\mathbb{C}$ ([35] VI §4), donat per

$$\psi : \mathbb{C}/\Lambda \to E$$

$$z \mapsto (\wp(z) : \wp'(z) : 1)$$

A més, si $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ és un model de Weierstrass per a la corba E llavors $\psi^*(\frac{dx}{2y+a_1x+a_3}) = dz$.
Posem doncs:

$$\varphi : \Gamma_0(N)\backslash\overline{\mathbb{H}} \to \mathbb{C}/\Lambda$$

Si z denota la variable en $\mathbb{C}/\Lambda$ i τ en $\mathbb{H}$, aleshores dz és una diferencial holomorfa en $\mathbb{C}/\Lambda$ i podem considerar la diferencial regular $\varphi^*(dz)$ de $X_0(N)$.

Proposició 8.2.1. *Hi ha un isomorfisme entre*

$$S_2(\Gamma_0(N)) \to \Omega_{X_0(N)}$$

$$f \mapsto 2\pi i f(\tau)d\tau$$

on $\Omega_{X_0(N)}$ denota l'espai de les diferencials regulars de la corba $X_0(N)$.

Així a una parametrització modular li correspon una forma cuspidal de pes 2 en $\Gamma_0(N)$.
Considerem ara per a cada superfície de Riemann el seu recobridor universal:

$$\pi_1 : \overline{\mathbb{H}} \to X_0(N)$$

$$\pi_2 = proj : \mathbb{C} \to \mathbb{C}/\Lambda$$

Per la propietat del lifting d'aplicacions existeix $\tilde{\varphi} : \overline{\mathbb{H}} \to \mathbb{C}$ fent el següent diagrama commutatiu:

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \longleftarrow & \mathbb{C} \\ \uparrow & & \uparrow \\ X_0(N) & \longleftarrow & \overline{\mathbb{H}} \end{array}$$

Abans hem observat que $\varphi^*(dz) = d(z \circ \varphi) = 2\pi i f(\tau)d\tau$ és una diferencial exacta de $X_0(N)$. Recordem el següent resultat ([16] 10.8)

Teorema 8.2.2. *Suposem que X és una superfície de Riemann i sigui $\pi' : \tilde{X} \to X$ el seu recobriment universal. Suposem que ω és una diferencial holomorfa tancada i F una primitiva de $\pi'^*(\omega)$ en $\tilde{X}$ (que sempre existeix*

([16] 10.6). Primitiva vol dir $dF = \omega$). Si $c : [0,1] \to X$ és una corba diferenciable a trossos i si $\hat{c} : [0,1] \to \tilde{X}$ és un lifting de c, llavors s'obté:

$$\int_c \omega = F(\hat{c}(1)) - F(\hat{c}(2)) = \int_{\hat{c}} \pi'^* \omega$$

A més, no depèn de la elecció de la primitiva F ni del lifting de la corba c.

Apliquem l'anterior resultat. Pel diagrama commutatiu:

$$(proj \circ \tilde{\varphi})^*(dz) = (\varphi \circ \pi_1)^*(dz)$$

d'on tenim $\tilde{\varphi}^*(dz) = {\pi_1}^*(2\pi i f(\tau)d\tau)$. Fixem punts $\tau_0 \in X_0(N)$ i $\tilde{\tau_0} \in \overline{\mathbb{H}}$ amb $\pi_1(\tilde{\tau_0}) = \tau_0$; i per a qualsevol altre punt $\tau_1 \in X_0(N)$ sigui c un camí de τ_0 en τ_1. Aleshores

$$\int_c 2\pi i f(\tau)d\tau = \int_{\hat{\tau_0}}^{\hat{c}(1)} \tilde{\varphi}^*(d\tau) = \tilde{\varphi}(\hat{c}(1)) - \tilde{\varphi}(\hat{\tau_0})$$

i d'aquí

$$\tilde{\varphi}(\hat{c}(1)) - \tilde{\varphi}(\hat{\tau_0}) = \int_{\hat{\tau_0}}^{\hat{c}(1)} \pi_1^*(2\pi i f(\tau)d\tau$$

Observem que π_1 és realment l'acció de $\pi_1(X_0(N))$ a $\overline{\mathbb{H}}$ que correspon a l'acció de $\Gamma_0(N)$. Llavors

$$\varphi_f(\hat{\tau}) := \int_{\hat{\tau_0}}^{\tilde{\tau}} 2\pi i f(\tau)d\tau = \tilde{\varphi}(\hat{\tau}) - \tilde{\varphi}(\hat{\tau_0})$$

i, per tant, llevat d'una constant podem pensar $\tilde{\varphi} = \varphi_f$.
Sigui $\sigma \in \pi_1(X_0(N))$. Tenim:

$$\int_\sigma \varphi^*(dz) = \int_{\hat{\tau_0}}^{\gamma\hat{\tau_0}} 2\pi i f(\tau)d\tau \in \mathbb{C}$$

per algun $\gamma \in \Gamma_0(N)$. Pel diagrama commutatiu, $\int_\sigma \varphi^*(dz) \in \Lambda$. Tot $\gamma \in \Gamma_0(N)$ dona un camí en $\pi_1(X_0(N))$ i si denotem per $\Lambda' = \{\int_\sigma \varphi^*(dz) | \sigma \in \pi_1(X_0(N))\} \subset \Lambda$ (que forma un subgrup additiu de $\mathbb{C}$ pel fet que $\int_{\sigma\delta} \varphi^*(dz) = \int_\sigma \varphi^*(dz) + \int_\delta \varphi^*(dz)$. A més és abelià), podem substituir $\pi_1(X_0(N))$ per $H_1(X_0(N), \mathbb{Z})$ d'on φ factoritza a través de $\psi' : X_0(N) \to \mathbb{C}/\Lambda'$. Observem tot seguit que $\Lambda = \Lambda'$. En efecte, tenim

$$X_0(N) \xrightarrow{\psi'} \mathbb{C}/\Lambda' \xrightarrow{proj} \mathbb{C}/\Lambda$$

on $\varphi = proj \circ \psi'$. Com que φ és de fibra finita, Λ' és una xarxa de $\mathbb{C}$. A més $\psi'^*(dz) = 2\pi i f(\tau)d\tau$ i $\varphi^*(dz) = \psi'^*(dz)$, d'on $proj^* = \pm id$ i $\Lambda = \Lambda'$.

Proposició 8.2.3. *Si $\varphi : X_0(N) \to \mathbb{C}/\Lambda$ és una parametrització modular amb $\varphi^*(dz) = 2\pi i f(\tau)d\tau$ podem pensar-la com $\varphi(P) = \int_{P_0}^{P} 2\pi i f(\tau)d\tau$, on P_0 és un punt fixat i $\Lambda = \{\int_\sigma 2\pi i f(\tau)d\tau |\ \sigma \in H_1(X_0(N)(\mathbb{C}), \mathbb{Z})\}$.*

Partim tot seguit d'una $f \in S_2(\Gamma_0(N))$ i considerem

$$\varphi_f(\tau) = \int_{\tau_0}^{\tau} 2\pi i f(\tau')d\tau'$$

per $\tau \in \mathbb{H}$ i τ_0 un punt fixat de $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$; i definim

$$\varphi_f(s) = lim_{w \to s} \int_{\tau_0}^{w} 2\pi i f(\tau')d\tau'$$

si $s \in \overline{\mathbb{H}} \setminus \mathbb{H}$ i $w \in \mathbb{H}$.

Proposició 8.2.4. *Denotem per $r_f(\gamma)_\tau = \varphi_f(\gamma\tau) - \varphi_f(\tau)$, on $\gamma \in \Gamma_0(N)$. Es té llavors que $r_f(\gamma)_\tau$ no depèn de τ i l'aplicació:*

$$r_f : \Gamma_0(N) \to \mathbb{C}$$

dóna un morfisme de grups abelians.

