Rev.R.Acad.Cienc.Exact.Fis.Nat. (Esp)
Vol. 94, N.º 3, pp 383-390, 2000
Monográfico: Contribuciones al estudio algorítmico de problemas de moduli aritméticos

SOBRE LAS $\mathbb{Q}$-CURVAS ASOCIADAS A PUNTOS RACIONALES DE CURVAS COCIENTES DE $X_0(N)$[1]

($\mathbb{Q}$-curva/curva modular/función elíptica modular/involución de Atkin-Lehner)

J. GONZÁLEZ

Escola Universitària Politècnica de Vilanova i la Geltrú. Departament de Matemàtica Aplicada i Telemàtica. Av. Víctor Balaguer, s/n, 0880 Vilanova i la Geltrú, Spain. E-mail: josepg@mat.upc.es

RESUMEN

Ofrecemos métodos para parametrizar las $\mathbb{Q}$-curvas asociadas a los puntos racionales no cuspidales de las curvas de género ≤ 1 que son cocientes de las curvas modulares $X_0(N)$ por subgrupos propios del grupo de las involuciones de Atkin-Lehner, cuando N es libre de cuadrados.

ABSTRACT

We present a method which parametrizes the $\mathbb{Q}$-curves attached to non cusp rational points on the curves of genus ≤ 1 which are quotients of modular curves $X_0(N)$ by proper subgroups of the group of the Atkin-Lehner involutions, for N squarefree.

INTRODUCCIÓN

Una $\mathbb{Q}$-curva es una curva elíptica definida sobre $\overline{\mathbb{Q}}$ que es isógena a cada una de sus conjugadas por la acción del grupo de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. El interés sobre estas curvas ha aumentado notablemente después de que Ribet **[Ri 92]** haya demostrado que, bajo la conjetura $(3.2.4_?)$ de Serre **[Se 87]**, las $\mathbb{Q}$-curvas son las curvas elípticas obtenidas como cocientes de las jacobianas de las curvas modulares $X_1(N)$.

Elkies **[El 93]** ha demostrado que toda $\mathbb{Q}$-curva sin multiplicación compleja es isógena a una $\mathbb{Q}$-curva asociada a un punto racional no cuspidal de la curva $X^*(N) := X_0(N)/B(N)$ para un cierto entero $N \geq 1$ libre de cuadrados y donde $B(N)$ denota el grupo de las involuciones de Atkin-Lehner $\{w_d : d|N\}$.

En todo lo que sigue, $N > 1$ es un entero libre de cuadrados que tiene n divisores primos. Denotamos por g^* el género de $X^*(N)$ y por π^* la proyección natural de $X_0(N)$ en $X^*(N)$. Cuando $g^* \leq 1$, en **[Go-La 98]** se parametrizan los puntos no cuspidales de $X_0(N)$ que proporcionan puntos racionales de $X^*(N)$. Dicha parametrización se basa en la idea siguiente. Para cada divisor positivo $d|N$, designamos por $j_d(z) := j(z)|w_d = j(dz)$, en donde j designa la función modular elíptica. Se consideran las funciones simétricas elementales de las funciones $\{j_d\}_{d|N}$:

$$J_1 = \sum_{d|N} j_d, \ldots, J_{2^n} = \prod_{d|N} j_d,$$

y el polinomio en T:

$$J_N^*(T) := \prod_{d|N} (T - j_d) =$$

$$= T^{2^n} + \sum_{i=1}^{2^n} (-1)^i J_i T^{2^n - i} \in \mathbb{Q}\left(X^*(N)\right)[T].$$

Se determina un sistema mínimo de generadores de $\mathbb{Q}(X^*(N))$ sobre $\mathbb{Q}$, es decir uno o dos generadores dependiendo de que g^* sea 0 o bien >0. Cada una de las funciones J_i pertenece a $\mathbb{Q}(X^*(N))$ y, por lo tanto, es una función $\mathbb{Q}$-racional en dichos generadores. Los valores racionales de los generadores proporcionan $\mathbb{Q}$-curvas, cuyos j-invariantes satisfacen la relación algebraica $J_N^*(j) = 0$. Así, para cada morfismo $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ existe un entero positivo $d_\sigma|N$ tal que ${}^\sigma j = j_{d_\sigma}$ y d_σ es el grado de una isogenia existente entre una curva elíptica de invariante j y su conjugada por σ.

En el caso racional ($g^* = 0$), se determina un módulo principal F de $X^*(N)$ con un polo en $\pi^*(i\infty)$, tal que su desarrollo de Fourier en $q = e^{2\pi i z}$ es normalizado y tiene coeficientes enteros. En este caso, cada función J_i es un polinomio mónico en F con coeficientes enteros. Se obtiene así una parametrización de J_N^* en F:

$$J_N^* \in \mathbb{Z}[T, F].$$

[1] Este trabajo ha sido financiado parcialmente por la DGES, PB96-0970-C02-02.

En el caso elíptico ($g^* = 1$), se considera la curva elíptica E definida sobre $\mathbb{Q}$ que se obtiene al fijar el punto $\pi^*(i\infty)$ como origen en $X^*(N)$. Se determina su clase de $\mathbb{Q}$-isomorfía, que siempre tiene rango 1. También se determinan funciones $X,\ Y \in \mathbb{Q}(X^*(N))$ que satisfacen las ecuaciones de un modelo minimal de Weierstrass de E sobre $\mathbb{Q}$ y cuyo q-desarrollo de Fourier es normalizado. En este caso, las funciones $X,\ Y$ obtenidas tienen q-desarrollos de Fourier con coeficientes enteros y cada función J_i es un polinomio en $X,\ Y$ con coeficientes enteros. Se obtiene, ahora, una parametrización de J_N^* en X e Y:

$$J_N^* \in \mathbb{Z}[T,\ X,\ Y].$$

Los j-invariantes de las $\mathbb{Q}$-curvas correspondientes quedan parametrizados por los valores $(X,\ Y) \in E(\mathbb{Q})$.

