Capítulo 2

Curvas hiperelípticas

En este capítulo hacemos un breve resumen de resultados ya conocidos sobre curvas hiperelípticas, que serán utilizados en los capítulos posteriores. Enunciaremos definiciones básicas y algunos resultados de los que daremos las correspondientes referencias. De algunos expondremos nuestras propias demostraciones debido a que no hemos encontrado referencias de ellos o porque hemos considerado conveniente mostrarlas.

Cualquier libro de superficies de Riemann trata el caso de curvas hiperelípticas definidas sobre $\mathbb{C}$. Dos estupendas referencias son [FK80] y [Rey89]. Para el caso en el que el cuerpo de definición no es necesariamente $\mathbb{C}$, pero sí algebraicamente cerrado, casi cualquier libro de geometría algebraica básica contiene un apartado tratando el caso de curvas hiperelípticas. Una referencia básica es [Har77]. Ahora, para cuerpos no algebraicamente cerrados, es decir, cuando nos movemos en el campo de la Geometría Aritmética, hay pocos libros que tratan este tema. Dos buenas referencias son [Lor96] y [HS00], aunque no tratan con detalle el caso de curvas hiperelípticas. Por estos motivos, hemos utilizado los apuntes del *Seminari de corbes de gènere* 2 impartido por G. Cardona y E. Nart ([CN99]) y el trabajo [Car97] de G. Cardona, donde se pueden encontrar buenos resúmenes de los resultados básicos de la teoría de curvas hiperelípticas definidas sobre cuerpos no necesariamente algebraicamente cerrados.

2.1 Definiciones y resultados básicos

En lo que sigue K denotará un cuerpo de característica cero y $\overline{K}$ una clausura algebraica fijada de K. La recta proyectiva definida sobre K se denotará por $\mathbb{P}^1_K$. Dado un subcuerpo L de $\overline{K}$, diremos que un morfismo de variedades es un L-morfismo si está definido sobre L. Si C es una curva definida sobre K, se denotará por $\mathrm{Aut}(C)$ al grupo de los $\overline{K}$-automorfismos de C y por $\mathrm{Aut}_L(C)$ al subgrupo de $\mathrm{Aut}(C)$ formado por los L-automorfismos de C.

Proposición 2.1. *Sea C una curva proyectiva no singular definida sobre K de género mayor que 1. Las dos condiciones siguientes son equivalentes:*

(i) Existe un K-morfismo $\pi : C \to \mathbb{P}^1_K$ de grado 2.

(ii) Existe una K-involución $w : C \to C$ tal que $C/\langle w\rangle$ es K-isomorfa a $\mathbb{P}^1_K$.

Diremos que C es hiperelíptica si satisface estas condiciones.

Veamos que (i) implica (ii). Debido a que la extensión $K(C)/\pi^*K(\mathbb{P}^1_K)$ tiene grado 2 y a que toda extensión de grado 2 en característica cero es de Galois, tenemos que el grupo de Galois de la extensión $K(C)/\pi^*K(\mathbb{P}^1_K)$ está generada por un único elemento $\widehat{w}$ de orden 2. Este automorfismo del grupo de Galois induce un automorfismo de C, $w : C \to C$, de orden 2. Como $\widehat{w}$ deja fijo $\pi^*K(\mathbb{P}^1_K)$, se tiene que $\pi \circ w = \pi$, lo que demuestra la implicación de (i) a (ii).

La implicación de (ii) a (i) se sigue inmediatamente del hecho de que la proyección dada por $\pi : C \to C/\langle w\rangle$ tiene grado 2 y de que $C/\langle w\rangle$ es K-isomorfo a $\mathbb{P}^1_K$.

Observación 2.1. Aunque algunos autores incluyen el caso de género menor que 2 en la definición de curva hiperelíptica, nosotros no hemos optado por ésta.

Obsérvese que π no está determinado de forma única, ya que podemos componerlo con un automorfismo de $\mathbb{P}^1_K$ para obtener otro K-morfismo de grado 2 de C en $\mathbb{P}^1_K$. Sin embargo, la involución w sí que es canónica de la curva C. De hecho, se tiene el siguiente resultado:

Proposición 2.2. *Sea C una curva hiperelíptica definida sobre K, entonces un K-morfismo $\pi : C \to \mathbb{P}^1_K$ de grado 2 está determinado de forma única salvo*

transformaciones lineales fraccionarias definidas sobre K. En particular, la involución w está canónicamente determinada por la curva C y la llamaremos la involución hiperelíptica de C. Además, w está en el centro de $\mathrm{Aut}_K(C)$.

Demostración: Ver proposición 4 de [CN99] y corolario 3 de la sección III.7.9 de [FK80]. □

Proposición 2.3. *Toda curva de género* 2 *es hiperelíptica.*

Demostración: Sección A.4.5 de [HS00]. □

Definición 2.1. Sea C una curva proyectiva no singular de género g y sea $P \in C(\overline{K})$. Diremos que P es un *punto de Weierstrass de* C si existe una función no constante en C que tiene un polo de orden $\leq g$ en P. Al conjunto de puntos de Weierstrass de C lo denotaremos por $\mathrm{Wei}(C)$.

Este conjunto de puntos proporciona información sobre la curva. Acerca de estos puntos se tiene el siguiente resultado:

Proposición 2.4. *Sea C una curva proyectiva no singular de género g. Entonces*

$$2g + 2 \leq \#\,\mathrm{Wei}(C) \leq g^3 - g.$$

Además se tiene que $\#\,\mathrm{Wei}(C) = 2g + 2$ si y sólo si C es hiperelíptica.

Demostración: La primera parte es el corolario de la sección III.5.11 de [FK80], mientras que la segunda afirmación se puede encontrar en el teorema de la sección III.7.3 de [FK80]. □

La siguiente proposición caracteriza el conjunto de estos puntos cuando C es hiperelíptica.

Proposición 2.5. *Sea C una curva hiperelíptica de género g definida sobre K y sea w su involución hiperelíptica. Entonces*

$$\mathrm{Wei}(C) = \{P \in C(\overline{K}) \,|\, w(P) = P\} = \{P \in C(\overline{K}) \,|\, \pi \text{ ramifica en } P\}\,.$$

Demostración: Ver corolarios 5 y 7 de [CN99]. □

La siguiente proposición nos proporcionará modelos afines de curvas hiperelípticas.

Proposición 2.6. *Sea C una curva hiperelíptica definida sobre K con involución hiperelíptica w. Entonces existen dos funciones $x, y \in K(C)$ tales que:*

(i) $K(C) = K(x, y)$,

(ii) $x \circ w = x$ *con* $\operatorname{div} x = (Q) + (w(Q)) - (P) - (w(P))$ *para* $P, Q \in C(\overline{K})$,

(iii) La curva C tiene un modelo afín de la forma

$$C : y^2 = F(x),$$

donde $F \in K[X]$ no tiene raíces múltiples. Además el grado de F es $2g+2$ (resp. $2g+1$) si $P \notin \mathrm{Wei}(C)$ (resp. $P \in \mathrm{Wei}(C)$) y las raíces de F son $x(P_i)$ donde $P_i \in \mathrm{Wei}(C)$ (resp. $P_i \in \mathrm{Wei}(C) \smallsetminus \{P\}$).

Demostración: Ver sección 2.2 de [Car97]. □

El siguiente resultado es el recíproco del anterior.

Proposición 2.7. *Sea $C : y^2 = F(x)$ tal que $F(X) \in K[X]$ sin raíces repetidas de grado n. Entonces C es K-birracionalmente equivalente a una curva hiperelíptica definida sobre K de género $[\frac{n-1}{2}]$.*

Demostración: Ver [CN99].

Así, para dar una curva hiperelíptica C de género g definida sobre K es suficiente dar una ecuación de la forma

$$C : y^2 = F(x)$$

donde $F \in K[X]$ es un polinomio de grado $2g+2$ ó $2g+1$ sin raíces múltiples. A una ecuación de C de esta forma la llamaremos *ecuación hiperelíptica de C*. De esta forma tenemos que el morfismo $\pi : C \to \mathbb{P}^1_K$ está definido por $\pi(x, y) = x$ y la involución hiperelíptica actua de la forma $w(x, y) = (x, -y)$.

Proposición 2.8. *Sea $C : y^2 = F(x)$ una curva hiperelíptica de género g definida sobre K y sea $P \in C(\overline{K})$ un polo simple de x. Entonces, el K-espacio vectorial $H^0(C, \Omega^1_{C/K})$ tiene la siguiente base canónica*

$$\left\{ \frac{dx}{y}, x\frac{dx}{y}, \ldots, x^{g-1}\frac{dx}{y} \right\}.$$

Además, para $i = 0, \ldots, g-1$ se tiene:

$$\operatorname{ord}_P x^i \frac{dx}{y} = \begin{cases} 2g-2-2i & \text{si } P \in \mathrm{Wei}(C), \\ g-1-i & \text{si } P \notin \mathrm{Wei}(C). \end{cases} \tag{2.1}$$

Demostración: La primera parte del enunciado es suficientemente conocida. Ahora vamos a demostrar el segundo apartado. Supongamos que $P \notin \mathrm{Wei}(C)$. Denotemos $\mathrm{Wei}(C) = \{P_1, \ldots, P_{2g+2}\}$; entonces, utilizando la proposición 2.6, se obtiene

$$y^2 = k \prod_{i=1}^{2g+1} (x - x(P_i)).$$

De nuevo usando la proposición 2.6, se tiene

$$\begin{array}{rcl} \mathrm{div}(x) & = & (R) + (w(R)) - (P) - (w(P)), \\ \mathrm{div}(y) & = & (P_1) + \cdots + (P_{2g+2}) - (g+1)(P) - (g+1)(w(P)), \\ \mathrm{div}(dx) & = & (P_1) + \cdots + (P_{2g+2}) - 2(P) - 2(w(P)). \end{array}$$

Así, llegamos a

$$\mathrm{ord}_P\, x^i \, \frac{dx}{y} = g - 1 - i.$$

El caso $P \in \mathrm{Wei}(C)$ se demuestra de forma análoga. □

Proposición 2.9. *Sean $C : y^2 = F(x)$ y $C' : {y'}^2 = F'(x')$ curvas hiperelípticas de género g definidas sobre K. Entonces todo K-isomorfismo $u : C \to C'$ está dado por una expresión de la forma*

$$(x, y) \mapsto \left(\frac{a\,x + b}{c\,x + d}, \frac{e\,y}{(c\,x + d)^{g+1}} \right),$$

para alguna matriz $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ y $e \in K^*$. Diremos que el par (M, e) es un representante de u. Además, si $u' : C' \to C''$ es otro K-isomorfismo con representante (M', e'), entonces el par $(M'M, e'e)$ representa al isomorfismo $u' \circ u$.

Demostración: Denotemos por $X = x' \circ u$ y por $Y = y' \circ u$. Así, X es un módulo principal de $C/\langle w \rangle$ definido sobre K y, por lo tanto, existe una matriz $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ tal que $X = (ax + b)/(cx + d)$. Sean w y w' las involuciones hiperelíptica de C y C' respectivamente. Como w está en el centro de $\mathrm{Aut}_K(C)$ y $u \circ w = w' \circ u$, se tiene que Y/y es una función de $C/\langle w \rangle$ definida sobre K. Luego, existen dos polinomios $P_1(X), P_2(X) \in K[X]$ tales que $Y/y = P_1(x)/P_2(x)$ y $\mathrm{mcd}(P_1, P_2) = 1$. Ahora, por el hecho de que las diferenciales

$$\frac{dX}{Y} = \frac{\det M\, P_2(x)}{P_1(x)(cx + d)^2} \frac{dx}{y} \quad \text{y} \quad X^{g-1} \frac{dX}{Y} = \frac{\det M\, (ax + b)^{g-1} P_2(x)}{P_1(x)(cx + d)^{g+1}} \frac{dx}{y}$$

están en $H^0(C, \Omega^1_{C/K})$ y usando que $\{dx/y, \ldots, x^{g-1}dx/y\}$ es una base de este K-espacio vectorial, obtenemos $P_1(X) \in K^*$, $(c\,X + d)^{g+1}$ divide $P_2(X)$ y el grado de $P_2(X)$ es igual al de $(c\,X + d)^{g+1}$. El resto del enunciado se obtiene fácilmente. □

El siguiente resultado es debido a A. Ogg.

Lema 2.10. *Sea C una curva hiperelíptica de género g con involución hiperelíptica w y sea u otra involución. Sea $v = wu$. Entonces los conjuntos de puntos fijos de v, w y u son disjuntos dos a dos. Si g es par, entonces u y v tienen dos puntos fijos cada una. Si g es impar, entonces v tiene cuatro puntos fijos y u ninguno, o viceversa.*

Demostración: Proposición 1 de [Ogg74]. □

Corolario 2.11. *Sean C una curva hiperelíptica de género g, $u \in \mathrm{Aut}(C)$ una involución no hiperelíptica y $C' = C/\langle u \rangle$ la curva cociente. Si denotamos por g' el género de C', se tiene:*

(i) Si g es par entonces $g' = g/2$, mientras que si g es impar entonces $g' = (g-1)/2$ ó $(g+1)/2$.

(ii) Si $g' > 1$, entonces C' es hiperelíptica.

Demostración: La parte (i) es una consecuencia inmediata del lema 2.10 y de la fórmula de Hurwitz. La segunda parte se obtiene del hecho de que w induce una involución en C', que seguimos denotando por w, tal que $C'/\langle w \rangle$ tiene género 0.

□

Capítulo 3

Curvas hiperelípticas modulares

En el capítulo 1 definimos las curvas modulares como las compactificaciones de los cocientes del semiplano superior de Poincaré por subgrupos de congruencias. En este capítulo generalizaremos la noción de curva modular, así como la de variedad abeliana modular. Diremos que una curva C es *modular* si existe un morfismo no constante $X_1(N) \to C$ para algún entero positivo N y que una variedad abeliana es *modular* si es isógena a un factor de $J_1(N)$, para algún entero positivo N. Obsérvese que esta noción de modularidad generaliza la expuesta en el capítulo 1. Además, introduciremos dos nuevos conceptos para una curva modular (resp. variedad abeliana modular), el de nueva y el de primitiva.