Demostració. La primera afirmació es desprèn de la igualtat:

$$\frac{d}{d\tau}(\varphi_f(\gamma\tau) - \varphi_f(\tau)) = 2\pi i((c\tau + d)^{-2} f(\gamma\tau) - f(\tau)) = 0$$

per a tot $\tau \in \mathbb{H}$.
Finalment, la igualtat

$$r_f(\gamma\beta) = \varphi_f(\gamma\beta\tau) - \varphi_f(\beta\tau) + \varphi_f(\beta\tau) - \varphi_f(\tau)$$

prova la segona afirmació. □

Corol·lari 8.2.5. *Si $Im(r_f) \subset \Lambda$, on Λ és una xarxa de $\mathbb{C}$, llavors φ_f indueix una parametrització modular:*

$$\varphi : \Gamma_0(N) \backslash \overline{\mathbb{H}} \to \mathbb{C}/\Lambda$$

Anem a estudiar què podem dir del $deg(\varphi)$. Recordem que si tenim $f, g \in S_2(\Gamma_0(N))$ formes cuspidals tenim definit el producte intern de Petersson donat per

$$< f, g >= \int_{\mathcal{D}(\Gamma_0(N))} f(\tau')\overline{g(\tau')}dudv$$

on $\tau' = u + iv$ i $\mathcal{D}(\Gamma_0(N))$ denota un domini fonamental per a $\Gamma_0(N)$.

Proposició 8.2.6 (Zagier). *Sigui φ una parametrització modular. Si es té $\varphi^*(dz) = 2\pi i f(\tau)d\tau$, llavors*

$$||f||^2 = \frac{1}{4\pi^2} deg(\varphi) Vol(E = \mathbb{C}/\Lambda)$$

Demostració.

$$\begin{aligned} ||f||^2 &= \frac{i}{2}\int_{\mathcal{D}(\Gamma_0(N))} f(\tau')d\tau' \wedge \overline{f(\tau')}\overline{d\tau'} \\ &= \frac{i}{8\pi^2}\int_{\mathcal{D}(\Gamma_0(N))} \varphi^*(dz) \wedge \overline{\varphi^*(dz)} \\ &= \frac{i}{8\pi^2} deg(\varphi)\int_E dz \wedge \overline{dz} = \frac{1}{4\pi^2} deg(\varphi) Vol(E) \end{aligned}$$

on $Vol(E)$ és l'àrea del parel.lelepípede fonamental per a la xarxa Λ. □

Ens interessa d'alguna manera poder calcular els anteriors valors per a un càlcul efectiu de $deg(\varphi)$. Considerem $\mathcal{D}(\Gamma_0(N))$ de manera que sigui un polígon hiperbòlic (i.e. els seus vèrtexs són punts interiors o de la frontera de $\mathbb{H}$) que té un nombre finit de costats identificats dos a dos a $\mathbb{H}/\Gamma_0(N)$. Numerem els vèrtexs P_j amb j en un conjunt d'índexs $J = \mathbb{Z}/r$ de forma que P_{j+1} és el successor de P_j amb la orientació natural. Sigui e_j el costat P_jP_{j+1}, i e_j^* el costat que s'identifica amb e_j i $\gamma_j \in \Gamma_0(N)$ l'element que els identifica; llavors es té $\gamma_{j^*} = \gamma_j^{-1}$ i $\gamma_j(P_j) = P_{j^*+1}$. L'aplicació $T : J \to J$ tal que $T(j) = j^* + 1$ trenca J en un nombre finit d'òrbites $[j] = \{j = T^l(j), T(j), \ldots, T^{l-1}(j)\}$, de manera que dos vèrtexs P_j i $P_{j'}$ estan identificats en $\mathbb{H}/\Gamma_0(N)$ si i sols si j, j' són de la mateixa òrbita. Triem un punt base j_0 en cada òrbita i definim un ordre parcial en J per: $j < j'$ si

$$[j] = [j'] \; i \; j = T^\alpha(j_0),\; j' = T^\beta(j_0),\; amb\; 0 \le \alpha < \beta < l$$

Teorema 8.2.7 (Zagier). *Sigui $f \in S_2(\Gamma_0(N))$ i sigui $\{\gamma_j\}_{j\in J}$ un sistema de generadors de $\Gamma_0(N)$ obtingut a partir de $\mathcal{D}(\Gamma_0(N))$ (com l'explicitat anteriorment). Llavors:*

$$||f||^2 = \frac{1}{8\pi^2}\sum_{\substack{j,j'\in J \\ j<j'}} Im(r_f(\gamma_j)\overline{r_f(\gamma_{j'})})$$

A més, si $r_f(\Gamma_0(N)) \subset \Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ ($\tau = \omega_1/\omega_2 \in \mathbb{H}$) es té:

$$deg(\varphi) = \frac{1}{2}\sum_{\substack{j,j'\in J \\ j<j'}} (n_1(\gamma_j)n_2(\gamma_{j'}) - n_2(\gamma_j)n_1(\gamma_{j'}))$$

on n_1 i n_2 són els morfismes de grup d'escriure $r_f(\gamma) = n_1(\gamma)\omega_1 + n_2(\gamma)\omega_2$.

Per a la prova consulteu [41]. Més endavant, pel cas en que f és una forma cuspidal, $f = \sum a_i q^{ni}$ $q = e^{2\pi i}$ amb $a_i \in \mathbb{Q}$ es prova un càlcul per a $deg(\varphi)$.

Nota 8.2.8. *Notem que el fet que $r_f(\Gamma_0(N))$ sigui una xarxa és una condició supèrflua si f, la forma modular, ve donada per una parametrització modular que en el nostre treball sempre suposarem que existeix i, per tant, això serà d'utilitat per a la computació del $deg(\varphi)$, aplicant els resultats de les proposicions 8.2.3,8.2.6 i el teorema 8.2.7.*

8.3 Parametritzacions fortes

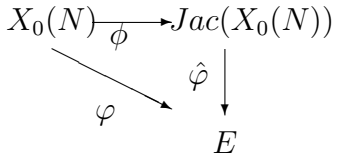
Considerem en aquesta secció una parametrització modular definida sobre $\mathbb{Q}$, $\varphi : X_0(N) \to E$. Llavors, la diferencial canònica del model de Néron és

$$\omega = \frac{dx}{2y + a_1 x + a_3}$$

on $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ és un model de Weierstrass minimal per a E. Podem pensar que la parametrització modular φ satisfà $\varphi(i\infty) = 0$ (fent una translació en E, si cal). Observem que $\varphi^*\omega = 2\pi i f(\tau)d\tau$ i pel fet d'estar tot definit sobre $\mathbb{Q}$, $f = \sum_{n\geq 1} a_n q^n$ amb $a_i \in \mathbb{Q}$.

Proposició 8.3.1. *Sigui φ una parametrització modular definida sobre $\mathbb{Q}$. Llavors, $\varphi^*\omega = f\frac{dq}{q}$ i f és vector propi per a tots els operadors de Hecke T_p, $(p, N) = 1$.*

Demostració.



La descomposició de la Jacobiana en factors $\mathbb{Q}-$simples , $Jac(X_0(N)) \sim_{\mathbb{Q}} \prod A_i^{m_i}$, es correspon amb la descomposició de l'espai $S_2(\Gamma_0(N)) = \oplus S_{i,m_i}$, on $S_{i,m_i} =< \{f^\sigma|_{B_{d_i}}\} >$ i σ recorre les immersions del cos de coeficients de la forma modular $K_f = \mathbb{Q}(\{a_n\})$. Els elements de cada subespai S_{i,m_i} són vectors propis dels operadors de Hecke T_p,$(p, N) = 1$, i tenen, llevat d'un nombre finit de p's, els mateixos valors propis. A més, l'anterior descomposició de $S_2(\Gamma_0(N))$ indueix una descomposició a l'espai de les diferencials regulars de $Jac(X_0(N))$ i també a $\Omega_{X_0(N)}$ via l'isomorfisa que envia $\omega \in \Omega_{Jac(X_0(N))}$ a $\omega \circ \phi$.

