El teorema de Stark-Heegner vía curvas modulares asociadas a subgrupos de Cartan *non-split* de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$

Daniel Mejail

26/09/2016

1 Introducción

El objectivo de esta monografía es repasar algunas de las soluciones al problema del número de clases igual a 1, con un interés particular en una interpretación modular. Concretamente, nos interesará entender la relación entre órdenes en cuerpos cuadráticos imaginarios y puntos enteros en las curvas modulares asociadas a subgrupos de Cartan *non-split* de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ y sus normalizadores. Esta relación aparece mencionada en [13], y, a lo largo de los últimos cuarenta años han ido aparenciendo soluciones al problema basadas en un estudio de estas curvas.

Comenzamos este trabajo enunciando el teorema de Stark-Heegner y, siguiendo [13], verificamos parte del enunciado. A continuación, en la sección 2, describimos, en mayor o menor detalle, algunas de las propiedades de los objetos de interés: definimos los subgrupos de Cartan *non-split* y los objetos modulares correspondientes. Si $\Gamma(N)$ es un subgrupo principal de congruencia de nivel N, dado un subgrupo H de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, podemos asociarle una superficie de Riemann como cociente del semiplano complejo superior, X_H, y un cociente de una curva, $H\backslash X(N)$, donde $X(N)$ es, esencialmente, una unión disjunta de copias de $\Gamma(N)\backslash\mathfrak{h}^*$. Para terminar, en la sección 3, resumimos diversas demostraciones del teorema de Stark-Heegner cuyo punto de contacto es la interpretación modular del problema.

Si llamamos $X(1)$ a la superficie de Riemann $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{h}^*$, se puede ver que existen morfismos naturales $X_H \to X(1)$. Si la curva X_H está definida sobre $\mathbb{Q}$, dicho morfismo también es un $\mathbb{Q}$-morfismo, y resulta ser relativamente sencillo, directo, determinar si un punto de X_H es *íntegro* en función de propiedades que pueda tener su imagen en $X(1)$.

Existen distintas maneras de determinar los puntos enteros sobre las curvas X_H; cada uno de ellos indica una conexión con un objeto distinto. En [9], se obtiene una parametrización de la curva $X_{ns}^+(7)$ (ver más adelante sección 2) por medio de la relación con formas de Klein, de acuerdo con la descripción en [10]. En [1], [2], [4] y [5], el método consiste en extraer, de las parametrizaciones de las curvas correspondientes, ecuaciones diofánticas. Determinar las soluciones a estas ecuaciones permite, luego, determinar los puntos enteros en cada caso. En [11], la metodología para determinar puntos enteros es

completamente distinta, basada en formas lineales en logaritmos y en la existencia de un isomorfismo entre $X_{ns}^+(11)$, la curva modular estudiada en el trabajo citado, y una curva elíptica.

Independientemente del método, la conexión con el problema del número de clases, y la motivación que por este lado pueda venir para estudiar las curvas asociadas a subgrupos de Cartan de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, ya se encuentra en las observaciones de Serre en el apéndice a [13]. El problema de determinar los cuerpos cuyo número de clases es igual a 1 no es la única motivación para estudiar las curvas asociadas a distintos tipos de subgrupos de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Como se verá en los ejemplos, no es cierto que exista una correspondencia entre cuerpos cuadráticos imaginarios de número de clase 1 y puntos íntegros en las curvas $X_{ns}^+(N)$. Estas curvas parametrizan clases de isomorfismo de curvas elípticas incorporando una *estructura de nivel*. En estos términos, no todos los puntos íntegros de $X_{ns}^+(N)$ están asociados a curvas elípticas con multiplicación compleja; los que sí, tendrán que ver con órdenes en cuerpos cuadráticos imaginarios. Según [3], contar puntos en curvas asociadas a subgrupos de Cartan *non-split* de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ y sus normalizadores está relacionado con el siguiente problema: determinar si existe una constante tal que, para todo primo p mayor que dicha constante, si E es una curva elíptica sin multiplicación compleja, entonces la representación de Galois *modulo* p asociada es sobreyectiva. El problema parece reducirse a determinar si existe una constante $C > 0$ tal que, si $p > C$, entonces los únicos puntos $\mathbb{Q}$-racionales en $X_{ns}^+(p)$ son puntos CM, puntos asociados a curvas elípticas con multiplicación compleja.

Por otro lado, el tipo de soluciones mencionado permite relacionar y encarar desde un mismo punto algunas de las demostraciones ya existentes del teorema de Stark-Heegner: la solución presentada en [5] es una interpretación modular de la solución dada por Siegel, y en [4], siguiendo la sugerencia en [13], se intenta hacer lo mismo con la demostración de Heegner.

1.1 El teorema de Stark-Heegner y su relación con formas cuadráticas

Relación con formas cuadráticas Describimos brevemente la relación entre formas cuadráticas y órdenes en cuerpos cuadráticos imaginarios. En cuanto a las definiciones necesarias, remitimos a [6].

Sea I un orden en un cuerpo cuadrático imaginario K de discriminante $D < 0$, y sea d_K el discriminante del cuerpo. Sea $f = ax^2 + bxy + cy^2$ una forma cuadrática (primitiva y definida positiva) de discriminante D. Como D es negativo, existe una única raíz τ del polinomio cuadrático $f(x, 1)$ perteneciente al semiplano complejo superior, $\mathfrak{h}$. Porque f es definida positiva, τ, en términos del discriminante y de los coeficientes de f, es igual a $(-b + \sqrt{D})/2a$.

Sea f el conductor del orden I, de manera que $D = f^2 d_K$, y sea $w_K \in K$ el elemento

$$w_K := \frac{d_K + \sqrt{d_K}}{2} .$$

Por un lado, $\mathcal{O}_K$, el anillo de enteros de K, es igual, en tanto $\mathbb{Z}$-módulo, a $(1, w_K)_{\mathbb{Z}}$, el módulo generado por 1 y w_K en K. Se puede ver que $(1, a\tau)_{\mathbb{Z}} = (1, f w_K)_{\mathbb{Z}} = I$, con lo que $(a, a\tau)_{\mathbb{Z}}$ es un ideal propio de I en K.

Dadas dos formas f y g, ellas son propiamente equivalentes, si, y sólo si sus raíces en $\mathfrak{h}$, τ y τ', pertenecen a la misma órbita en el semiplano por la acción de $\mathrm{SL}_2(\mathbb{Z})$. Esto último es, a su vez, equivalente a que los retículos $[1,\tau]$ y $[1,\tau']$ en $\mathbb{C}$ estén relacionados por una homotecia definida sobre K: que exista λ en K tal que

$$[1,\tau] \;=\; \lambda[1,\tau'] \;.$$

Todo esto muestra que, si f es una forma cuadrática, cuya raíz asociada es τ, la aplicación $f \mapsto [a, a\tau]$ determina una aplicación biyectiva del grupo de clases de formas de discriminante D en el grupo de clases del orden I. (En principio, esta aplicación es inyectiva, pero la sobreyectividad se sigue de que todo ideal propio de I está generado, en tanto $\mathbb{Z}$-módulo, por dos elementos de K). Esta aplicación resulta ser un morfismo de grupos, con lo que ambos son isomorfos. Los números de los grupos de clases, $h(D)$ y $h(I)$, respectivamente, son, entonces, iguales.

El teorema de Stark-Heegner Sea K un cuerpo cuadrático imaginario y sea d_K su discriminante. En ese caso, d_K siendo un discriminante fundamental, d_K es un entero libre de cuadrados congruente a 1 *modulo* 4, o es igual a $-4n$, donde n es un entero libre de cuadrados, no congruente a 3 *modulo* 4.

Si n es un entero positivo, entonces el número de clases de formas cuadráticas de discriminante $-4n$ es igual a 1, si, y sólo si n pertenece al conjunto $\{1,2,3,4,7\}$. Una demostración elemental de esto se puede encontrar en el teorema 2.18 de [6]. Esto muestra que, para un cuerpo cuadrático K de discriminante d_K, si $d_K = -4n$, entonces $h(K) = 1$ únicamente en los casos en que n sea igual a 1 o a 2.

La demostración de que los cuerpos $K = \mathbb{Q}(\sqrt{d_K})$, con $-d_K$ igual a 3, 4, 7, 8, 11, 19, 43, 67 o 163 tienen número de clases igual a 1 es elemental: para $d_K = -3$, -4, -8, los cuerpos correspondientes son $K = \mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, cuyos anillos de enteros son dominios euclídeos.

Si consideramos la familia de formas cuadráticas de discriminante d_K, hay exactamente $2^{\mu-1}$ géneros de formas, donde μ es la cantidad de factores primos en d_K. Pero, si el número de clases es 1, el número de géneros también lo es, y $\mu = 1$, es decir, $d_K = -p$, para algún primo $p \equiv 3\,(4)$. Si p es congruente a 7 *modulo* 8, entonces, comparando con el orden I de conductor 2 en $\mathcal{O}_K$, la relación entre los números de clases es

$$h(I) \;=\; h(\mathcal{O}_K)\frac{2}{|\mathcal{O}_K^\times : I^\times|}\left(1 - \left(\frac{d_K}{2}\right)\frac{1}{2}\right) \;,$$

y el factor que multiplica a $h(\mathcal{O}_K)$ es un entero (teorema 7.24 de [6]). Pero, entonces, $|\mathcal{O}_K^\times : I^\times| = 1$ y $(d_K/2)$ (el símbolo de Kronecker en d_K) es igual a 1, con lo cual, $h(-4p) = h(I) = h(\mathcal{O}_K) = h(-p) = 1$ y $p = 7$ es la única opción.

La proposición que ahora enunciamos, y el argumento que le sigue, se pueden encontrar en el apéndice de [13].

Proposición 1.1. *Las siguientes propiedades de un primo $p > 3$ congruente a 3 modulo 4 son equivalentes:*

i) $h(-p) = 1$*;*

ii) $\left(\frac{l}{p}\right) = -1$ *para todo primo* $l < p/4$*;*

ii)' $\left(\frac{l}{p}\right) = -1$ *para todo primo* $l < \sqrt{p/3}$*;*

iii) (si $p > 7$*)* $p \equiv 3\,(8)$ *y* $R - N = 3$*, si* R *(respectivamente,* N*) es el número de residuos (no residuos) cuadráticos modulo* p *en* $[1, (p-1)/2]$*;*

iv) si $x \in [\![0, (p-7)/4]\!]$*,* $P_p(x) = x^2 + x + (p+1)/4$ *es primo;*

iv)' si $x \in [0, 1/2(\sqrt{p/3} - 1)]$*,* $P_p(x)$ *es primo.*

Demostración. El anillo de enteros de $\mathbb{Q}(\sqrt{-p})$ es $\mathbb{Z}[w]$, donde $w = \frac{1+\sqrt{-p}}{2}$; un primo l es inerte en $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$, si, y sólo si $(l/p) = -1$ (ver [6]). Dicho de otra manera, si $h(-p) = 1$, la condición $(l/p) = -1$ implica que l es una norma: existe $\alpha \in \mathbb{Z}[w]$, $\alpha = x + yw$, tal que $\mathrm{Nm}(\alpha) = l$. Pero $\mathrm{Nm}(\alpha)$ es igual a $(x + \frac{y}{2})^2 + (\frac{y}{2})^2 p$. Así, l es primo, $y \neq 0$ y $\mathrm{Nm}(\alpha) \geq p/4$. Recíprocamente, asumamos que $(ii)'$ se cumple. Entonces, si $\mathfrak{l} \subset \mathbb{Z}[w]$ es un ideal primo, y vale $\mathrm{Nm}(\mathfrak{l}) < \sqrt{p/3}$, dado l primo que divide a $\mathrm{Nm}(\mathfrak{l})$, es $l < \sqrt{p/3}$. En particular, $(l/p) = -1$, por hipótesis, y $\mathfrak{l} = (l)$ es un ideal principal. Todo ideal de norma menor que $\sqrt{p/3}$ es, entonces, principal. Pero toda clase en $\mathsf{Cl}(\mathbb{Z}[w])$ contiene un elemento con esta propiedad.

El resto de la demostración (excepto las equivalencias con (iii)) es, también, elemental. □

Sea $p \equiv 3\,(\mathrm{mod}\,4)$ un primo, $3 < p < 75$, y sea $m = (p+1)/4$. En este caso, por (iv)', $h(-p) = 1$ es equivalente a que m y $m + 2$ sean primos. Esto último es cierto para m en el conjunto $\{3, 5, 11, 17\}$. El primo p es 11, 19, 43 o 67.

Teorema 1.2. *Sea* $d_K < 0$ *el discriminante de un cuerpo cuadrático imaginario. Entonces* $h(d_K) = 1$*, si, y sólo si* d_K *es igual a* -3*,* -4*,* -7*,* -8*,* -11*,* -19*,* -43*,* -67 *o a* -163*.*

2 Generalidades

Sea $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ un retículo en $\mathbb{C}$, generado por ω_1 y ω_2 tales que $\omega_1/\omega_2 \in \mathfrak{h}$. Los puntos de N-torsión de $\mathbb{C}/\Lambda$ conforman el grupo $\langle(\omega_1/N) + \Lambda\rangle \times \langle(\omega_2/N) + \Lambda\rangle$ isomorfo a $(\mathbb{Z}/N\mathbb{Z})^2$. Sea μ_N el grupo de raíces N-ésimas de la unidad en $\mathbb{C}$, $\mu_N = \langle e^{2\pi i/N}\rangle$. Dados P y Q en $\mathbb{C}/\Lambda$ de N-torsión, existe $\gamma \in \mathrm{M}_{2\times 2}(\mathbb{Z}/N\mathbb{Z})$ tal que

$$\begin{bmatrix} P \\ Q \end{bmatrix} = \gamma \begin{bmatrix} (\omega_1/N) + \Lambda \\ (\omega_2/N) + \Lambda \end{bmatrix} .$$

Definimos $e_N(P, Q) := e^{2\pi i \det(\gamma)/N}$, el *pairing* de Weil en P y Q. Esto define, vía la correspondencia con curvas elípticas definidas sobre $\mathbb{C}$, una aplicación, $E[N] \times E[N] \to \mu_N$, en pares de puntos de N-torsión de una curva elíptica E, tomando valores en el conjunto de raíces N-ésimas de la unidad.