Nos restringiremos al caso en el cual el cuerpo de definición es $\mathbb{Q}$. Veremos que si C es una curva definida sobre $\mathbb{Q}$ de género 0 ó 1, basta con que $C(\mathbb{Q}) \neq \emptyset$ para que la curva sea modular y que, en este caso, los conceptos de nueva, primitiva y modular son equivalentes. Sin embargo, esta situación cambiará completamente cuando el género de C sea mayor que 1. En este sentido, veremos las múltiples posibilidades que se presentan en este caso.

Por último, nos centraremos en el estudio de las curvas hiperelípticas modulares nuevas definidas sobre $\mathbb{Q}$. Para éstas, haremos un estudio exhaustivo que nos permitirá llegar a demostrar el principal resultado teórico de esta tesis:

Teorema 3.11. *El conjunto de curvas hiperelípticas modulares nuevas, salvo $\mathbb{Q}$-isomorfismo, es finito.*

Además este Teorema será completado con el Teorema 3.10, que proporciona acotaciones sobre el género de tales curvas dependiendo las cotas de que estas curvas puedan ser recubiertas por curvas modulares $X_0(N)$ o no.

3.1 Definiciones

En esta sección introduciremos los principales objetos de estudio de esta tesis, las curvas que son recubiertas por alguna curva modular $X_1(N)$ y que, aún a riesgo de confusión con las curvas X_Γ, seguiremos llamando *curvas modulares*. Introducimos la noción de modularidad, en primer lugar, para una variedad abeliana y, posteriormente, para una curva proyectiva y no singular.

Definición 3.1. Sea A una variedad abeliana definida sobre un cuerpo de números K. Diremos que A es *K-modular de nivel N* si existe un K-morfismo exhaustivo

$$\nu : J_1(N) \twoheadrightarrow A.$$

En tal caso diremos que:

(i) A es *K-nueva de nivel N* si ν factoriza a traves de la parte nueva de $J_1(N)$. Es decir, existe un K-morfismo $\tilde{\nu} : J_1(N)^{\text{new}} \to A$ que hace conmutativo el siguiente diagrama:

$$\begin{array}{ccc} J_1(N) & \xrightarrow{\quad\nu\quad} & A\,. \\ & {\scriptstyle \text{pr}_{\text{new}}} \searrow \quad \nearrow {\scriptstyle \tilde{\nu}} & \\ & J_1(N)^{\text{new}} & \end{array}$$

(ii) A es *K-primitiva de nivel N* si para cualquier divisor propio $M|N$, A no es K-modular de nivel M.

Definición 3.2. Sea C una curva proyectiva lisa definida sobre un cuerpo de números K, diremos que es *K-modular de nivel N* si existe un K-morfismo no constante

$$\pi : X_1(N) \to C.$$

Análogamente al caso de variedades modulares, introducimos las nociones de nueva y primitiva para una curva modular.

Definición 3.3. Sea C una curva K-modular de nivel N. Diremos que C es *K-nueva de nivel N* (resp. *K-primitiva de nivel N*) si la jacobiana de C, $J(C)$, es K-nueva de nivel N (resp. K-primitiva de nivel N).

Observación 3.1. Es conveniente resaltar que:

(i) La modularidad depende del cuerpo de definición. Es posible tener una curva C (resp. variedad abeliana A), definida sobre un cuerpo K, que no es K-modular y tal que, tomando una extensión apropiada de cuerpos L/K, sea L-modular. Por ejemplo, consideremos la curva elíptica definida por

$$E : y^2 = x^3 + A\,x + B, \quad \begin{cases} A &= -135 - 156\sqrt{-3}, \\ B &= 82 - 1092\sqrt{-3}\,, \end{cases}$$

es una curva (o variedad abeliana) K-modular de nivel $N = 63$ para $K = \mathbb{Q}(\sqrt{-3})$ (ver E_{63B} de la tabla 6.4). De hecho, E es una $\mathbb{Q}$-curva de grado 3 completamente definida sobre K, es decir, hay una isogenia de grado 3 de E en su conjugada de Galois definida sobre K. La curva elíptica torcida $E_\gamma : y^2 = x^3 + \gamma^2 A\,x + \gamma^3 B$, donde $\gamma = 2 + \sqrt{-3}$, no es K-modular para ningún nivel N, porque no está completamente definida sobre K (cf.[GL01]). Sin embargo, E_γ es L-modular para $L = K(\sqrt{\gamma})$.

(ii) Si C es una curva K-modular, entonces $C(K) \neq \emptyset$, ya que π está definida sobre K e $i\infty \in X_1(N)(\mathbb{Q})$.

Cuando sea necesario utilizar el morfismo $\nu : J_1(N) \to A$, respectivamente $\pi : X_1(N) \to C$, para una variedad abeliana modular A, resp. curva modular C, de nivel N, utilizaremos la notación (A, ν), resp. (C, π).

Si (C, π) es una curva K-modular de nivel N, se tiene que el morfismo asociado entre las jacobianas $\pi_* : J_1(N) \to J(C)$ está definido sobre K. Por lo tanto, si C es K-modular de nivel N, $J(C)$ es también K-modular de nivel N. En este caso tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} J_1(N) & \xrightarrow{\pi_*} & J(C) \\ \uparrow & & \uparrow \\ X_1(N) & \xrightarrow{\pi} & C\,. \end{array}$$

Sin embargo, el recíproco es falso en general, es decir, si existe un morfismo exhaustivo entre las jacobianas $J_1(N)$ y $J(C)$, no tiene por qué existir un morfismo entre las respectivas curvas. En la sección 7.2 se mostrarán diversos ejemplos al respecto.

A partir de ahora, sólo consideraremos el caso racional, es decir, $K = \mathbb{Q}$, y si no se especifica el cuerpo de definición, curva (resp. variedad abeliana) modular significará curva (resp. variedad abeliana) $\mathbb{Q}$-modular.

Vamos a ver la relación que hay entre curvas modulares nuevas y primitivas de un cierto nivel N. Dado que estas dos nociones para curvas se expresan a través de sus jacobianas, estudiaremos la relación entre las variedades abelianas modulares nuevas y primitivas. No obstante, como veremos más adelante, existen curvas modulares que no son primitivas para ningún nivel mientras que una variedad abeliana modular A siempre es primitiva para algún nivel, aunque éste no sea necesariamente único. De hecho, si A tiene como $\mathbb{Q}$-factor el cuadrado de una variedad abeliana modular, entonces A es primitiva para infinitos niveles. Por ejemplo, $J_0(22)$ és una variedad abeliana modular primitiva de nivel $11\,p$ para todo primo p que no divide a 22, ya que $J_0(11\,p) \overset{\mathbb{Q}}{\sim} J_0(11)^2 \times J_0(p)^2 \times J_0(11\,p)^{\text{new}}$ y $J_0(22) \overset{\mathbb{Q}}{\sim} J_0(11)^2$.

Sea (A, ν) una variedad abeliana modular de nivel N. Debido a la descomposición de $J_1(N)$ sobre $\mathbb{Q}$, existen k formas nuevas $f_1, \ldots, f_k$, con niveles que dividen a N, tales que

$$A \overset{\mathbb{Q}}{\sim} A_{f_1}^{n_1} \times \cdots \times A_{f_k}^{n_k}\,.$$

Obsérvese que si A es nueva de nivel N, entonces cada f_i es una forma nueva en $S_2(N)$ y $n_i = 1$. En este caso, se tiene

$$\nu^*(H^0(A, \Omega^1)) = \bigoplus_{i=1}^{k} S_2(A_{f_i})\,\frac{dq}{q}\,.$$

En particular, esto demuestra que ser nueva de nivel N implica ser primitiva de nivel N, ya que N es el mínimo nivel en el que A es modular. Pero, el recíproco no es cierto en general, como demuestra el siguiente ejemplo.

Ejemplo 3.1. La variedad abeliana modular $J_0(22)$ es primitiva de nivel 22 pero no es nueva para ningún nivel. Esto es debido a que $S_2(22,1)^{\text{new}} = \{0\}$ y por lo tanto $J_0(22) = J_0(22)^{\text{old}}$.

Si la variedad abeliana A es $\mathbb{Q}$-simple, pero no necesariamente nueva, se tiene $A \overset{\mathbb{Q}}{\sim} A_f$ para alguna forma nueva $f \in S_2(M)$ con $M|N$ y

$$\nu^*(H^0(A,\Omega^1)) \subseteq \bigoplus_{0<d|N/M} \langle {}^{\sigma}f(q^d)\,\frac{dq}{q} : \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\rangle_{\mathbb{C}}\,.$$

Si además A es primitiva de nivel N, entonces $M = N$. Es decir, hemos visto que en el caso en el cual A es $\mathbb{Q}$-simple, ser nueva de nivel N es equivalente a ser primitiva de nivel N.

Como consecuencia de lo expuesto, se obtiene el resultado siguiente.

Proposición 3.1. *Sea A una variedad abeliana modular.*

(i) Si A es nueva de nivel N, entonces A es primitiva de nivel N.

(ii) Si A es $\mathbb{Q}$-simple, entonces A es nueva de nivel N si y sólo si A es primitiva de nivel N.

Notación 3.1. Para un entero $g \geq 0$ denotaremos por $\mathcal{MC}_g$ (resp. $\mathcal{MC}_g^{\mathrm{new}}$, resp. $\mathcal{MC}_g^{\mathrm{prim}}$) al conjunto de clases de $\mathbb{Q}$-isomorfía de curvas modulares (resp. nuevas, resp. primitivas) de género g.

Empezando por el género inferior, obsérvese que toda curva de género 0 con un punto racional es $\mathbb{Q}$-isomorfa a $\mathbb{P}^1_{\mathbb{Q}}$. Por lo tanto, toda curva modular de género 0 es $\mathbb{Q}$-isomorfa a $X_1(1)$. Así, se tiene

$$\mathcal{MC}_0 = \mathcal{MC}_0^{\mathrm{new}} = \mathcal{MC}_0^{\mathrm{prim}} = \{X_1(1)\}\,.$$

En particular, $\#\mathcal{MC}_0 = 1$. Obsérvese que en este caso no tiene sentido hablar de la noción de primitiva y de nueva, ya que las jacobianas de tales curvas son triviales.

Sea C ahora una curva definida sobre $\mathbb{Q}$ de género 1. Entonces, si $C(\mathbb{Q}) = \emptyset$, C no puede ser modular, por la observación 3.1. Por ejemplo, la curva definida por la ecuación $3\,x^3 + 4\,y^3 + 5\,z^3 = 0$ no tiene ningún punto racional (ver [Sel51],[Sel54]) y, por tanto, no es modular. Ahora supongamos que $C(\mathbb{Q}) \neq \emptyset$, es decir, C es una curva elíptica definida sobre $\mathbb{Q}$. Entonces existe un isomorfismo canónico entre C y $J(C)$. Por lo tanto, para el caso de curvas elípticas sobre $\mathbb{Q}$ la condición de que C sea modular es equivalente a la condición de que $J(C)$ lo sea. En este caso, es bien conocido que

$$\mathcal{MC}_1 = \mathcal{MC}_1^{\mathrm{new}} = \mathcal{MC}_1^{\mathrm{prim}}.$$

Pero hoy tenemos ya más información. Los trabajos de A. Wiles [Wil95] y de Wiles-Taylor [TW95], que permitieron demostrar el *Último Teorema de Fermat*, han sido recientemente completados por C. Breuil, B. Conrad, F. Diamond y R. Taylor [BCDT01]. Así, ha sido demostrada la llamada *Conjetura de Shimura-Taniyama-Weil*, cuyo enunciado ahora en forma de teorema puede ser formulada como sigue.

Teorema 3.2. *Toda curva elíptica C definida sobre $\mathbb{Q}$ es modular nueva de nivel igual a su conductor geométrico $\mathcal{N}_{\mathbb{Q}}(C)$.*

Demostración: Las referencias principales son [Wil95] y [BCDT01]. □

En particular, se tiene

$$\#\mathcal{MC}_1 = \infty.$$

Cuando consideramos curvas modulares de género mayor que 1, esta situación cambia completamente. La existencia de puntos racionales para una curva C no garantiza su modularidad. A diferencia del caso de curvas elípticas definidas sobre $\mathbb{Q}$, existen curvas que no son modulares para un nivel, pero cuyas jacobianas sí lo son para dicho nivel. También existen curvas modulares que no son primitivas para ningún nivel. Las curvas siguientes son ejemplos de curvas modulares no primitivas, como se demostrará en la sección 7.2.

Ejemplo 3.2. La curva de género 4 definida por

$$C_{376}^{2,2} : y^2 = (x^5 - x^3 + 2x^2 - 2x + 1)(x^5 + 4x^4 + 3x^3 - 2x^2 + 2x + 5)$$

es modular. El nivel mínimo de su modularidad es 94, mientras que su jacobiana es primitiva de nivel 47. De hecho, se tiene

$$J(C) \overset{\mathbb{Q}}{\sim} J_0(47) \qquad \text{y} \qquad C \ncong X_0(47).$$

Ejemplo 3.3. La curva de género 3 definida por

$$C_{544}^{2,3} : y^2 = x(x-1)(x^2 + x - 4)(x^4 - x^2 - 4)$$

es modular de nivel 136 y no es modular de nivel 68. Sin embargo, su jacobiana es primitiva de nivel 68 y no es $\mathbb{Q}$-simple.

Los siguientes ejemplos de curvas muestran las nuevas situaciones que se presentan cuando el género es mayor que 1, atendiendo al carácter $\mathbb{Q}$-simple de sus jacobianas.

Ejemplo 3.4. $X_0(23)$ es nueva de nivel 23 y $J_0(23)$ es $\mathbb{Q}$-simple.

Ejemplo 3.5. $X_0(50)$ es nueva de nivel 50 y $J_0(50)$ es no $\mathbb{Q}$-simple.