En ser $\hat{\varphi} : \prod_i A_i^{m_i} \to E$ amb $A_i^{m_i}$ no $\mathbb{Q}$-isògens dos a dos tenim $\hat{\varphi} = \prod_i \hat{\varphi}_i$. Si $\hat{\varphi}_i \neq 0$ això ens diu que E és $\mathbb{Q}$-isògen a algun factor de $A_i^{m_i}$ i, per tant, només hi pot haver un i tal que $\hat{\varphi}_i \neq 0$.
Així, la diferencial $\omega' = \hat{\varphi}^*(\omega)$ correspon al factor en la descomposició de les diferencials regulars que prové de $A_i^{m_i}$ i $\omega' \circ \phi = f\frac{dq}{q} = \varphi^*(\omega)$. D'aquí que f ha de correspondre al factor que prové de S_{i,m_i}. □

Si f és una forma nova llavors ([4]) podem escriure f com

$$f = cq(1 + \sum_{n\geq 1} a_{n+1}q^n) = cg,$$

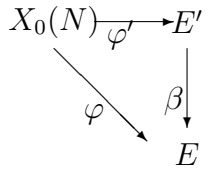
amb $c \in \mathbb{Q}^*$ i g és una forma nova normalitzada.

Definició 8.3.2. *Si φ és una parametrització modular definida sobre $\mathbb{Q}$ tal que $\varphi^*(\omega) = 2\pi i f(\tau)d\tau$, amb la notació anterior, i f és una forma modular nova, en el sentit que es ortogonal respecte del producte escalar de Petersson al subespai generat per les formes cuspidals de pes 2 velles, diem que φ és una parametrització dèbil de Weil.*

Definició 8.3.3. *Suposem que tenim una parametrització dèbil de Weil φ. Aleshores $\varphi^*(\omega) = f(\tau)\frac{dq}{q}$, on $f(\tau) = c(1 + \sum_{n\geq 1} a_{n+1}q^n)q$ amb $c \in \mathbb{Q}^*$. Definim la constant de Manin de la parametrització φ com el valor $c \in \mathbb{Q}^*$.*

Anem a fer un petit estudi sobre les parametritzacions modulars dèbils de Weil.

Definició 8.3.4. *Considerem dos parametritzacions modulars dèbils de Weil que es trobin formant el següent diagrama commutatiu:*



Diem llavors que φ' domina a φ i ho denotem $\varphi' \geq \varphi$. Observem que en l'anterior situació $ker(\beta)$ és finit i, per tant, E' i E estan dins de la mateixa classe de $\mathbb{Q}$-isogènia i, en particular, tenen ambdues el mateix conductor geomètric.

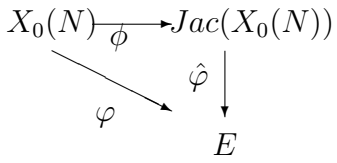
En [40], [25] i [13] s'anota el següent resultat

Teorema 8.3.5. *Considerem totes les parametritzacions dèbils de Weil dins d'una classe de $\mathbb{Q}$-isogènia de E, corba el·líptica sobre $\mathbb{Q}$ que admet una parametrització dèbil de Weil. Llavors n'existeix una de maximal respecte de la relació $\geq$. A més, aquesta parametrització maximal és única llevat del signe i l'anomenem parametrització modular forta de Weil.*

Per a la prova de l'anterior resultat cal notar que si tenim una parametrització modular forta de Weil llavors $E \hookrightarrow Jac(X_0(N))_{\mathbb{Q}}$ és una immersió tancada. Del principi de multiplicitat 1 de formes modulars se segueix que aquesta immersió és única llevat del signe, i la parametrització modular s'obté de

$$X_0(N) \to \widehat{Jac(X_0(N))} \cong Jac(X_0(N)) \to \widehat{E} \cong E$$

on $X_0(N) \to Jac(X_0(N)$ és l'aplicació natural i l'altra és l'aplicació dual de la immersió, [13].
Ens interessa, donada una parametrització modular φ definida sobre $\mathbb{Q}$, estudiar el $deg(\varphi)$. Pel nostre propòsit caldrà centrar-nos en parametritzacions modulars fortes ja que tota parametrització dèbil de Weil factoritza a traves d'una forta i ens interessa el càlcul de parametritzacions amb $deg(\varphi) = 2$.
Observem, a més, que si tenim una parametrització dèbil de Weil considerant altre cop el diagrama commutatiu següent:



i seguint el mateix argument que en la proposició 8.3.1 podem escriure $Jac(X_0(N)) \sim_{\mathbb{Q}} \prod A_i^{m_i}$, A_i són factors simples corresponents a una descomposició de $S_2(\Gamma_0(N))$. Com que estem suposant ara que la parametrització modular $\varphi : X_0(N) \to E$ ve donada per una forma cuspidal nova de pes 2 , aquesta diferencial correspon a un S_{i,m_i}. Pel fet de ser $f = \varphi^*(\omega)$ nova i definida sobre $\mathbb{Q}$ li correspon un únic factor A_i de la jacobiana sobre $\mathbb{Q}$ amb $m_i = 1$ i $dim A_i = 1$ via el teorema 3.2.7(f correspon a un S_{i,m_i} que té dimensió 1). Per tant, E és $\mathbb{Q}$-isògen al factor A_i, factor simple de la Jacobiana; s'obté el següent resultat:

Teorema 8.3.6 (Birch-Swinnerton-Dyer,[40]). *Hi ha una bijecció entre les corbes el·líptiques definides sobre $\mathbb{Q}$ que són imatges de $X_0(N)$ però no de $X_0(M)$, amb $M < N$, i les formes noves de $\Gamma_0(N)$ amb coeficients a $\mathbb{Q}$.*

Anem a caracteritzar quines són aquestes possibles corbes el·líptiques

Teorema 8.3.7 (Carayol, [6],[7],[8]). *Si tenim una parametrització modular dèbil de Weil $\varphi : X_0(N) \to E$ llavors el conductor geomètric de E és justament N.*

Conjectura 8.3.8 (Weil). [1] *Sigui E una corba el·líptica definida sobre $\mathbb{Q}$ amb conductor geomètric N. Aleshores hi ha una aplicació no constant $X_0(N) \to E$ definida sobre $\mathbb{Q}$.*

Anem a examinar l'enunciat de l'anterior conjectura: si E és una corba el·líptica sobre $\mathbb{Q}$, la funció zeta de la corba es defineix com $\zeta_E(s) = \prod_p L(E_p, p^{-s})$, on E_p és la reducció de la corba el·líptica en $\overline{\mathbb{F}_p}$, $L(E_p, u) = \prod_{i=1}^{2}(1-\alpha_i u)^{-1}$, i els α_i es calculen per la fórmula $N_v = 1+p^v-\sum \alpha_i^v$, $\alpha_1\alpha_2 = p$ on N_v denota el nombre de punts sobre $\mathbb{F}_{p^v}$. Si $\zeta_E(s)$ compleix unes certes equacions funcionals [40], pel teorema de Weil, $\zeta_E(s)$ és la transformada de Mellin d'una forma cuspidal de pes 2 que és vector propi per tots els operadors de Hecke T_p, $(p, N) = 1$. A més, es pot veure que és una forma nova [40]; això defineix una corba el·líptica i una parametrització modular $X_0(N) \to E'$ sobre $\mathbb{Q}$. Llavors es prova el resultat:

Teorema 8.3.9 (Swinnerton-Dyer-Birch,[40]). *Considerem $X_0(N)$, suposem que E és una corba el·líptica definida sobre $\mathbb{Q}$ que és un factor simple de la Jacobiana de $X_0(N)$. Considerem el pullback de la diferencial de E en $X_0(N)$ i normalitzem l'anterior forma cuspidal de pes 2, escrivint-la com $F(\tau) = q+\dots$. Llavors, llevat d'un nombre finit de factors, la transformada de Mellin de $F(\tau)$ és igual a la funció zeta de E.*

Així, tant la corba el·líptica E com E' tenen la mateixa funció zeta, llevat d'un nombre finit de factors i si l'invariant j de E no és un enter, E i E' són $\mathbb{Q}$-isògenes (teorema de Serre[34]).
La conjectura de Weil equival a afirmar que cada corba el·líptica definida sobre $\mathbb{Q}$ és un factor $\mathbb{Q}$-isògen a la jacobiana de $X_0(N)$ on N és el conductor geomètric de la corba el·líptica.
Nosaltres partim d'una parametrització modular dèbil de Weil φ i obtenim una parametrització modular forta. En la taula 1 de [43] s'hi troben totes les corbes el·líptiques (de conductor$N \leq 210$) que poden admetre una parametrització modular forta. Si $\varphi : X_0(N) \to E$ és una parametrització modular forta, $\varphi^*(\omega) = 2\pi i f(\tau)d\tau$ amb f nova. Considerant que f és normalitzada (és a dir amb constant de Manin $= \pm 1$) en [3] i [41] s'indica el còmput de $||f||$ corresponent a E. Això juntament amb el teorema 8.2.6 ens permet calcular el grau de les parametritzacions modulars fortes, (veure taula 22 de [42]). El fet d'haver considerat que f és una forma normalitzada, és a dir que la constant de Manin té valor ± 1, es recolza en la següent conjectura:

Conjectura 8.3.10 (Manin). *Si φ és una parametrització forta de Weil llavors la constant de Manin associada a la parametrització és igual a ± 1.*

[1] Anotem la importància d'aquesta conjectura, ja que la seva prova quan E és una corba el·líptica semiestable ha permès a Andrew Wiles provar el teorema de Fermat.