Genéricamente, las parametrizaciones dadas en **[Go-La 98]** proporcionan los j-invariantes de $\mathbb{Q}$-curvas tales que $[\mathbb{Q}(j) : \mathbb{Q}] = \#B(N) = 2^n$. Ello es debido al hecho de que las extensiones $\mathbb{C}(X_0(N))/\mathbb{C}(X^*(N))$, $\mathbb{Q}(X_0(N))/\mathbb{Q}(X^*(N))$ son abelianas y su grupo de Galois es isomorfo a $B(N) \simeq \simeq (\mathbb{Z}/2\mathbb{Z})^n$. No obstante, para algunos valores racionales de los parámetros $\{F\}$ o $\{X,\ Y\}$, el polinomio $J_N^*(T)$ es $\mathbb{Q}$-reducible. Para estos casos especiales, la parametrización dada no es óptima. Por ejemplo, consideremos las $\mathbb{Q}$-curvas sin multiplicación compleja definidas sobre un cuerpo cuadrático y cuyo grado (de una isogenia con su conjugada) es 6. Sea F un módulo principal racional de $X^*(6)$. Para los valores racionales de F que determinan dichas $\mathbb{Q}$-curvas, el polinomio $J_6^*(T,\ F)$ descompone sobre $\mathbb{Q}$ en dos factores $(T - j_1)(T - j_6)$ y $(T - j_2)(T - j_3)$. La determinación directa de los valores racionales de F para los que $(T - j_1)(T - j_6) \in \mathbb{Q}[T]$ es complicada. Sin embargo, podemos parametrizar dichas $\mathbb{Q}$-curvas a través de un camino alternativo, utilizando el hecho de que estas curvas están asociadas a puntos racionales de la curva $X_0(6)/\langle w_6 \rangle$.

El propósito de este trabajo es proporcionar métodos para parametrizar los puntos no cuspidales de $X_0(N)$ que proporcionan puntos racionales de las curvas que son cocientes de $X_0(N)$ por subgrupos propios de $B(N)$ y tienen género ≤ 1. Tales puntos determinan puntos racionales de $X^*(N)$ y, por lo tanto, $\mathbb{Q}$-curvas cuya peculiaridad reside en el hecho de estar definidas en extensiones abelianas de $\mathbb{Q}$, con grupo de Galois isomorfo a un subgrupo propio de $B(N)$.

1. $\mathbb{Q}$-CURVAS ESPECIALES

Sea $B'(N)$ un subgrupo propio de $B(N)$. Denotamos por $X'(N) = X_0(N)/B'(N)$, por g' su género y por $\pi' : X_0(N) \longrightarrow \longrightarrow X'(N)$, $\pi'' : X'(N) \longrightarrow X^*(N) = X'(N)/(B(N)/B'(N)$ las proyecciones naturales. Tenemos el diagrama siguiente

$$X_0(N) \xrightarrow{\pi'} X'(N) \xrightarrow{\pi''} X^*(N),$$

con $\pi'' \circ \pi' = \pi^*$. Notemos que los puntos racionales de $X'(N)$ proporcionan puntos racionales de $X^*(N)$ y que $g^* \leq g'$. En particular, $g' \leq 1$ implica que $g^* \leq 1$.

Definición 1.1. *Diremos que un punto P no racional de $X_0(N)$ y sin multiplicación compleja es* especial *si existe un subgrupo propio $B'(N)$ de $B(N)$ tal que $\pi'(P) \in \in X'(N)(\mathbb{Q})$.*

Denominaremos $\mathbb{Q}$-curvas *especiales* de nivel N a las $\mathbb{Q}$-curvas asociadas a puntos especiales de $X_0(N)$. Genéricamente, los puntos racionales de $X'(N)$ proporcionarán j-invariantes de $\mathbb{Q}$-curvas tales que $\mathrm{Gal}(\mathbb{Q}(j)/\mathbb{Q})$ es isomorfo a $B'(N)$. No obstante, algunos puntos racionales de $X'(N)$ pueden provenir de puntos racionales de un cociente entre $X_0(N)$ y un subgrupo propio de $B'(N)$. Por ello, a cada punto especial $P \in X_0(N)$ le asociamos el subgrupo de $B(N)$:

$$B_P(N) = \bigcap_{\{B'(N) :\ \pi'(P) \in X'(N)(\mathbb{Q})\}} B'(N).$$

Es evidente que el punto P proporciona un punto racional en la curva $X_0(N)/B_P(N)$, también en $X^*(N)$, y que el conjunto $\mathcal{D}_P(N) = \{d|N : w_d \in B_P(N)\}$ coincide con el conjunto de los grados mínimos de las isogenias entre una $\mathbb{Q}$-curva asociada a P y sus conjugadas. En este caso, el cuerpo obtenido al adjuntar a $\mathbb{Q}$ el j-invariante de una $\mathbb{Q}$-curva asociada al punto P es una extensión abeliana de $\mathbb{Q}$ cuyo grupo de Galois es isomorfo al grupo $B_P(N)$.

Definición 1.2. *Diremos que un punto especial P de $X_0(N)$ es primitivo de nivel N si para todo divisor estricto $M|N$ el punto P, mediante la proyección natural*

$$X_0(N) \longrightarrow X_0(M) \longrightarrow X^*(M),$$

proporciona un punto no racional de $X^*(M)$.

Denominaremos $\mathbb{Q}$-curvas *especiales primitivas* de nivel N a aquellas $\mathbb{Q}$-curvas asociadas a puntos especiales de $X_0(N)$ que son primitivos.

Notemos que si tomamos $B'(6) = \langle w_6 \rangle$, los puntos especiales de $X_0(6)$ relativos a $B'(6)$ son primitivos. Sin embargo, si tomamos $B'(6) = \langle w_2 \rangle$, los puntos especiales de $X_0(6)$ relativos a $B'(6)$ no son primitivos, ya que sus proyecciones en $X^*(2)$ son puntos racionales. De hecho, un punto especial P de $X_0(N)$ es primitivo si y sólo si el mínimo común múltiplo de los enteros del conjunto $\mathcal{D}_P(N)$ es N. De manera más general, si el mínimo común múltiplo de los enteros del conjunto $\{d|N : w_d \in \in B'(N)\}$ es N entonces los puntos racionales de $X'(N)$ parametrizan genéricamente $\mathbb{Q}$-curvas especiales primitivas.