Los cuatro ejemplos mostrados corresponden a curvas hiperelípticas. La siguiente tabla muestra una más amplia gama de posibilidades que en el caso elíptico:

C	Primitiva	Nueva	$J(C)$ $\mathbb{Q}$-simple
$X_0(23)$	Si	Si	Si
$X_0(50)$	Si	Si	No
$X_0(22)$	Si	No	No
$C_{544}^{2,3}$	No	No	No
$C_{376}^{2,2}$	No	No	Si

Para cada curva existen morfismos de grado finito en $\mathbb{P}^1$. Esto permite clasificar las curvas dependiendo del grado mínimo de estos recubrimientos.

Definición 3.4. Sea C una curva definida sobre $\mathbb{C}$. La $\mathbb{C}$-*gonalidad* de C es el menor grado de un morfismo no constante de C en $\mathbb{P}^1$.

Así, las curvas de género $g \geq 2$ con gonalidad 2 son las curvas hiperelípticas.

Notación 3.2. Para dos enteros $g \geq 2$ y $G \geq 2$ denotaremos por $\mathcal{MC}_g(G)$ (resp. $\mathcal{MC}_g^{\text{new}}(G)$ y $\mathcal{MC}_g^{\text{prim}}(G)$) al conjunto de clases de $\mathbb{Q}$-isomorfía de curvas modulares (resp. nuevas y primitivas) de género g y gonalidad G. Con mayor generalidad, denotaremos por $\mathcal{MC}(G)$ (resp. $\mathcal{MC}^{\text{new}}(G)$ y $\mathcal{MC}^{\text{prim}}(G)$) a la unión de los conjuntos $\mathcal{MC}_g(G)$ (resp. $\mathcal{MC}_g^{\text{new}}(G)$ y $\mathcal{MC}_g^{\text{prim}}(G)$) para $g \geq 2$.

Nos limitaremos a estudiar las curvas modulares nuevas para el caso de gonalidad más sencillo, que es $G = 2$. En otras palabras, nuestro objeto de estudio será el conjunto $\mathcal{MC}^{\text{new}}(2)$ y la determinación de ecuaciones explícitas de las curvas de este conjunto.

3.2 Automorfismos de curvas modulares nuevas

Nuestro estudio se limitará a las curvas modulares nuevas. El siguiente resultado nos será de utilidad en el estudio de estas curvas.

Lema 3.3. *Sean X, Y y Z curvas proyectivas no singulares definidas sobre un subcuerpo K de $\mathbb{C}$ tal que el género de Y es mayor que 1. Sea $\pi : X \to Y$ un K-morfismo no constante. Se tiene:*

(i) Si $\phi : X \to Z$ es un K-morfismo no constante tal que $\pi^* H^0(Y, \Omega^1_{Y/K}) \subseteq \phi^* H^0(Z, \Omega^1_{Z/K})$, entonces existe un K-morfismo no constante $\pi' : Z \to Y$ tal que $\pi' \circ \phi = \pi$. Es decir, el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} X & \xrightarrow{\pi} & Y\,. \\ & {\scriptstyle\phi}\searrow \quad \nearrow{\scriptstyle\pi'} & \\ & Z & \end{array}$$

(ii) Si $u \in \mathrm{Aut}_K(X)$ deja estable $\pi^* H^0(Y, \Omega^1_{Y/K})$, entonces existe un único automorfismo $v \in \mathrm{Aut}_K(Y)$ tal que $\pi \circ u = v \circ \pi$, es decir, haciendo conmutativo el diagrama siguiente:

$$\begin{array}{ccc} X & \xrightarrow{u} & X \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ Y & \xrightarrow{v} & Y\,. \end{array}$$

Demostración: El apartado (i) es equivalente a la inclusión $\pi^* K(Y) \subseteq \phi^* K(Z)$. Obsérvese que cualquier función en X que es un cociente de dos diferenciales regulares no nulas de $\phi^* K(Z)$ es una función en $\phi^* K(Z)$. Si Y no es hiperelíptica, el cuerpo de funciones de Y, $K(Y)$, está generado por cocientes de pares de diferenciales regulares no nulas de $H^0(Y, \Omega^1_{Y/K})$. Por lo tanto, la inclusión es inmediata. En el caso en el que Y es hiperelíptica, se tiene $K(Y) = K(x, y)$, donde $y^2 = F(x)$ es una ecuación hiperelíptica de Y definida sobre K. En este caso, el cuerpo generado por cocientes de diferenciales regulares no nulas de $H^0(Y, \Omega^1_{Y/K})$ coincide con $K(x)$. Utilizando este hecho y que

$$y = \frac{x dx}{x\, dx/y},$$

se obtiene (i).

Para demostrar (ii), sea $\psi : X \to Z$ un K-morfismo tal que satisface $\psi^* K(Z) = (\pi \circ u)^* K(Y)$. Entonces, $\pi^* H^0(Y, \Omega^1_{Y/K}) = \psi^* H^0(Z, \Omega^1_{Z/K})$ y, aplicando el apartado (i), existe un K-morfismo $\pi' : Z \to Y$ tal que $\pi' \circ \psi = \pi$.

Como el género de Y es mayor que 1 y $\dim H^0(Y,\Omega^1_{Y_{/K}}) = \dim H^0(Z,\Omega^1_{Z_{/K}})$, π' es un isomorfismo. Así, $\psi^*K(Z) = \pi^*K(Y)$ y, por lo tanto, u deja estable $\pi^*K(Y)$. □

Como consecuencia de este lema, si (C,π) es una curva modular nueva de nivel N entonces los operadores diamante $\langle d\rangle$ y la involución de Weil W_N inducen automorfismos en C, que seguiremos denotando por $\langle d\rangle$ y W_N respectivamente. Además, si $J(C)$ es $\mathbb{Q}$-simple, es decir $J(C) \overset{\mathbb{Q}}{\sim} A_f$ con f una forma nueva de $S_2(N,\varepsilon)$, entonces $\mathrm{Aut}(C)$ contiene al subgrupo de los automorfismos de C generado por éstos automorfismos, el cual es isomorfo al grupo diedral con $2n$ elementos, donde n es el orden del carácter ε. Además, el morfismo π factoriza a través de $X(N,\varepsilon)$, es decir, se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccc} X_1(N) & \xrightarrow{\quad\pi\quad} & C\,. \\ & {\scriptstyle \mathrm{pr}_\varepsilon} \searrow \quad \nearrow {\scriptstyle \pi_\varepsilon} & \\ & X(N,\varepsilon) & \end{array}$$

3.3 Curvas hiperelípticas modulares nuevas

El propósito de esta sección es caracterizar de una forma efectiva la clase de curvas hiperelípticas modulares nuevas.

Lema 3.4. *Sea (C,π) una curva hiperelíptica modular de nivel N definida sobre $\mathbb{C}$ de género g tal que $\pi^*(H^0(C,\Omega^1)) = \bigoplus_{i=1}^k H^0(A_{f_i},\Omega^1)$ para algunas formas nuevas $f_i \in S_2(N)$, $1 \le i \le k$. Denotemos por $f^{(j)} = \sum_{n\ge1} a_n^{(j)}\, q^n$, $1 \le j \le g$, la base normalizada de formas nuevas de $\bigoplus_{i=1}^k S_2(A_{f_i})$. Fijemos $P = \pi(i\infty)$, entonces*

(i) El morfismo π no es ramificado en la punta $i\infty$.

(ii) Existe una base $\{h_1,\dots,h_g\}$ de $\bigoplus_{i=1}^k S_2(A_{f_i})$ tal que para $i = 1,\dots,g$:

$$\begin{cases} h_i = q^i \qquad\qquad + \qquad O(q^{g+1}) & \text{si } P \notin \mathrm{Wei}(C), \\ h_i = q^{2i-1} + \displaystyle\sum_{j\ge i}^{g-1} b_{2j}^{(i)} q^j + O(q^{2g}) & \text{si } P \in \mathrm{Wei}(C). \end{cases}$$

(iii) Además,

(a) Si $P \notin \mathrm{Wei}(C)$, *entonces* $\det(a_i^{(j)})_{1\le i,j\le g} \neq 0$.

(b) Si $P \in \mathrm{Wei}(C)$, *entonces* $\det(a_{2i-1}^{(j)})_{1\le i,j\le g} \neq 0$.

Demostración: Denotemos por $e = e_\pi(i\infty)$ el índice de ramificación de π en la punta $i\infty$. Si π es ramificada en $i\infty$ se tendrá $e > 1$. Entonces para toda diferencial regular $w \in H^0(C, \Omega^1)$ distinta de cero se tiene que

$$\mathrm{ord}_{i\infty}\, \pi^*(w) \ge e - 1 > 0.$$

Este resultado contradice que $\mathrm{ord}_{i\infty}\, f^{(j)}(q)dq/q = 0$ y, por tanto, $e = 1$.

Como C es hiperelíptica, existe una base del espacio vectorial complejo $H^0(C, \Omega^1)$ formada por g diferenciales regulares $\{w_1, \ldots, w_g\}$ con la propiedad (ver proposición 2.8):

$$\mathrm{ord}_P\, w_i = \begin{cases} g-1-i & \text{si } P \notin \mathrm{Wei}(C), \\ 2g-2-2i & \text{si } P \in \mathrm{Wei}(C). \end{cases}$$

Para $i = 1, \ldots, g$, sea $h_i' = \pi^*(w_i)\, q/dq$. Utilizando el apartado (i), obtenemos que la base $\{h_1', \ldots, h_g'\}$ de $\bigoplus_{i=1}^k S_2(A_{f_i})$ satisface:

$$\begin{cases} h_i' = q^i + O(q^{i+1}) & \text{si } P \notin \mathrm{Wei}(C), \\ h_i' = q^{2i-1} + O(q^{2\,i}) & \text{si } P \in \mathrm{Wei}(C). \end{cases}$$

Aplicando la reducción Gaussiana a la matriz de los coeficientes de Fourier de $\{h_1', \ldots, h_g'\}$ obtenemos (ii).

Para demostrar (iii), obsérvese que la matriz en *(a)* ó en *(b)*, es la matriz de cambio de base de $\{f^{(1)}, \ldots, f^{(g)}\}$ a $\{h_1, \ldots, h_g\}$. □

Observación 3.2. Obsérvese que si el espacio vectorial complejo $\bigoplus_{i=1}^k S_2(A_{f_i})$ tiene una base $\{h_1, \ldots, h_g\}$ como en (ii) del lema anterior, entonces es única y, además, cada h_i tiene sus coeficientes de Fourier en $\mathbb{Q}$, ya que $\bigoplus_{i=1}^k S_2(A_{f_i})$ tiene una base con q-expasiones racionales.

Observación 3.3. En el capítulo 5 probaremos que en el caso $P \in \mathrm{Wei}(C)$ la base $\{h_1, \ldots, h_g\}$ satisface

$$h_i = q^{2i-1} + O(q^{2g}),$$

para $i = 1, \ldots, g$.

La siguiente proposición nos proporciona un criterio efectivo para determinar cuándo un $\mathbb{Q}$-factor de $J_1(N)^{\text{new}}$, esto es, una variedad abeliana modular nueva de nivel N, es $\mathbb{Q}$-isógena a la jacobiana de una curva hiperelíptica modular nueva de nivel N.

Proposición 3.5. *Sean $f_1, \ldots, f_k \in S_2(N)$ formas nuevas tales que $A = \prod_{i=1}^k A_{f_i}$ es un cociente de $J_1(N)^{\text{new}}$ definido sobre $\mathbb{Q}$. Entonces, las siguientes condiciones son equivalentes:*

(i) Existe una curva hiperelíptica modular nueva C de nivel N tal que $J(C)$ es $\mathbb{Q}$-isógena a A.

(ii) Existe una curva hiperelíptica modular nueva (C', π') de nivel N definida sobre $\mathbb{C}$ tal que $\pi'^*(H^0(C', \Omega^1)) = \bigoplus_{i=1}^k H^0(A_{f_i}, \Omega^1)$.

(iii) Existe una base $\{h_1, \ldots h_g\}$ de $\bigoplus_{i=1}^k S_2(A_{f_i})$ como en (ii) del lema anterior tal que para cualquier par $g_1, g_2 \in \bigoplus_{i=1}^k S_2(A_{f_i})$ linealmente independientes cumpliendo $\langle g_1, g_2 \rangle = \langle h_{g-1}, h_g \rangle$ y $g_2 \in \langle h_g \rangle$, existe un polinomio $F(X) \in \mathbb{C}[X]$ de grado $2g+1$ ó $2g+2$ sin raíces múltiples tal que las funciones en $X_1(N)$ dadas por

$$x = \frac{g_1}{g_2} \qquad e \qquad y = \frac{q\, dx/dq}{g_2}$$

satisfacen la ecuación $y^2 = F(x)$.

Demostración: Trivialmente se observa que (i) implica (ii). Para demostrar que (iii) implica (i) basta con tomar $g_1 = h_{g-1}$ y $g_2 = h_g$. Así, las funciones modulares x e y tienen q-expansiones con coeficientes racionales y por lo tanto el correspondiente polinomio $F(X)$ tiene coeficientes racionales.

Ahora supondremos cierto (ii) y veremos que este implica (iii). Por el lema anterior, sabemos que existe la base $\{h_1, \ldots, h_g\}$. Como en dicho lema, tomamos $P = \pi'(i\infty)$. Sean u y v funciones en C' tales que:

- $\operatorname{div} u = (Q) + (w(Q)) - (P) - (w(P))$.
- $v^2 = G(u)$, donde $G(X) \in \mathbb{C}[X]$ es de grado $2g+1$ ó $2g+2$ y no tiene raíces múltiples.