Referent a l'anterior constant s'obté el següent resultat en [13]

Teorema 8.3.11 (Edixhoven). *La constant de Manin per una parametrització modular forta de Weil és un enter.*

Per tant, pel teorema de Edixhoven, les taules de [42] que calculen el $deg(\varphi)$ (amb valor de la constant de Manin=1) ens són de gran utilitat i pels valors de N tal que $deg(\varphi) > 2$ podem afirmar que la corba modular $X_0(N)$ no pot ser biel·líptica donada per una parametrització amb el pullback de la diferencial forma nova. En particular,

Corol·lari 8.3.12. *Mòdul la conjectura de Manin* [2] *els únics N tal que la involució biel·líptica ve donada per una forma parabòlica nova són per N*

26	*30*	*34*	*35*	*37*	*38*	*39*	*40*	*43*	*44*
45	*48*	*50*	*51*	*53*	*54*	*55*	*56*	*61*	*62*
64	*65*	*69*	*79*	*83*	*89*	*92*	*94*	*101*	*131*

(Consultar la taula 22 de [42]) Obtenim així, utilitzant la taula 20 de [42], i seguint la notació de [43]:

Corol·lari 8.3.13.

$X_0(35)/w_5 = 35B$	$X_0(37)/w_{37} = 37A$	$X_0(37)/\alpha w_{37} = 37C$
$X_0(39)/w_3 = 39B$	$X_0(43)/w_{43} = 43A$	$X_0(50)/w_2 = 50E$
$X_0(50)/w_{25} = 50A$	$X_0(53)/w_{53} = 53A$	$X_0(61)/w_{61} = 61A$
$X_0(62)/w_{31} = 62A$	$X_0(65)/w_{65} = 65A$	$X_0(69)/w_{23} = 69A$
$X_0(79)/w_{79} = 79A$	$X_0(83)/w_{83} = 83A$	$X_0(89)/w_{89} = 89C$
$X_0(92)/w_{23} = 92A$	$X_0(94)/w_{47} = 94A$	$X_0(101)/w_{101} = 101A$
	$X_0(131)/w_{131} = 131A$	

Per a caracteritzar algun més d'aquests quocients de les corbes modulars utilitzem la següent conjectura:

Conjectura 8.3.14 (Birch-Stephens). *Sigui E una corba dèbil de Weil de conductor N. Llavors el rang del grup de Mordell-Weil de E és senar si i només si la parametrització modular $X_0(N) \to E$ factoritza a través de $X_0(N)/w_N$.*

Corol·lari 8.3.15. *Suposant certa la conjectura de Birch-Stephens per corbes fortes de Weil, tenim llavors: $X_0(55)/w_{11} = 55B$, $X_0(51)/w_{17} = 51A$, $X_0(38)/w_{19} = 38A$, $X_0(44)/w_{11} = 44A$, $X_0(54)/w_{27} = 54A$ i $X_0(56)/w_7 = 56C$.*

[2] En l'article [25] s'estudien les parametritzacions modulars fortes donades en fer quocients per involucions d'Atkin-Lehner, i s'obté la llista del corol·lari a excepció de N =40, 45, 48, 64 i 65. Pel cas $N = 65$, en la llista 1 de [25] falta anotar-hi aquest cas, ja que la involució biel·líptica és única i és w_{65}.

Demostració. Sol cal observar les taules de la pag 16 de [25], la caracterització de les involucions biel·líptiques i la conjectura de Birch-Stephens. □

8.4 Parametritzacions no fortes

L'existència d'una parametrització modular sobre $\mathbb{Q}$, $\varphi : X_0(N) \to E$, en la que la diferencial no correspongui a un forma modular nova, ens ve a dir que la corba el·líptica E pot ser també imatge de $X_0(M)$ amb $M|N$. A nosaltres ens interessa el comportament dels graus. Denotem per φ la parametrització modular sobre $\mathbb{Q}$. Tenim llavors el següent diagrama commutatiu, gràcies al teorema 3.2.7:

$$\begin{array}{ccc} X_0(N) & \xrightarrow{\phi} & \prod_{\{\sigma f\}} J^{m(f)}_{\{\sigma f\}} \\ & \searrow^{\varphi} & \downarrow \hat{\varphi} \\ & & E \end{array}$$

Com que els $J_{\sigma f}$ són $\mathbb{Q}$-simples llavors $\hat{\varphi} : Jac(X_0(N)) \to E$ s'expressa com $\hat{\varphi} = \prod_i \hat{\varphi}_i \in \prod_{\{\sigma f\}} End(J^{m(f)}_{\{\sigma f\}}, E)$. A més, sols hi ha una $\hat{\varphi}_i$ que és no nul·la (argumentant de la mateixa manera que en la prova 8.3.1). Sigui doncs $\hat{\varphi}_i \in End(J^{m(f)}_{\sigma f}, E)$, on la diferencial $f\frac{dq}{q}$ és vella. Notem que $m(f) \geq 2$, ja que, si $m(f) = 1$, el factor $\mathbb{Q}$-simple $J_{\sigma f}$ és $\mathbb{Q}$-isògen a E, ja que $K_f = \mathbb{Q}$, i, per tant, E seria una factor simple de $Jac(X_0(N))$. Pels teoremes 8.3.6 i 3.2.7 deduim que la diferencial de la parametrització és nova, en contra del cas actual; per tant $m(f) \geq 2$.

Així $J_{\sigma f}$ és $\mathbb{Q}$-isògen a E, i E pot ser parametritzat per $X_0(M)$, on M és el nivell de f, ja que $J_{\sigma f}$ es correspon amb un factor $\mathbb{Q}$-simple en la jacobiana de $X_0(M)$ (veure teorema de Shimura 3.2.7). El pullback de φ en $Jac(X_0(N))$ es troba en l'espai de les diferencials regulars de $J^{m(f)}_{\sigma f}$ que es correspon via l'isomorfisme $\circ\phi$ amb un subespai de $S_2(\Gamma_0(N))$: $W =< f, f|B_d, \ldots, f|B_{N/M} >$, on $f|_{B_d} = \sum a_n q^{dn}$ si $f = \sum a_n q^n$. Per tant, $\varphi^*(\omega) = 2\pi i h(\tau) d\tau$, amb $h \in W$, per factoritzar a través de la jacobiana. Després d'aquestes consideracions, podem preguntar-nos si el que esta passant a nivell de $\mathbb{Q}$-isogènia pot passar a nivell de morfismes, és a dir:

Pregunta 8.4.1. *Sigui $\varphi : X_0(N) \to E$ parametrització modular sobre $\mathbb{Q}$ amb $\varphi^*(\omega) \in W$. Factoritza φ a través de $X_0(M)$ i de manera que el pull-back de la diferencial és una forma cuspidal nova?*

Anem a estudiar l'anterior qüestió utilitzant superfícies de Riemann.