Cuando $g' \leq 1$, la filosofía que utilizaremos para parametrizar los puntos de $X_0(N)$ que proprocionan puntos racionales de $X'(N)$ es esencialmente la misma que la

usada con los puntos racionales de $X^*(N)$. Consideraremos las funciones simétricas elementales $\{J_1, \ldots, J_{2^m}\}$ de las funciones $\{j_d : w_d \in B'(N)\}$, donde $\#B'(N) = 2^m$, y mostraremos el método para calcular un sistema mínimo de generadores de $\mathbb{Q}(X'(N))$ así como las funciones $\mathbb{Q}$-racionales en estos generadores que proporcionan las funciones J_i. Para ello, determinamos, a continuación, las partes polares de las funciones J_i.

Dada una función G de $X_0(N)$ cuyo divisor es $\sum_j (P_j) - \sum_i (Q_i)$ con $P_i \neq Q_j$ para todo i, j, denotamos por $\mathrm{div}^-(G) = \sum_i (Q_i)$. Recordamos que las puntas de $X_0(N)$ quedan descritas por el conjunto $\{1/d : 0 < d|N\}$ y que el grupo $B(N)$ actúa transitivamente sobre éstas, mediante la acción $1/d' \mapsto 1/w_d(d')$, donde $w_d(d') := dd'/(d, d')^2$ (cf. **[Ogg 74]**).

Proposición 1.3. *Sean $J_1, \ldots, J_{2^m}$ las funciones simétricas elementales de las funciones $\{j_d : w_d \in B'(N)\}$. Sea $d'|N$ y denotemos por $r_{i,d'}$ la multiplicidad del polo que tiene la función J_i en la punta $1/d'$. Entonces,*

$$r_{i,d'} = \max\left\{ \sum_{k=1}^{i} \frac{N}{w_{d_k}(d')} : w_{d_k} \in B'(N),\ d_1 < \cdots < d_i \right\}.$$

Demostración. De las relaciones

$$\mathrm{div}^-(j) = \sum_{d'|N} \frac{N}{d'}\left(\frac{1}{d'}\right) \quad \text{y} \quad j|w_d = j_d,$$

obtenemos las igualdades

$$\mathrm{div}^-(j_d) = \sum_{d'|N} \frac{N}{d'}\left(\frac{1}{w_d(d')}\right) = \sum_{d'|N} \frac{N}{w_d(d')}\left(\frac{1}{d'}\right) \quad \text{para cada } d|N.$$

La proposición es una consecuencia inmediata de estas igualdades. □

Finalmente, notamos que si $B(N)$ tiene un subgrupo propio, necesariamente N es un número compuesto y, en este caso, el grupo de Newman de $X_0(N)$ (cf. **[Go 91]**) es un grupo libre de rango >2. Las funciones de este grupo juegan un papel esencial en los métodos que mostramos en este artículo.

2. PARAMETRIZACIONES RACIONALES DE $\mathbb{Q}$-CURVAS ESPECIALES

Como en la sección anterior, $B'(N)$ es un subgrupo propio de $B(N)$, con $\#B(N) = 2^n$ y $\#B'(N) = 2^m$. La proposición siguiente se utilizará para la parametrización de las $\mathbb{Q}$-curvas asociadas a los puntos racionales de $X'(N)$ cuando $g' = 0$.

Proposición 2.1. *Supongamos que $X'(N) = X_0(N)/B'(N)$ es de género 0. Sea F un módulo principal de $X'(N)$ con un polo en $\pi'(i\infty)$ y tal que su q-desarrollo de Fourier es normalizado y con coeficientes enteros. Para cada función $J \in \mathbb{Q}(X_0(N))$ que es invariante por $B'(N)$ y que tiene polos únicamente en las puntas, existen enteros $k_2, k_3, \ldots, k_{2^{n-m}}$ independientes de J y enteros $r_2, r_3, \ldots, r_{2^{n-m}} \geq 0$ (dependientes de J) tales que*

$$J \prod_{j=2}^{2^{n-m}} (F - k_j)^{r_j} = P(F), \quad \text{con} \quad P(X) \in \mathbb{Q}[X].$$

Demostración. Denotamos por $[1/d]$ la órbita de $1/d$ bajo la acción de $B'(N)$. Sean $\{1/q_1, \ldots, 1/q_{2^{n-m}}\}$ un sistema de respresentantes de las órbitas de las puntas de $X_0(N)$. Ya que J es invariante por $B'(N)$, se tiene que

$$\mathrm{div}^-(J) = \sum_{j=1}^{2^{n-m}} r_j \left(\sum_{1/d \in [1/q_j]} \left(\frac{1}{d}\right)\right), \quad r_j \geq 0.$$

Supongamos que $[1/q_1]$ es la órbita de $i\infty$. Para cada $q_j \neq q_1$ existe un módulo principal F_j de $X'(N)$ normalizado tal que su divisor en $X'(N)$ es $\mathrm{div}\, F_j = (\pi'(1/q_j)) - (\pi'(1/q_1))$. Por lo tanto, $F_j = F - k_j$ para un cierto $k_j \in \mathbb{C}$. Ya que N no es primo, las funciones F_j pueden ser elegidas en el grupo de Newman de $X_0(N)$. Por lo tanto, el desarrollo de Fourier de F_j es normalizado, con coeficientes enteros y, por consiguiente, $k_j \in \mathbb{Z}$.

La función $J \prod_{j=2}^{2^{n-m}} (F - k_j)^{r_j}$ es una función de $X'(N)$ con un único polo en $\pi'(i\infty)$ y, en consecuencia, es un polinomio en F, $P(F)$. Los coeficientes de P son racionales debido a la racionalidad de los coeficientes de Fourier de F y J. Si J tiene un q-desarrollo normalizado y entero, entonces P es mónico y $P(X) \in \mathbb{Z}[X]$. □

Los casos genéricos correspondientes a $\mathbb{Q}$-curvas especiales primitivas de nivel N tales que $g' = 0$ son mostrados en la tabla 1 del apéndice. A continuación, damos dos ejemplos en los que aplicamos las proposiciones 1.3 y 2.1.