Usando que el morfismo π' es no ramificado en $i\infty$ y viendo el orden de du/v y $u\,du/v$ en P, tenemos que

$$\pi'^*\left(u\,\frac{du}{v}\right) \in \langle h_{g-1}(q), h_g(q)\rangle \frac{dq}{q} \qquad \text{y} \qquad \pi'^*\left(\frac{du}{v}\right) \in \langle h_g(q)\rangle \frac{dq}{q}.$$

Esto implica

$$\left\langle \pi'^*\left(\frac{du}{v}\right), \pi'^*\left(u\,\frac{du}{v}\right)\right\rangle = \langle h_{g-1}(q), h_g(q)\rangle \frac{dq}{q} \text{ y } \left\langle \pi'^*\left(\frac{du}{v}\right)\right\rangle = \langle h_g(q)\rangle \frac{dq}{q}.$$

Entonces para cualquier par de formas modulares g_1 y g_2 como en (iii) existe una matriz $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$ tal que

$$\begin{cases} g_1(q)\dfrac{dq}{q} = a\,\pi'^*\left(u\,\dfrac{du}{v}\right) + b\,\pi'^*\left(\dfrac{du}{v}\right), \\ g_2(q)\dfrac{dq}{q} = d\,\pi'^*\left(\dfrac{du}{v}\right). \end{cases}$$

Se puede calcular fácilmente que las funciones modulares

$$x = \frac{g_1}{g_2} \qquad \text{e} \qquad y = \frac{q\,dx/dq}{g_2}$$

satisfacen la ecuación $y^2 = F(x)$, donde

$$F(X) = \frac{a^2}{d^4} G\left(\frac{aX+b}{d}\right).$$

□

Aunque la proposición anterior proporciona un criterio efectivo teórico para determinar curvas hiperelípticas modulares nuevas, en la práctica su aplicación presenta la dificultad de que las formas nuevas estan dadas por series de Fourier con infinitos coeficientes. El siguiente resultado dota de efectividad computacional a la proposición anterior.

Proposición 3.6. *Sean X una curva proyectiva lisa definida sobre $\mathbb{C}$ de género $g_X > 1$ y q un uniformizante de un punto de X. Asimismo sean ω_1 y ω_2 diferenciales regulares no nulas de X y pongamos*

$$x = \frac{\omega_1}{\omega_2} \qquad e \qquad y = \frac{dx}{\omega_2}.$$

En estas condiciones, si existe un polinomio $F(u) \in \mathbb{C}[u]$ de grado m tal que

$$y^2 - F(x) = O(q^c) \quad \text{con } c \geq (2g_X - 2) \cdot \max\{6, m\} + 1,$$

se tiene que $y^2 = F(x)$.

Demostración: Sea

$$\operatorname{div}(\omega_2) = \sum_{i=1}^{h} m_i \, Q_i \,, \quad \text{con} \quad Q_i \in X \quad \text{y} \quad Q_i \neq Q_j \quad \text{si} \quad i \neq j \,.$$

Por el teorema de Riemann-Roch, tenemos

$$\operatorname{grado}\left(\operatorname{div}(\omega_2)\right) = \sum_{i=1}^{h} m_i = 2\, g_X - 2 \,.$$

Para un divisor D de X, denotaremos por D^- al divisor positivo que corresponde a la parte polar de D. Si $D = \operatorname{div}(f)$, entonces pondremos $\operatorname{div}^- f$ para hacer referencia a D^-. Así, tendremos

$$\begin{aligned} \operatorname{div}^-(x) &= \operatorname{div}^-\left(\frac{\omega_1}{\omega_2}\right) \leq \operatorname{div}(\omega_2) \,, \\ \operatorname{div}^-(y) &= \operatorname{div}^-\left(\frac{dx}{\omega_2}\right) \leq \operatorname{div}^-(dx) + \operatorname{div}(\omega_2) \\ &\leq \sum_{i=1}^{h} (m_i + 1) Q_i + \operatorname{div}(\omega_2) \leq 3 \operatorname{div}(\omega_2) \,. \end{aligned}$$

El enunciado ahora es una consecuencia inmediata de la siguiente desigualdad

$$\operatorname{grado}(\operatorname{div}^-(y^2 - F(x))) \leq (2g_X - 2) \cdot \max\{6, m\} \,.$$

□

3.4 Resultados de finitud

En esta sección demostraremos que el conjunto de curvas hiperelípticas modulares nuevas, salvo $\mathbb{Q}$-isomorfismos, es finito, es decir, $\#\mathcal{MC}^{\text{new}}(2) < \infty$. La prueba se dividirá en dos partes. Primero veremos que fijado un entero $g \geq 2$

existe un numero finito de curvas hiperelípticas modulares nuevas de género g, o lo que es lo mismo $\mathcal{MC}_g^{\text{new}}(2) < \infty$. Después demostraremos que los posibles géneros están acotados.

El siguiente lema será utilizado para demostrar la finitud de tales curvas para un género fijado.

Lema 3.7. *Sea (C, π) una curva hiperelíptica modular nueva de nivel N y género g tal que $J(C) \overset{\mathbb{Q}}{\sim} \prod_{i=1}^{k} A_{f_i}$. Denotemos por $f^{(j)} = \sum_{n\geq 1} a_n^{(j)} q^n$, $1 \leq j \leq g$, la base de formas nuevas normalizadas de $\bigoplus_{i=1}^{k} S_2(A_{f_i})$. Sea $P = \pi(i\infty)$. Entonces cualquier ecuación hiperelíptica de C depende sólo de los primeros $6g+1$ (resp. $3g+2$) coeficientes de $f^{(1)}, \ldots, f^{(g)}$ si $P \in \text{Wei}(C)$ (resp. si $P \notin \text{Wei}(C)$).*

Demostración: Supongamos primero que $P \in \text{Wei}(C)$. Por el lema 3.4 sabemos que existe una base $\{h_1, \ldots, h_g\}$ de $\bigoplus_{i=1}^{k} S_2(A_{f_i})$ tal que para todo $i = 1, \ldots, g$ la forma parabólica h_i tiene una q-expansión de la forma

$$h_i = q^{2i-1} + \cdots + O(q^n).$$

Definamos

$$x = \frac{h_{g-1}}{h_g} \qquad \text{e} \qquad y = \frac{q\, dx/dq}{-2\, h_g}\,.$$

Entonces, las q-expansiones de x e y son de la forma

$$x = q^{-2}(1 + \cdots + O(q^{n-2g+1})) \qquad \text{e} \qquad y = q^{-2g+1}(1 + \cdots + O(q^{n-2g+1})).$$

Ahora, x e y satisfacen una ecuación de la forma $y^2 = F(x)$ donde el polinomio $F(X) \in \mathbb{C}[X]$ es de grado $2g+1$. Así F queda determinado si $n - 2g + 1 > 2(2g+1)$, es decir $n \geq 6g+2$. Por lo tanto, cualquier ecuación hiperelíptica de C depende sólo de los primeros $6g+1$ coefficientes de $f^{(1)}, \ldots, f^{(g)}$.

El caso en que $P \notin \text{Wei}(C)$ es totalmente análogo a éste. □

Observación 3.4. B. Poonen ha observado que la cota $6g+1$ (resp. $3g+2$) se puede reemplazar por $4g+5$ (resp. $2g+4$) utilizando la idea que describimos a continuación. Como antes, tomamos $x = h_{g-1}/h_g$. Consideramos la base $h_i' = x^{g-i} h_g$, $1 \leq i \leq g$, de $\bigoplus_{i=1}^{k} S_2(A_{f_i})$. Determinamos las combinaciones lineales de la base $\{h_1, \ldots, h_g\}$ que proporcionan h_1' y h_2'. Utilizando estas combinaciones obtenemos tantos coeficientes de h_1' y de h_2' como los tomados

para la base $\{h_1, \ldots, h_g\}$. Por último, utilizamos h_1' y h_2' para construir la ecuación tomando

$$x = \frac{h_1'}{h_2'} \qquad \text{e} \qquad y = x^{g-1} \frac{q\, dx/dq}{-2\, h_1'}\,.$$

La ventaja de este método es que habiendo tomado los primeros M coeficientes de Fourier de la base de formas nuevas, obtenemos más coeficientes de Fourier para x e y utilizando h_1' y h_2' que utilizando h_1 y h_2.

Teorema 3.8. *Sea $g \geq 2$ un entero. El conjunto de curvas hiperelípticas modulares nuevas de género g, salvo $\mathbb{Q}$-isomorfismo, es finito. Es decir,*

$$\#\mathcal{MC}_g^{\mathrm{new}}(2) < \infty.$$

Demostración: En primer lugar, observemos que el enunciado del teorema es equivalente a que el conjunto de conjuntos de formas nuevas $f_1, \ldots, f_k \in S_2(N)$ para las cuales existe una curva hiperelíptica C modular nueva de nivel N y de género g que cumple $J(C) \overset{\mathbb{Q}}{\sim} \prod_{i=1}^{k} A_{f_i}$ es finito.

Para facilitar la comprensión de los argumentos utilizados, suponemos que $J(C)$ es $\mathbb{Q}$-simple, es decir, $J(C) \overset{\mathbb{Q}}{\sim} A_f$. Sean $\sigma_1, \ldots, \sigma_g$ las $\mathbb{Q}$-inmersiones de K_f en una clausura algebraica fijada de $\mathbb{Q}$.

Sea a_n el autovalor de f por el operador de Hecke T_n. Entonces a_n es una raíz del polinomio

$$H_n(X) = \prod_{i=1}^{g} (X - {}^{\sigma_i}a_n) = X^g + A_{g-1}^{(n)} X^{m-1} + \cdots + A_0^{(n)}.$$

Se tiene $H_n(X) \in \mathbb{Z}[X]$, ya que $a_n \in \mathcal{O}_{K_f}$. Ahora, utilizando la desigualdad $|{}^{\sigma_i}a_n| \leq \sigma_0(n)\sqrt{n}$ obtenemos la siguiente cota para los coeficientes de $H_n(X)$:

$$|A_{g-i}^{(n)}| \leq \left(\begin{array}{c} g \\ i \end{array} \right) (\sigma_0(n)\sqrt{n})^i \qquad \text{si } 1 \leq i \leq g\,.$$

Con esto queda demostrado que para cada n hay un número finito de posibles valores de a_n. Por el lema 3.7 sabemos que una ecuación hiperelíptica de C depende tan sólo de los primeros $6g+1$ coeficientes de las q-expansiones de una base normalizada de formas nuevas de $S_2(A_f)$ y, por lo tanto, el enunciado queda probado para las curvas con jacobiana $\mathbb{Q}$-simple.

Cuando $J(C)$ no es $\mathbb{Q}$-simple, los mismos argumentos se aplican sin dificultad para cada partición de g, esto es, $1 \leq m_1 \leq \cdots \leq m_k \leq g$ tal que $\sum_{i=1}^{k} m_i = g$, considerando las descomposiciones sobre $\mathbb{Q}$ de $J(C)$ tales que $J(C) \overset{\mathbb{Q}}{\sim} \prod_{i=1}^{k} A_{f_i}$ y $\dim A_{f_i} = m_i$. □

El siguiente resultado será importante para acotar los géneros de las curvas hiperelípticas modulares nuevas.

Teorema 3.9. *Sea (C, π) una curva hiperelíptica modular nueva de nivel N, género $g > 2$ e involución hiperelíptica w. Si C tiene un automorfismo $u \neq \mathrm{id}$ que corresponde a un operador diamante, entonces u es una involución no hiperelíptica y, además, las curvas $C' = C/\langle uw \rangle$ y $C'' = C/\langle u \rangle$ son modulares nuevas de nivel N que satisfacen:*

(i) $J(C) \overset{\mathbb{Q}}{\sim} J(C') \times J(C'')$,

(ii) *C' tiene género 2 y* $J(C') \overset{\mathbb{Q}}{\sim} A_f$, *donde* $f \in S_2(N, \varepsilon)$ *y* $\operatorname{ord} \varepsilon = 2$,

(iii) *$J(C'')$ es un $\mathbb{Q}$-factor de $J_0(N)$ y C'' tiene género 1 ó 3.*

Demostración: Supongamos que C tiene un operador diamante $u \neq \mathrm{id}$. Entonces,

$$J(C) \overset{\mathbb{Q}}{\sim} \prod_{i=1}^{k} A_{f_i} \times A,$$

donde A es un $\mathbb{Q}$-factor de $J_0(N)$ y $f_i \in S_2(N, \varepsilon_i)$ es una forma nueva tal que $\varepsilon_i \neq 1$, si $i = 1, \ldots, k$. Sea W la involución W_N ó $W_N w$, con la condición de que la curva $C' = C/\langle W \rangle$ tenga género $g' \geq 2$ (cf. corolario 2.11). Denotamos por $\phi : C \to C'$ la proyección natural y por K el cuerpo de números que se obtiene como la composición de los cuerpos $K_i = \overline{\mathbb{Q}}^{\ker \varepsilon_i}$ para $i = 1, \ldots, k$. Obsérvese que K es el mínimo cuerpo de definición de W actuando en C. Así, tenemos que C' y ϕ están definidas sobre K. Ahora, utilizando que $\phi^*(H^0(C', \Omega^1)) = H^0(C, \Omega^1)^W$ se tiene

$$(\phi \circ \pi)^*(H^0(C', \Omega^1)) = \pi^*(H^0(C, \Omega^1)^W).$$

Por construcción, tenemos $\pi^*(H^0(C, \Omega^1)) \cap H^0(A_{f_i}, \Omega^1) = S_2(A_{f_i}) dq/q$. Los elementos de $S_2(A_{f_i})$ que quedan estables por W son los pertenecientes al espacio vectorial complejo generado por ${}^{\sigma} f_i + W\, {}^{\sigma} f_i$, donde σ recorre los elementos

de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Por tanto, obtenemos

$$(\phi\circ\pi)^*(H^0(C',\Omega^1))\frac{q}{dq}\cap S_2(A_{f_i}) = \langle {}^\sigma f_i + \lambda_{\sigma,i}\overline{{}^\sigma f_i} \,:\, \sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\rangle_{\mathbb{C}}.$$

Además, este espacio vectorial tiene dimensión $1/2\dim A_{f_i}$, ya que K_{f_i} es una extensión cuadrática imaginaria de un cuerpo de números totalmente real. Como K_i es el mínimo cuerpo de definición de W en A_{f_i}, se tiene que hay algún $\lambda_{\sigma,i}\neq -1$ y esto implica que $\phi\circ\pi$ es no ramificada en $i\infty$. Sea $P=(\phi\circ\pi)(i\infty)$. Utilizando argumentos similares a los de la demostración del apartado (ii) del lema 3.4 y aplicándolos a la curva C', obtenemos que existe una base $\{h_1,\ldots,h_{g'}\}$ de $(\phi\circ\pi)^*(H^0(C',\Omega^1))q/dq$ tal que para cada $i=1,\ldots,g'$ se tiene

$$\begin{cases} h_i &=& q^i &+& O(q^{i+1}) & \text{si } P\notin \mathrm{Wei}(C'),\\ h_i &=& q^{2i-1} &+& O(q^{2\,i}) & \text{si } P\in \mathrm{Wei}(C'). \end{cases}$$

Además, aplicando los argumentos utilizados en la demostración de la proposición 3.5 obtenemos que para cualquier par g_1,g_2 de formas parabólicas linealmente independientes tales que $\langle g_1,g_2\rangle=\langle h_{g'-1},h_{g'}\rangle$ y $g_2\in\langle h_{g'}\rangle$ existe $G(x)\in\mathbb{C}[x]$ de grado $2g'+1$ ó $2g'+2$ sin raíces múltiples tal que las funciones en $X_1(N)$ definidas por

$$X=\frac{g_1}{g_2}\qquad\text{e}\qquad Y=\frac{q\,dX/dq}{g_2}$$

satisfacen la ecuación $Y^2=G(X)$.