Sean E y E' dos curvas complejas, y sean (P,Q) y (P',Q') pares de puntos de orden N en E y en E', respectivamente, tales que $e_N(P,Q) = e_N(P',Q') = e^{2\pi i/N} = \zeta_N$. La dupla E, junto con (P,Q) se dice relacionada con E', con (P',Q'), si existe un isomorfismo $E \xrightarrow{\sim} E'$ (definido sobre $\mathbb{C}$) tal que $P \mapsto P'$ y $Q \mapsto Q'$. Esto determina una relación de equivalencia, y denotamos $S'(N)$ al conjunto que resulta de tomar las clases de equivalencia correspondientes en

$$\{(E,(P,Q)) \,:\, E \text{ curva elíptica sobre } \mathbb{C}, e_N(P,Q) = \zeta_N\} \ ,$$

y con $[E,(P,Q)]$ a la clase de $(E,(P,Q))$.

Sea, ahora, $\Gamma(N)$ el subgrupo principal de congruencia de nivel N, el núcleo del morfismo sobreyectivo $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ dado por reducir coordenadas *modulo* N. Sean $Y'(N)$ la superficie de Riemann $\Gamma(N)\backslash\mathfrak{h}$, y $X'(N) = \Gamma(N)\backslash\mathfrak{h}^*$ su compactificación agregando las cúspides correspondientes a $\Gamma(N)$. El conjunto $S'(N)$ está dado por

$$\{[\mathbb{C}/\Lambda_\tau,\, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)] \,:\, \tau \in \mathfrak{h}\} \ ,$$

y dos puntos $[\mathbb{C}/\Lambda_\tau,\, (\tau/N+\Lambda_\tau, 1/N+\Lambda_\tau)]$ y $[\mathbb{C}/\Lambda_{\tau'},\, (\tau'/N+\Lambda_{\tau'}, 1/N+\Lambda_{\tau'})]$ son iguales, si, y sólo si $\Gamma(N)\tau = \Gamma(N)\tau'$. La aplicación $[\mathbb{C}/\Lambda_\tau,\, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)] \mapsto \Gamma(N)\tau$ da una biyección entre $S'(N)$ y la curva $Y'(N)$. Es decir, $X'(N)$ parametriza (clases de equivalencia de) curvas elípticas junto con un par de generadores de la N-torsión y con un *pairing* particular. [8]

Las curvas en las que fijaremos nuestra atención serán ciertos cocientes de las curvas $X'(N)$. Sea $E/\mathbb{C}$ una curva elíptica, y sea $E[N]$ su subgrupo de N-torsión. Fijar un isomorfismo $\varphi : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$ equivale a dar una base de $E[N]$, es decir, dos puntos P y Q de E que generen $E[N]$. En este sentido, la información relativa a la torsión que brinda un par (E,φ) es menos específica que la contenida en los pares $(E,(P,Q))$. Dados dos pares (E,φ) y (E',φ'), los mismos son equivalentes, si existe un isomorfismo $E \xrightarrow{\sim} E'$ tal que $\varphi \mapsto \varphi'$, es decir, si $\{P,Q\}$ es la base de $E[N]$ y $\{P',Q'\}$ la de $E'[N]$, $P \mapsto P'$ y $Q \mapsto Q'$. La relación es la misma; simplemente estamos permitiéndonos ver otros puntos que antes, en $X'(N)$, no consideramos. Ésta es una relación de equivalencia, y denotamos $S(N)$ al conjunto de clases de pares (E,φ) (denotadas $[E,\varphi]$) por dicha relación.

Sea $E/\mathbb{C}$ una curva elíptica, y sea $\varphi : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ una estructura de nivel. Sea $e_N : E[N] \times E[N] \to \mu_N$ una forma alternada, no degenerada, el *pairing* de Weil, sea $\zeta_N := e^{2\pi i/N}$ y $\zeta(\varphi)$ la raíz de la unidad

$$\zeta(\varphi) := e_N\left(\varphi^{-1}\left(\begin{bmatrix}1\\0\end{bmatrix}\right), \varphi^{-1}\left(\begin{bmatrix}0\\1\end{bmatrix}\right)\right) \ .$$

El par (E,φ) es equivalente a uno de la forma $(\mathbb{C}/\Lambda,\, (\tau/N + \Lambda_\tau, 1/N + \Lambda))$, $\tau \in \mathfrak{h}$, si, y sólo si $\zeta(\varphi) = \zeta_N$.

En general, la forma alternada e_N determina una función $S(N) \to \mu_N$. Haciendo de ésta una función continua, vemos que se puede obtener una superficie de Riemann compacta $X(N)$ a partir de $S(N)$, y, como $e_N(aP + bQ, cP + dQ) = e_N(P,Q)^{\det(\gamma)}$, para $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, la curva $X(N)$ es disconexa. Más precisamente, es la

unión disjunta de $\phi(N)$ componentes. Cada una de estas componentes es una copia de $X'(N)$ y están en correspondencia con las raíces primitivas N-ésimas de 1: si ζ_N^k es una de ellas, la componente correspondiente es la que contiene las clases $[E, \varphi]$ con $\zeta(\varphi) = \zeta_N^k$ (sección 7 de [4] y [7]). Para ser más claros, el grupo $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ actúa sobre los puntos no cuspidales de la curva compactificada $X(N)$. Esta acción está determinada por $(E, \phi) \mapsto (E, \gamma \circ \varphi)$.

Sea H un subgrupo de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ tal que $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$. A través del determinante, $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ permuta las componentes de la curva $X(N)$. Como la imagen de H por $\det(\cdot)$ es todo $(\mathbb{Z}/N\mathbb{Z})^\times$, el cociente $H\backslash X(N)$ es conexo. En el caso en que H es igual a todo el grupo general lineal, obtenemos $X(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{h}^*$.

Dado un subgrupo arbitrario H de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, llamamos H' a la intersección $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, y Γ_H a la preimagen de H' por $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Notando que Γ_H es un subgrupo de congruencia (de nivel N), definimos

$$X_H \ := \ \Gamma_H\backslash\mathfrak{h}^* \ .$$

Esta curva se identifica con el cociente $H'\backslash X'(N)$, y también con $H\backslash X(N)$, si $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$. En otras palabras, X_H es el cociente de $X'(N)$ por la acción del subgrupo de automorfismos determinado por H'.

Necesitaremos saber en qué casos estas curvas están definidas sobre $\mathbb{Q}$.

Proposición 2.1. *Sea H un subgrupo de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ tal que su imagen por el determinante cubra $(\mathbb{Z}/N\mathbb{Z})^\times$. Entonces $X_H = H\backslash X(N)$ es una variedad algebraica conexa definida sobre $\mathbb{Q}$.*

El enunciado de esta proposición, como su demostración se pueden encontrar en el teorema 43 de [4].

Demostración. Primero se definen ciertas funciones modulares para el grupo $\Gamma(N)$ [8]: sea $v = (c_v, d_v)$ un par donde c_v y d_v son enteros y sus reducciones no son ambas divisibles por N, es decir, $\overline{v}(\overline{c_v}, \overline{d_v}) \neq 0$ en $(\mathbb{Z}/N\mathbb{Z})^2$. Dado $(\mathbb{C}/\Lambda, (P, Q))$ con $e_N(P.Q) = \zeta_N$, definimos

$$F_0^{\overline{v}}(\mathbb{C}/\Lambda, (P, Q)) \ = \ \frac{g_2(\Lambda)}{g_3(\Lambda)}\wp_\Lambda(c_v P + d_v Q) \ ,$$

donde g_2 y g_3 son las funciones que se obtienen de las series de Eisenstein G_4 y G_6, y $\wp_\Lambda$ es la función de Weierstraß del retículo Λ. De manera equivalente, si $\tau \in \mathfrak{h}$, podemos definir

$$f_0^{\overline{v}}(\tau) \ = \ \frac{g_2(\tau)}{g_3(\tau)}\wp_\tau(\frac{c_v\tau + d_v}{N}) \ ,$$

y $f_0^{\overline{v}}(\tau) = F_0^{\overline{v}}(\mathbb{C}/\Lambda_\tau, (\tau/N, 1/N))$. Las funciones $F_0^{\overline{v}}$ no dependen del representante de la clase de $(\mathbb{C}/\Lambda, (P, Q))$, y las funciones $f_0^{\overline{v}}$ dependen sólo de la órbita $\Gamma(N)\tau \subset \mathfrak{h}$. Se veifica que éstas son funciones invariantes por $\Gamma(N)$ y meromorfas, tanto en $\mathfrak{h}$, como en las cúspides de $\Gamma(N)$. Es decir, son funciones meromorfas en $X'(N)$.

Sea $\mathbb{C}(X'(N))$ el cuerpo de funciones meromorfas en $X'(N)$, y sea

$$\begin{aligned}\theta \,:\, \mathrm{SL}_2(\mathbb{Z}) &\to \mathrm{Aut}(\mathbb{C}(X'(N)))\,|\\ \gamma &\mapsto (\theta(\gamma):\, f \mapsto f^{\theta(\gamma)} = f\circ\gamma)\ .\end{aligned}$$

Esta aplicación es un morfismo de grupos, y $\ker(\theta)$ contiene a $\widetilde{\Gamma}(N) := \{\pm\}\Gamma(N)$. Notemos, por otra parte, que dos funciones $f_0^{\overline{u}}$ y $f_0^{\overline{v}}$ son iguales, si, y sólo si $\overline{u} = \pm\overline{v}$, pues $\wp_\tau(z) = \wp_\tau(z')$, si, y sólo si $z + \Lambda_\tau = \pm z' + \Lambda_\tau$. Además, $(f_0^{\overline{v}})^{\theta(\gamma)} = f_0^{\overline{v}}\circ\gamma = f_0^{\overline{v\gamma}}$, con lo que, como $f_0^{\overline{v}} \in \mathbb{C}(X'(N))$, el núcleo $\ker(\theta)$ está contenido en $\widetilde{\Gamma}(N)$.

Ahora, $\theta(\mathrm{SL}_2(\mathbb{Z}))$ es un subgrupo del grupo de automorfismos del cuerpo $\mathbb{C}(X'(N))$, y su cuerpo fijo es $\mathbb{C}(X(1)) = \mathbb{C}(j)$. En definitiva, la extensión $\mathbb{C}(X'(N))/\mathbb{C}(X(1))$ es galoisiana con grupo de Galois

$$\theta(\mathrm{SL}_2(\mathbb{Z})) \,\simeq\, \mathrm{SL}_2(\mathbb{Z})/\widetilde{\Gamma}(N) \,\simeq\, \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}\ .$$

El mismo argumento que los únicos elementos de $\mathrm{SL}_2(\mathbb{Z})$ que actúan trivialmente sobre $\mathbb{C}(j, \{f_0^{\pm\overline{v}} \,:\, \pm\overline{v} \in ((\mathbb{Z}/N\mathbb{Z})^2 \smallsetminus \{\overline{(0,0)}\})/\{\pm 1\}\})$ son los pertenecientes a $\widetilde{\Gamma}(N)$. Lo mismo es cierto para el cuerpo $\mathbb{C}(j, f_0^{\pm\overline{(0,1)}}, f_0^{\pm\overline{(1,0)}})$, que coincide, entonces, con $\mathbb{C}(X'(N))$.

El siguiente paso consiste en demostrar que la extensión $\mathbb{Q}(\mu_N, j, \{f_0^{\pm\overline{v}}\})/\mathbb{Q}(j)$ también es Galois y que su grupo se identifica con $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. Si σ es un elemento del grupo de Galois de esta extensión, entonces

$$\begin{bmatrix} (f_0^{\pm(1,0)})^\sigma \\ (f_0^{\pm(0,1)})^\sigma \end{bmatrix} \,=\, \rho(\sigma) \begin{bmatrix} f_0^{\pm(1,0)} \\ f_0^{\pm(0,1)} \end{bmatrix}$$

para alguna transformación lineal $\rho(\sigma) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Si $\mu = e_N(P,Q)$ es una raíz N-ésima primitiva de la unidad,

$$\begin{aligned}\mu^\sigma \,&=\, \sigma(e_N(P,Q)) \,=\, e_N(P^\sigma, Q^\sigma)\\ &=\, e_N(P,Q)^{\det(\rho(\sigma))} \,=\, \mu^{\det(\rho(\sigma))}\ .\end{aligned}$$

Finalmente, si $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ es un subgrupo que satisface $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$, definimos los cuerpos

$$\begin{aligned}K_1 \,&=\, \mathbb{Q}(\mu_N, j, \{f_0^{\pm\overline{v}}\})^{\Gamma_H}\\ K_2 \,&=\, \mathbb{C}(j, \{f_0^{\pm\overline{v}}\})^{H'/\{\pm 1\}}\ .\end{aligned}$$

Un poco de Teoría de Galois muestra que $K_1 = \mathbb{Q}(j, \{f_0^{\pm\overline{v}}\})^{H'/\{\pm 1\}}$ y que $K_1 \cap \overline{\mathbb{Q}} = \mathbb{Q}$, correspondiéndose con una curva poryectiva, no singular, y esta curva está definida sobre $\mathbb{Q}$. Con respecto a K_2, este cuerpo tiene que ser el cuerpo de funciones del cociente $H'\backslash X'(N)$, ya que, para $f \in \mathbb{C}(X'(N))$, $f^{\theta(\gamma)} = f\circ\gamma$. Ahora bien, el cuerpo de funciones de la curva definida sobre los números complejos que se obtiene a partir de las ecuaciones que definen la curva correspondiente al cuerpo funcional K_1, coincide con K_2. Es decir, $H\backslash X(N)$ es isomorfa sobre $\mathbb{C}$ a una curva definida sobre $\mathbb{Q}$. Usaremos la misma notación para referirnos tanto a $H\backslash X(N)$ como a su modelo sobre $\mathbb{Q}$.

□

2.1 Subgrupos de Cartan

Sea E una curva elíptica con CM. Su anillo de endomorfismos es un orden $I = [1, \tau]$ en un cuerpo cuadrático imaginario. Si $N > 1$ es un entero coprimo con el discriminante de I y $p \in \mathbb{Z}$ es un primo divisor de N, entonces p se parte o es inerte en I. Sea $A := I/NI$. Este anillo es una $(\mathbb{Z}/N\mathbb{Z})$-álgebra con base $\{1, \tau\}$, y, dependiendo de p, si se parte o no en I, el cociente A/pA es isomorfo a $\mathbb{F}_p \times \mathbb{F}_p$ o a $\mathbb{F}_{p^2}$, respectivamente.