2.2. Parametrización de $\mathbb{Q}$-curvas cuadráticas de grado 6

Sea $X_0(6)$ y consideremos el subgrupo $B'(6) = \langle w_6 \rangle$ de $B(6)$. Como antes, escribimos $J_1 := j_1 + j_6$ y $J_2 := j_1 j_6$. Sea F la función de $X_0(6)$ dada por

$$F(z) = \frac{\eta(2z)^{12}\eta(3z)^{12}}{\eta(z)^{12}\eta(6z)^{12}},$$

donde η denota la función de Dedekind. La función F es invariante por $B'(6)$ y es un módulo principal de $X'(6)$, ya que su divisor en $X_0(6)$ es $(1/2) + (1/3) - (1/1) - (1/6)$. Por lo tanto, tenemos que

$$J_1 F^3 = P_1(F), \quad J_2 F^5 = P_2(F),$$

donde P_1, P_2 son polinomios de grados 9 y 12 respectivamente. Utilizando los desarrollos de Fourier de J_1, J_2 y F, se obtiene:

$$P_1 = 1 - 35X + 174X^2 + 1.464X^3 - 4.823X^4 + 31.878X^5 - \\ - 14.280X^6 + 1.692X^7 - 72X^8 + X^9,$$

$$P_2 = (1 + X)^3(1 - 21X + 219X^2 + X^3)^3.$$

Por lo tanto, los j-invariantes de las $\mathbb{Q}$-curvas cuadráticas de grado 6 satisfacen la ecuación:

$$j^2 - \frac{P_1(F)}{F^3} j + \frac{P_2(F)}{F^5} = 0,$$

para un cierto valor racional no nulo de F. Notemos que el valor $F = 0$ parametriza las puntas 1/2, 1/3 de $X_0(6)$.

2.3. Resolución explícita de la extensión $\mathbb{Q}(X_0(30))/\mathbb{Q}(X^*(30))$

La curva $X_0(30)$ tiene género 3, es hiperelíptica y w_{15} es su involución hiperelíptica (cf. **[Ogg 74]**). El grupo de Galois de la extensión $\mathbb{Q}(X_0(30))/\mathbb{Q}(X^*(30))$ es isomorfo a $B(30) \simeq (\mathbb{Z}/2\mathbb{Z})^3$. Tenemos la siguiente cadena de extensiones de grado 2:

$$\mathbb{Q}(X^*(30)) = \mathbb{Q}(X_0(30))^{B(30)} \subset \mathbb{Q}\,(X_0(30))^{\langle w_3,\, w_{15}\rangle} \subset \\ \subset \mathbb{Q}\,(X_0(30))^{\langle w_{15}\rangle} \subset \mathbb{Q}\,(X_0(30)).$$

Sea t un módulo principal de $X^*(30)$ definido sobre $\mathbb{Q}$. Entonces, se tiene que $\mathbb{Q}(X^*(30)) = \mathbb{Q}(t)$ y $\mathbb{Q}(X_0(30)) = \mathbb{Q}(t)(j)$. La extensión $\mathbb{Q}(X_0(30))/\mathbb{Q}(X^*(30))$ queda determinada por el polinomio de grado 8 en T,

$$J^*_{30}(T) = \prod_{d|30}(T - j_d) \in \mathbb{Q}(t)\,[T].$$

Queremos determinar las ocho raíces de $J^*_{30}(T)$ en función de t, a través de las sucesivas extensiones de grado 2.

La extensión $\mathbb{Q}(X_0(30))/\mathbb{Q}(X_0(30))^{\langle w_{15}\rangle}$. La involución w_{15} es la involución hiperelíptica de $X_0(30)$. Las funciones de $X_0(30)$

$$r = \frac{\eta(z)\eta(6z)^2\eta(10z)^2\eta(15z)}{\eta(2z)^2\eta(3z)\eta(5z)\eta(30z)^2},$$

$$G_1 = \frac{\eta(z)^2\eta(6z)\eta(10z)^2\eta(15z)^2}{\eta(2z)^2\eta(3z)\eta(5z)\eta(30z)^2},$$

$$G_2 = \frac{\eta(3z)\eta(5z)}{\eta(2z)\eta(30z)}$$

son invariantes por w_{15} y sus divisores son respectivamente:

$$\left(\frac{1}{6}\right) + \left(\frac{1}{10}\right) - \left(\frac{1}{2}\right) - \left(\frac{1}{30}\right), \quad \left(\frac{1}{1}\right) + \left(\frac{1}{15}\right) - \left(\frac{1}{2}\right) - \left(\frac{1}{30}\right), \\ \left(\frac{1}{3}\right) + \left(\frac{1}{5}\right) - \left(\frac{1}{2}\right) - \left(\frac{1}{30}\right).$$

Por lo tanto, r, G_1 y G_2 son módulos principales de $X_0(30)/\langle w_{15}\rangle$ y difieren entre ellos en una constante aditiva, ya que los tres tienen un polo simple en el mismo punto $\pi'(i\infty)$ y q-desarrollos de Fourier normalizados. Utilizando sus desarrollos de Fourier, obtenemos $G_1 = r - 1$ y $G_2 = r + 1$.

Como r es un módulo principal de $X_0(30)/\langle w_{15}\rangle$, tenemos que $\mathbb{Q}(X_0(30))^{\langle w_{15}\rangle} = \mathbb{Q}(r)$. Ya que $\mathbb{Q}(X_0(30)) = \mathbb{Q}(r)(j)$, la extensión queda determinada por el polinomio en T:

$$(T - j_1)(T - j_{15}).$$

Las funciones $J_1 = j_1 + j_{15}$, $J_2 = j_1 j_{15}$ tienen parte polar

$$\mathrm{div}^-(J_1) = 30\left(\left(\frac{1}{1}\right) + \left(\frac{1}{15}\right)\right) + 10\left(\left(\frac{1}{3}\right) + \left(\frac{1}{5}\right)\right) + \\ + 5\left(\left(\frac{1}{6}\right) + \left(\frac{1}{10}\right)\right) + 15\left(\left(\frac{1}{2}\right) + \left(\frac{1}{30}\right)\right),$$

$$\mathrm{div}^-(J_2) = 32\left(\left(\frac{1}{1}\right) + \left(\frac{1}{15}\right)\right) + 16\left(\left(\frac{1}{3}\right) + \left(\frac{1}{5}\right)\right) + \\ + 8\left(\left(\frac{1}{6}\right) + \left(\frac{1}{10}\right)\right) + 16\left(\left(\frac{1}{2}\right) + \left(\frac{1}{30}\right)\right).$$