Obsérvese que las q-expansiones de las formas parabólicas $h_1,\ldots h_{g'}$ tienen coeficientes en K. Por lo tanto, tomando

$$\begin{cases} g_1 = h_{g'-1}+a\,h_{g'},\\ g_2 = h_{g'}, \end{cases}$$

con $a\in K$, tenemos $Y^2=G(X)$ con $G(x)\in K[x]$. Además, tendremos que la q-expansión de X estará normalizada, es decir, tendrá un desarrollo de Fourier en $i\infty$ de la forma

$$X=\begin{cases} \frac{1}{q}+x_0+\ldots & \text{si } P\notin \mathrm{Wei}(C'),\\ \frac{1}{q^2}+\frac{x_{-1}}{q}+x_0+\ldots & \text{si } P\in \mathrm{Wei}(C'). \end{cases}$$

Cambiando a si es necesario, podemos asumir sin pérdida de generalidad que el coeficiente de la q-expansión de X de grado 0 es cero, es decir, $x_0=0$.

Ahora realizamos el siguiente cambio

$$Y = \begin{cases} -Y & \text{si } P \notin \mathrm{Wei}(C'), \\ -\frac{Y}{2} & \text{si } P \in \mathrm{Wei}(C'). \end{cases}$$

Así, obtenemos que el correspondiente polinomio G es mónico.

Para cualquier $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, definamos

$$X_\tau = \frac{{}^\tau g_1}{{}^\tau g_2} \qquad \text{e} \qquad Y_\tau = \begin{cases} -\frac{q\, dX_\tau/dq}{{}^\tau g_2} & \text{si } P \notin \mathrm{Wei}(C'), \\ -\frac{q\, dX_\tau/dq}{2\,{}^\tau g_2} & \text{si } P \in \mathrm{Wei}(C'). \end{cases}$$

Por construcción, se tiene que X y X_τ (resp. Y e Y_τ) tienen q-expansiones conjugadas por τ. Por lo tanto,

$$Y_\tau^2 = {}^\tau G(X_\tau).$$

Ahora, asumamos que $u = v^2$ para algún operador diamante $v \neq \mathrm{id}$. Vamos a probar que esto no es posible, con lo que quedará demostrado que el orden de u es 2. Sea $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ tal que

$${}^\tau W = Wu = v^{-1}Wv.$$

Entonces, v^{-1} induce un isomorfismo $\psi : C' \to {}^\tau C'$ que hace comutativo el siguiente diagrama

$$\begin{array}{ccc} C & \xrightarrow{v^{-1}} & C \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle{}^\tau\phi} \\ C' & \xrightarrow{\psi} & {}^\tau C'. \end{array}$$

Por lo tanto, existe una matriz $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ y un escalar $e \in K^*$ tales que

$$X_\tau = \frac{aX + b}{cX + d} \qquad \text{e} \qquad Y_\tau = \frac{ey}{(cx + d)^{g'+1}}.$$

Entonces $(\phi \circ \pi)^*\mathbb{C}(C') = ({}^\tau\phi \circ \pi)^*\mathbb{C}({}^\tau C')$ y, por lo tanto,

$$(\phi \circ \pi)^*(H^0(C', \Omega^1)) = ({}^\tau\phi \circ \pi)^*(H^0({}^\tau C', \Omega^1)).$$

Pero esto no es posible, ya que sabemos que existe alguna forma nueva f_i de modo que u no actúa trivialmente en A_{f_i}. Así, se tiene

$$({}^\tau\phi \circ \pi)^*(H^0({}^\tau C', \Omega^1))\frac{q}{dq} \cap S_2(A_{f_i}) = \langle\, {}^\sigma f_i + \lambda_{\sigma,i}\, {}^\sigma\zeta\overline{{}^\sigma f_i} : \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\rangle_{\mathbb{C}},$$

para alguna raíz de la unidad $\zeta \neq 1$. Sin embargo, este espacio vectorial complejo es distinto de

$$(\phi \circ \pi)^*(H^0(C', \Omega^1))dq/q \cap S_2(A_{f_i}) = \langle {}^{\sigma} f_i + \lambda_{\sigma,i} \overline{{}^{\sigma} f_i} : \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rangle_{\mathbb{C}}.$$

Por tanto, concluimos que u no es el cuadrado de ningún operador diamante, lo que demuestra que ord u=2.

Ahora vamos a considerar dos casos dependiendo de si $\sum_{i=1}^{k} \dim A_{f_i}$ es igual o mayor que 2. Primero veamos que el caso mayor que 2 es imposible. Denotemos por $K_0 = \bigcap_{i=1}^{m} K_i$. Como hemos visto antes, todo operador diamante actuando en C tiene orden 2 y, por lo tanto, K_i es un cuerpo cuadrático para $i = 1, \ldots, k$. Utilizando esto, vamos a ver que K_0 es un cuerpo cuadrático; de hecho, probaremos que $K_0 = K$. Supongamos que no es así, es decir, $K_0 = \mathbb{Q}$ y, sin pérdida de generalidad, podemos suponer que $K_1 \cap K_2 = \mathbb{Q}$. En consecuencia, existen $d_1, d_2 \in (\mathbb{Z}/N\mathbb{Z})^*$ tales que

$$\varepsilon_i(d_j) = \delta_{i,j},$$

donde $\delta_{i,j}$ es la función delta de Kronecker con $i, j = 1, 2$. Por lo tanto, los operadores diamante $\langle d_1 \rangle$ y $\langle d_2 \rangle$ actúan en C como automorfismos de orden 2. Además el grupo que generan no contiene a la involución hiperelíptica w y es isomorfo al grupo $(\mathbb{Z}/2\mathbb{Z})^2$. De esta forma, el grupo generado por $\langle d_1 \rangle$, $\langle d_2 \rangle$, w y W_N es isomorfo a $(\mathbb{Z}/2\mathbb{Z})^4$. Pero esto no es posible, ya que una curva hiperelíptica no puede tener un tal subgrupo de automorfismos (Teorema 2.1 de [BGG93]). Con esto, hemos demostrado que $K_0 \neq \mathbb{Q}$, y, por lo tanto, K_0 es un cuerpo cuadrático. Además, por construcción, $K_0 = K$ y u es el único automorfismo de C distinto de la identidad que proviene de un diamante. Denotemos por $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ la conjugación no trivial y por $\langle d \rangle$ el diamante correspondiente a u, entonces

$${}^{\tau} W_N = W_N \langle d \rangle \qquad \text{y} \qquad \varepsilon_i(d) = -1 \quad \text{para } i = 1, \ldots, k\,.$$

Consideramos la curva cociente $C' = C/\langle \langle d \rangle\, w \rangle$. Por definición se obtiene que

$$J(C') \overset{\mathbb{Q}}{\sim} \prod_{i}^{k} A_{f_i}.$$

Así, la curva C' es también hiperelíptica modular nueva de nivel N y, por lo tanto, sin pérdida de generalidad, podemos suponer que $A = \{0\}$. En este caso, u es la involución hiperelíptica de C.

Tomemos pues la curva $C/\langle W_N, u\rangle$. Esta curva es de género 0, ya que es cociente de C por su involución hiperelíptica. Se observa que las funciones X y X_τ son módulos principales de esta curva con un polo simple en la proyección de P. Como ambas tienen q-expansiones normalizadas y $x_0 = {}^\tau x_0 = 0$, deducimos la igualdad

$$X = X_\tau. \tag{3.1}$$

Debido a que W_N actua en el conjunto de puntos de Weierstrass de C como una permutación sin puntos fijos (cf. [Ogg74]), podemos agrupar los $2g+2$ puntos de Weierstrass de C en parejas como sigue:

$$\{Q_1, W_N(Q_1)\}, \ldots, \{Q_{g+1}, W_N(Q_{g+1})\}.$$

Así, tenemos que $W_N(Q_i) \neq Q_i$ para $i = 1, \ldots, g$. Entonces el conjunto de puntos de Weierstrass de C' será $\{\phi(Q_1), \ldots, \phi(Q_{g+1})\}$ y las raíces del polinomio G coinciden con los valores del conjunto $\{X(Q_1), \ldots, X(Q_{g+1})\}$ que son distintos de ∞, donde aquí X se toma como una función en C. Esto también es cierto para ${}^\tau G(x)$, por la igualdad (3.1). Por lo tanto

$$G = {}^\tau G,$$

ya que G y ${}^\tau G$ son mónicos y tienen las mismas raíces. En consecuencia, Y_τ debe de ser Y ó $-Y$. Esto nos asegura que C' y ${}^\tau C'$ son isomorfas, pero entonces

$$(\phi \circ \pi)^*(H^0(C', \Omega^1)) = ({}^\tau\phi \circ \pi)^*(H^0({}^\tau C', \Omega^1)),$$

que es imposible, como hemos visto anteriormente.

Por lo tanto, hemos demostrado que el único caso que se puede dar es $J(C) \overset{\mathbb{Q}}{\sim} A_f \times A$, con A un $\mathbb{Q}$-factor de $J_0(N)$ y $f \in S_2(N, \varepsilon)$ una forma nueva tal que $\operatorname{ord} \varepsilon = 2$ y $\dim A_f = 2$. El grupo de automorfismos generado por u, w y W_N es isomorfo a $(\mathbb{Z}/2\mathbb{Z})^3$. Aplicando el teorema 2.1 de [BGG93], obtenemos que $4 \mid 2(g+1)$ y por lo tanto g es impar. Sea $C' = C/\langle uw\rangle$; entonces por definición se obtiene que C' es una curva hiperelíptica modular nueva de nivel N. Además, se tiene $J(C') \overset{\mathbb{Q}}{\sim} A_f$. Utilizando la fórmula de Hurwitz, obtenemos que los únicos valores posibles para el género de C son 3, 4 ó 5. Como g es impar, sólo es posible $g = 3$ ó 5. La curva $C'' = C/\langle u\rangle$ es una curva modular nueva de nivel N tal que $J(C'') \overset{\mathbb{Q}}{\sim} A$ y, por lo tanto, si $g = 5$ entonces C'' tiene género 3 y es hiperelíptica. Esto concluye la demostración. □

En el siguiente resultado damos cotas explícitas de los posibles géneros de las curvas hiperelípticas modulares nuevas.

Teorema 3.10. *Si (C, π) es una curva hiperelíptica modular nueva de nivel N de género $g > 2$, entonces $g \leq 10$. Además,*

(i) Si $J(C)$ es cociente de $J_0(N)$ y $3|N$, entonces $J(C)$ no es $\mathbb{Q}$-simple, $g = 3$ y $9 \not| N$.

(ii) Si $J(C)$ no es cociente de $J_0(N)$, entonces $J(C)$ es no $\mathbb{Q}$-simple y $g = 3$.

Demostración: La dividiremos en dos partes, dependiendo de si $J(C)$ es un cociente de $J_0(N)$ o no.

Caso 1: $J(C)$ es un cociente de $J_0(N)$: En este caso, se tiene que el morfismo π factoriza a través de $X_0(N)$, es decir, el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} X_1(N) & \xrightarrow{\quad\pi\quad} & C\,. \\ & {\scriptstyle \mathrm{pr}_0} \searrow \quad \nearrow {\scriptstyle \pi_0} & \\ & X_0(N) & \end{array}$$

Por lo tanto, existen k formas nuevas $f_1, \ldots, f_k \in S_2(N, 1)$ tales que se tiene $J(C) \overset{\mathbb{Q}}{\sim} \prod_{i=1}^{k} A_{f_i}$. Denotamos por $f^{(j)} = \sum_{n \geq 1} a_n^{(j)}\, q^n$, $1 \leq j \leq g$, la base de formas nuevas normalizadas de $\bigoplus_{i=1}^{k} S_2(A_{f_i})$. Si $3 \not| N$, tenemos la siguiente desigualdad (ver [Ogg74]):

$$2^{\omega(N)} + \frac{\psi(N)}{6} \leq \#\widetilde{X}_0(N)(\mathbb{F}_9)\,, \tag{3.2}$$

donde $\psi(N) = N \prod p(1 + 1/p)$ con p variando en el conjunto de primos que dividen a N, $\omega(N)$ denota el número de primos dividiendo a N y $\widetilde{X}_0(N)$ denota la reducción de $X_0(N)$ a $\mathbb{F}_9$. Como C es hiperelíptica y $3 \not| N$, tenemos que la reducción de C a $\mathbb{F}_9$, que denotamos por $\widetilde{C}$, también es hiperelíptica. Por lo tanto, $\#\widetilde{C}(\mathbb{F}_9) \leq 20$. De aquí se deduce

$$\#\widetilde{X}_0(N)(\mathbb{F}_9) \leq \operatorname{grado} \pi_0 \cdot \widetilde{C}(\mathbb{F}_9) \leq 20 \operatorname{grado} \pi_0. \tag{3.3}$$

Las proposiciones 1.40 y 1.43 de [Shi71a] nos aseguran que el género de $X_0(N)$ está acotado por $1 + \psi(N)/12$. Ahora, utilizando esta cota y la fórmula de Hurwitz obtenemos

$$\operatorname{grado} \pi_0 \leq \frac{\psi(N)}{12(g-1)}\,.$$

Por tanto, si juntamos esta desigualdad con la cota inferior (3.2) y la cota superior (3.3), obtenemos

$$(g-1)\left(2^{\omega(N)}+\frac{\psi(N)}{6}\right)\leq 10\frac{\psi(N)}{6}\,,$$

que implica $g\leq 10$.