Definición. Dada A un álgeba sobre $\mathbb{Z}/N\mathbb{Z}$, libre, conmutativa, de rango 2 y tal que, si $p|N$, entonces A/pA es isomorfo a $\mathbb{F}_p \times \mathbb{F}_p$ o a $\mathbb{F}_{p^2}$, el grupo de unidades, $A^\times$, actúa sobre A por multiplicación. Elegir una base de A sobre $\mathbb{Z}/N\mathbb{Z}$, equivale a establecer un morfismo

$$\iota \,:\, A^\times \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

–elegir otra base resulta en un subgrupo conjugado a $\iota(A^\times)$. Decimos que un subgrupo de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ es *de Cartan*, si es de la forma $\iota(A^\times)$ para algún álgebra A que cumpla con las condiciones especificadas. Con respecto a la última de estas condiciones, también se dice que A es *étale*. Si $A/pA \simeq \mathbb{F}_{p^2}$, se dice que A es *non-split* en p, y *split* en el otro caso. Un subgrupo de Cartan se dice *non-split*, si el álgebra correspondiente lo es en todo primo que divide a N.

Ejemplo. Si I es un orden en un cuerpo cuadrático imaginario, $A = I/NI$ y N es coprimo con $\mathrm{disc}(I)$ y todo divisor primo de N es inerte en I, entonces si A es *non-split* y, fijando una base, $\iota(A^\times) \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ es un subgrupo de Cartan *non-split*. Denotamos con $C_{ns}(N)$ al subgrupo $\iota(A^\times)$.

Si $N = p$ es primo, $|A^\times| = |\mathbb{F}_{p^2}^\times| = p^2 - 1$. Si $N = p^r$, $r \geq 1$, todo elemento de $(I/pI)^\times$ se levanta a una unidad en I/p^rI, y cada elemento tiene $p^{2(r-1)}$ preimágenes; entonces

$$|(I/p^rI)^\times| \,=\, p^{2(r-1)}(p^2 - 1)\ .$$

Para $N > 1$ entero coprimo con $\mathrm{disc}(I)$, el orden $|A^\times|$ es igual a

$$|(I/NI)^\times| = N^2 \prod_{p|N} (1 - (1/p^2))\ .$$

Este es el orden del grupo de Cartan *non-split* $C_{ns}(N)$.

2.2 El normalizador de $C_{ns}(N)$ en $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ y la curva modular asociada

En la descripción que hacemos a continuación tomamos como referencia a [2]. Sean $I = [1, \tau]$ un orden en un cuerpo cuadrático imaginario K tal que $(N, \mathrm{disc}(I)) = 1$ y todo primo que divide a N es inerte en I, y sea $A = I/NI$. Sea $C_{ns}(N) = \iota(A^\times)$. Si τ satisface el polinomio $X^2 - uX + v \in \mathbb{Z}[X]$, definimos una involución en τ por $\bar{\cdot} : \tau \mapsto (u - \tau)$, y también $\sigma_p : A \to A$ como el único automorfismo en $A = I/NI$ que coincide con esta

involución en $I/p^{r(p)}I$ y con la identidad en $I/\frac{N}{p^{r(p)}}I$, donde $r(p)$ es la máxima potencia de p que divide a N. La misma elección de base que determina la inclusión ι determina una matriz $S_p \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ que representa a σ_p.

Sea $N = p^r$, $p \in \mathbb{Z}$ un primo y $r \geq 1$. Podemos identificar $C_{ns}(N)$ con el grupo $A^\times$ de unidades de $A = I/p^rI$. Si α es un elemento de A, tiene una matriz asociada, en $\mathrm{M}_{2\times 2}(\mathbb{Z})$: $\gamma(\alpha) := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, determinada por

$$\alpha \cdot \begin{bmatrix} 1 \\ \tau \end{bmatrix} = \begin{bmatrix} \alpha \\ \alpha\tau \end{bmatrix} = \begin{bmatrix} a+b\tau \\ c+d\tau \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ \tau \end{bmatrix} .$$

Si $\tau^2 - u\tau + v = 0$, con u y v en $\mathbb{Z}$, la matriz de τ es $\gamma(\tau) := \left[\begin{smallmatrix} 0 & 1 \\ -v & u \end{smallmatrix}\right]$. Como A es *non-split*, $A/pA \simeq \mathbb{F}_{p^2}$. Pero $\tau \notin pA$, con lo que τ es una unidad en I/pI, es decir que la matriz $\gamma(\tau)$ es una unidad en $\mathrm{M}_{2\times 2}(\mathbb{Z}/p\mathbb{Z})$. Entonces, $v = \det(\gamma(\tau))$ es una unidad en $\mathbb{Z}/p\mathbb{Z}$. En particular, p no divide a v, y $\det(\gamma(\tau)) \in (\mathbb{Z}/p^r\mathbb{Z})^\times$. En otras palabras, τ es una unidad en A.

Si ahora tomamos $\kappa \in \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$ tal que $\kappa C_{ns}(p^r) = C_{ns}(p^r)\kappa$, κ induce un automorfismo de $A^\times$ por conugación: si $\alpha \in A^\times$, definimos $t_\kappa(\alpha)$ como la primera coordenada de

$$\kappa\gamma(\alpha)\kappa^{-1} \cdot \begin{bmatrix} 1 \\ \tau \end{bmatrix} .$$

Si $n \in \mathbb{Z}$ es coprimo con p, $n \cdot 1_A \in A^\times$ y $\gamma(n1_A)$ es la matriz diagonal $\left[\begin{smallmatrix} n & 0 \\ 0 & n \end{smallmatrix}\right]$. Así, $t_\kappa(n1_A) = n1_A$. Extendemos t_κ a un endomorfismo de la $(\mathbb{Z}/p^r\mathbb{Z})$-álgebra A. En particular, $t_\kappa(\tau) \in A$ tiene que ser un cero de $f = X^2 - uX + v$. Las soluciones τ y $u - \tau$ de f son distintas en $I/pI \simeq \mathbb{F}_{p^2}$ y $f'(\tau) = \tau - (u - \tau) \neq 0$, entonces, si $\alpha \in I$ es solución de f *modulo* $p^{r'}I$ para algún r', por el argumento del lema de Hensel, se levanta a única solución *modulo* $p^{r'+1}I$. Entonces $t_\kappa(\tau) = \tau$ o $u - \tau$, con lo que el automorfismo t_κ de A es, o bien, σ_p, o bien la identidad. En términos de matrices, o bien $\kappa z \kappa^{-1} = z$, o bien $\kappa z \kappa^{-1} = S_p z S_p$ (S_p tiene orden 2). O bien κ, o bien $S_p\kappa$, pertenece al centralizador de $C_{ns}(p^r)$. Pero el centralizador de $C_{ns}(p^r)$ es el mismo grupo. Así κ pertenece a $C_{ns}(p^r)$, o a $S_pC_{ns}(p^r)$, es decir que el normalizador de $C_{ns}(p^r)$ es el subgrupo de $\mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$ generado por $C_{ns}(p^r)$ y por S_p. En general, para $N > 1$, el normalizador de $C_{ns}(N)$ es $\langle C_{ns}(N), \{S_p : p|N\}\rangle$. Lo denotamos $C^+_{ns}(N)$. Su orden es

$$N^2 2^\omega \prod_{p|N} \left(1 - \frac{1}{p^2}\right) = |A^\times| 2^\omega ,$$

donde ω es la cantidad de primos distintos que dividen a N.

Los grupos $C_{ns}(N)$ y $C^+_{ns}(N)$ son subgrupos de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, y, como tales, podemos asociarles las curvas modulares

$$\begin{aligned} X_{ns}(N) &:= C_{ns}(N)\backslash X(N) \\ X^+_{ns}(N) &:= C^+_{ns}(N)\backslash X(N) . \end{aligned}$$

Llamamos $Y_{ns}(N)$ e $Y_{ns}^+(N)$ a los abiertos que son complementos de las cúspides de $X_{ns}(N)$ y $X_{ns}^+(N)$, respectivamente.

La curva $X_{ns}^+(N)$ está definida sobre $\mathbb{Q}$: $\det(C_{ns}^+(N)) = (\mathbb{Z}/N\mathbb{Z})^\times$ [4], el argumento es el siguiente: sean $m \in \mathbb{Z}$ coprimo con N, y $p|N$ un primo. Como p se supone inerte en K (el cuerpo cuadrático que contiene al orden $I = [1, \tau]$), $K_p/\mathbb{Q}_p$ es una extensión cuadrática de cuerpos locales. Existe, entonces, $\mu_p \in K_p^\times$ íntegro tal que

$$\mathrm{Nm}_{K_p/\mathbb{Q}_p}(\mu_p) \,=\, \pm m \ .$$

Si $p^{r(p)}||N$, elegimos $\widetilde{\mu}_p \in I$ que aproxime μ_p a orden $p^{r(p)}$:

$$\mu_p \,\equiv\, \widetilde{\mu}_p \, (p^{r(p)}) \ .$$

Así, $\mathrm{Nm}_{K_p/\mathbb{Q}_p}(\widetilde{\mu}_p)$ es congruente con $\pm m \, (p^{r(p)})$. Haciendo esto para cada primo que divide a N, se toma $\mu \in I$ que satisfaga $\mu \equiv \widetilde{\mu}_p$ *modulo* $p^{r(p)}$ para cada p. De esta manera, $\mathrm{Nm}_{K/\mathbb{Q}}(\mu) \equiv \pm m \, (p^{r(p)})$ para cada primo. Corrigiendo con las matrices S_p (cuyo determinante es -1 en el factor correspondiente a p, y 1 en el resto), vemos que $\det : C_{ns}^+(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ es sobreyectiva.

Observación. Hemos demostrado, también, que

$$\det \,:\, C_{ns}(p^r) \to (\mathbb{Z}/p^r\mathbb{Z})^\times/\{\pm 1\}$$

es sobre.

Sean $C_{ns}^+(N)' = C_{ns}^+(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ y $\Gamma_{C_{ns}^+(N)}$ el subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ conformado por las matrices que caen en $C_{ns}^+(N)'$ al reducir las coordenadas *modulo* N. Como $\det : C_{ns}^+(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ es sobreyectiva y su núcleo es $C_{ns}^+(N)'$, el índice $|C_{ns}^+(N) : C_{ns}^+(N)'|$ es igual a $\phi(N)$, con lo cual,

$$\begin{aligned} |\mathrm{SL}_2(\mathbb{Z}) : \Gamma_{C_{ns}^+(N)}| \,&=\, |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : C_{ns}^+(N)'| \\ &=\, \frac{\phi(N)}{2^\omega N^2 \prod_{p|N}(1-(1/p^2))} N^3 \prod_{p|N}(1-(1/p^2)) \,=\, \frac{N\phi(N)}{2^\omega} \ . \end{aligned}$$

Tenemos morfismos

$$X_{ns}(N) \xrightarrow{\Phi_1} X_{ns}^+(N) \xrightarrow{\Phi_2} X(1) \ ,$$

de grados $\deg(\Phi_1) = 2^\omega$ y $\deg(\Phi_2) = N\phi(N)/2^\omega$.

En resumen, existe una curva modular, $X_{ns}^+(N)$, isomorfa a $\Gamma_{C_{ns}^+(N)}\backslash\mathfrak{h}^*$, y definida sobre $\mathbb{Q}$. El abierto $Y_{ns}^+(N) = X_{ns}^+(N) \smallsetminus \{$ cúspides $\}$ parametriza clases de equivalencia de pares (E, φ), donde $E/\mathbb{C}$ es una curva elíptica y $\varphi : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ un isomorfismo; dos pares (E, φ) y (E', φ') son equivalentes, si existe $\gamma \in C_{ns}^+(N)$ tal que los puntos $[E, \varphi]$ y $[E', \gamma \circ \varphi']$ sean iguales en $X(N)$. Olvidando la estructura de nivel, φ en cada par (E, φ), resulta un morfismo de $X_{ns}^+(N)$ en $X(1)$ de grado $N\phi(N)/2^\omega$.

2.3 Puntos racionales e íntegros

En tanto $X_{ns}^+(N)$ tiene un modelo sobre $\mathbb{Q}$, podemos referirnos a sus puntos racionales y a sus puntos enteros. Para $N = 5$ o $N \geq 7$, los puntos $\mathbb{Q}$-racionales de $X_{ns}^+(N)$ pertenecen a $Y_{ns}^+(N)$, es decir, no están entre las cúspides [2]. Recordemos que existe un morfismo $X(N) \to X_{ns}^+(N)$ que nos permite ver $X_{ns}^+(N)$ como un cociente de $X(N)$ y sus cúspides como órbitas por la acción de $C_{ns}^+(N)$ sobre las cúspides de $X(N)$. Si $[E, \varphi] \in Y(N)(\overline{\mathbb{Q}})$ y $\sigma \in \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$[E, \varphi]^\sigma \ = \ [E^\sigma, \varphi \circ \sigma]$$

determina una acción del grupo de Galois absoluto sobre los puntos $\overline{\mathbb{Q}}$-racionales en el abierto $Y(N)$. Además, si E es una curva elíptica definida sobre $\mathbb{Q}$, $\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ actúa sobre $E[N]$, dando lugar a una representación

$$\rho_N \ : \ \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[N]) \ \simeq \ \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \ ,$$

donde $\mathrm{Aut}(E[N])$ se identifica con $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ vía el isomorfismo φ en el par $[E, \varphi]$.

Sea $[E, \varphi] \in Y(N)(\overline{\mathbb{Q}})$ y $\overline{[E, \varphi]}$ su imagen en $Y_{ns}^+(N)(\overline{\mathbb{Q}})$. Este punto es la órbita de $[E, \varphi]$ por $C_{ns}^+(N)$:

$$\overline{[E, \varphi]} \ = \ \big\{ [E, \gamma \circ \varphi] \ : \ \gamma \in C_{ns}^+(N) \big\} \ .$$

Y esta órbita define un punto $\mathbb{Q}$-racional en $Y_{ns}^+(N)$, si, y sólo si es estable por la acción de Galois: si para σ en $\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ existe γ_σ en $C_{ns}^+(N)$ tal que $[E^\sigma, \varphi \circ \sigma] = [E, \gamma_\sigma \circ \varphi]$. Para E definida sobre $\mathbb{Q}$, esto equivale a que la imagen de Galois por la representación ρ_N esté contenida en el normalizador de un subgrupo de Cartan *non-split*.