Por lo tanto,

$$J_1(r-1)^{30}(r+1)^{10}r^5 = P_1(r), \quad J_2(r-1)^{32}(r+1)^{16}r^8 = P_2(r),$$

donde P_1 y P_2 son polinomios fácilmente computables de grados 60 y 72 respectivamente. Por razones obvias de espacio omitimos sus descripciones explícitas. La extensión queda definida mediante la ecuación

$$j^2 - \frac{P_1(r)}{(r-1)^{30}(r+1)^{10}r^5} j + \frac{P_2(r)}{(r-1)^{32}(r+1)^{16}r^8} = 0.$$

El discriminante obtenido de esta ecuación de segundo grado es de la forma siguiente:

$$(-1 + r + r^2)(-1 + 4r + r^2)(1 - r + 2r^2 + r^3 + r^4)\left(\frac{P(r)}{(r-1)^{30}(r+1)^{10}r^5}\right)^2,$$

con $P(X) \in \mathbb{Z}[X]$. Notemos que los valores racionales de $r \neq -1, 0, 1$ parametrizan (genéricamente) puntos especiales no primitivos de $X_0(30)$ que tienen asociados $\mathbb{Q}$-curvas cuadráticas de grado 15. Los valores $r = 0, \pm 1$ parametrizan todas las puntas de $X_0(30)$ diferentes de 1/2, 1/30.

La extensión $\mathbb{Q}(X_0(30))^{\langle w_{15}\rangle}/\mathbb{Q}(X_0(30))^{\langle w_3, w_{15}\rangle}$. La acción de las involuciones de Atkin-Lehner en el grupo de Newman de $X_0(N)$ está descrita en **[Go 91]**. Se comprueba fácilmente que $r|w_3 = -1/r$. Por lo tanto, $s = = r - 1/r$ es un módulo principal de $X_0(30)/\langle w_3, w_{15}\rangle$ y $\mathbb{Q}(X_0(30))^{\langle w_3, w_{15}\rangle} = \mathbb{Q}(s)$. La ecuación $r^2 - rs - 1 = 0$ define la extensión en cuestión. Genéricamente, los valores racionales no nulos de s parametrizan puntos especiales no primitivos de $X_0(30)$ que tienen asociados $\mathbb{Q}$-curvas bicuadráticas de grados los divisores de 15.

La extensión $\mathbb{Q}(X_0(30))^{\langle w_3, w_{15}\rangle}/\mathbb{Q}(X^*(30))$. La función del grupo de Newman de $X_0(30)$:

$$F(z) = \frac{\eta(z)\eta(3z)\eta(5z)\eta(15z)}{\eta(2z)\eta(6z)\eta(10z)\eta(30z)}$$

es una función invariante por $\langle w_3, w_{15}\rangle$. Un sencillo cálculo muestra que $F|w_{30} = 4/F$. Calculando su divisor, se obtiene que F es un módulo principal de $X_0(30)/\langle w_3, w_{15}\rangle$ con un polo en la proyección de $i\infty$. Por lo tanto, $F - s \in \mathbb{Z}$. Mediante los desarrollos de Fourier de F y s, obtenemos $F = s$. En consecuencia, $t = s + 4/s$ es un módulo principal de $X^*(30)$. La ecuación de la extensión es $s^2 - st + 4 = 0$. Ahora, los valores racionales de s parametrizan, genéricamente, $\mathbb{Q}$-curvas tricuadráticas de grados los divisores de 30.

Resolución:

Las relaciones siguientes:

$$s = \frac{t \pm \sqrt{t^2 - 16}}{2}, \quad r = \frac{s \pm \sqrt{s^2 + 4}}{2},$$

$$\sqrt{s^2 + 4} = \sqrt{t(t+4)}\left(1 \pm \frac{\sqrt{t^2 - 16}}{t + 4}\right),$$

$$(-1 + r + r^2)(-1 + 4r + r^2)(1 - r + 2r^2 + r^3 + r^4) =$$
$$= r^4 s^2 (t + 5)(t + 1),$$

permiten parametrizar explícitamente en t las ocho soluciones de j y a la vez mostrar $\mathbb{Q}(t, j)$ como la composición de las tres extensiones cuadráticas de $\mathbb{Q}(t)$:

$$\mathbb{Q}(t)\left(\sqrt{t^2 - 16}\right), \quad \mathbb{Q}(t)\left(\sqrt{t(t+4)}\right), \quad \mathbb{Q}(t)\left(\sqrt{(t+5)(t+1)}\right).$$

3. PARAMETRIZACIONES ELÍPTICAS DE $\mathbb{Q}$-CURVAS ESPECIALES

Sea, ahora, $B'(N)$ un subgrupo propio de $B(N)$ tal que $g' = 1$. En particular, $g^* \leq 1$. Si $g^* = g' = 1$, las curvas elípticas $E = \left(X^*(N), \pi(i\infty)\right)$ y $E' = \left(X'(N), \pi'(i\infty)\right)$ son $\#B(N)/B'(N)$-isógenas. En este caso, todos los puntos no racionales y sin multiplicación compleja de $X_0(N)$ que proporcionan puntos racionales en $X^*(N)$ son especiales. Esta situación sólo se produce cuando $N = 65$ y $B'(65) = \langle w_{65}\rangle$.

Los casos correspondientes a $\mathbb{Q}$-curvas especiales genéricamente primitivas de nivel N tales que $g' = 1$ son mostrados en la tabla 2 del apéndice. En la tabla 3 se muestra que si $g' = 1$ y $g^* = 0$, entonces el rango de la curva elíptica $\left(E', \pi'(i\infty)\right)$ es cero. Por lo tanto, en este caso el conjunto de los correspondientes puntos especiales y primitivos es finito.

Para parametrizar los puntos de $X_0(N)$ que proporcionan puntos racionales de $X'(N)$, procederemos siguiendo los pasos que describimos a continuación.