Considerem

$$\varphi : X_0(N) \to E = \mathbb{C}/\Lambda \ ,$$

on $\varphi^*(dz) = 2\pi i h(\tau)d\tau$ i l'aplicació

$$\varphi_h : \mathbb{H} \to \mathbb{C}$$
$$\tau \mapsto \int_{i\infty}^{\tau} 2\pi i h(\tau')d\tau' \ .$$

Observem que

$$\frac{d}{d\tau}\{\varphi_h(\frac{a\tau+b}{c\tau+d}) - \varphi_h(\tau)\} = 2\pi i\{(c\tau+d)^{-2}h(\frac{a\tau+b}{c\tau+d}) - h(\tau)\} = 0$$

per a $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ i $g \in \Gamma_0(N)$. D'aquí obtenim que $\varphi_h(\gamma\tau) - \varphi_h(\tau) = C(\gamma)\ \forall \gamma \in \Gamma_0(N)$.
Considerem, a partir d'ara, $h \in S_2(\Gamma_0(N))$ de la forma $h(\tau) = f(e\tau)$ on $e|\frac{N}{M}$ i $f \in S_2(\Gamma_0(M))^{new}$. Anem a estudiar si pot factoritzar a través de $X_0(M)$. Tenim l'aplicació

$$\varphi_h : X_0(N) \to \mathbb{C}/\Lambda_1$$

on $\Lambda_1 = \{\int_{i\infty}^{\gamma i\infty} 2\pi i h(\tau')d\tau' | \gamma \in \Gamma_0(N)\}$. Definim

$$\varphi'_f : \overline{\mathbb{H}} \to \mathbb{C}$$

com $\varphi'_f(\tau) = \frac{1}{e}\int_{i\infty}^{\tau} 2\pi i f(\tau')d\tau'$. Observem que $\frac{d}{d\tau}(\varphi'_f(\gamma\tau) - \varphi'_f(\tau)) = 0$, $\gamma \in \Gamma_0(N)$ i triant $\tau = i\infty$, tenim $\varphi'_f(\gamma\tau) - \varphi'_f(\tau) = C(\gamma) = \frac{1}{e}\int_{i\infty}^{\gamma i\infty} 2\pi i f(\tau'')d\tau''$. Per tant φ'_f ens defineix una aplicació $\varphi'_f : X_0(M) \to \mathbb{C}/\Lambda_2$ on $\Lambda_2 = \{\frac{1}{e}\int_{i\infty}^{\gamma i\infty} 2\pi i f(\tau')d\tau' | \gamma \in \Gamma_0(M)\}$. Denotem per $e : X_0(N) \to X_0(M)$ multiplicar per e.

Lema 8.4.2. *Tenim el següent diagrama commutatiu:*

$$\begin{array}{ccc} X_0(N) & \to & \mathbb{C}/\Lambda_1 \\ e \downarrow & & \downarrow \ proj \\ X_0(M) & \to & \mathbb{C}/\Lambda_2 \end{array}$$

Demostració. Si $\tau \in X_0(N)$, $\varphi'_f \circ e(\tau) = \varphi'_f(e\tau) = \frac{1}{e}\int_{i\infty}^{e\tau} 2\pi i f(\tau')d\tau' = \int_{i\infty}^{\tau} 2\pi i h(\tau'')d\tau''$=$\varphi_h(\tau)$. Només cal veure que $\Lambda_1 \subset \Lambda_2$. En efecte, $C_1(\gamma) = \varphi_h(\gamma i\infty) = \frac{1}{e}\int_{i\infty}^{e\gamma i\infty} 2\pi i f(\tau'')d\tau''$ d'on si $\gamma = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix}$ llavors

$$e\gamma = \begin{pmatrix} a & be \\ \frac{Nc}{e} & d \end{pmatrix} e = \delta e$$

Observem que $\delta \in \Gamma_0(N/e, e) \subset \Gamma_0(M)$, d'aquí $C_1(\gamma) = C_2(\delta)$. □

Lema 8.4.3. *En la situació anterior $deg(e) > deg(proj)$, si $e \neq 1$.*

Demostració. Observem que $\Gamma_0(N/e, e) \cong \Gamma_0(N)$ via $\gamma \mapsto e\gamma\frac{1}{e}$ i que per a tot $\delta \in \Gamma_0(N/e, e) \subset \Gamma_0(M)$ tenim $C_2(\delta) = C_1(\gamma)$ amb $\gamma \in \Gamma_0(N)$ i viceversa. Per tant, si denotem per $1, \alpha_1, \ldots, \alpha_n$ un sistema de representants per la dreta de $\Gamma_0(M)/\Gamma_0(N/e, e)$, de l'anterior isomorfisme es desprèn $deg(e) = [\Gamma_0(M) : \Gamma_0(N)] \geq [\Gamma_0(M) : \Gamma_0(N/e, e)] = n$. Notem que $deg(proj) = (\Lambda_2 : \Lambda_1)$. Com que $\Lambda_2 = \cup_{i=1}^{n} \alpha_i \Lambda_1$, llavors la xarxa Λ_2 serà més gran que Λ_1, tot depenent dels valors $C_2(\alpha_j) = C_{2,j} = \frac{1}{e}\int_{i\infty}^{\alpha_j i\infty} 2\pi i f(\tau')d\tau'$. Posem $\alpha_j = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \notin \Gamma_0(N/e, e)$ per j de 0 fins a $e-1$. Com que tots aquests deixen la punta $i\infty$ fixa, aleshores $C_{2,j} = 0$ i, per tant, sols els elements de les classes laterals α_i amb $i \geq e$ poden donar una xarxa més gran que Λ_1. Finalment, en ser C_2 un morfisme additiu (8.2.4) , s'obté $deg(proj) < n$. □

Proposició 8.4.4. *Seguint la notació anterior suposem que $e^2|N$ i $M = N/e$. Llavors tota parametrització modular de diferencial $2\pi i h(e\tau)$ factoritza a través de $X_0(M)$ a la mateixa corba el·líptica.*

Demostració. El mateix argument que en la demostració anterior però pensant que, en aquest cas, $n = e$ i el sistema de representants de $\Gamma_0(M)/\Gamma_0(N/e, e)$ és

$$\left\{ \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \notin \Gamma_0(N/e, e) \mid j = 1, \ldots, e-1 \right\} \cup \{id\}$$

i, per tant, $\Lambda_1 = \Lambda_2$.(Ja que en les condicions de l'enunciat de la proposició $e = [\Gamma_0(M) : \Gamma_0(N)] = [\Gamma_0(M) : \Gamma_0(M, e)]$ i $C_2(\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}) = 0$). □

Corol·lari 8.4.5. *Si $X_0(N)$ és biel·líptica amb $4|N$ i φ és la parametrització de grau 2 que té per diferencial $2\pi i f(2^n\tau)$ amb $1 \leq n \leq [\frac{v_2(N)}{2}]$ ($f \in S_2(\Gamma_0(N))$) llavors la parametrització modular és $X_0(N) \to X_0(N/2)$ on $X_0(N/2)$ és una corba el·líptica.*

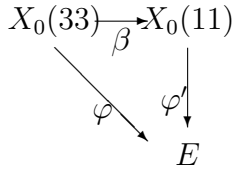
Demostració. Efectivament per la proposició anterior tenim $\Lambda_1 = \Lambda_2$ i per graus obtenim que $X_0(N/2)$ té gènere 1. □

Corol·lari 8.4.6. *Si $X_0(N)$ és biel·líptica amb $p^2|N$, p primer senar, i φ és la parametrització de grau 2 , llavors la diferencial $\varphi^*(\omega) = f\frac{dq}{q}$ i f no és de la forma $h(p^n\tau)$, on $h \in S_2^{new}(nivell(h))$ amb $1 \leq n \leq [\frac{v_p(N)}{2}]$.*

Demostració. Si la diferencial tingués l'anterior forma, la parametrització factoritzaria per $X_0(N/p)$ i, per tant, i comparant graus arribariem a contradicció. □

Podríem fer un estudi semblant per a cada una de les $f|_{B_d}$ i encara faltaria estudiar les parametritzacions que provenen de combinacions lineals dels elements de W, per a poder donar una resposta completa a la pregunta 8.4.1. En general s'obté:

Nota 8.4.7. *La pregunta 8.4.1 no té resposta afirmativa en general. És a dir, si el pullback d'una parametrització modular és vella, no necessàriament factoritza. Un exemple es troba en la taula 20 de [42]. Considerem la corba biel·líptica $X_0(33)$ amb única involució biel·líptica w_{33}. S'obté $X_0(33)/w_{33} = E$, $E = 11A$, en la notació de [43]. Si factoritzés a través de $X_0(M)$, amb $M|33$, l'única possibilitat, mirant els gèneres, és per $M = 11$ i, per tant, obtindríem el següent diagrama commutatiu:*



on calculant els graus arribem a contradicció.