Sea I un orden en un cuerpo cuadrático imaginario K, sea $\mathsf{Cl}(I)$ su grupo de clases y sea $h(I) = \#\mathsf{Cl}(I)$. Sea $\mathrm{CM}(I)$ el conjunto de curvas elípticas definidas sobre $\mathbb{C}$ con anillo de endomorfismos I, salvo $\mathbb{C}$-isomorfismo, y sea $\psi : \mathsf{Cl}(I) \to \mathrm{CM}(I)$ la biyección dada por $M \mapsto \mathbb{C}/M$ sobre un I-ideal M en K [6]. Si $h(I) = 1$, hay una única curva elíptica con CM por I, salvo isomorfismo, y, en consecuencia, el orden I determina un punto $j(I) = j(E) \in X(1)$, donde E es cualquier representante de $\mathrm{CM}(I)$. Dado que $j(E^\sigma) = j(E)^\sigma$ para $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, y que E^σ también es CM con anillo de endomorfismos I, $j(E)^\sigma = j(E)$, y $j(E)$ queda fijo por $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. Al ser racional, pertenece a $\mathbb{Z}$ (el j-invariante de una curva elíptica con multiplicación compleja es un entero algebraico).

Sea K un cuerpo cuadrático imaginario con número de clases 1, y sea $\mathcal{O}_K$ su anillo de enteros. Fijemos E una curva elíptica definida sobre $\mathbb{Q}$, con CM por $\mathcal{O}_K$ y con j-invariante $j(E) = j(\mathcal{O}_K) \in \mathbb{Z}$. Fijamos, también, un entero $N \geq 1$ coprimo con el discriminante de $\mathcal{O}_K$, y un isomorfismo $\varphi : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$. Sea ρ_N la representación de $\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ en $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ correspondiente a φ, es decir, identificando $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ con $\mathrm{Aut}(E[N])$ vía φ. Por restricción, contamos con un morfismo de anillos $f : \mathrm{End}(E) = \mathcal{O}_K \to \mathrm{End}(E[N])$ que se factoriza por $N\mathcal{O}_K$,

$$f' \ : \ A \ = \ \mathcal{O}_K/N\mathcal{O}_K \to \mathrm{End}(E[N]) \ .$$

Vía f' y φ, obtenemos el grupo de Cartan *non-split* $f'(A^\times) \subset \mathrm{Aut}(E[N]) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Llamemos $C_{ns}(N)$, G y C a los subgrupos de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ $f'(A^\times)$, $\rho_N(\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ y $\rho_N(\mathsf{Gal}(\overline{\mathbb{Q}}/K)$, respectivamente. Si $\tau \in \mathcal{O}_K$, $\sigma \in \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ y $w \in E[N]$, o bien $\tau = \tau^\sigma$, o bien $\tau \neq \tau^\sigma$. En el primer caso, $\tau \cdot w^\sigma = (\tau w)^\sigma$ y $\rho_N(\sigma)$ conmuta con $f'(\tau)$. En el segundo, $(\tau w^\sigma)^{\sigma-1} = \tau^{\sigma^{-1}} w$ y, como $\tau^{\sigma^{-1}}$ pertenece a $\mathcal{O}_K$ (la extensión $K/\mathbb{Q}$ es normal), $\rho_N(\sigma)$ pertenece al normalizador de $f'(A^\times)$. En definitiva, $C \subset C_{ns}(N)$ y $G \subset C^+_{ns}(N)$.

Proposición 2.2. *Sea K un cuerpo cuadrático imaginario y sea $N \geq 1$ un entero tal que todo primo $p|N$ es inerte en K. Si el número de clases de K es igual a 1, cualquier curva elíptica con CM por K da lugar a un punto $\overline{[E,\varphi]} \in Y^+_{ns}(N)(\overline{\mathbb{Q}})$, donde E está definida sobre $\mathbb{Q}$ y la imagen de la representación de Galois asociada, ρ_N, está contenida en $C^+_{ns}(N)$. En particular, $\overline{[E,\varphi]}$ es un punto $\mathbb{Q}$-racional y $j(E)$ es íntegro.*

De un punto $\overline{[E,\varphi]}$ en $Y^+_{ns}(N)(\overline{\mathbb{Q}})$ tal que $\rho_N(\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subset C^+_{ns}(N)$ y E definida sobre $\mathbb{Q}$ (equivalentemente, $\mathbb{Q}$-racional), y tal que $j(E) \in \mathbb{Z}$, se dice que es un punto íntegro de $Y^+_{ns}(N)$ [13].

2.4 Parametrizaciones

Dado un cuerpo cuadrático imaginario K y $N \geq 1$ entero tal que sus divisores primos sean inertes en K, se obtiene, a partir de una curva elíptica definida sobre $\mathbb{Q}$ con CM por el orden $\mathcal{O}_K$, un único punto íntegro en $Y^+_{ns}(N)$. El método para resolver el problema del número de clases 1 usando las curvas modulares correspondientes a grupos de Cartan *non-split* consiste en hallar los puntos enteros de $X^+_{ns}(N)$. Para conseguir este objetivo es crucial elegir las curvas de manera adecuada: de forma que el género y número de cúpides sean suficientemente pequeños para poder hallar una parametrización de $X^+_{ns}(N)$ y suficientemente grandes para permitir sólo una cantidad finita de puntos enteros.

Sea X una curva proyectiva, no singular, definida sobre $\mathbb{Q}$ y de género 0. Para fijar ideas, y porque este es el caso que nos interesará, sea X una de las curvas $X^+_{ns}(N)$ (si bien no todas ellas tienen género 0). Si X tiene, al menos, un punto $\mathbb{Q}$-racional, existe un isomorfismo definido sobre $\mathbb{Q}$

$$t : X \to \mathbb{P}^1 ,$$

único salvo $\mathbb{Q}$-automorfismo.

Sean $\widetilde{X}$ y X dos curvas proyectivas, no singulares, definidas sobre $\mathbb{Q}$ y cada una con, al menos, un punto $\mathbb{Q}$-racional. Asumamos que existe un morfismo $\pi : X \to \widetilde{X}$ definido sobre $\mathbb{Q}$ tal que $\pi(X) = \widetilde{X}$ (por ejemplo este morfismo podría ser la proyección $X^+_{ns}(N) \to X(1)$). Existe un diagrama

$$\begin{array}{ccc} X & \xrightarrow{u} & \mathbb{P}^1 \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \phi_\pi} \\ \widetilde{X} & \xrightarrow{j} & \mathbb{P}^1 \end{array} .$$

Ya sea describiendo el morfismo ϕ_π en coordenadas afines, o identificando los cuerpos de funciones de las curvas con $\mathbb{Q}(u)$ y con $\mathbb{Q}(j)$, obtenemos polinomios mónicos P, Q con coeficientes en el cuerpo $\mathbb{Q}$ y una constante λ, también racional, tales que,

$$\pi^* j \,=\, \lambda \frac{P(u)}{Q(u)}\,,$$

donde $\pi^* j$ es el *pullback* de j por π. Por *parametrización* de una curva X como arriba, nos referiremos a una elección de morfismos u, j, junto con su correspondiente relación en términos de P, Q y λ. Los morfismos como u y j reciben el nombre de *uniformizadores*.

Cambiemos, por un momento, el cuerpo de base, $\mathbb{Q}$, por $\mathbb{C}$. Podemos repetir el mismo argumento de arriba para obtener, una vez elegidos los uniformizadores (ahora definidos sobre los complejos), una relación $\pi^* j = \lambda P(u)/Q(u)$ (sobre $\mathbb{C}$). Supongamos, ahora, que $X = X_{ns}^+(N)$ (o la compactificación de cualquier cociente de $\mathfrak{h}$ por un subgrupo de congruencia) y que $\widetilde{X} = X(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{h}^*$. La función j, el j-invariante, es un ejemplo de uniformizador para la curva modular $X(1)$. Pero, además, en esta situación, un uniformizador se identifica con una función definida en $\mathfrak{h}$, meromorfa en $\mathfrak{h}$, invariante por cierto subgrupo de congruencia y meromorfa en las cúspides. Así, la función $\pi^* j$ no es más que la misma función j, pero considerada, no como una función modular para $\mathrm{SL}_2(\mathbb{Z})$, sino considerada como función modular para un subgrupo de congruencia.

Sean $X = X_{ns}^+(N)$ para cierto $N \geq 1$ entero, y $\widetilde{X} = X(1)$. Asumimos que el conjunto de puntos $\mathbb{Q}$-racionales $X(\mathbb{Q})$ es no vacío. Elegimos el j-invariante como uniformizador para $X(1)$. Este uniformizador está definido sobre $\mathbb{Q}$. Es decir, los puntos $\rho = e^{2\pi i/3}$, $i = \sqrt{-1}$, ∞ de $X(1)$ son $\mathbb{Q}$-racionales, y el j-invariante –que, a cada clase de isomorfismo de curvas elípticas le asigna el correspondiente invariante– coincide con el uniformizador que, a estos tres puntos, asigna los valores 0, 1728, ∞, respectivamente (y éste es un uniformizador para $X(1)$ en tanto curva definida sobre $\mathbb{Q}$). De manera análoga, podemos elegir un uniformizador para X definido sobre $\mathbb{Q}$, y, así, la relación entre u y j es $j = \lambda P(u)/Q(u)$, donde $P, Q \in \mathbb{Q}[T]$ y $\lambda \in \mathbb{Q}$. Ahora bien, sobre $\mathbb{C}$, j, pensada como función en X, tiene que cumplir con lo siguiente: todo cero es un punto en la preimagen de ρ, el único cero de $j \in \mathbb{C}(X(1))$, y todo polo es un punto arriba de ∞, el único polo de j en $X(1)$. Es decir, la relación entre los uniformizadores es

$$j \,=\, \lambda \frac{\prod_{z|\rho} (u \,-\, u(z))^{e_z}}{\prod_{z|\infty} (u \,-\, u(z))^{e_z}}\,,$$

donde, si $\pi : X \to X(1)$ es la proyección dada por olvidar la estructura de nivel, $z|a$ indica que z pertenece a $\pi^{-1}(a)$ y e_z denota el índice de ramificación de π en z. [5]

2.5 Ramificación

Para poder sacar provecho de las curvas X_H será útil obtener una parametrización de las mismas. Para conseguirlo es necesario considerar los morfismos $X_H \to X(1)$, y la información relativa a la ramificación del cubrimiento, en tanto superficies de Riemann. Para los normalizadores de subgrupos de Cartan *non-split* de nivel N, sabemos que el grado del morfismo es $N\phi(N)/2^\omega$, donde ω es la cantidad de primos distintos que dividen a N. Excepto sobre los puntos elípticos y las cúspides de $X(1)$, la fibra contiene dicha cantidad de puntos. En general, la suma de los índices de ramificación en cada una de las preimágenes de un punto es igual al grado del morfismo.

Sea Γ un subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ que contiene la matriz -1. Sea π la proyección $\Gamma\backslash\mathfrak{h}^* \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{h}^*$. Si $z \in \mathfrak{h}^*$, denotamos con Γ_z su estabilizador en Γ. Si z es un punto elíptico para Γ, es decir, si Γ_z contiene propiamente a $\{\pm 1\}$, entonces Γ_z es un grupo cíclico finito (proposición 2.2.2 de [8]). Si a pertenece a $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{h}^*$, si $z \in \mathfrak{h}^*$ es un punto arriba a y $b \in \Gamma\backslash\mathfrak{h}^*$ es tal que $\pi(b) = a$, entonces el índice de ramificación e_b de π en b es igual al índice $|\mathrm{SL}_2(\mathbb{Z})_z : \Gamma_w|$, donde $w \in \mathfrak{h}^*$ es un punto arriba de b. Si, además, $w = \sigma z$ para algún elemento σ en $\mathrm{SL}_2(\mathbb{Z})$, entonces e_b también es igual a $|\mathrm{SL}_2(\mathbb{Z})_z : \sigma^{-1}\Gamma\sigma \cap \Gamma_z|$.

El estabilizador de un punto elíptico para $\mathrm{SL}_2(\mathbb{Z})$ es de orden 4 o 6 (el orden del punto es, respectivamente, 2 o 3). *Modulo* $\mathrm{SL}_2(\mathbb{Z})$, el único punto elíptico de orden 2 es i, y el único de orden 3 es ρ. Si $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ y $\{\gamma_j\}_j$ es un conjunto (finito) de representantes de las coclases de Γ en $\mathrm{SL}_2(\mathbb{Z})$, entonces un punto elíptico para Γ tiene que ser de la forma $\Gamma\gamma_j \cdot i$ o $\Gamma\gamma_j \cdot \rho$ para algún j. En definitiva, e_b es igual a 2 o a 1, si z es elíptico de orden 2, o bien igual a 3 o a 1, si z es elíptico de orden 3. Además, si b es un punto elíptico de $\Gamma\backslash\mathfrak{h}^*$ (si w es un punto elíptico para Γ), $\Gamma_w \neq \{\pm 1\}$ implica $e_b = 1$, es decir, si el orden del punto elíptico es mayor a 1, entonces el índice de ramificación tiene que ser 1.

Describiremos, ahora, un sistema de representantes de las coclases de Γ en $\mathrm{SL}_2(\mathbb{Z})$ para grupos Γ particulares. Sea $H = C_{ns}(N)$ o $H = C_{ns}^+(N)$ un grupo de Cartan *non-split* de nivel N, o el normalizador de un grupo tal. Sea $H' = H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ y sea Γ_H el subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ de matrices pertenecientes a H' al reducir coordenadas *modulo* N. Esta reducción establece, además, una biyección entre las coclases de Γ_H en $\mathrm{SL}_2(\mathbb{Z})$ y las de H' en $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Sea I el orden en un cuerpo cuadrático imaginario con $\mathbb{Z}$-base $\{1, \tau\}$, donde τ es raíz de un polinomio de la forma $X^2 - uX + v$, $u, v \in \mathbb{Z}$. Sea $A = I/NI$. Definimos una involución en A por $1 \mapsto 1$ y $\tau \mapsto u - \tau$, y denotamos por $\overline{y}$ el conjugado de un elemento $y \in A$. Definimos la *norma* de un elemento y en A como $\nu(y) := y\overline{y}$.