Paso 1: Determinación del conductor de E'

El método para determinar el conductor de E' y su clase de $\mathbb{Q}$-isogenia es el siguiente. Puesto que el género de $X'(N)$ es 1, existe una única forma $f \in S_2\left(\Gamma_0(N)\right)$ normalizada, vector propio de los operadores de Hecke T_p, $p \nmid N$, e invariante por $B'(N)$. Para cada divisor $d|N$, la forma modular f determina el valor propio de f, $\varepsilon(d)$, bajo la acción de la involución w_d ($w_1 :=$ Id) en $S_2\left(\Gamma_0(N)\right)$. Notemos que $\varepsilon(d) = 1$ para cada $w_d \in B'(N)$. Si f es una forma nueva, entonces el conductor de E' es N. En caso contrario, determinamos el único entero $N'|N$ para el que existe una forma $h \in S_2\left(\Gamma_0(N')\right)$, normalizada, vector propio de todos los operadores de Hecke y satisfaciendo:

$$h|w_{d'} = \varepsilon(d')h, \quad \text{para todo } d'|N'.$$

El conductor de E' es N'. La relación de la forma f con la forma h es la siguiente. Dado un primo $\ell|N/N'$, la forma normalizada $h(q) + \varepsilon(\ell)\ell h(q^\ell) \in S_2\left(X_0(\ell N')\right)$ es un vector propio de los operadores de Hecke T_p, $p \nmid \ell N'$, y también de cada involución $w_{d'}$, $d'|\ell N'$, con valor propio $\varepsilon(d')$. Así, obtenemos que

$$f(q) = \sum_{d|N/N'} \varepsilon(d) d h(q^d).$$

Notemos que la forma h es única y ésta, a su vez, determina la forma f y la curva elíptica E', salvo $\mathbb{Q}$-isogenias.

Paso 2: Relación entre el invariante diferencial de E' y la forma f

Sea F una curva elíptica definida sobre $\mathbb{Q}$ dada por una ecuación minimal y cuya clase de $\mathbb{Q}$-isogenia es la de E'; denotamos por ω_F el invariante diferencial de F. Denotamos por E una curva como F, tal que $\phi : X_0(N') \to E$ es una parametrización fuerte de Weil. Para los valores N que se nos presentan, es conocido que:

i) E' no tiene multiplicación compleja.

ii) La constante de Manin relativa a E es ± 1. Es decir, $\phi^*(\omega_E) = \pm h$.

iii) Si $\phi_F : F \to E$ es una isogenia cíclica, entonces $\phi_F{}^*(\omega_E) = c(F)\,\omega_F$ donde $c(F)$ es un entero que divide al grado de ϕ_F. Ya que E' no tiene multi-

plicación compleja, el conjunto de las isogenias de F en E coincide con el conjunto $\{[m]\phi_F : m \in \mathbb{Z}\}$. Notemos que si $\mu = [m]\phi_F$ entonces $\mu^*(\omega_E) = c\omega_F$, con $c = mc(F) \in \mathbb{Z}$.

La siguiente proposición muestra la relación entre la forma modular f y el invariante diferencial de E'.

Proposición 3.1. *Sea* $R(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$ *tal que* $R(x, y) = 0$ *es un modelo minimal de* E' *sobre* $\mathbb{Q}$. *Sean* X, Y *funciones de* $X_0(N)$ *invariantes por* $B'(N)$, *regulares fuera de* $\pi'(i\infty)$ *y tales que* $R(X, Y) = 0$. *Sean* $f \in S_2(\Gamma_0(N))$ *como antes y* $\omega_{E'} = dX/(2Y + a_1X + a_3)$ *el invariante diferencial de* E'. *Entonces* $\pi'^*(\omega_{E'}) = \pm f(q)dq/q$.

Demostración. Como antes N' es el conductor de E', $\{\varepsilon(d)\}_{d|N}$ son los valores propios de f bajo la acción de las involuciones $\{w_d\}_{d|N}$ y h es la forma de $S_2(X_0(N'))$ tal que $f = \sum_{d|N/N'} \varepsilon(d)h|w_d$. Denotamos por $\mathrm{pr} : X_0(N) \to X_0(N')$ la proyección natural y por $\phi : X_0(N') \to E$ la parametrización fuerte de Weil correspondiente a la clase de $\mathbb{Q}$-isogenia de E'. Como es habitual, $J_0(N)$ y $J_0(N')$ son las jacobianas de $X_0(N)$ y $X_0(N')$ respectivamente. Fijamos la punta del infinito para sumergir $X_0(N)$ y $X_0(N')$ en sus respectivas jacobianas.

Sea W el endomorfismo de $J_0(N)$ definido por:

$$W = \sum_{d|N/N'} \varepsilon(d)w_d = \prod_{p|N/N'} (\mathrm{Id} + \varepsilon(p)w_p).$$

Designamos por Φ la composición de los siguientes morfismos

$$J_0(N) \xrightarrow{W} J_0(N) \xrightarrow{\mathrm{pr}_*} J_0(N') \xrightarrow{\phi_*} E.$$

Notemos que $\Phi^*(\omega_E) = \pm f$, ya que la constante de Manin relativa a E es ± 1 y $W^*(h) = f$.

Primero, demostraremos que Φ es invariante por $B'(N)$, es decir que $\Phi \circ w = \Phi$ para toda involución $w \in B'(N)$. Sean $p_1, \ldots, p_k$ los primos que dividen N'. Consideremos el endomorfismo de $J_0(N)$:

$$\mathrm{w} = \prod_{i=1}^{k} (\mathrm{Id} + \varepsilon(p_i)\mathrm{w}_{p_i}).$$

Cada endomorfismo $\mathrm{Id} + \varepsilon(p_i)w_{p_i}$ es también un endomorfismo de $J_0(N')$ y actúa sobre la forma h duplicándola. Como las acciones de w_{p_i} en $J_0(N)$ y $J_0(N')$ son compatibles con la proyección pr_*, se obtiene

$$\Phi \circ [2^k] = \Phi \circ \prod_{i=1}^{k} (\mathrm{Id} + \varepsilon(p_i)w_{p_i}) = \phi_* \circ \mathrm{pr}_* \circ \prod_{p|N} (\mathrm{Id} + \varepsilon(p)w_p).$$

Puesto que el endomorfismo $\prod_{p|N}(\mathrm{Id} + \varepsilon(p)w_p) = \sum_{d|N} \varepsilon(d)w_d$ es invariante por $B'(N)$, también lo es Φ. En consecuencia, el morfismo Φ factoriza a través de π'_* y, por lo tanto, existe una isogenia $\mu : E' \to E$ tal que $\Phi = \mu \circ \pi'_*$. Por un lado, tenemos que $\Phi^*(\omega_E) = \pm f$ y que $\mu^*(\omega_E) = \mathrm{c}\omega_{E'}$ con $c \in \mathbb{Z}$. Por otro lado, con los argumentos usados en la proposición 2 de **[Ed 91]**, se obtiene que $\pi'_*(\omega_{E'}) = c'f$ con $c' \in \mathbb{Z}$. Se sigue que $c \cdot c' = \pm 1$ y, por lo tanto, $c' = \pm 1$. □

Conocida la clase de $\mathbb{Q}$-isomorfía de $E' = (X'(N), \pi'(\mathrm{i}\infty))$, elegiremos un modelo minimal $R(x, y) = 0$ de E' sobre $\mathbb{Q}$. Las relaciones:

$$R(X, Y) = 0, \quad X = \frac{1}{q^2} + \sum_{n \geq -1} b_n q^n, \quad Y = 1/q^3 + \sum_{n \geq -1} c_n q^n,$$

$$Y = -\left(\frac{qdX/dq}{f} + a_1X + a_3\right)/2, \quad (*)$$

determinan recursivamente los valores b_n y c_n. En todos los casos, los coeficientes b_n y c_n obtenidos son enteros.