Ahora supongamos que $3|N$. Debido al apartado (iii) del lema 3.4, no es posible que $a_3^{(j)}=a_3^{(i)}$ para todo $1\leq i,j\leq g$. Por lo tanto, $9\not|N$, ya que de lo contrario tendríamos $a_3^{(i)}=0$ para todo $i\leq g$ (ver teorema 1.6). Denotemos por $\epsilon_i(3)$ el valor propio de f_i bajo la involución de Atkin-Lehner W_3. Entonces, existen dos formas nuevas f_i y f_j tales que $\epsilon_i(3)=-\epsilon_j(3)$. Sea la curva cociente $C'=C/\langle W_3\rangle$. Entonces, C' también es modular de nivel N y, además,

$$J(C')\overset{\mathbb{Q}}{\sim}\prod_{\epsilon_i(3)=1}A_{f_i}\,.$$

En consecuencia, el género de C' es mayor que 0. Aplicando de nuevo el lema 3.4 a C' obtenemos que no es hiperelíptica y, por lo tanto, el género de C' es 1. Así, C es una curva bielíptica, es decir, hay un morfismo de grado 2 de C en una curva elíptica. Aplicando la fórmula de Hurwitz a este morfismo, obtenemos que $g\leq 3$.

Caso 2: $J(C)$ no es un cociente de $J_0(N)$: En el teorema 3.9, vimos que en este caso se tiene que $g=3$ ó 5 y que $J(C)\overset{\mathbb{Q}}{\sim}J(C')\times J(C'')$, donde C' es una curva modular nueva de género 2 y $J(C')\overset{\mathbb{Q}}{\sim}A_f$ con $f\in S_2(N,\varepsilon)$ tal que $\operatorname{ord}\varepsilon=2$. En el capítulo 4 determinamos todas las curvas modulares nuevas de género 2 junto con sus niveles, ecuaciones hiperelípticas y sus correspondientes formas nuevas. De estas curvas, sólo hay 11 tales que sus correspondientes formas nuevas tienen carácteres de orden 2. Utilizando las proposiciones 3.5 y 3.6, obtenemos que sólo cinco de éstas admiten recubrimientos de curvas hiperelípticas modulares nuevas, todas ellas de género 3. De hecho, en la sección 6.3.1 demostramos que sólo hay 7 de tales curvas que se muestran en la tabla 6.5. □

Como un corolario de los Teoremas 3.8 y 3.11, obtenemos el principal resultado teórico de esta tesis.

Teorema 3.11. *El conjunto de curvas hiperelípticas modulares nuevas, salvo $\mathbb{Q}$-isomorfismo, es finito. Es decir,*

$$\#\mathcal{MC}^{\mathrm{new}}(2)<\infty\,.$$

Capítulo 4

Curvas modulares nuevas de género 2

Tras haber demostrado en el capítulo 3 que hay un número finito de curvas hiperelípticas modulares nuevas, el objetivo que nos planteamos es el de determinarlas. Es decir, queremos encontrar ecuaciones y los correspondientes morfismos que las hacen modulares. En este capítulo nos restringiremos al caso de curvas de género 2. Recuérdese que toda curva de género 2 es hiperelíptica y, por lo tanto, sabemos que existe sólo un número finito de curvas modulares nuevas de género 2.

Este capítulo está dividido en dos secciones. En la primera mostramos cómo hemos calculado las curvas modulares nuevas de género 2 cuyas jacobianas son $\mathbb{Q}$-simples, mientras que la segunda está dedicada a las curvas que tienen jacobianas no $\mathbb{Q}$-simples.

En ambos casos, el proceso que seguiremos es el siguiente:

(1) **Cálculo de candidatos.** Calcular explícitamente un conjunto de curvas de género 2 que contenga al conjunto de todas las curvas modulares nuevas de este género. Un tal conjunto será denominado un conjunto de candidatos. Para obtener este conjunto, hemos utilizado programas en MATHEMATICA y GP-PARI que hemos creado con este objetivo y están basados en los resultados obtenidos en el capítulo anterior.

(2) **Eliminación.** Establecer cribas suficientemente buenas para descartar del conjunto de candidatos aquéllos que no cumplan alguna de las propiedades

que han de satisfacer las soluciones a nuestro problema. Estas cribas están basadas en propiedades de curvas de género 2 y/o de jacobianas de curvas modulares.

(3) **Búsqueda.** Determinar las correspondientes formas nuevas para cada una de las curvas que han pasado las cribas. Cuando la jacobiana es $\mathbb{Q}$-simple buscamos una forma nueva $f \in S_2(N, \varepsilon)$ tal que $J(C) \overset{\mathbb{Q}}{\sim} A_f$, mientras que en el caso en que no lo sean buscamos dos formas nuevas $f_1, f_2 \in S_2(N, 1)$ tales que $J(C) \overset{\mathbb{Q}}{\sim} A_{f_1} \times A_{f_2}$.

(4) **Comprobación.** Utilizar el criterio de la proposición 3.6 para comprobar que todas las curvas que han pasado las cribas son modulares nuevas. Para ello calcularemos la q-expansión de las formas nuevas encontradas en el anterior paso hasta una determinada cota que dependerá del nivel de la curva modular y comprobaremos que la ecuación hiperelíptica se satisface para esta cota.

Para facilitar el cálculo, este proceso se ha dividido en dos subprocesos dependiendo de si la jacobiana es $\mathbb{Q}$-simple o no. Además, el primero de estos dos casos se ha subdividido a su vez en dos subcasos dependiendo de si la forma nueva asociada tiene un torcimiento extra o no.

Como consecuencia de este laborioso proceso, probaremos que sólo hay 213 curvas modulares nuevas de género 2, salvo $\mathbb{Q}$-isomorfismos. De ellas, 149 tienen jacobiana $\mathbb{Q}$-simple y 64 jacobiana no $\mathbb{Q}$-simple. El resultado principal de este capítulo es el siguiente:

Teorema 4.1. *El conjunto $\mathcal{MC}_2^{\text{new}}$ está formado por las curvas de las tablas 6.1, 6.2 y 6.3. En particular, $\#\mathcal{MC}_2^{\text{new}} = 213$.*

4.1 Con jacobiana $\mathbb{Q}$-simple

A partir de ahora (C, π) será una curva modular nueva de nivel N de género 2 cuya jacobiana es $\mathbb{Q}$-simple. En el capítulo 3, vimos que en este caso existe una forma nueva $f \in S_2(N, \varepsilon)$ tal que el siguiente diagrama es conmutativo

$$\begin{array}{ccc} J_1(N) & \twoheadrightarrow & A_f \overset{\mathbb{Q}}{\sim} J(C) \\ \uparrow & & \uparrow \\ X_1(N) & \twoheadrightarrow & C\,. \end{array}$$

Como se puede observar, este diagrama es similar al existente en el caso de una curva elíptica definida sobre $\mathbb{Q}$, aunque ahora dim $A_f = \dim J(C) = 2$ y, en consecuencia, el cuerpo K_f es un cuerpo cuadrático en lugar de $\mathbb{Q}$. Además, en este caso, $\mathcal{N}_{\mathbb{Q}}(J(C)) = \mathcal{N}_{\mathbb{Q}}(A_f) = N^2$, mientras que en el caso elíptico el conductor geométrico coincide con el nivel.

La forma nueva normalizada f tendrá una q-expansión de la forma

$$f = \sum_{n\geq 1} a_n\, q^n\,,$$

cuyos coeficientes pertenecerán a un cuerpo cuadrático $K_f = \mathbb{Q}(\sqrt{d})$, siendo d un entero libre de cuadrados. Denotamos por σ al automorfismo no trivial de $\mathrm{Gal}(K_f/\mathbb{Q})$. Definamos las formas modulares siguientes

$$\begin{cases} h_1 = \dfrac{f + {}^{\sigma}f}{2} = q + \displaystyle\sum_{n\geq 2} \frac{a_n + {}^{\sigma}a_n}{2}\, q^n\,, \\ h_2 = \dfrac{f - {}^{\sigma}f}{2\sqrt{d}} = \displaystyle\sum_{n\geq 2} B_n\, q^n\,. \end{cases}$$

Por construcción se tiene

$$S_2(A_f) = \langle h_1, h_2\rangle_{\mathbb{C}} \qquad \text{y} \qquad h_1, h_2 \in \frac{1}{2}\,\mathbb{Z}[[q]].$$

Ahora definimos

$$n_0 = \min\{n \in \mathbb{Z} \,:\, B_n \neq 0\} = \min\{n \in \mathbb{Z} : a_n \notin \mathbb{Z}\}\,.$$

El lema 3.4 y la proposición 3.5 aplicados a este caso establecen el siguiente resultado.

Proposición 4.2. *Sea $P = \pi(i\infty)$. Entonces las funciones de $X_1(N)$ definidas por*

$$x = \frac{h_1}{h_2} \qquad e \qquad y = \frac{q\,dx/dq}{h_2},$$

satisfacen una ecuación $y^2 = F(x)$ con $F(X) \in \mathbb{Q}[X]$ sin raíces múltiples tal que:

(i) Si $P \notin \mathrm{Wei}(C)$ entonces $n_0 = 2$, en cuyo caso $K_f = \mathbb{Q}(a_2)$ y el grado de F es 6.

(ii) Si $P \in \mathrm{Wei}(C)$ *entonces* $n_0 = 3$*, en cuyo caso* $K_f = \mathbb{Q}(a_3)$ *y el grado de* F *es* 5*.*

Para facilitar los cálculos, el siguiente resultado nos será de gran utilidad.

Proposición 4.3. *Si* $P \in \mathrm{Wei}(C)$*, entonces* $a_{2n} = 0$ *para todo* $n \geq 1$ *y, en particular,* $4 \mid N$*.*

Demostración: Supongamos que $P \in \mathrm{Wei}(C)$. Denotemos por a_n a $A_n + B_n\sqrt{d}$ donde $A_n, B_n \in \mathbb{Q}$. Sabemos por la proposición anterior que $n_0 = 3$, y en particular $B_2 = 0$ y $B_3 \neq 0$. Denotemos por $\varepsilon(2)$ a $C_2 + D_2\sqrt{d}$ y tomemos la base de $S_2(A_f)$ formada por

$$g_1 = \frac{f + {}^{\sigma}f}{2} \qquad \text{y} \qquad g_2 = \frac{f - {}^{\sigma}f}{2B_3\sqrt{d}}.$$

Definamos también las funciones

$$u = \frac{g_1}{g_2} = q^{-2} + O(q^{-1}) \qquad \text{y} \qquad v = \frac{q\,dx/dq}{g_2} = q^{-5} + O(q^{-4}).$$

Como x e y satisfacen $y^2 = F(x)$, la proposición 3.5 nos asegura que u y v satisfacen $v^2 = G(u)$, donde G un polinomio de grado 5 sin raíces repetidas. Para construir G, empezamos igualando los coeficientes de v^2 y u^5 de menor grado. Así, obtenemos

$$v^2 - u^5 = -4\left(\frac{A_2B_3 + D_2}{B_3}\right) q^{-9} + O(q^{-8}).$$

Como $\mathrm{ord}_{i\infty}\, u = 2$ se tiene que $A_2B_3 + D_2 = 0$. Veremos que $A_2 = 0 = D_2$, y para ello diferenciamos dos casos:

- $2|N$: En este caso, $D_2 = 0$ y concluimos que $A_2 = 0$.
- $2\not|N$: A partir de la igualdad $\overline{a_2} = \overline{\varepsilon}(2)\, a_2$, deducimos que $A_2 = 0$ ó $\varepsilon(2) = 1$. De cualquiera de las dos condiciones obtenemos $A_2 = 0 = D_2$.

Ahora igualando los coeficientes de q^{-8} se tiene

$$v^2 - \left(u^5 + \frac{5\,A_3B_3 - 3\,B_5}{B_3}\, u^4\right) = 12\,C_2\, q^{-7} + O(q^{-6}).$$

Por lo tanto, $C_2 = 0$. Hemos visto que $a_2 = 0 = \varepsilon(2)$. Esto implica, por las relaciones de recurrencia de los coeficientes de la q-expansión de una forma nueva, que $a_{2n} = 0$ para $n \geq 1$. Para demostrar que $4|N$ basta con observar que si $p|N$ y $a_p = 0$, entonces $p^2|N$. □

En primer lugar, vamos a delimitar los posibles cuerpos K_f, de los cuales sabemos que

$$K_f = \mathbb{Q}(a_{n_0}) = \mathbb{Q}[X]/\langle R_{n_0}(X)\rangle \qquad n_0 = 2 \text{ ó } 3,$$

donde $R_{n_0}(X) = X^2 + r_{n_0}\, X + s_{n_0} \in \mathbb{Z}[X]$ es el polinomio irreducible de a_{n_0}. Como n_0 es primo, la desigualdad de Weil nos asegura que el valor absoluto de cada una de sus raíces es menor o igual que $2\sqrt{n_0}$. Sean $a_n = A_n + B_n\sqrt{d}$ con $A_n, B_n \in \frac{1}{2}\,\mathbb{Z}$. Dependiendo de si a_2 ó a_3 genera K_f tenemos:

- Si $K_f = \mathbb{Q}(a_2)$ entonces

$$0 < |B_2|\sqrt{|d|} = \frac{|a_2 - {}^{\sigma}a_2|}{2} \leq \frac{|a_2| + |{}^{\sigma}a_2|}{2} \leq 2\,\sqrt{2}\,.$$

  El mínimo valor para $|B_2|$ es $\frac{1}{2}$ ó 1 dependiendo de si $d \equiv 1 \pmod 4$ o no. Por lo tanto,

$$|d| \leq \begin{cases} 31 & \text{si } d \equiv 1 \pmod 4, \\ 7 & \text{si } d \not\equiv 1 \pmod 4. \end{cases}$$

- Si $K_f = \mathbb{Q}(a_3)$, obtenemos

$$|d| \leq \begin{cases} 47 & \text{si } d \equiv 1 \pmod 4, \\ 11 & \text{si } d \not\equiv 1 \pmod 4, \end{cases}$$

  con un argumento similar al caso $K_f = \mathbb{Q}(a_2)$.