Supongamos que $N = p^r$. El subgrupo $\nu(A^\times)$ puede no ser todo $(\mathbb{Z}/p^r\mathbb{Z})^\times$, pero, para una unidad, a, en $\mathbb{Z}/p^r\mathbb{Z}$, existe $y_a \in A^\times$ tal que $\nu(y_a) = \pm a$ (c.f. la demostración de que $\det : C_{ns}^+(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ es sobreyectivo). Para cada $\pm a \in (\mathbb{Z}/p^r\mathbb{Z})^\times/\{\pm 1\}$, elegimos $y_{\pm a}$ de norma a o $-a$, y definimos

$$\mathcal{Y} := \left\{ y_{\pm a} \,:\, \pm a \in (\mathbb{Z}/p^r\mathbb{Z})^\times/\{\pm 1\} \right\} .$$

Lema 2.3. *Sean $x \in \mathbb{Z}/p^r\mathbb{Z}$ e $y \in \mathcal{Y}$. Sea $\gamma_{x,y}$ la matriz que representa la transformación lineal determinada por $1 \mapsto y^{-1}$ y $\tau \mapsto \overline{y}(\tau + x)$. Entonces las matrices $\gamma_{x,y}$ constituyen un sistema de representantes de las coclases de $C_{ns}^+(p^r)' = C_{ns}^+(p^r) \cap \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$.*

Demostración. Ya hemos visto que el índice de $C_{ns}^+(p^r)'$ en $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ es igual al de $C_{ns}^+(p^r)$ en $\mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$, y que éste es igual a $p^r\phi(p^r)/2$. Por otra parte, si llamamos M_y al morfismo dado por multiplicación por un elemento $y \in A^\times$, los elementos de $C_{ns}^+(p^r)$ son de la forma M_y para y de norma 1, o $\sigma_p \circ M_y$ –σ_p es, esencialmente, conjugación compleja (N, en este caso, es divisible por un único primo)– para y de norma -1. Ahora, si $\gamma_{x,y}$ y $\gamma_{x',y'}$ son dos elementos de aquellos considerados en el enunciado, y si los mismos pertenecen a la misma coclase de $C_{ns}^+(p^r)'$ en $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$, entonces existe z tal que

$$\begin{aligned} \nu(z) = 1 \text{ y } \gamma_{x,y} &= M_z\gamma_{x',y'} \text{ , o} \\ \nu(z) = -1 \text{ y } \gamma_{x,y} &= \sigma_p M_z \gamma_{x',y'} . \end{aligned}$$

Evaluando en $1 \in A$, se deduce que $\nu(y) = \pm\nu(y')$ y que $y = y'$ por la definición del conjunto $\mathcal{Y}$. Evaluando en τ, deducimos que x y x' han de ser iguales en $\mathbb{Z}/p^r\mathbb{Z}$. Los pares (x, y) dan lugar a representantes de coclases distintas, pero, por cardinalidad, las coclases representadas han de ser todas. □

El género g de una curva como $X_{ns}(N)$ o $X_{ns}^+(N)$, al igual que el género de cualquier curva asociada a un subgrupo de congruencia, está dado por

$$g = 1 + \frac{\mu}{12} - \frac{\mu_2}{4} - \frac{\mu_3}{3} - \frac{\mu_\infty}{2} .$$

El entero μ es el índice del grupo en $\mathrm{SL}_2(\mathbb{Z})$, los números μ_k denotan la cantidad de puntos elípticos de orden k en la curva y μ_∞ denota la cantidad de cúspides. Las cantidades μ_2, μ_3 y μ_∞ son multiplicativas en N para las curvas $X_{ns}(N)$ y $X_{ns}^+(N)$, por lo que es suficiente considerar niveles $N = p^r$.

Lo demostrado hasta ahora es suficiente para calcular la cantidad de cúspides en $X_{ns}^+(p^r)$: el estabilizador de ∞ en $\mathrm{SL}_2(\mathbb{Z})$ está generado por la matriz $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. Si $a \in \mathbb{Z}$ es tal que

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in \gamma C_{ns}^+(p^r)\gamma^{-1}$$

donde γ es alguno de los representantes del lema anterior, existe $\zeta \in C_{ns}^+(p^r)$ tal que, en tanto endomorfismos de A, $\gamma^{-1}\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] = \zeta\gamma^{-1}$. Evaluando en la $(\mathbb{Z}/p^r\mathbb{Z})$-base de A, se deduce que a tiene que ser divisible por p^r. En particular, el índice de ramificación de cualquier cúspide de $X_{ns}^+(p^r)$ es igual a p^r. Como el grado de $X_{ns}^+(p^r) \to X(1)$ es $p^r\phi(p^r)/2$, la curva asociada al normalizador de un subgrupo de Cartan *non-split* de $\mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$ tiene, precisamente, $\phi(p^r)/2$ cúspides.

En [2] se encuentran resultados más completos. Por ejemplo, para terminar la descripción de $X_{ns}^+(p^r)$ $(p \neq 2)$, la cantidad de puntos elípticos de orden 3 es

$$\mu_3 = \begin{cases} 1 & \text{si } p \equiv 2 \pmod 3, \\ 0 & \text{si no.} \end{cases}$$

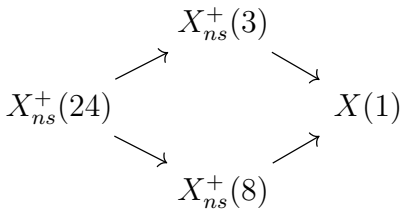
La cantidad de puntos elípticos de orden 2 es

$$\mu_2 = \begin{cases} \frac{1}{2}p^r\left(1 - \frac{1}{p}\right) & \text{si } p \equiv 1 \pmod 4 , \\ 1 + \frac{1}{2}p^r\left(1 + \frac{1}{p}\right) & \text{si } p \equiv 3 \pmod 4 , \\ 2^{r-1} & \text{si } p = 2 . \end{cases}$$

3 Soluciones al problema del número de clases igual a 1

3.1 Nivel 24

Sea $N = 24$. La referencia para la solución al problema del número de clases 1 usando la curva de nivel 24 es la [4] (sección 9). Para poder encontrar los puntos enteros de $X_{ns}^+(24)$, nos concentraremos en las curvas $X_{ns}^+(3)$ y $X_{ns}^+(8)$. Existen morfismos naturales definidos sobre $\mathbb{Q}$:



En particular, todo punto $\mathbb{Q}$-racional en $X_{ns}^+(24)$ se proyecta a un par de puntos $\mathbb{Q}$-racionales en $X_{ns}^+(3)$ y en $X_{ns}^+(8)$. Estas dos últimas curvas, son de género 0 y definidas sobre $\mathbb{Q}$.

Teniendo en cuenta lo desarrollado en secciones anteriores, la curva $X_{ns}^+(3)$ es ramificada en ρ y en ∞. Los índices de ramificación son, en ambos casos, iguales a 3. Arriba de i, hay tres puntos elípticos no ramificados. Ya hemos mencionado que, en $X(1)$, el punto ρ y la cúspide ∞ son racionales (al igual que i). Como sólo existe un punto, $P \in X_{ns}^+(3)$, que se proyecta sobre ∞ y sólo uno, Q, arriba de ρ, vemos que tienen que ser invariantes por la acción de $\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Son, entonces, puntos $\mathbb{Q}$-racionales.

Sea $s : X_{ns}^+(3) \to \mathbb{P}^1$ un uniformizador definido sobre $\mathbb{Q}$. Componiendo s con un automorfismo de $\mathbb{P}^1$ (definido sobre $\mathbb{Q}$), podemos suponer que $s(P) = \infty$ y que $s(Q) = 0$. La relación entre j y s tiene, así, el siguiente aspecto:

$$j = \lambda s^3 ,$$

donde la constante λ es un número racional. Pero, además, λ tiene que ser un cubo, y, modificando nuevamente s, obtenemos $j = s^3$.

Por un procedimiento similar, se obtiene una parametrización para $X_{ns}^+(8)$.

Teorema 3.1. *Existen uniformizadores*

$$\begin{aligned} s &: X_{ns}^+(3) \to \mathbb{P}^1 , \\ v &: X_{ns}^+(8) \to \mathbb{P}^1 \end{aligned}$$

definidos sobre $\mathbb{Q}$ *tales que*

$$\begin{aligned} j &= s^3 , \\ j &= \frac{-2^{17}(v+1)^3(8(v+1)3 + (v^2-2)^2)^3}{(v^2-2)^8} . \end{aligned}$$

Un punto íntegro en $X_{ns}^+(24)$, un punto racional con j-invariante entero, se proyecta a un punto racional en la curva de nivel 3 y a un punto racional en la curva de nivel 8. Si j ha de ser entero, tanto s, como v, deberán ser racionales, pero s deberá ser entero también. De las parametrizaciones de $X_{ns}^+(3)$ y de $X_{ns}^+(8)$ se deduce que s y v tienen que cumplir con

$$s^3 \;=\; \frac{-2^{17}(v+1)^3(8(v+1)3+(v^2-2)^2)^3}{(v^2-2)^8}\;. \tag{1}$$

Suponiendo que (v,s) es una solución, y que v es de la forma $v=x/y$, con x e y enteros coprimos, homogeneizamos y obtenemos la relación

$$t^3 \;=\; \frac{2^{17}y(x+y)^3(8(x+y)3+(x^2-2y^2)^2)^3}{(x^2-2y^2)^8}\;,$$

donde $t=-s$. El único primo que puede dividir a x^2-2y^2 es $p=2$, y como x e y son coprimos, 4 no divide. Todo se reduce, entonces a hallar las soluciones enteras (x,y) de $x^2-2y^2=\pm1,\pm2$. En cualquier caso, como t tiene que ser un entero, el lado derecho tiene que ser un cubo en $\mathbb{Z}$. Si $x^2-2y^2=\pm1$, el único factor que no es, *a priori*, un cubo es $2^{17}y$. Pero, entonces $y=2z^3$, para algún entero z. Reemplazando y definiendo $w:=2z^2$, el problema pasa a ser el de hallar las soluciones enteras de $x^2=w^3\pm1$. Si, en cambio, $x^2-2y^2=\pm2$, el entero y tiene que un cubo z^3. Así, x tiene que ser par, y, reemplazando x por $2x_1$, llegamos a la ecuación $2x_1^2=z^6\pm1$.

En la sección 12 de [6], la demostración de que no existe un décimo cuerpo cuadrático imaginario con número de clases 1, basada en la original de Heegner, reduce el problema a hallar las soluciones a las cuatro ecuaciones

$$\begin{aligned} x^2 &= w^3+1\;,\\ x^2 &= w^3-1\;,\\ z^6+1 &= 2x_1^2\;,\\ (-w)^3+1 &= -2x_1^2\;,\text{ haciendo el cambio } w=z^2\;. \end{aligned}$$

Las soluciones a estas ecuaciones son (x,w) igual a $(0,-1)$, $(\pm1,0)$ o $(\pm3,2)$ para la primera, $(x,w)=(0,1)$ para la segunda, $(x_1,z)=(\pm1,\pm1)$ para la tercera y $(x_1,w)=(0,1)$ para la cuarta (ver la sección 6 de [4] o la sección 12 de [6] para una idea de cómo demostrarlo). Pero, desandando el proceso que nos condujo a estas ecuaciones, no todas las soluciones a las mismas dan lugar a posibles valores de v y de t. Por ejemplo, una solución a $x^2=w^3\pm1$ con x igual a 0 y $w=\pm1$ no da lugar a $v=x/y$ con y de la forma $2z^3$, pues w no es de la forma $2z^2$.

Los posibles valores para el uniformizador s son 0, -32, -96, -960, -5280 y -640320. Ya sabemos que el punto de $X_{ns}^+(3)$ con $s=0$ es ρ, y que este punto se obtiene a partir del cuerpo cuadrático imaginario $K=\mathbb{Q}(\sqrt{-3})$: recordemos que el punto asociado es $[E,\varphi]$, donde E es una curva elíptica definida sobre $\mathbb{Q}$ con CM por el anillo de enteros de K y $\varphi:\; E[n]\xrightarrow{\sim}(\mathbb{Z}/N\mathbb{Z})^2$ es una estructura de nivel. La función j en $[E,\varphi]$ toma el valor $j(E)$, el j-invariante de la curva elíptica, que coincide con $j(\mathcal{O}_K)$, viendo a $\mathcal{O}_K$

como retículo en $\mathbb{C}$. Éste es el procedimiento general para obtener un punto asociado a un cuerpo cuadrático imaginario, K, cuyo número de clases es igual a 1 y tal que todo divisor primo del nivel, N, es inerte en K. De las propiedades equivalentes en la proposición 1.1, deducimos que, si K es el cuerpo cuarático imaginario de discriminante d, y $h(d) = 1$, todo primo menor que $(1 + |d|)/4$ es inerte. Visto del otro lado, esto dice que, fijado N, toda curva elíptica con multiplicación compleja por un cuerpo cuadrático imaginario de discriminante $d \geq 4p$ (donde p es el primo de valor absoluto mayor entre aquellos que dividen a N) y número de clases 1 da lugar a un punto íntegro en $Y_{ns}^{+}(N)$.

Si d es un discriminante fundamental, y $h(d) = 1$, el j-invariante del orden cuadrático imaginario de discriminante d está dado por la siguiente tabla:

d	j
-3	0
-4	$2^6 \cdot 3^3$
-7	$-3^3 \cdot 5^3$
-8	$2^6 \cdot 5^3$
-11	-2^{15}
-19	$-2^{15} \cdot 3^3$
-43	$-2^{18} \cdot 3^3 \cdot 5^3$
-67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
-163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

Volvamos a la curva de nivel 24. Si P es un punto $\mathbb{Q}$-racional de $X_{ns}^{+}(24)$ tal que $j(P)$ es uno de 0, $(-32)^3$, $(-96)^3$, $(-960)^3$, $(-5280)^3$ o $(-640320)^3$, entonces $s(P)$ es la única raíz racional de $j(P)$ y $s(P)$ pertenece al conjunto de los posibles valores enteros calculados para s. Esto que parece obvio lo aplicamos de la siguiente manera: conocemos el valor de $j(\mathcal{O}_K)$ para cada cuerpo cuadrático imaginario de discriminante d que aparece en la tabla. Algunos de estos cuerpos dan puntos enteros en $X_{ns}^{+}(24)$ y cada uno de estos puntos tiene asociado un valor de j. Por otro lado, si $j(\mathcal{O}_K) = j(\mathcal{O}_{K'})$, entonces $K = K'$ y los órdenes son iguales. Si $d \geq 12$ y K es el cuerpo cuadrático de discriminante d, y si $h(d) = 1$, K tiene asociado un punto íntegro P en la curva. Evaluando j en P, obtenemos $j(P) = j(\mathcal{O}_K)$ y tiene que ser el cubo de uno de los posibles de s. Pero todo valor de s entero viene de un punto asociado a uno de los cuerpos de discriminante -3, -11, -19, -43, -67 y -163, con lo cual, K, cuyo discriminante d es $d \leq -12$, tiene que ser uno de estos seis. Como para $0 > d > -12$, los únicos con $h(d) = 1$ son los de la tabla, esto demuestra que no hay un décimo cuerpo cuadrático imaginario con número de clases 1.