Paso 3: Determinación de la clase de $\mathbb{Q}$-isomorfía de E'

Proposición 3.2. *Con la misma notación que en la proposición* 3.1, *sea una función* $G \in \mathbb{Q}(X_0(N))$, *invariante por* $B'(N)$, *con q-desarrollo de Fourier con coeficientes enteros y que, mirada como función de* $X'(N)$, *tenga un único polo en* $\pi'(i\infty)$. *Entonces, existe un polinomio* $P(U, V) \in \mathbb{Z}[U, V]$ *tal que* $G = P(X, Y)$.

Demostración. Por el teorema de Riemann-Roch, tenemos que toda función de la curva elíptica E' con un único polo en el origen es un polinomio en las funciones X, Y con coeficientes en $\mathbb{C}$. En nuestro caso, los coeficientes son enteros debido al hecho de que los q-desarrollos de Fourier de G, X e Y tienen coeficientes enteros y los de X e Y son normalizados. □

Determinamos la clase de $\mathbb{Q}$-isomorfía de E' como sigue. Utilizando la relaciones $(*)$, calculamos los q-desarrollos de Fourier de X e Y para cada posible clase de $\mathbb{Q}$-isomorfía en la clase de $\mathbb{Q}$-isogenia de E'. Elegimos una función G del grupo de Newman de $X_0(N)$ como en la proposición anterior y descartamos aquellas clases de $\mathbb{Q}$-isomorfía para las que G no es un polinomio en X e Y.

Paso 4: Cálculo de las $\mathbb{Q}$-curvas parametrizadas por $E'(\mathbb{Q})$

Suponemos conocida la clase de $\mathbb{Q}$-isomorfía de E'. Para determinar las funciones racionales en X e Y que proporcionan las funciones $J_1, \ldots, J_{2^m}$, procederemos como sigue. Para cada una de las puntas de $X'(N)$ distinta de $\pi'(i\infty)$, elegimos una función G_k, $1 \leq k \leq 2^{n-m}$, del grupo de Newman de $X_0(N)$ que sea invariante por $B'(N)$, con un único polo en $\pi'(i\infty)$ y con un único cero en dicha punta.

Calculamos los menores enteros positivos $\{n_{k,i}\}$ tal que $J_i \prod_k G_k^{n_{k,i}}$ tiene un único polo en $\pi'(i\infty)$. Por consiguiente, existe un polinomio $Q_i(U, V) \in \mathbb{Z}[U, V]$, fácilmente computable, tal que $J_i \prod_k G_k^{n_{k,i}} = Q_i(X, Y)$. Substituyendo cada G_k por el polinomio correspondiente en X e Y, $P_k(X, Y)$, obtenemos

$$J_i = \frac{Q_i(X, Y)}{\prod_k P_k(X, Y)^{n_{k,i}}}.$$

A continuación, damos un ejemplo que muestra el procedimiento descrito.

3.3. Parametrización de $\mathbb{Q}$-curvas cuadráticas de grado 22

Consideremos la curva modular $X_0(22)$, que tiene género 2, y el subgrupo $B'(22) = \langle w_{22} \rangle$ de $B(22)$. La curva $X'(22) = X_0(22)/B'(22)$ tiene género 1. Con la notación anterior, se comprueba que $f|w_2 = f|w_{11} = -f$ y $\dim S_2(X_0(22))^{\text{new}} = 0$. Sea $h \in S_2(X_0(11))^{\text{new}}$ tal que $h|w_{11} = -h$. Entonces $f(q) = h(q) - 2h(q^2)$.

Existe una única clase de $\mathbb{Q}$-isogenia de conductor 11 que contiene tres clases de $\mathbb{Q}$-isomorfía. Con la notación de **[Cr 92]**, éstas son A1, A2, A3. Tenemos que identificar cual de estas clases coincide con $E' = (X'(N), \pi'(i\infty))$. Sean X, Y funciones de $X_0(22)$ invariantes por w_{22} tal que $R(X, Y) = 0$, donde $R(x, y) = 0$ es un modelo minimal de E'. Para cada posible clase de $\mathbb{Q}$-isomorfía y utilizando las relaciones $(*)$, obtenemos para X e Y:

clase	X	Y
A1	$1/q^2 + 4/q + 13 + 33q + \quad 80q^2 + \cdots$	$1/q^3 + 6/q^2 + 25/q + 83 + \quad 242q + \cdots$
A2	$1/q^2 + 4/q + 13 + 33q + 1642q^2 + \cdots$	$1/q^3 + 6/q^2 + 25/q + 83 - 1320q + \cdots$
A3	$1/q^2 + 4/q + 13 + 33q + \quad 78q^2 + \cdots$	$1/q^3 + 6/q^2 + 25/q + 83 + \quad 244q + \cdots$