Nota 8.4.8. *Igualment, si tenim una parametrització modular sobre $\mathbb{Q}$ $\varphi : X_0(N) \to E$, E correspon a un factor de la jacobiana mòdul $\mathbb{Q}$-isogènia. Si no correspon a la part nova, correspon a $J_{\sigma f}^{m(f)}$, $m(f) \geq 2$. D'on E és $\mathbb{Q}$-isògena a $J_{\sigma f}$ i, gràcies al teorema de Carayol, a una corba el·líptica de conductor exactament nivell(f), amb nivell$(f)|N$. Per tant,*

Proposició 8.4.9. *Donada una parametrització modular sobre $\mathbb{Q}$:*

$$\varphi : X_0(N) \to E,$$

el conductor geomètric de E divideix N.

Corol·lari 8.4.10. *Els N que compleixen $\#\Gamma_2(X_0(N), \mathbb{Q}) = \infty$, amb gènere de $X_0(N) \geq 2$ són únicament:*

22	*23*	*26*	*28*	*29*
30	*31*	*33*	*35*	*37*
39	*40*	*41*	*43*	*46*
47	*48*	*50*	*53*	*59*
61	*65*	*71*	*79*	*83*
	89	*101*	*131*	

Demostració. Per a cada N recordem que $\#\Gamma_2(X_0(N), \mathbb{Q}) = \infty$ equival a que $X_0(N)$ sigui hiperel·líptica o biel·líptica sobre $\mathbb{Q}$, en l'últim cas a una corba el·líptica E amb $rank_{\mathbb{Q}} E \geq 1$. Els N tals que $X_0(N)$ és hiperel·líptica ja els coneixem [30]. En els casos biel·líptics fem la hipòtesi que tot està definit sobre $\mathbb{Q}$. Per la proposició 8.4.9 el conductor de E divideix N, i de les taules de [9] descartem els N tals que tots els seus divisors dónen corbes el·líptiques E amb rang nul. En els altres casos, la parametrització modular forta de Weil seria l'única parametrització modular (p.e. $X_0(92)$). Així de la taula 20 de [42] i de la taula de [9] podem descartar-ne la resta. Un observa, però, que l'anterior procés recorre tots els N tals que $X_0(N)$ és biel·líptica, provant l'enunciat. □

Capítol 9

Recull dels resultats

Com a conseqüència dels lemes 3.4.1, 3.4.2, 3.4.3, els resultats de teoria de reducció, les proposicions 5.5.1,6.6.1 i el corol·lari 5.5.2, s'obté el següent resultat:

Teorema 9.1. *Hi ha exactament quaranta un valors de N, tals que la corba modular $X_0(N)$ és biel·líptica (gènere ≥ 2). A més, $X_0(N)$ admet una involució biel·líptica del tipus Atkin-Lehner, llevat del cas $X_0(72) = X_0(2^3 3^2)$. El llistat dels N amb $N \neq 72$ és el següent:*

22	*26*	*28*	*30*	*33*	*34*	*35*	*37*	*38*	*39*
40	*42*	*43*	*44*	*45*	*48*	*50*	*51*	*53*	*54*
55	*56*	*60*	*61*	*62*	*63*	*64*	*65*	*69*	*75*
79	*81*	*83*	*89*	*92*	*94*	*95*	*101*	*119*	*131*

[1]

Teorema 9.2. *Quan $X_0(N)$ és una corba biel·líptica i $N \not\equiv 0$ $(mod\ 4)$ i $(mod\ 9)$ determinem totes les involucions biel·líptiques corresponents (llistades en el lema 3.4.1). En el cas $N \equiv 0(mod\ 4)$ determinem totes les involucions biel·líptiques per a N =28,40,44,48,56,60 i 92.*

Teorema 9.3. *Les corbes modulars $X_1(N)$ i $X(N)$ no són biel·líptiques pels $N \geq 132$. A més, per a $N \leq 131$ tampoc són biel·líptiques pels següents valors:*

[1] Observem que utilitzant que les corbes $X_0(N)$ amb gènere més gran que 6 tenim parametritzacions modulars definides sobre $\mathbb{Q}$. Del treball de [25] sobre els quocients de $X_0(N)$ per involucions d'Atkin-Lehner, la taula 20 de [42] i la conjectura de Manin obtenim que si $X_0(N)$ biel·líptica,excepte $N = 81$ podem definir una parametrització modular sobre $\mathbb{Q}$.

52	*57*	*58*	*66*	*67*	*68*	*70*	*73*	*74*	*76*
77	*78*	*80*	*82*	*84*	*85*	*86*	*87*	*88*	*90*
91	*93*	*96*	*97*	*98*	*99*	*100*	*102*	*103*	*104*
105	*106*	*107*	*108*	*109*	*110*	*111*	*112*	*113*	*114*
115	*116*	*117*	*118*	*120*	*121*	*122*	*123*	*124*	*125*
126	*127*	*128*	*129*	*130*					

Corol·lari 9.4. *Pels N de l'anterior teorema obtenim que $\#\Gamma_2(X_\Gamma, L) < \infty$ per a tot cos de nombres L i $\Gamma = \Gamma_0(N)$, $\Gamma_1(N)$, $\Gamma(N)$. Per a $\Gamma = \Gamma_0(N)$ aquests N són els únics amb aquesta propietat.*

Teorema 9.5. *Sigui $X_0(N)$ amb gènere ≥ 2. Llavors $X_0(N)$ té un nombre finit de punts quadràtics sobre $\mathbb{Q}$ si i només si N no apareix a la següent família excepcional:*

22	*23*	*26*	*28*	*29*
30	*31*	*33*	*35*	*37*
39	*40*	*41*	*43*	*46*
47	*48*	*50*	*53*	*59*
61	*65*	*71*	*79*	*83*
	89	*101*	*131*	

Acabem el treball amb la següent conjectura

Conjectura 9.6. *Siguin a, b, c, d nombres enters complint $a^b - c^d = 1$, amb $a, c \neq 1$ i $b, d \geq 2$. Llavors la corba modular $X_0(a^b c^d)$ és biel·líptica però no admet cap involució biel·líptica del tipus d'Atkin-Lehner.*

Conjectura 9.7 (Catalan). *Considerem la equació diofantina $a^b - c^d = \pm 1$ on a, b, c i d són nombres enters amb $a, c \neq 1$ i $b, d \geq 2$. Llavors els únics valors que compleixen l'anterior equació diofantina són $a = 3$, $b = 2$, $c = 2$ i $d = 3$ o $a = 2$,$b = 3$,$c = 3$ i $d = 2$.*

Lema 9.8. *La conjectura 9.6 és equivalent a la conjectura de Catalan.*

Demostració. Conseqüència directa del teorema 9.1. □

Apèndix A

Un altre estudi per a $X_0(40)$ i $X_0(48)$

Pel lema 3.4.2, $X_0(40)$ i $X_0(48)$ són corbes biel·líptiques que admeten alguna involució biel·líptica del tipus d'Atkin-Lehner. Donem aquí una manera de determinar totes les seves involucions biel·líptiques. De [30] obtenim

Lema A.1. *$X_0(40)$, $X_0(48)$ i $X_0(37)$ són les úniques corbes modulars dins de la família $\Gamma_0(N)$ que són corbes hiperel·líptiques amb involució hiperel·líptica no del tipus d'Atkin-Lehner. Si denotem per υ la involució hiperel·líptica, llavors $\upsilon = \begin{pmatrix} -10 & 1 \\ -120 & 10 \end{pmatrix}$ per a $X_0(40)$ i $\upsilon = \begin{pmatrix} -6 & 1 \\ -48 & 6 \end{pmatrix}$ per a $X_0(48)$.*

Per tant, de les taules del lema 3.4.2 obtenim que $40, 48$ són els únics valors que admeten una involució hiperel·líptica i pels que no coneixem totes les involucions biel·líptiques.