Observación. De la relación entre los uniformizadores s y v, la ecuación 1, notemos que s será racional, si $4/(v^2-2)^2$ es un cubo. Equivalentemente, será suficiente que $4(v^2-2)$ sea un cubo. Para hallar los posibles valores de s, uno podría intentar encontrar los puntos racionales en la curva elíptica $v'^2 = u^3 + 8$ tales que, si $v = v'/2$, entonces s sea entero.

3.2 Nivel 7

Sea $F/\mathbb{Q}$ la extensión cúbica totalmente real generada por $\zeta_7 + \zeta_7^{-1}$, donde $\zeta_7 = e^{2\pi i/7}$ es una raíz séptima primitiva de la unidad en $\mathbb{C}$. Una unidad ε de F se dirá *excepcional*, si existe otra unidad ε_1 tal que $\varepsilon + \varepsilon_1 = 1$. Kenku [9] muestra la existencia de una correspondencia entre los puntos de $X_{ns}^{+}(7)$, íntegros sobre $\mathbb{Z}[1/7]$ y cierto subconjunto de las unidades excepcionales de la extensión totalmente real $F/\mathbb{Q}$. Un punto es íntegro

sobre $\mathbb{Z}[1/7]$, si es $\mathbb{Q}$-racional y su j-invariante pertenece a $\mathbb{Z}[1/7]$.

La curva $X_{ns}^+(7)$ tiene $\phi(7)/2 = 3$ cúspides que, en el peor de los casos, son $\mathbb{Q}(\zeta_7)$-racionales. Pero $\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permuta las cúspides, con lo que quedan definidas sobre $F = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Sea $\sigma(z) = 1 - \frac{1}{z}$ el automorfismo de $\mathbb{P}^1$ que permuta cíclicamente los puntos ∞, 1 y 0. Este automorfismo es de orden tres. La curva $X_{ns}^+(7)$ está definida sobre $\mathbb{Q}$, tiene género cero y cuenta con tres puntos F-racionales que corresponden a las cúspides. Si $s \in \mathsf{Gal}(F/\mathbb{Q})$ es el automorfismo de F que actúa como σ sobre las cúspides, existe un uniformizador (K-isomorfismo, en este caso)

$$f \,:\, X_{ns}^+(7) \to \mathbb{P}^1$$

que hace corresponder las cúspides con ∞, 1 y 0, y tal que $f^s = 1 - \frac{1}{f}$.

Sea $m \in \mathbb{Z}$ un entero, y sea Q_m el polinomio

$$Q_m(X) \,=\, X^3 \,-\, mX^2 \,+\, (m-3)X \,+\, 1\ .$$

Existen exactamente 24 unidades excepcionales en F que son ceros de Q_m para algún entero m. La relación con los puntos $\mathbb{Q}$-racionales con j-invariante en $\mathbb{Z}[1/7]$ está dada por el siguiente lema. La demostración se puede hallar en [9].

Lema 3.2. *Sea $\overline{[E,\varphi]} \in X_{ns}^+(7)$ un punto $\mathbb{Q}$-racional tal que $j(E) \in \mathbb{Z}[1/7]$. Si $\varepsilon := f(\overline{[E,\varphi]})$, entonces ε es una unidad de F y $s(\varepsilon) = 1 - \varepsilon^{-1}$. Además, resulta ser una unidad excepcional que es cero de algún polinomio Q_m.*

Recíprocamente, si $\varepsilon \in F$ satisface $s(\varepsilon) = 1 - \varepsilon^{-1}$, cumple con ser una unidad excepcional y cero de Q_m para algún entero m, entonces corresponde vía $f : X_{ns}^+(7) \to \mathbb{P}^1$ a un punto $\mathbb{Q}$-racional con j-invariante en $\mathbb{Z}[1/7]$.

Resta encontrar una parametrización para $X_{ns}^+(7)$. Recordemos que existe un morfismo $\pi : X_{ns}^+(7) \to X(1)$ de grado $7\phi(7)/2 = 21$. Supongamos que existe una curva Z y una factorización de π como en el diagrama siguiente

$$X_{ns}^+(7) \xrightarrow{\Phi_3} Z \xrightarrow{\Phi_7} X(1)\ ,$$

con Φ_3 de grado 3 y Φ_7 de grado 7. Supongamos, además, que contamos con un uniformizador $z : Z \to \mathbb{P}^1$ tal que los únicos puntos de $X_{ns}^+(7)$ en los cuales z toma el valor ∞ son aquellos en los que f toma los valores ∞, 1 y 0 (es decir, las cúspides), y supongamos que hay un único punto, en $X_{ns}^+(7)$, arriba de $z = 0$ (y que, por ende, ramifica con orden 3). La relación entre los uniformizadores z y f es

$$z \,=\, \frac{a(f-b)^3}{f(f-1)}\ ,$$

para ciertas constantes a y b en $\mathbb{Q}(\zeta_7)$.

La curva $X_{ns}^+(7)$ se obtiene como cociente de $X'(7)$ a partir del subgrupo de automorfismos determinado por el subgrupo

$$C_{ns}^{+}(7)'/\{\pm 1\} \subset \mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})/\{\pm 1\} ,$$

donde $C_{ns}^{+}(7)'$ es $C_{ns}^{+}(7) \cap \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. Sea $S \subset \mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$ un subgrupo isomorfo al grupo de permutaciones de curatro elementos, $\mathbb{S}_4$. Conjugando, podemos asumir que S contiene a $C_{ns}^{+}(7)'/\{\pm 1\}$. Sea $\widetilde{S}$ su preimagen por la proyección $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) \to \mathrm{PGL}_2(\mathbb{Z}/7\mathbb{Z})$. La acción de $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ sobre las raíces de la unidad estaba dada por el determinante (ver 2.1). Como S está contenido en $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$, si $\kappa \in \widetilde{S}$, su determinante es un cuadrado *modulo* 7, es decir, 1, 2 o 4. Por otra parte, si

$$w = 2\zeta_7^4 + 2\zeta_7^2 + 2\zeta_7 + 1 ,$$

entonces $w^2 = -7$. En particular, w queda fijo por $\widetilde{S}$, mientras que ζ_7 no. De esto se deduce que $\mathbb{Q}(j, \{f_0^{\pm\overline{v}}\})^S \cap \mathbb{Q}(\zeta_7)$ es igual a $\mathbb{Q}(\sqrt{-7})$, y que existe una curva correspondiente al grupo S que da una factorización de $X_{ns}^{+}(7) \to X(1)$ y que cuenta con las propiedades de la curva Z de antes. [9][10]

Sea Z esta curva, y sea $z : Z \to \mathbb{P}^1$ un uniformizador tal que su relación con j sea

$$j = z(z^2 + 7\lambda z + 7\lambda - 21)^3 ,$$

donde $\lambda := (1 + \sqrt{-7})/2$. Usando el método expuesto en el capítulo 2 de [10], se pueden hallar los valores de a y de b, y obtener la siguiente tabla:

d	j	f
-4	$2^6 \cdot 3^3$	$-(\zeta_7 + \zeta_7^6)$
-8	$2^6 \cdot 5^3$	$-(\zeta_7^2 + \zeta_7^5)$
-11	-2^{15}	$-(\zeta_7^3 + \zeta_7^4)$
-43	$-2^{18} \cdot 3^3 \cdot 5^3$	$-(\zeta_7 + \zeta_7^6)^3(\zeta_7^2 + \zeta_7^5)^4$
-16	$2^3 \cdot 3^3 \cdot 11^3$	$(\zeta_7^2 + \zeta_7^5)^3(\zeta_7^3 + \zeta_7^4)^4$
-67	$2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	$-(\zeta_7^3 + \zeta_7^4)^3(\zeta_7 + \zeta_7^6)^4$
-3	0	$-(\zeta_7^3 + \zeta_7^4)^3(\zeta_7^2 + \zeta_7^5)^2$
	$2^2 \cdot 5^3 \cdot 7^3$	$-(\zeta_7^2 + \zeta_7^5)^3(\zeta_7 + \zeta_7^6)^2$
	$7^5 \cdot 2^5$	$-(\zeta_7 + \zeta_7^6)^3(\zeta_7^3 + \zeta_7^4)^2$
-163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	$-440 + 244(\zeta_7^2 + \zeta_7^5) - 305(\zeta_7^3 + \zeta_7^4)$
	$2^9 \cdot 17^6 \cdot 19^3 \cdot 29^3 \cdot 149^3$	$-135 + 305(\zeta_7^2 + \zeta_7^5) + 549(\zeta_7^3 + \zeta_7^4)$
	$2^6 \cdot 11^3 \cdot 23^3 \cdot 149^3 \cdot 269^3$	$-684 - 549(\zeta_7^2 + \zeta_7^5) - 244(\zeta_7^3 + \zeta_7^4)$

3.3 Nivel 5 (o 15)

Hemos visto que la curva $X_{ns}^{+}(3)$ admite un uniformizador s que satisface $j = s^3$. En particular, se deduce que toda curva elíptica E definida sobre $\overline{\mathbb{Q}}$ da lugar a un punto $\mathbb{Q}$-racional en $X_{ns}^{+}(3)$, si, y sólo si $j(E)$ es un cubo en $\mathbb{Q}$. Si d es igual a -7, -8, -28, -43, -67 o a -163, entonces, en el orden cuadático imaginario I de discriminante d, el primo 3 es no ramificado y 5 es inerte. Se obtienen, así, al menos seis puntos $\mathbb{Q}$-racionales en $X_{ns}^{+}(3)$ y en $X_{ns}^{+}(5)$ cuyos j-invariantes son cubos en $\mathbb{Z}$. Si d es menor a

-163, tanto 3, como 5, es inerte en el orden de discriminante d. Por lo tanto, a partir de un orden cuadrático imaginario I de discriminante $d < -163$ con número de clases igual a 1, se obtiene un punto $\mathbb{Q}$-racional en $X_{ns}^+(5)$ con j un cubo entero. Pero, por medio de una parametrización de dicha curva, se obtiene la lista completa de los posibles puntos con los que se debe corresponder. Como los seis órdenes mencionados y aquel de discriminante -3 dan cuenta de todos estos puntos, I debe ser uno de ellos. En [5], el autor obtiene una parametrización de $X_{ns}^+(5)$, permitiéndole dar una solución al problema del número de clases igual a 1, como también interpretar la solución por Siegel del problema (en un trabajo titulado *Zum Beweise des Starkschen Satzes*) en términos de $X_{ns}^+(5)$. A continuación resumimos el proceso que conduce a dicha parametrización.

Como en los dos ejemplos anteriores, consideremos el cubrimiento de $X_{ns}^+(5)$ sobre $X(1)$. Recordemos que los puntos elípticos de orden dos o tres en $X_{ns}^+(5)$ son puntos que se proyectan, respectivamente, sobre i o ρ en $X(1)$ y cuyo índice de ramificación es igual a 1. Por otra parte, las fórmulas al final de 2.5 indican que, para esta curva, hay un único punto elíptico de orden tres (y, por lo tanto, otros tres puntos arriba de ρ cuyo índice de ramificación es 3), y dos de orden dos (y cuatro puntos arriba de i cuyo índice es 2). Con respecto a las cúspides, las mismas fórmulas nos muestran que $X_{ns}^+(5)$ cuenta con dos cúspides, y la ramificación es, en ambas, de índice 5. Como el grupo de Galois actúa por permutaciones sobre el conjunto de cúspides, y dado que las cúsides de $X_{ns}^+(5)$ están definidas sobre $\mathbb{Q}(\zeta_5)$, donde $\zeta_5 := e^{2\pi i/5}$, si $\sigma \in \mathsf{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, entonces σ^2 actúa trivialmente sobre dicho conjunto. En particular, las cúspides están definidas sobre la subextensión cuadrática $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$.

Sea $\eta : X_{ns}^+(5) \to \mathbb{P}^1$ un uniformizador definido sobre $\mathbb{Q}$. Componiendo η con un $\mathbb{Q}$-automorfismo de $\mathbb{P}^1$, podemos suponer que las cúspides de $X_{ns}^+(5)$ son las raíces de $X^2 - 5$. Por otra parte, como la curva tiene un único punto elíptico de orden tres, el mismo tiene que ser un punto $\mathbb{Q}$-racional de $X_{ns}^+(5)$, tiene que quedar fijo por la acción del grupo de Galois. Podemos asumir también que η en este punto toma el valor 0. Entonces, la parametrización de la curva va a estar dada por una relación de la forma:

$$j \;=\; \lambda \frac{\eta(\eta - A)^3(\eta^2 - B\eta + C)^3}{(\eta^2 - 5)^5} \;.$$

Las constantes A, B y C están determinadas por el valor de η en los puntos de $X_{ns}^+(5)$ arriba de ρ cuyo índice de ramificación es 3. Usando un cubrimiento intermedio de manera similar a lo explicado en 3.2 es posible calcular los valores de estas constantes. A través de la transformación $z \mapsto 2z/(z+5)$, se llega a la relación siguiente [5]

$$j \;=\; 5^3 \frac{\eta(2\eta + 1)^3(2\eta^2 + 7\eta + 8)^3}{(\eta^2 + \eta - 1)^5} \;.$$

Una vez hallada esta parametrización de $X_{ns}^+(5)$, si llamamos t al uniformizador de $X_{ns}^+(3)$ que es la raíz cúbica de j, sabemos que, dado un orden cuadrático imaginario I cuyo número de clases es 1, y elegida una curva elíptica E (definida sobre $\mathbb{Q}$) con multiplicación compleja por I, si el primo 3 no ramifica en I y 5 es inerte, entonces, por medio de t y η, obtenemos enteros m, x e y tales que $j(E) = m^3$, $\eta = x/y$ y $(x, y) = 1$. Además,

por la relación con j, sabemos que la terna (x, y, m) tiene que ser una solución en $\mathbb{Z}$ a la ecuación

$$m^3 \;=\; u(x,y) \;:=\; 5^3 \frac{x(2x+y)^3(2x^2+7xy+8y^2)^3}{(x^2+xy-y^2)^5} \;.$$

Las soluciones con $m = 0$ son $(0, 1, 0)$, $(0, -1, 0)$, $(-1, 2, 0)$ y $(1, -2, 0)$.