La función

$$G(z) = \frac{\eta(2z)^{12}\eta(11z)^{12}}{\eta(z)^{12}\eta(22z)^{12}}$$

es una función de $X_0(22)$ invariante por w_{22} y su divisor es $5(1/2) + 5(1/11) - 5(1/1) - 5(1/22)$. Por lo tanto, G es un polinomio en X e Y. Sólo en el caso A3 se satisface esta condición, mediante la igualdad $G = XY + 2X^2 - 2X + 1$. Por lo tanto, E' corresponde a la clase A3. El orden de su grupo de torsión es 5 y $R(x, y) = y^2 + y - x^3 + x^2$. Como tenemos

$$\text{div}^-(j_1 + j_{22}) = 11(1/2) + 11(1/11) + 22(1/1) + 22(1/22),$$

$$\text{div}^-(j_1 j_{22}) = 13(1/2) + 13(1/11) + 23(1/1) + 23(1/22),$$

entonces $(j_1 + j_{22})G^3 = P_1(X, Y)$, $(j_1 j_{22})G^3 = P_2(X, Y)$, con $P_1(U, V)$, $P_2(U, V) \in \mathbb{Z}[U, V]$. Para los valores $(x, y) \in E'[\mathbb{Q}]$ que no provienen de puntas, los invariantes de las $\mathbb{Q}$-curvas asociadas satisfacen la ecuación:

$$j^2 - \frac{P_1(x, y)}{(xy + 2x^2 - 2x + 1)^3} j + \frac{P_2(x, y)}{(xy + 2x^2 - 2x + 1)^3} = 0,$$

Los puntos racionales de E' distintos de su origen son $\{(0, 0), (0, -1), (1, 0), (1, -1)\}$. El punto $(1, -1)$ parametriza las puntas $\{1/2, 1/11\}$, ya que éstas son ceros de G. Los tres restantes puntos racionales de torsión anulan el discriminante de la ecuación de segundo grado. El punto $(0, 0)$ proporciona el invariante $j = 8000$, mientras que los puntos $(0, -1)$ y $(1, 0)$ proporcionan el mismo invariante $j = -3375$. Por lo tanto, no existen $\mathbb{Q}$-curvas cuadráticas de grado 22 sin multiplicación compleja.

Para finalizar, en la tabla 3 del apéndice ofrecemos los resultados obtenidos para las parametrizaciones elípticas de $\mathbb{Q}$-curvas especiales y primitivas génericamente cuadráticas. En ella, puede observarse que sólo un punto racional ha parametrizado $\mathbb{Q}$-curvas cuadráticas sin multiplicación compleja cuando $N = 119$ y $B'(N) = \langle w_{119} \rangle$.

4. APÉNDICE

Tabla 1. Casos genéricamente primitivos con $g' = 0$

Casos cuadráticos:

N	6	10	14	15	21	26	35	39

con $B'(N) = \langle w_N \rangle$.

Casos bicuadráticos:

N	30	30	30	42	42	70	78
$B'(N)$	$\langle w_2, w_{15} \rangle$	$\langle w_5, w_6 \rangle$	$\langle w_6, w_{15} \rangle$	$\langle w_3, w_{14} \rangle$	$\langle w_6, w_{14} \rangle$	$\langle w_{10}, w_{14} \rangle$	$\langle w_6, w_{26} \rangle$

Tabla 2. Casos genéricamente primitivos con $g' = 1$

N' es el conductor de la curva elíptica $E' = (X_0(N)/B'(N), \pi'(i\infty))$.

Casos cuadráticos:

N	22	30	33	34	38	51	55	65	95	119
N'	11	15	11	17	19	17	11	65	19	17

con $B'(N) = \langle w_N \rangle$.

Casos bicuadráticos:

N	30	42	42	66	70	70	78	78	105	105	105	110	110
N'	15	14	21	11	14	35	26	39	15	15	105	11	55

con $B'(N) = \langle w_3, w_{10} \rangle$, $\langle w_2, w_{21} \rangle$, $\langle w_7, w_6 \rangle$, $\langle w_2, w_{33} \rangle$, $\langle w_2, w_{35} \rangle$, $\langle w_5, w_{14} \rangle$, $\langle w_2, w_{39} \rangle$, $\langle w_3, w_{26} \rangle$, $\langle w_3, w_{35} \rangle$, $\langle w_5, w_{21} \rangle$, $\langle w_{15}, w_{21} \rangle$, $\langle w_2, w_{55} \rangle$, $\langle w_{11}, w_{10} \rangle$, respectivamente.

Tabla 3. Casos genéricamente primitivos y cuadráticos con $g' = 1$, $g^* = 0$

N' es el conductor de $E' = (X_0(N)/B'(N), \pi'(i\infty))$,

cl es la clase de E' en la terminología de Cremona,

T es el cardinal del subgrupo de puntos de torsión del grupo de Mordell-Weil,

np es el número de puntas en $X'(N)$,

j son los f-invariantes de las $\mathbb{Q}$-curvas parametrizadas por los puntos racionales no cuspidales de $X'(N)$.

N	$B'(N)$	N'	cl	T	np	j
22	$\langle w_{22}\rangle$	11	A3	5	2	8000, −3375
30	$\langle w_{30}\rangle$	15	A8	4	4	—
33	$\langle w_{33}\rangle$	11	A3	5	2	8000, −32768
34	$\langle w_{34}\rangle$	17	A4	4	2	1728, 8000
38	$\langle w_{38}\rangle$	19	A3	3	2	8000
51	$\langle w_{51}\rangle$	17	A4	4	2	8000
55	$\langle w_{55}\rangle$	11	A3	5	2	−32768, −884736
95	$\langle w_{95}\rangle$	19	A3	3	2	−884736
119	$\langle w_{119}\rangle$	17	A4	4	2	-884736, $-884736 \pm \sqrt{-154039006}$

REFERENCIAS

1. **[Cr 92]** Cremona, J. E. (1992), Algorithms for modular elliptic curves, *Cambridge Univ. Press.*
2. **[Ed 91]** Edixhoven, J. B. (1991), On the Manin constants of modular elliptic curves, *Progr. Math.*, **89**, 25-39.
3. **[El 93]** Elkies, N. (1993), Remarks on elliptic K-curves. Preprint.
4. **[Go 91]** González, J. (1991), Equations of hyperelliptic modular curves, *Ann. Inst. Fourier,* **41**, 779-795.
5. **[Go-La 98]** González, J. & Lario, J. C. (1998), Rational and Elliptic Parametrizations of $\mathbb{Q}$-curves, *J. Number Theory,* **72**, 13-31.
6. **[Ogg 74]** Ogg, A. P. (1974), Hyperelliptic Modular Curves, *Bull. Soc. Math. France,* **102**, 449-462.
7. **[Ri 92]** Ribet, K. (1992), Abelian varieties over $\mathbb{Q}$ and modular forms, *Proceedings of KAIST Mathematics Workshop Korea Advanced Institute of Science and Technology,* 53-59.
8. **[Se 87]** Serre, J. P. (1987), Sur les represéntations modulaires de degreé 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.*, **54**, 179-230.