Lema A.2. *Sigui C una corba hiperel·líptica amb involució hiperel·líptica υ i sigui α una altra involució. Considerem la involució $\beta = \upsilon\alpha$. Si denotem per g el gènere de C s'obté que si $g \equiv 0(2)$ llavors β i α tenen dos punts fixos cadascuna. Si $g \equiv 1(2)$ llavors o bé β té 4 punts fixos i α cap o viceversa.*

Demostració. Denotem per n_α, n_β el nombre de punts fixos de α i β respectivament, els quals són parells per la fórmula de Hurwitz. Com que $\upsilon \in Z(Aut(C))$, υ i α commuten i, per tant, actuen sobre el conjunt de punts fixos de l'altra involució. Així, si tenen un punt fix comú també en tenen un segon. Anomenem-los P i Q. Considerem el divisor

$$(P) - (Q)$$

com a divisor de C, C/α, C/υ. Com que C/υ té gènere 0 tenim $(P) - (Q) = div(f)$, d'on $f \circ \alpha = \pm f$. El signe de f ha de ser positiu per tenir un zero

d'ordre parell. Per tant, ens dóna una funció de grau 1 a C/α que té gènere superior a zero, cosa que no pot passar. D'aquí deduïm que υ i α no tenen punts fixos comuns i, de manera anàloga es veu per a υ i β i per a β i α. Com que tots els punts fixos de la involució hiperel·líptica corresponen als punts de Weierstrass, els punts fixos de α no són de Weierstrass. Si $n_\alpha > 0$ llavors $gènere(C/\alpha) = [g/2]$ d'on, per Hurwitz, $n_\alpha = 2$, si g és parell, i $n_\alpha = 4$, si g és senar, on g denota el gènere de C. Considerem el subgrup $H =< \alpha, \upsilon >$. Aleshores

$$C \to C/H = \mathbb{P}^1$$

té grau 4. En ser els punts fixos disjunts, obtenim de la fórmula de Hurwitz:

$$2g - 2 = 4(-2) + n_\upsilon + n_\alpha + n_\beta = -8 + 2g + 2 + n_\beta + n_\alpha$$

i, per tant, $4 = n_\alpha + n_\beta$. □

Corol·lari A.3. *Totes les involucions biel·líptiques de* $X_0(40)$ *són*

$$w_{40}, S_2, w_8S_2w_8, S_2w_8S_2w_8, w_5S_2w_8S_2$$

Demostració. Ara $C = X_0(40)$ i $g = 3$. Per tant, tota altra involució tindrà 0 o 4 punts fixos. Les involucions amb 4 punts fixos són justament les involucions biel·líptiques. Com que la involució hiperel·líptica $\upsilon = w_5w_8S_2w_8S_2$ i com que w_5 i w_8 no són biel·líptiques aleshores $w_8S_2w_8S_2$ i $w_5S_2w_8S_2$ són involucions biel·líptiques. Igualment, com que w_{40} és biel·líptica, $S_2w_8S_2$ no té punts fixos i, per tant, no és biel·líptica. La involució S_2 té alguna punta fixa. Així, S_2 és biel·líptica i $w_5w_8S_2w_8$ no ho és. Un comprova que $w_8S_2w_8$ té punts fixos a les puntes i, per tant, l'anterior involució és biel·líptica i w_5S_2 no té cap punt fix i per tant no pot ser una involució biel·líptica. Utilitzant que coneixem la caracterització del grup dels automorfismes (3.1.6, i rectificacions) s'obté que totes les involucions de $X_0(40)$ són les estudiades anteriorment. □

Corol·lari A.4. *Totes de les involucions biel·líptiques de* $X_0(48)$ *són:*

$$w_{48}, S_2w_{16}S_2w_{16}, w_3S_2w_{16}S_2, S_2, w_{16}S_2w_{16}$$

$$w_3S_4, w_3S_4^3, w_3w_{16}S_4w_{16}, w_3w_{16}S_4^3w_{16}$$

Demostració. Aquest cas es molt més complicat ja que 3.1.6 no està en suma directa. Observem que $S_4w_3 \neq w_3S_4$. Per tant cal fer un estudi del grup $Norm(\Gamma_0(48))$ semblant al que s'ha fet per $Norm(\Gamma_0(N))$ amb $\upsilon(N) = 3$. Un prova en aquest cas que tot $u \in Norm(\Gamma_0(48))$ s'escriu com:

$$w_m\beta$$

on $\beta \in \{w_{16}, S_4 | S_4^4 = w_{16}^2 = (w_{16}S_4)^3 = 1\}$. També es veu que totes les involucions són

$$\begin{array}{ccccc} S_2 & w_{16} & w_{16}S_2w_{16}S_2 & S_2w_{16}S_2 & S_4^3w_{16}S_4 \\ S_4w_{16}S_4^3 & w_{16}S_2w_{16} & w_{16}S_2w_{16}S_4 & S_4w_{16}S_2w_{16} & w_3 \\ w_{48} & w_3S_2 & w_3w_{16}S_2w_{16} & w_3S_2w_{16}S_2 & w_3S_4^3 \\ w_3S_4 = S_4^3w_3 & w_3w_{16}S_4w_{16} & w_3w_{16}S_4^3w_{16} & & \end{array}$$

$w_3S_2w_{16}S_2w_{16}$ és la involució hiperel·líptica de $X_0(48)$. Apliquem el lema A.2. Com que w_{16} i w_3 no són biel·líptiques aleshores $w_3S_2w_{16}S_2$ i $w_{16}S_2w_{16}S_2$ són involucions biel·líptiques. Com que w_{48} és biel·líptica $S_2w_{16}S_2$ no ho és. Observem que S_2 i $w_{16}S_2w_{16}$ deixen puntes fixes i, per tant, per ser el gènere senar són involucions biel·líptiques d'on $w_3w_{16}S_2w_{16}$ i S_2w_3 no ho són. Per a $S_4w_{16}S_4^3$ observem que si τ és un punt fix de $Y_0(48)$ d'aquesta involució, es té

$$\begin{pmatrix} 19 & 31 \\ 30 & 49 \end{pmatrix} 2\tau = \delta 2\tau \tag{A.1}$$

$\delta \in \Gamma_0(24,2)$. Com que la matriu de l'esquerra de A.1 és de $\Gamma_0(6)$ llavors $\pi(\tau)$ és un punt el·líptic de $X_0(6)$ on $\pi : X_0(48) \to X_0(6)$ és multiplicar per 2, com que no té punts el·líptics així no té cap punt fix, és a dir, $S_4w_{16}S_4^3$ no és una involució biel·líptica. Exactament el mateix argument prova que la involució $S_4^3w_{16}S_4$ no és biel·líptica. Per a les involucions $S_4w_{16}S_2w_{16}$ i $w_{16}S_2w_{16}S_4$ l'argument és exactament el mateix que per a la involució $S_4w_{16}S_4^3$ però $\pi : X_0(48) \to X_0(6)$ és multiplicar en aquests casos per 4. Finalment, utilitzant el lema A.2 obtenim que w_3S_4, $w_3S_4^3$, $w_3w_{16}S_4w_{16}$ i $w_3w_{16}S_4^3w_{16}$ són biel·líptiques. □

Apèndix B

Un estudi per a la corba modular $X_0(63)$

Hem vist que una involució biel·líptica de $X_0(63)$ és w_{63}. Anem a provar que únicament té $X_0(63)$ dues involucions biel·líptiques més.