En general, si (x, y, m) es solución a la ecuación, también lo es $(-x, -y, m)$. Sea $m \neq 0$ y (x, y, m) una solución. Si l es un primo racional que divide a $x^2 + xy - y^2$, entonces $(x, y) = 1$ implica que l no puede dividir ni a x, ni a y. Dado que $u(x, y)$ es un entero y l divide al denominador en la expresión para $u(x, y)$, el primo l tiene que ser 5. Esto se deduce de que el sistema de ecuaciones *modulo* l (con l primo)

$$\begin{aligned} z^2 \,+\, z \,-\, 1 \;&\equiv\; 0 \,(\mathrm{mod}\, l) \\ 2z \,+\, 1 \;&\equiv\; 0 \,(\mathrm{mod}\, l) \end{aligned}$$

tiene soluciones en enteras sólo si $l = 5$, y de que lo mismo es cierto para

$$\begin{aligned} z^2 \,+\, z \,-\, 1 \;&\equiv\; 0 \,(\mathrm{mod}\, l) \\ 2z^2 \,+\, 7z \,+\, 8 \;&\equiv\; 0 \,(\mathrm{mod}\, l) \;. \end{aligned}$$

Pero la ecuación $z^2+z-1 \equiv 0\,(5^2)$ no admite soluciones en $\mathbb{Z}$. En definitiva, si (x, y, m) es una solución para $m^3 = u(x, y)$ con x, y y m en $\mathbb{Z}$ y $(x, y) = 1$, la expresión $x^2 + xy - y^2$ es igual a ± 5 o ± 1. En el primer caso, $u(x, y)$ no es un cubo en $\mathbb{Z}$. Por esta razón, $x^2 + xy - y^2 = \pm 1$.

Si denotamos con ϵ al elemento $(-1+\sqrt{5})/2$ de $F := \mathbb{Q}(\sqrt{5})$, y $\mathcal{O}_F$ al anillo de enteros de este cuerpo, la condición sobre $x^2 + xy - y^2$ equivale a que la norma de $x + y\epsilon \in \mathcal{O}_F$ sea igual a 1 o a -1, a que $x + y\epsilon$ sea una unidad en este anillo. Pero las unidades de $\mathcal{O}_F = \mathbb{Z}[\epsilon]$ son de la forma

$$\pm\epsilon^n \;=\; \pm(x_n \,+\, y_n\epsilon) \;,$$

donde $x_n := (-1)^{n+1}F_n$ e $y_n := (-1)^n F_{n+1}$ (F_n es el n-ésimo número de Fibonacci). En particular, Dada la solución (x, y, m), tenemos $x = \pm x_n$ para algún n. Pero, de la expresión para $u(x, y)$, deducimos que x es un cubo en $\mathbb{Z}$, y que, entonces x_n también lo es.

Los únicos números de Fibonacci que son cubos son $F_1 = 1$, $F_2 = 1$ y $F_6 = 8$ (ver [5]). Si definimos

$$\begin{aligned} &L_1 := 1 \;,\; L_2 := 3 \;,\; L_{n+1} \,=\, L_n \,+\, L_{n-1} \;, \\ &a \,=\, \frac{1+\sqrt{5}}{2} \;,\; b \,=\, \frac{1-\sqrt{5}}{2} \;, \end{aligned}$$

inductivamente,

$$F_n = \frac{a^n - b^n}{\sqrt{5}} \ , \ L_n = a^n + b^n \text{ y}$$
$$L_n^2 - 5F_n^2 = 4(-1)^n \ .$$

Sobre la curva de nivel 24 el problema de hallar los puntos enteros se reducía a hallar soluciones a ciertas ecuaciones diofánticas. Sobre la curva de nivel 5, la ecuación diofántica es

$$Y^2 = 5Z^6 \pm 4 \ .$$

En resumen, las posibles soluciones (x, y, m) a $m^3 = u(x, y)$ en $\mathbb{Z}$ con $(x, y) = 1$, cumplen con $x = 0$, ± 1 o ± 8. Requiriendo que y en (x, y, m) sea positivo, las posibles soluciones son las ternas en la siguiente tabla.

d	$j = t^3$	(x, y, m)
-3	0	$(0, 1, 0)$
-3	0	$(-1, 2, 0)$
-7	$-3^3 \cdot 5^3$	$(-1, 1, -15)$
-8	$2^6 \cdot 5^3$	$(1, 0, 20)$
-28	$3^3 \cdot 5^3 \cdot 7^3$	$(1, 1, 255)$
-43	$-2^{15} \cdot 3^3$	$(1, 2, -96)$
-67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	$(-8, 5, -5280)$
-163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	$(8, 13, -640320)$

3.4 Nivel 9

En la solución al problema del número de clases igual a 1 que damos a continuación, y que se encuentra en [1], el método es similar al que se puede encontrar en [5] y que está detrás de la descripción en la sección anterior.

Sea r : $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ el morfismo dado por reducción de coordenadas *modulo* 3, y sea N el núcleo de este morfismo. Si llamamos H al subgrupo de $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ generado por las matrices $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ y $\left[\begin{smallmatrix} -1 & -4 \\ -4 & 1 \end{smallmatrix}\right]$, y N' al generado por $\left[\begin{smallmatrix} 1 & -3 \\ 3 & 1 \end{smallmatrix}\right]$, entonces H normaliza a N' y $C_{ns}^+(9)' = C_{ns}^+(9) \cap \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ es el producto semidirecto de N' por H. Si N'' es el subgrupo generado por $\left[\begin{smallmatrix} 1 & -3 \\ 3 & 1 \end{smallmatrix}\right]$ y por $\left[\begin{smallmatrix} -2 & 3 \\ 3 & 4 \end{smallmatrix}\right]$, entonces H normaliza a N'' también, y

$$C_{ns}^+(9)' \simeq N' \rtimes H \text{ y } r^{-1}(C_{ns}^+(3)) \simeq N \rtimes H \ .$$

Además, valen las inclusiones $C_{ns}^+(9) \subset N'' \rtimes H \subset r^{-1}(C_{ns}^+(3))$, ambas de índice 3. Llamaremos B al subgrupo de $r^{-1}(C_{ns}^+(3))$ isomorfo a $N'' \rtimes H$, y Γ_B al subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ conformado por las matrices congruentes a algún elemento de B al reducir coordenadas *modulo* 9.

En cuanto a las inclusiones $\Gamma_{ns}^+(9) \subset \Gamma_B \subset \Gamma_{ns}^+(3)$ los índices son, también, 3. En particular, los cubrimientos Φ_1 y Φ_2 en

$$X_{ns}^+(9) \xrightarrow{\Phi_1} X_B \xrightarrow{\Phi_2} X_{ns}^+(3) \xrightarrow{\Phi_3} X(1) \ ,$$

son, ambos, de grado 3. El grado del cubrimiento Φ_3 también es 3. A continuación hacemos uso de la información de ramificación de estos cubrimientos, refiriendo a [1] con respecto a los detalles de cómo obtenerla.

Sabemos que las curvas $X_{ns}^+(3)$ y $X_{ns}^+(9)$ están definidas sobre $\mathbb{Q}$ y que los morfismos $\Phi_2 \circ \Phi_1$ y Φ_3 son $\mathbb{Q}$-morfismos. Si consideramos el subgrupo $(\mathbb{Z}/9\mathbb{Z})^\times \cdot B$ de $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, y argumentando como con el grupo S al tratar la curva de nivel 7, vemos que X_B está definida sobre $\mathbb{Q}(\sqrt{-3})$.

En cuanto a $X_{ns}^+(3)$ elgimos el uniformizador t tal que $j = t^3$. En esta curva hay un único punto ρ' arriba de $\rho \in X(1)$ y un único punto ∞' arriba de ∞. Sobre el punto $i \in X(1)$, en cambio, se proyectan tres, i_1, i_2 e i_3, eligiendo los subíndices de manera que $t(i_1) = 12$, $t(i_2) = 12\zeta_3^{-1}$ y $t(i_3) = 12\zeta_3$, donde $\zeta_3 = e^{2\pi i/3}$.

En X_B hay una única cúspide, que denotamos ∞''. Hay dos puntos $i_{3,1}$ e $i_{3,2}$ en X_B tales que $\Phi_2(i_{3,k}) = i_3$. El índice de ramificación de Φ_2 en $i_{3,1}$ es 1 y en $i_{3,2}$ es igual a 2. Éstos son los únicos puntos arriba de i_3; la acción de $\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$ los permuta. Pero uno es ramificado y el otro no, entonces los tiene que dejar fijos, es decir, son $\mathbb{Q}(\sqrt{-3})$-racionales.

Proposición 3.3. *Existe un uniformizador $w : X_B \to \mathbb{P}^1$, definido sobre $\mathbb{Q}(\sqrt{-3})$ y tal que $w(\infty'') = \infty$, $w(i_{3,1}) = 2\sqrt{-3}$ y $w(i_{3,2}) = -\sqrt{-3}$. Además, la relación entre w y t es*

$$t \ = \ \zeta_3^{-1}(w^3 \ + \ 9w \ - \ 6) \ .$$

Demostración. Supongamos que $\eta : X_B \to \mathbb{P}^1$ es el uniformizador determinado por $\eta(\infty'') = \infty$, $\eta(i_{3,1}) = 1$ y $\eta(i_{3,2}) = 0$. Sabemos que, entonces, la relación con t tiene que ser de la forma (ver la sección 2.4)

$$t \ = \ \lambda \prod_{k=1}^{3} (\eta \ - \ \eta(\rho_k)) \ = \ \lambda(\eta^3 \ + \ A\eta^2 \ + \ B\eta \ + \ C)$$

ya que los puntos ρ_k, arriba de ρ', son no ramificados. Las constantes $\lambda \neq 0$, A, B y C pertenecen al cuerpo $\mathbb{Q}(\sqrt{-3})$. También podemos expresar t en términos de los valores de η en otros puntos: por ejemplo, teniendo en cuenta la ramificación de Φ_2,

$$\begin{aligned} t \ &= \ \lambda(\eta \ - \ \eta(i_{3,2}))^2(\eta \ - \ \eta(i_{3,1})) \ + \ t(i_3) \\ &= \ \lambda(\eta \ - \ \eta(i_{1,2}))^2(\eta \ - \ \eta(i_{1,1})) \ + \ t(i_1) \ . \end{aligned}$$

El valor de t en i_3 es $12\zeta_3$ y, en i_1, 12. Evaluando en $i_{3,2}$, se deduce que el valor de λC es $12\zeta_3$, y, como el índice de ramificación de Φ_2 en $i_{3,2}$ es igual a 2, que $t - t(i_3)$ tiene un cero doble en $i_{3,2}$. En particular, la constante B tiene que ser igual a 0. Por otra parte, evaluando en $i_{3,1}$, se ve que el valor de A es -1. De la misma manera, al evaluar en $i_{1,1}$ e $i_{1,2}$, se obtiene un sistema de ecuaciones que relacionan las constantes λ y C con $\eta(i_{1,1})$

y $\eta(i_{1,2})$ de donde se puede deducir los valores de estos cuatro elementos de $\mathbb{Q}(\sqrt{-3})$. La relación entre los uniformizadores es

$$t \,=\, -81(\zeta_3 \,-\, 1)\left(\eta^3 \,-\, \eta^2 \,+\, \frac{-4(\zeta_3-1)}{81}\right) \,.$$

El enunciado de la proposición se puede deducir de hacer un cambio de variables: $w = -(\sqrt{-3})(-3\eta+1)$. □

Proposición 3.4. *Existe un uniformizador $y : X_{ns}^{+}(9) \to \mathbb{P}^1$, definido sobre $\mathbb{Q}$, tal que su relación con el uniformizador t está dada por*

$$t \,=\, \frac{-3(y^3+3y^2-6y+4)(y^3+3y^2+3y+4)(5y^3-3y^2-3y+2)}{(y^3-3y+1)^3} \,. \qquad (2)$$

Demostración. El uniformizador y se define en términos de w y un conjugado. Veamos, en primer lugar, que X_B no puede estar definida sobre $\mathbb{Q}$ de manera compatible con $X_{ns}^{+}(9)$. Es decir, sabemos que X_B está definida sobre $K := \mathbb{Q}(\sqrt{-3})$, y que el cuerpo de funciones $K(X_B)$ está contenido en $K(X_{ns}^{+}(9))$. Si σ un generador de $\mathsf{Gal}(K/\mathbb{Q})$, entonces, lo que queremos decir con que no es posible que X_B esté definida de manera compatible sobre $X_{ns}^{+}(9)$ es que σ no deja fijo al subcuerpo $K(X_B)$ bajo la acción de $\mathsf{Gal}(K/\mathbb{Q})$ sobre $K(X_{ns}^{+}(9))$. La razón de esto es que, por ejemplo, los puntos i_1 e i_2 de $X_{ns}^{+}(3)$ son conjugados, pero uno ramifica en X_B y el otro no, con lo cual Φ_2 no puede ser un $\mathbb{Q}$-morfismo y X_B estar definida sobre $\mathbb{Q}$.

La imagen del cuerpo $K(X_B) = K(w)$ por el automorfismo σ es $K(w')$, donde $w' = w^\sigma$. Dado el grado de $K(X_{ns}^{+}(9))/K(t)$, resulta que $K(X_{ns}^{+}(9)) = K(w, w')$. Por otra parte, dado que $t^\sigma = t$, se deduce la igualdad

$$\zeta_3^{-1}(w^3+9w-6) \,=\, \zeta_3(w'^3+9w'-6) \,.$$

Esta igualdad permite escribir w en términos de $u := (w-\sqrt{-3})/(w'+\sqrt{-3})$. La relación que se obtiene es

$$w \,=\, 3u\sqrt{-3}\left(\frac{-u^2-\zeta_3^{-1}}{u^3-\zeta_3^{-1}}\right) \,+\, \sqrt{-3} \,.$$

En conjunto con la relación entre t y w, podemos expresar la relación entre los uniformizadores u y t. Pero u está definido sobre $\mathbb{Q}(\sqrt{-3})$. Haciendo el cambio de variables $u = (y+\zeta_3)/(\zeta_3 y+1)$, y cumple con que $y^\sigma = y$ y, además, con que la relación con t es la del enunciado. □

Una vez encontrada esta parametrización, con el fin de determinar los puntos enteros en $X_{ns}^{+}(9)$, el paso siguiente es determinar las soluciones (y,t), con t un número entero e $y = m/n$ (m, n enteros coprimos), de la ecuación 2.