Este resultado puede mejorarse, reduciendo los posibles valores para d, si distinguimos los casos en que f tiene un torcimiento extra o no.

En el caso en que f tenga un torcimiento extra (σ, χ), los autovalores a_p y d satisfacen condiciones adicionales. Así, si el orden de χ es igual a 2 entonces para todo primo $p \not| N$ se tiene

$$a_p = \begin{cases} x_p & \in \mathbb{Z} & \text{si } \chi(p) = 1\,, \\ y_p\sqrt{d} & \in \mathbb{Z}[\sqrt{d}] & \text{si } \chi(p) = -1\,. \end{cases} \tag{4.1}$$

Si por el contrario $\operatorname{ord}\chi \neq 2$, entonces $\varepsilon \neq 1$ y $\operatorname{ord}\varepsilon > 2$. Debido a las leyes de recurrencia de los coeficientes de la q-expansión de una forma nueva $f \in S_2(N,\varepsilon)$, sabemos que el cuerpo generado por los valores del carácter ε es un subcuerpo del cuerpo de coeficientes de f, es decir, $\operatorname{Im}\varepsilon \subset K_f$. Ahora, como K_f es un cuerpo cuadrático, se tiene que los únicos órdenes posibles para ε son $1, 2, 3, 4$ ó 6. Por lo tanto, si p es un primo tal que $p|N$ obtenemos que $\varepsilon(p) = 0$, mientras que si $p\not|N$, se tiene

$$\varepsilon(p) \in (\operatorname{Im}\varepsilon)^* = \begin{cases} \{1\} & \text{si } \operatorname{ord}\varepsilon = 1, \\ \{\pm 1\} & \text{si } \operatorname{ord}\varepsilon = 2, \\ \{\pm 1, \pm\zeta^2\} & \text{si } \operatorname{ord}\varepsilon = 3, \\ \{\pm 1, \pm i\} & \text{si } \operatorname{ord}\varepsilon = 4, \\ \{\pm 1, \pm\zeta, \pm\zeta^2\} & \text{si } \operatorname{ord}\varepsilon = 6, \end{cases} \tag{4.2}$$

donde ζ es una raíz sexta primitiva de la unidad.

Utilizando estos hechos junto al resultado de que K_f es totalmente real si y sólo si $\varepsilon = 1$, se obtiene

$$K_f = \begin{cases} \mathbb{Q}(\sqrt{d}) & d > 0 \quad \text{si ord } \varepsilon = 1, \\ \mathbb{Q}(\sqrt{d}) & d < 0 \quad \text{si ord } \varepsilon = 2, \\ \mathbb{Q}(\sqrt{-3}) & \quad\;\; \text{si ord } \varepsilon = 3 \text{ ó } 6, \\ \mathbb{Q}(i) & \quad\;\; \text{si ord } \varepsilon = 4, \end{cases}$$

y las siguientes posibilidades para d:

- Caso con torcimiento extra:
  - Si $n_0 = 2$, $d \in \{-1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7\}$.
  - Si $n_0 = 3$, $d \in \{-1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7, \pm 10, \pm 11\}$.
- Caso sin torcimiento extra:
  - Si $n_0 = 2$, $d \in \{2, 3, 5, 6, 7, 13, 17, 21, 29\}$.
  - Si $n_0 = 3$, $d \in \{2, 3, 5, 6, 7, 10, 11, 13, 17, 21, 29, 33, 37, 41\}$.

4.1.1 Cálculo de candidatos

En esta sección vamos a calcular un conjunto de curvas de género 2 que contendrá todas las curvas modulares nuevas de género 2 tales que sus jacobianas sean $\mathbb{Q}$-simples.

Para calcular las posibles ecuaciones de estas curvas, primero hemos creado dos programas en MATHEMATICA, uno para el caso en el cual el polinomio $F(X)$, como en la proposición 4.2, es de grado 5, es decir, $n_0 = 3$, y otro cuando $F(X)$ es de grado 6, esto es, $n_0 = 2$. Los pasos del programa son los siguientes

(1) Introducimos una expresion formal

$$f = q + a_2\, q^2 + \cdots + a_{M_{n_0}}\, q^{M_{n_0}} + O(q^{M_{n_0}+1}),$$

que representa una forma nueva normalizada genérica de carácter ε y donde

$$M_{n_0} = \begin{cases} 22 & \text{si } n_0 = 3, \\ 16 & \text{si } n_0 = 2. \end{cases}$$

Los coeficientes de f son de la forma

$$a_n = A_n + B_n\sqrt{d}$$

para ciertas variables A_n, B_n y d. Estos coeficientes satisfacen las leyes de recurrencia de los coeficientes de la q-expansión de una forma nueva normalizada y, por lo tanto, sólo dependen de A_p y B_p donde

$$p = \begin{cases} 3,5,7,11,13,17,19 & \text{si } n_0 = 3, \\ 2,3,5,7,11,13, & \text{si } n_0 = 2, \end{cases}$$

y de

$$\begin{cases} \varepsilon(3) & \text{si } n_0 = 3, \\ \varepsilon(2), \varepsilon(3) & \text{si } n_0 = 2, \end{cases}$$

ya que por la proposición 4.3, impondremos las condiciones adicionales $a_2 = \varepsilon(2) = 0$, para el caso $n_0 = 3$.

Denotaremos $\varepsilon(p) = C_p + D_p\sqrt{d}$ para $p = 2, 3$.

(2) Calculamos x e y de la siguiente forma. Primero calculamos

$$h_1 = \frac{f + {}^{\sigma}f}{2} \qquad \text{y} \qquad h_2 = \frac{f - {}^{\sigma}f}{2B_{n_0}\sqrt{d}}.$$

A partir de éstas obtenemos

$$x = \frac{h_1}{h_2} \qquad \text{e} \qquad y = \frac{q\, dx/dq}{h_2}\,.$$

(3) Calculamos el polinomio

$$F_{n_0}(X) = \sum_{i=0}^{6} A_{n_0,i}\, X^i$$

tal que $y^2 - F_{n_0}(x) = O(q)$.

(4) Calculamos el polinomio en q

$$y^2 - F_{n_0}(x) = \sum_{m=1}^{8} Q_{n_0,m}(\{a_n\}_{2\le n\le M_{n_0}})\, q^m\,,$$

obteniendo que $Q_{n_0,1}, \ldots, Q_{n_0,8} \in \frac{1}{2}\mathbb{Z}[a_2, \ldots, a_{M_{n_0}}]$.

Así, toda curva modular nueva de género 2 es $\mathbb{Q}$-isomorfa a $y^2 = F_{n_0}(x)$, con $n_0 = 2$ ó $n_0 = 3$ y para ciertos valores $a_2, \ldots, a_{M_{n_0}}$ que corresponden a los primeros M_{n_0} coeficientes de la q-expansión de la forma nueva correspondiente. Además, como $y^2 = F_{n_0}(x)$, se tendrá

$$Q_{n_0,1}(\{a_n\}_{2\le n\le M_{n_0}}) = \cdots = Q_{n_0,8}(\{a_n\}_{2\le n\le M_{n_0}}) = 0.$$

Es decir, tenemos un método para calcular un conjunto de candidatos. Para hacer efectivo este método, el siguiente paso que haremos es precisar todas las posibilidades para cada a_p, $p \le M_{n_0}$.

Fijados d y $\operatorname{ord}\varepsilon$, determinaremos dos subconjuntos $S_p^{\mathrm{n}}(d)$ y $S_p^{\mathrm{s}}(d)$ del anillo de enteros de $\mathbb{Q}(\sqrt{d})$, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, tales que $a_p \in S_p^{\mathrm{n}}(d)$ cuando $p \nmid N$ y $a_p \in S_p^{\mathrm{s}}(d)$ cuando $p|N$. Para determinar $S_p^{\mathrm{n}}(d)$ diferenciaremos dos casos según que f tenga un torcimiento extra o no. Tomaremos el conjunto $S_p(d) = S_p^{\mathrm{n}}(d) \cup S_p^{\mathrm{s}}(d)$ y $a_p \in S_p(d)$ para todo primo p.

En primer lugar, consideramos el caso $p|N$. Tenemos:

- Si $\varepsilon = 1$, entonces $a_p \in \{0, \pm 1\}$.
- Si $\varepsilon \neq 1$, entonces, o bien $a_p = 0$, o bien $|a_p|^2 = 1$ ó p. Obsérvese que estas últimas condiciones sólo tienen un número finito de soluciones, ya que a_p es un entero algebraico y K_f un cuerpo cuadrático imaginario.

Por lo tanto, tomamos

$$S_p^{\mathrm{s}}(d) = \begin{cases} \{0, \pm 1\} & \text{si } \varepsilon = 1, \\ \{\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \mid |\alpha|^2 = 0,\ 1 \text{ ó } p\} & \text{si } \varepsilon \neq 1. \end{cases}$$

Con torcimiento extra. Sea χ el carácter asociado a un torcimiento extra de f y supongamos que $p \nmid N$. Consideramos los siguientes casos:

- Si $\chi^2 = 1$, utilizando (4.1) y la cota de Weil obtenemos

$$S_p^{\mathrm{n}}(d) = \{a \in \mathbb{Z} \,|\, |a| \leq 2\sqrt{p}\} \cup \left\{ b\sqrt{d} \,|\, b \in \mathbb{Z}, |b| \leq 2\sqrt{\frac{p}{|d|}} \right\}.$$

- Si $\chi^2 \neq 1$, tomamos $\chi = \varepsilon^{-1}$ y usando de nuevo la cota de Weil, obtenemos los siguientes subcasos:
  - Si $\operatorname{ord}\varepsilon = 4$, entonces $d = -1$ y se tiene

$$S_p^{\mathrm{n}}(-1) = \left\{a \in \mathbb{Z} \,|\, |a| \leq 2\sqrt{p}\right\} \cup \left\{b\, i \,|\, b \in \mathbb{Z}, |b| \leq 2\sqrt{p}\right\} \cup \left\{a^{\,\sigma}(1+i) \,|\, a \in \mathbb{Z}, |a| \leq \sqrt{2p}, \sigma \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})\right\}.$$

  - Si $\operatorname{ord}\varepsilon = 3$, entonces $d = -3$ y se tiene

$$S_p^{\mathrm{n}}(-3) = \left\{a \in \mathbb{Z} \,|\, |a| \leq 2\sqrt{p}\right\} \cup \left\{a^{\,\sigma}\zeta \,|\, a \in \mathbb{Z}, |a| \leq 2\sqrt{p}, \sigma \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})\right\},$$

    donde ζ es una raíz sexta primitiva de la unidad.
  - Si $\operatorname{ord}\varepsilon = 6$, entonces $d = -3$ y el conjunto $S_p^{\mathrm{n}}(-3)$ es la unión del calculado anteriormente con el siguiente conjunto:

$$\left\{ b\sqrt{-3} \,|\, b \in \mathbb{Z}, |b| \leq 2\sqrt{\tfrac{p}{3}} \right\} \cup \left\{ b^{\,\sigma}(1+\zeta) \,|\, b \in \mathbb{Z}, |b| \leq 2\sqrt{\tfrac{p}{3}}, \sigma \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \right\}.$$

Por lo tanto, $S_p(d)$ está completamente determinado.

Sin torcimiento extra. Cuando f no tiene ningún torcimiento extra, los primos p que no dividen al nivel no nos proporcionan información adicional de los coeficientes a_p de la q-expansión, y sólo utilizaremos la cota de Weil para estos valores (que también se satisface cuando p divide al nivel). Así, dependiendo de d, tomaremos:

- Si $d \equiv 1 \pmod 4$:

$$\left\{ a + b\sqrt{d} \,|\, a, b \in \frac{1}{2}\mathbb{Z}, a + b \in \mathbb{Z}, |a| \leq 2\sqrt{p}, |b| \leq 2\sqrt{\frac{p}{|d|}} \right\}.$$

- Si $d \not\equiv 1 \pmod 4$:

$$\left\{ a + b\sqrt{d} \,|\, a, b \in \mathbb{Z}, |a| \leq 2\sqrt{p}, |b| \leq 2\sqrt{\frac{p}{|d|}} \right\}.$$

Además se tiene que $\varepsilon = 1$ y, por lo tanto, $d > 0$ e $\operatorname{Im} \varepsilon = \{0, \pm 1\}$.

Utilizando MATHEMATICA calcularemos, para cada d y cada $\operatorname{ord} \varepsilon$ posibles, los conjuntos $S_p(d)$ para los primos $p < M_{n_0}$ y distinguimos $S_p(d)$ según la forma nueva tenga un torcimiento extra o no. También, para cada $\operatorname{ord} \varepsilon$ posible calculamos $\operatorname{Im} \varepsilon$. Todos estos datos junto con los polinomios $F_{n_0}, Q_{n_0,1}, \ldots, Q_{n_0,8}$ los traducimos al lenguaje de GP-PARI [BBCO].