Proposició B.1 (Kenku-Momose,[21]). *Denotem per v l'element excepcional de $Aut(X_0(63))$ que compleix $v^2 = w_9$ i $vw_7 = w_7v$. La representació de $Aut(X_0(63))$ en l'espai tangent de $Jac(X_0(63))$ és la següent:*

$$S_3 = \begin{pmatrix} 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 0 \end{pmatrix}; \; v = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix}$$

$$w_9 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}; \; w_7 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Llavors de $Aut(X_0(63)) \cong \mathcal{S}_4 \times \mathbb{Z}/2$ en resulta el següent lema:

Lema B.2. *Totes les involucions de $Aut(X_0(63))$, a excepció de les tipus d'Atkin-Lehner, són:*

$$\begin{array}{cccc} S_3^2w_9S_3 & S_3w_9S_3^2 & S_3w_9S_3^2v & w_9S_3w_9S_3^2v \\ w_9S_3vS_3^2 & w_9S_3vw_9S_3^2 & w_9S_3^2vS_3 & w_9S_3^2vw_9S_3 \\ w_7S_3^2w_9S_3 & w_7S_3w_9S_3^2 & w_7S_3w_9S_3^2v & w_7w_9S_3w_9S_3^2v \\ w_7w_9S_3vS_3^2 & w_7w_9S_3vw_9S_3^2 & w_7w_9S_3^2vS_3 & w_7w_9S_3^2vw_9S_3 \end{array}$$

Recordem que si i és una involució biel·líptica, actua en l'espai de les diferencials com a -1 llevat d'un espai 1-dimensional en el que hi actua com a 1. A més, l'anterior proposició ens calcula l'acció de les involucions en l'espai de les diferencials regulars. De tot això es desprén:

Corol·lari B.3. *Les involucions de* $X_0(63)$*:*

$$\begin{array}{cccc} S_3^2w_9S_3 & S_3w_9S_3^2 & S_3w_9S_3^2v & w_9S_3w_9S_3^2v \\ w_9S_3vS_3^2 & w_9S_3vw_9S_3^2 & w_9S_3^2vS_3 & w_9S_3^2vw_9S_3 \\ & & w_7S_3w_9S_3^2v & w_7w_9S_3w_9S_3^2v \\ w_7w_9S_3vS_3^2 & w_7w_9S_3vw_9S_3^2 & w_7w_9S_3^2vS_3 & w_7w_9S_3^2vw_9S_3 \end{array}$$

no són biel·líptiques.

Proposició B.4. *Les úniques involucions biel·líptiques de* $X_0(63)$ *són* w_{63}*,* $w_7S_3^2w_9S_3$ *i* $w_7S_3w_9S_3^2$*.*

Demostració. Només cal veure que efectivament $w_7S_3^2w_9S_3$ i $w_7S_3w_9S_3^2$ són biel·líptiques. Això és conseqüència de que actuen com a -1 sobre un subespai de codimensió 1 de l'espai de les diferencials. Aquest fet és característic de les involucions biel·líptiques. □

Bibliografia

[1] Dan Abramovich and Joe Harris, *A*belian varieties and curves in $W_d(C)$; Compositio Mathematica 78, 227-238 (1991).

[2] R.D.M. Accola, *T*opics in the Theory of Riemann Surfaces; LNM 1595; Springer.

[3] A.Arenas and J.Quer, *P*arametritzacions modulars de alguns grups modulars; Apunts de STNB 1992.

[4] A.O.L. Atkin and J.Lehner, *H*ecke operators on $\Gamma_0(N)$; Math. Ann.185 (1970), 134-160.

[5] Arbarello, Cornalba, Griffiths and Harris, *G*eometry of algebraic Curves,vol I; Springer, New York 1985.

[6] H. Carayol, *S*ur les représentations l-adiques associées aux formes modulaires de Hilbert; Ann. scient. Ec. Norm. Sup. 19 (1986), 409-468.

[7] H. Carayol, *F*ormes modulaires et represéntations l-adiques; en el llibre *J*ournées Arithmétiques de Besançon, Astérisque, n. 147-148, 1987.

[8] H. Carayol, *S*ur les représentations galoisienes modulo l attachées aux formes modulaires; Duke Math. J. 59 (1989), 785-801.

[9] J.E. Cremona, *A*lgorithms for modular elliptic curves, Cambridge Univ. Press,1992.

[10] H. Cohen, *A* Course in Computational Algebraic Number Theory; GTM 138, Springer-Verlag.

[11] P.Deligne and M. Rapoport, *L*es schémas de modules de courbes elliptiques. En el llibre *Modular Functions of One Variable II*, Springer Verlag, LNM 349, 143-316.

[12] B. Edixhoven, J.H.Evertse, *D*iophantine Approximation and Abelian Varieties; LNM 1566, Springer.

[13] B. Edixhoven, *O*n the Manin constant of modular elliptic curves. En el llibre *A*rithmetic Algebraic Geometry PM 89, Birkhäuser, 25-40.

[14] N. Elkies, *T*he automorphism group $X_0(63)$; Compositio Mathm. 74, 203-208 (1990).

[15] Faltings, *D*iophantine aproximation on abelian varieties; Annuals of Math. 133 (1991) 549-576.

[16] Forster O., *L*ectures on Riemann Surfaces; GTM 81, Springer.

[17] Fricke, *L*ehrbuch der Algebra vol 3, Braunschweig, Vieweg(1928).

[18] J. Harris and J.H. Silvermann, *B*ielliptic curves and symmetric products; Proc. of Amer. Math. Soc.,112,2 June 1991

[19] M. Hindry, *P*oints quadratiques sur les courbes; C.R.Acad.Sci.Paris t.305, p.219-221,1987.

[20] J. Igusa, *K*roneckerian models of fields of elliptic modular functions; Amer. J. Math. 81 (1959), 561-577.

[21] M.A. Kenku and F. Momose, *A*utomorphism groups of the modular curves $X_0(N)$; Compositio Mathem. 65 (1988) 51-80.

[22] Kluit, *O*n the normalizer of $\Gamma_0(N)$. En el llibre Modular forms of one variable IV, LNM 601, Springer, 239-246.

[23] Y.Manin, *P*arabolic points and zeta functions of modular forms; Math.USSR-Izvestija,vol6,n1(1981)19-64.

[24] B. Mazur, *M*odular curves and the Eiseinstein ideals; Publ.Math. I.H.E.S. 47 (1977).

[25] B. Mazur and H.P.F. Swinnerton-Dyer, *A*rithmetic of Weil curves; Inventiones Math. 25 (1974), 1-64.

[26] D. Mumford, *C*urves and their Jacobians. The University of Michigan, second print 1976.

[27] E. Nart, *F*ormes modulars. Publicacions de la U.A.B.

[28] M. Newman, *S*tructure theorem for modular subgroups; Duke Math. J.22 (1955) 25-32.

[29] M. Newman, *C*onjugacy, genus, and class numbers; Math. Annalen, 196(1972) 198-217.

[30] A.P. Ogg, *H*yperelliptic modular curves; Bull. Soc. math. France 102 (1974) 449-462.

[31] A.P. Ogg, Ü*b*er die Automorphismengruppe von $X_0(N)$; Math. Ann. 228(1977)279-292.

[32] A.P. Ogg, *R*ational points on certain elliptic modular curves. Analityc Number Theory XXIV, Proceedings of Symposia in Pure Mathematics, 221-232.

[33] K.Ribet, *L*ettre à Andrew Ogg (29-11-74).

[34] J.P.Serre, *A*belian l-àdic representations and elliptic curves; New York, 1968.

[35] J.H. Silvermann, *T*he Arithmetic of Elliptic Curves; Springer, GTM 106.

[36] J.H. Silvermann, *A*dvanced Topics in the Arithmetic of Elliptic Curves; Springer, GTM 151.

[37] G. Shimura, *I*ntroduction to the arithmetic theory of automorphic functions; Princeton, 1971.

[38] G. Shimura, *O*n the factors of jacobian variety of modular functions fields; J. Math. Soc. Japan 25(1973) 525-544.

[39] M. Shimura, *D*efining Equations of Modular Curves $X_0(N)$; Tokyo J. Math. 18,2 (1995).

[40] H.P.F. Swinnerton-Dyer and B.J. Birch, *E*lliptic curves and modular functions; en el llibre Modular forms of one variable IV, LNM 601, 3-32, Springer.

[41] D. Zagier, *M*odular Parametrizations of elliptic curves; Canad. Math. Bull. 28(3) (1985), 372-384.

[42] *C*orbes modulars: Taules. Notes del seminari de Teoria de Nombres, UB-UAB-UPC, Barcelona 1992.

[43] Taules d'Antwerp; en el llibre *M*odular Functions of one variable IV LNM 601 .