Se puede ver de manera elemental que, si $(m/n, t)$ es una solución en $\mathbb{Z}$, con m y n coprimos, entonces

$$m^3 - 3mn^2 + n^3 = k \ , \tag{3}$$

con $k \in \{\pm 1, \pm 3\}$. El prolema queda reducido a hallar soluciones a la ecuación 3 con $k = 1$ o 3. Las soluciones en estos casos están completamente determinadas y son nueve pares (m, n). Los puntos que estos pares determinan en $X_{ns}^+(9)$ son los puntos enteros de la curva, y todos, excepto uno, se corresponden con órdenes en cuerpos cuadráticos imaginarios (tabla 5.2 en [1]). El caso excepcional es $j = 3^3 41^3 61^3 149^3$. Éste es el j-invariante de una curva elíptica que, si bien no es CM, parece serlo *modulo* 9. Concretamente, la acción de Galois sobre la 9-torsión de esta curva se realiza en el normalizador de un subgrupo de Cartan *non-split*.

3.5 Nivel 11

A diferencia de las curvas consideradas en las soluciones anteriores ($N = 3, 5, 7, 8, 9$), la curva de nivel 11, $X_{ns}^+(11)$ es $\mathbb{Q}$-isomorfa a la curva de género 1 dada por la primera de las siguientes ecuaciones de Weierstraß:

$$\begin{aligned} y^2 + y &= x^3 - x^2 - 7x + 10 \ , \\ y^2 + 11y &= x^3 + 11x^2 + 33x \ . \end{aligned}$$

La segunda de estas ecuaciones se obtiene tras reemplzar x e y por $x+4$ e $y+5$, y determina una curva isomorfa, que denotaremos C. Entonces, al igual que $X_{ns}^+(11)$, la curva elíptica C parametriza clases de isomorfismo de curvas elípticas con cierta estructura de nivel. En [11] se demuestra que un punto $\mathbb{Q}$-racional de C, P, corresponde a una curva elíptica cuyo j-invariante es un entero (racional), si, y sólo si $P = (x, y)$ tiene la propiedad de que $x/(xy - 11)$ pertenece a $\mathbb{Z}$. El problema de contar los puntos enteros de $X_{ns}^+(11)$ se convierte en el problema de contar los puntos racionales de C cuyas coordenadas tienen esta propiedad. El resultado central en [11] es:

Teorema 3.5. *Sea C la curva elíptica dada por la ecuación de Weierstraß*

$$y^2 + 11y = x^3 + 11x^2 + 33x \ .$$

Existen únicamente siete puntos $P = (x, y)$ en $C(\mathbb{Q})$ tales que $x/(xy-11)$ sea un número entero.

Por lo tanto, $X_{ns}^+(11)$ cuenta sólo con siete puntos enteros. Por otro lado, estos puntos enteros vienen exclusivamente de órdenes en cuerpos cuadráticos imaginarios: el primo 11 es inerte en los órdenes cuadráticos con número de clases 1 y de discriminante -3, -4, -12, -16, -27, -67 y -163. En particular, si $|d|$ es suficientemente grande, si $d < -44$ por ejemplo, como 11 es inerte en un orden de discriminante d, su número de clases no podrá ser igual a 1, excepto que d sea uno de los ya mencionados. Esta solución del problema difiere del resto en que el género de la curva modular es 1 (si bien para $N = 24$ el género también es 1, la solución, en ese caso, viene de considerar parametrizaciones de

las curvas de género 0 $X_{ns}^+(3)$ y $X_{ns}^+(8)$ [4]). Resumimos, a continuación, la demostración del teorema 3.5.

En la ecuación que define a C, reemplazando y por $(y-11)/2$ y luego $y/2$ por y, obtenemos

$$y^2 \;=\; x^3 \,+\, 11x^2 \,+\, 33x \,+\, \frac{121}{4} \;=:\; q(x)\ .$$

Llamemos $\widetilde{C}$ a la curva elíptica que esta ecuación determina. El polinomio q tiene un único cero en $\mathbb{R}$. En particular, dado que, si (x,y) es un punto de orden 2 de $\widetilde{C}$, y debe ser igual a 0 y x una raíz de q, el subgrupo $\widetilde{C}[2]$ no puede estar contenido en $\widetilde{C}(\mathbb{R})$. Esto implica que $\widetilde{C}(\mathbb{R})$ es isomorfo a $\mathbb{R}/\mathbb{Z}$ y, en particular, tiene una única componente conexa. Todo esto es cierto, también, para la curva C.

Sea t la función en C definida por la expresión $t = y - (11/x)$. Si (x,y) es un cero de t, entonces x es un cero del polinomio $x^5 + 11x^4 + 33x^3 - 121x - 121$. Las raíces de este polinomio son reales, con lo cual, los (cinco) puntos (x,y) que son ceros de la función t son todos reales. El morfismo $j : X_{ns}^+(11) \to \mathbb{P}^1$ determina un morfismo de la curva elíptica C en $\mathbb{P}^1$ a través de un isomorfismo definido sobre $\mathbb{Q}$ entre $X_{ns}^+(11)$ y C. Este isomorfismo es elegido de manera que las cúspides de $X_{ns}^+(11)$, que son cinco, se coprrespondan con los ceros de t (ver [11], y las referencias que allí se encuentran).

Sea $\omega = \omega_C = dx/(2y+11)$ el diferencial invariante de C. La integral $\int_{\mathcal{O}}^{P} \omega$ (donde $\mathcal{O}$ es el punto neutro de la curva elíptica y P un punto arbitrario) no está bien definida como elemento de $\mathbb{C}$, pero las posibles ambigüedades surgen de la elección del camino entre los puntos. Así, *modulo* el retículo que se le asocia a C vía sus períodos, podemos definir $\lambda(P)$ como el valor de esta integral *modulo* el retículo. Ahora, si P es un punto real de C, entonces existe un camino que lo une con $\mathcal{O}$ y que está contenido en $C(\mathbb{R})$. Esto muestra que $\lambda(P)$ es un número real, si P es un punto real. El grupo de puntos reales de C es isomorfo a $\mathbb{R}/\mathbb{Z}$ vía la aplicación λ y la elección de un período real para C. Por ejemplo, (identificando las curvas C y $\widetilde{C}$) se puede tomar $\Omega := \int_r^\infty dx/\sqrt{q(x)}$, donde r es la raíz real del polinomio q definido antes.

Antes de pasar a la demostración, es necesaria una última definición. Si f es una función en la curva C y si no es constante, dado un punto racional, $P \in C(\mathbb{Q})$, definimos la altura de P (respecto de f) como el producto $H_f(P) := \prod_v \max\{1, |f(P)|_v\}$, donde v recorre los lugares de $\mathbb{Q}$. La altura logarítmica asociada es $h_f(P) := \log(H_f(P))$ y, finalmente, si f es, además, una función par, la altura canónica se define como

$$\widehat{h}(P) \;:=\; \frac{1}{\deg(f)} \lim_{n\to\infty} \frac{h_f([2^n]P)}{4^n}\ .$$

La función $t = y - (11/x)$ no es par, pero se la puede relacionar con la altura canónica: si $P \in C(\mathbb{Q})$, entonces $\widehat{h}(P)$ está acotada por $(1/3)h_t(P) + 4,52$.

La idea de la demostración del teorema 3.5 es traducir las restricciones sobre un punto (x,y) tal que $x/(xy-11) \in \mathbb{Z}$ en estimaciones de una forma lineal en logaritmos. Supongamos que el rango del grupo $C(\mathbb{Q})$ es $r \geq 1$, y sean $P_1, \ldots, P_r$ generadores de la parte libre. Todo punto P se puede escribir como una combinación $m_1P_1 + \ldots + m_rP_r + T$,

donde los m_i son enteros y T es un punto de torsión. El primer objetivo es obtener una cota para $|t(P)|$ dependiente de los coeficientes m_i y, así, pasar a una cota superior sobre cierta forma lineal en $\lambda(P_i)$ y en Ω. El rango de la curva elíptica C es $r = 1$, lo que hace que sea más sencillo estimar la forma lineal. El mismo método, aplicado a encontrar puntos enteros en una curva elíptica de rango no necesariamente igual a 1 está descripto en [12].

Sea $P = (x, y)$ un punto de C, y sea $k \in \mathbb{Z}$ tal que $k = x/(xy - 11)$. Entonces $t(P) = y - (11/x)$ es igual a $1/k$. Si k es mayor que 20, exite un único punto $Q \in C$, correspondiente a una de las cúspides de $X_{ns}^{+}(11)$ y un intervalo I contenido en $U := \{\widetilde{P} \in C(\mathbb{R}) : t(\widetilde{P}) < 1/20\}$ tal que $P, Q \in I$ (lema 2.1 en [11]). Si ω es el diferencial invariante de C, entonces $\omega = dx/F_y = -dy/F_x$. Si f es una función en la curva, su diferencial, df, es igual a

$$df \;=\; f_x dx \,+\, f_y dy \;=\; (f_x F_y \,-\, f_y F_x)\; \omega \;.$$

Denotaremos con g al término entre paréntesis. Como P y Q pertenecen al intervalo I, podemos considerar que $\int_Q^P \omega$ es la integral de Q a P por un camino contenido en I. En I, el valor de $|g|$ se puede acotar por 1, y así

$$\left|\int_Q^P \omega\right| \;=\; \left|\int_0^{t(P)} \frac{dt}{g}\right| \leq |t(P)| \;.$$

Entonces, para algún entero m, tenemos la cota $|\lambda(P) - \lambda(Q) + m\Omega| \leq |t(P)|$. Por otra parte, como Q corresponde a una cúspide, $\lambda(Q) = (m'/11)\Omega$ para algún entero m' (ver lema 3.1 en [11]), y, al ser $1/t(P)$ un entero, la altura logarítmica $h_t(P)$ del punto P es igual a $-\log|t(P)|$. En definitiva, la siguiente cota es válida para cualquier punto P tal que $1/t(P)$ sea un entero mayor que 20.

$$\left|n\frac{\Omega}{11} \;-\; \lambda(P)\right| \;<\; \exp(13,56 - 3\widehat{h}(P)) \;.$$

El grupo $C(\mathbb{Q})$ es cíclico infinito, generado por $P_0 = (0, 0)$. Si P es un punto como los considerados en el párrafo anterior, $P = [m]P_0$. De esta igualdad se obtiene una cota superior sobre la forma lineal $n\Omega - m\lambda(11P_0)$. Por otro lado, por el hecho de que P_0 no es un punto de torsión de la curva, se puede obtener una cota inferior. Si $|m| \geq 12$, se deduce que $|m|$ debe estar acotado por una constante A. En principio, la cota dada por A no es suficiente, pero, se puede deducir que $|n\Omega - m\lambda(11P_0)| \leq 0,4\Omega/|m|$. En particular,

$$\left|\frac{n}{m} \;-\; \frac{\lambda(11P_0)}{\Omega}\right| \;<\; \frac{1}{2m^2} \;.$$

Calculando los valores de $\lambda(11P_0)$ y de Ω con precisión suficiente, se verifica que cualquier aproximaición p_k/q_k por fracciones continuas del cociente $\lambda(11P_0)/\Omega$, o bien no satisface $q_k < A$, o bien no satisface la cota superior sobre $|p_k\Omega - q_k\lambda(11P_0)|$. Se deduce que el

entero $|m|$ tiene que ser menor a 12. Luego se verifica que los únicos puntos $P = (x, y) = mP_0$ tales que $x/(xy - 11)$ es un número entero son aquellos para los que m es igual a -2, -1, 0, 1, 2, 3 o a 4.

Resta ver qué sucede si $k \leq 20$. En este caso, se verifica que $x/(xy - 11) = k$ tiene soluciones con $(x, y) \in C(\mathbb{Q})$, sólo si k es igual a 2, 0, -2, -6 o a -8. Los puntos que quedan determinados por este valor de k son los mismos que en el párrafo anterior: mP_0 con m como arriba.

Observación. Ya mencionamos que una particularidad de esta solución es que hace uso de una curva de género 1. Sin embargo, esto no quiere decir que los métodos utilizados para estudiar las curvas de género 0 no sean útiles en este caso. De hecho, en [2] se estudian las curvas $X_{ns}^+(21)$ de género 1 y $X_{ns}^+(16)$ y $X_{ns}^+(20)$ de género 2. Por último mencionamos que un estudio de las representaciones cuspidales de los grupos $\mathrm{GL}_2(\mathbb{F}_p)$ permite tratar la curva $X_{ns}^+(13)$ de género 3 y obtener una ecuación sobre $\mathbb{Q}$ para la misma [3].

Bibliografía

[1] B. Baran. *A Modular Curve of Level* 9 *and the Class Number One Problem.* Journal of Number Theory, 129 (2009), 715-728.

[2] B. Baran. *Normalizers of Non-split Cartan Subgroups, Modular Curves, and the Class Number One Problem.* Journal of Number Theory, 130 (2010), 2753-2772.

[3] B. Baran. *An Exceptional Isomorphism Between Modular Curves of Level* 13. Journal of Number Theory, 145 (2014), 273-300.

[4] J. Booher. *Modular Curves and the Class Number One Problem.*

[5] I. Chen. *On Siegel's Modular Curve of Level* 5 *and the Class Number One Problem.* Journal of Number Theory, 74 (1999), 278-297.

[6] D. A. Cox. *Primes of the Form* $x^2 + ny^2$*: Fermat, Class Field Theory, and Complex Multiplication.* Wiley, 1989.

[7] P. Deligne, M. Rapoport. *Les schémas de modules de courbes elliptiques.* Antwerp, 1972.

[8] F. Diamond, J. Shurman. *A First Course in Modular Forms.* Springer-Verlag New York, 2005.

[9] M. A. Kenku. *A Note on the Integral Points of a Modular Curve of Level* 7. Mathematika, 32 (1985), 45-48.

[10] G. Ligozat. *Courbes modulaires de niveau* 11. En J.-P. Serre, D. Zagier, eds. *Modular Functions of One Variable*, vol. V. Springer-Verlag New York, 1977.

[11] R. Schoof, N. Tzanakis. *Integral Points of a Modular Curve of Level* 11. Acta Arithmetica, 152 (2012), 39-49.

[12] R. J. Stroeker, N. Tzanakis. *Solving Elliptic Diophantine Equations by Estimating Linear Forms in Elliptic Logarithms*. Acta Arithmetica, 67 (1994), 177-196.

[13] J.-P. Serre. *Lectures on the Mordell-Weil Theorem*. 3^a ed. Vieweg+Teubner Verlag, 1997.