Ahora en GP-PARI implementamos dos algoritmos, dependiendo de si la forma nueva tiene o no algún torcimiento extra. Una vez fijados $d, \operatorname{ord} \varepsilon$ y n_0, estos algoritmos calculan un conjunto formado por elementos de la forma $(F(X), \{a_n\}_{2 \leq n \leq M_{n_0}}, \operatorname{ord} \varepsilon, d)$ tales que la curva definida por $C : Y^2 = F(X)$ es candidata a ser una curva modular nueva de género 2, donde $J(C) \overset{\mathbb{Q}}{\sim} A_f$, f es candidata a ser una forma nueva tal que el orden de su carácter es $\operatorname{ord} \varepsilon$, $K_f = \mathbb{Q}(\sqrt{d})$ y la q-expansión de f es de la forma $q + \sum_{n=2}^{M_{n_0}} a_n q^n + O(q^{M_{n_0}+1})$. Los pasos de cada uno de los dos algoritmos son los siguientes:

Algoritmo: Fijados: $d, \operatorname{ord} \varepsilon$ y n_0:
ENTRADA: $\{a_p \,|\, p < M_{n_0}$ con p primo y $a_p \in S_p(d)\}$ y $\varepsilon(2), \varepsilon(3) \in \operatorname{Im} \varepsilon$.
PASO 1: Calculamos a_n con $n \leq M_{n_0}$ utilizando las leyes de recurrencia.
PASO 2: Sustituimos $\{a_n\}_{2 \leq n \leq M_{n_0}}$ en $F = F_{n_0}, Q_{n_0,1}, \ldots, Q_{n_0,8}$.
SALIDA: Si $Q_{n_0,1}(\{a_n\}_{2 \leq n \leq M_{n_0}}) = \cdots = Q_{n_0,8}(\{a_n\}_{2 \leq n \leq M_{n_0}}) = 0$ y $F(X)$ no tiene raíces múltiples, el algoritmo devuelve $(F(X), \{a_n\}_{2 \leq n \leq M_{n_0}}, \operatorname{ord} \varepsilon, d)$.

Introducidas todas las posibles entradas en el algoritmo (aproximadamente un total de $4 \cdot 10^{14}$), el cálculo ha tardado unos 6 meses en varios ordenadores SUN. Tras este cálculo hemos obtenido un conjunto de candidatos, de los que algunos de éstos sólo difieren en el término $\{a_n\}_{2 \leq n \leq M_{n_0}}$. Para simplificar el proceso de eliminación hemos tomado las salidas de nuestro algoritmo de la forma $(F(X), \{a_n\}_{2 \leq n \leq M'_{n_0}}, k, d)$, donde

$$M'_{n_0} = \begin{cases} 11 & \text{si } n_0 = 3, \\ 7 & \text{si } n_0 = 2. \end{cases}$$

Si $(F(X), \{a_n\}_{2 \leq n \leq M'_{n_0}}, k, d)$ es un candidato, no tendremos en cuenta el candidato obtenido al cambiar $\{a_n\}_{2 \leq n \leq M'_{n_0}}$ por $\{{}^{\sigma}a_n\}_{2 \leq n \leq M'_{n_0}}$, ya que A_f es $\mathbb{Q}$-isógena a $A_{\sigma f}$ (σ es el automorfismo no trivial de K_f).

Así, obtenemos un total de 3168 candidatos, de ellos 1416 corresponden al caso sin torcimiento extra y 1752 al caso con torcimiento extra.

4.1.2 Criterios de eliminación

En esta sección estableceremos cribas para eliminar los candidatos que no corresponden a curvas modulares nuevas de género 2 con jacobiana $\mathbb{Q}$-simple. Estas cribas están basadas en propiedades de curvas modulares y de curvas hiperelípticas. Para ello separaremos el caso en el que hay torcimiento extra del que no lo hay.

Con torcimiento extra

Primero estableceremos seis cribas para el caso en el que la supuesta forma nueva tenga un torcimiento extra.

Primera criba. La siguiente proposición nos proporciona el primer criterio para eliminar las soluciones que no son buenas.

Proposición 4.4. *Sea $f \in S_2(N,\varepsilon)$ una forma nueva con un torcimiento extra y tal que* $\dim A_f = 2$. *Definamos*

$$n = \begin{cases} \operatorname{ord}\varepsilon & si \quad \varepsilon \neq 1, \\ 2 & si \quad \varepsilon = 1. \end{cases}$$

Entonces, para todo primo p tal que $p \nmid N$, el polinomio característico $Q_{p^n}(t)$ del endomorfismo de Frobenius Frob_{p^n} *actuando en el módulo de Tate de $A_{f/\mathbb{F}_p}$ es de la forma:*

$$Q_{p^n}(t) = (t^2 - a\,t + p^n)^2\,, \quad con \quad a \in \mathbb{Z}\,. \tag{4.3}$$

Demostración: Esta proposición es un caso particular de la proposición 6.2 de [BG97] para el caso de dimensión dos, aunque aquí también incluimos el caso con multiplicación compleja. Por la igualdad de Eichler-Shimura, si $p \nmid N$ tenemos que existe un entero algebraico α_p tal que:

$$a_p = \alpha_p + \overline{\alpha_p}\varepsilon(p)\,,\ \ \alpha_p\overline{\alpha_p} = p\,,\ \ Q_p(t) = (t^2 - a_p t + p\,\varepsilon(p))(t^2 - {}^{\sigma}a_p t + p\,{}^{\sigma}\varepsilon(p))\,.$$

Sea (σ, χ) un torcimiento extra de f, si $\varepsilon \neq 1$, tomaremos $\chi = \varepsilon^{-1}$. Así, se tiene que ${}^{\sigma}a_p = \chi(p)a_p$ y de aquí se sigue:

$$a_p^n \in \mathbb{Z} \qquad \text{y} \qquad a_p^2\chi(p) \in \mathbb{Z}\,,$$

donde recordemos que $n = \operatorname{ord}\,\chi$.

Pongamos $a = \alpha_p^n + (\overline{\alpha_p}\chi(p)^{-1})^n$, entonces utilizando el Lema 6.1 de [BG97] obtenemos que

$$a = \begin{cases} a_p^n \displaystyle\sum_{i=1}^{[n/2]} (-1)^i \frac{n}{n-i} p^i (a_p^2\chi(p))^{-i} & \text{si } a_p \neq 0, \\ 0 & \text{si } a_p = 0 \text{ y } n \equiv 1 \pmod 2, \\ 2(-1)^{n/2}(p\chi(p)^{-1})^{n/2} & \text{si } a_p = 0 \text{ y } n \equiv 0 \pmod 2. \end{cases}$$

Por lo tanto, $a \in \mathbb{Z}$ y concluimos que $Q_{p^n}(t) = (t^2 - a\,t + p^n)^2$. □

Aplicando la anterior proposición al conjunto de 1752 curvas eliminamos las curvas tales que el correspondiente polinomio $Q_{p^n}(t)$ asociado a su jacobiana no es de la forma (4.3) para algún primo $p < 100$ que no divide al discriminante de la ecuación hiperelíptica de la curva.

El número de candidatos ha descendido de 1752 a 288.

Segunda criba. Esta criba está basada en el siguiente resultado:

Teorema 4.5. *Sea A una variedad abeliana definida sobre $\mathbb{Q}$ y sea p un primo tal que $p \not| \mathcal{N}_{\mathbb{Q}}(A)$. Entonces*

$$\mathbb{Q} \otimes \operatorname{End}_{\mathbb{Q}}(A) \hookrightarrow \mathbb{Q} \otimes \operatorname{End}_{\mathbb{F}_p}(A_{/\mathbb{F}_p})\,.$$

Demostración: Ver [ST61]. □

En nuestro caso $A = A_f$ es una superficie abeliana para alguna forma nueva f. Por lo tanto,

$$\mathbb{Q} \otimes \operatorname{End}_{\mathbb{Q}}(A) = \mathbb{Q}(\sqrt{d}),$$

para algún entero d libre de cuadrados. Con este teorema hemos descartado las curvas tales que el correspondiente cuerpo cuadrático $\mathbb{Q}(\sqrt{d})$ no está contenido en la $\mathbb{Q}$-algebra de $\mathbb{F}_p$-endomorfismos de su jacobiana para algún primo $p \leq 29$ que no divide al discriminante de la ecuación hiperelíptica de la curva.

Tras esta criba, sólo 94 candidatos permanecen.

Observación 4.1. Calculando los invariantes de Clebsch (cf. [Bol88]), hemos comprobado que cada una de estas curvas tienen involuciones no hiperelípticas y por lo tanto sus jacobianas no son absolutamente simples.

Tercera criba. La observación 4.1 nos asegura que las 94 curvas que han pasado la segunda criba tienen jacobiana no $\overline{\mathbb{Q}}$-simple. De hecho, hemos comprobado que todas ellas tienen involuciones no hiperelípticas. Ahora, como A_f es $\mathbb{Q}$-simple, $J(C)$ ha de serlo también. El siguiente lema nos proporcionará un criterio para eliminar aquellas curvas tales que su jacobiana no sea $\mathbb{Q}$-simple; para ello utilizaremos las involuciones no hiperelípticas.

Lema 4.6. *Sea C una curva de género 2 definida sobre $\mathbb{Q}$ que tiene una involución no hiperelíptica definida sobre un cuerpo de números K. Entonces*

$$J(C) \overset{K}{\sim} E \times E' ,$$

donde E y E' son curvas elípticas definidas sobre K.

Demostración: Ver [CGLR99]. □

Hemos calculado las involuciones no hiperelípticas para las 94 curvas, así como sus cocientes elípticos. Descartamos las curvas que admiten involuciones hiperelípticas definidas sobre $\mathbb{Q}$, ya que sus jacobianas no son $\mathbb{Q}$-simples.

Esta criba la han pasado 79 candidatos.

Cuarta criba. Sea $f \in S_2(N, \varepsilon)$ una forma nueva normalizada tal que A_f es una superficie abeliana. Asimismo, sea p un primo que no divide a N y, como en la proposición 4.4, denotemos por $Q_p(t)$ el polinomio característico del endomorfismo de Frobenius Frob_p actuando en el módulo de Tate de $A_{f/\mathbb{F}_p}$. Por la congruencia de Eichler-Shimura, sabemos que

$$Q_p(t) = (t^2 - a_p\, t + \varepsilon(p)\, p)(t^2 - {}^{\sigma}a_p\, t + {}^{\sigma}\varepsilon(p)\, p) ,$$

donde a_p es el autovalor de f con respecto al operador de Hecke T_p.

Si tenemos un candidato y $p \leq M'_{n_0}$ es un primo que no divide al discriminante de la ecuación hiperelíptica de la curva con $a_p \neq 0$, entonces $\varepsilon(p)$ está determinado por a_p, ya que $\varepsilon(p) = a_p/{}^{\sigma}a_p$. Así, eliminamos los candidatos

tales que para algún primo p como antes, el polinomio $Q_p(t)$ asociado a la jacobiana de la curva no coincide con el polinomio

$$(t^2 - a_p\, t + \varepsilon(p)\, p)(t^2 - {}^{\sigma}a_p\, t + {}^{\sigma}\varepsilon(p)\, p).$$

Con esta criba hemos eliminado 15 candidatos y, por lo tanto, sólo 64 la han pasado.

Quinta criba. Si C es una curva modular nueva de género 2 con jacobiana $\mathbb{Q}$-simple, tenemos que $A_f \overset{\mathbb{Q}}{\sim} J(C)$ para alguna forma nueva $f \in S_2(N)$. Como ya hemos mencionado anteriormente, sabemos que

$$\mathcal{N}_{\mathbb{Q}}(A_f) = \mathcal{N}_{\mathbb{Q}}(J(C)) = N^2.$$

Con este resultado eliminamos las curvas tales que $\mathcal{N}_{\mathbb{Q}}(J(C))$ no es un cuadrado. Para ello hemos utilizado el programa `genus2reduction` de Quing Liu ([Liu]) que calcula la parte impar del conductor geométrico de la jacobiana de una curva de género 2 definida sobre $\mathbb{Q}$.

Con esta criba sólo hemos descartado dos candidatos. Así, sólo nos quedan 62.

Sexta criba. En el proceso de criba hemos obtenido candidatos tales que las correspondientes curvas son $\mathbb{Q}$-isomorfas. El quinto apartado del teorema 1.9 nos permitirá concluir que dos candidatos de esta forma no pueden ser soluciones a nuestro problema.

Observando los candidatos, vemos que de los 62 que pasaron la anterior criba, hay 9 parejas de soluciones que comparten curva, es decir que sólo hay 53 polinomios distintos. Por lo tanto, como mucho habrá 53 soluciones con torcimiento extra a nuestro problema.

En la sección 4.1.3 mostraremos el método para encontrar la forma nueva asociada a cada una de las 53 curvas que han pasado las seis cribas. Así determinaremos, de cada una de las 9 parejas de candidatos que comparten curva, cuál es la correcta.

Sin torcimiento extra

Ahora queremos determinar los casos en que la forma nueva asociada no tiene torcimiento extra. En este caso, la variedad abeliana es $\overline{\mathbb{Q}}$-simple, lo cual implica que una condición que tendrán que satisfacer los candidatos es que las jacobianas asociadas de sus curvas sean $\overline{\mathbb{Q}}$-simples.

Las cribas que utilizaremos para descartar candidatos en este caso serán algunas de las utilizadas en la sección anterior, junto con una basada en el hecho de que la jacobiana es $\overline{\mathbb{Q}}$-simple.

Primera criba. Esta criba está basada en el lema 4.6. Eliminaremos todos los candidatos tales que las curvas correspondientes tengan alguna involución no hiperelíptica. Para ello utilizaremos los resultados de Bolza [Bol88] que nos permiten, calculando los invariantes de Clebsch, determinar si una curva de género 2 tiene involuciones no hiperelípticas.

Con esta criba pasamos de 1416 candidatos a 1324.

Segunda criba. Utilizamos la segunda criba del caso con torcimiento extra que nos permite pasar a sólo 102 candidatos.

Tercera criba. En este paso utilizaremos la cuarta criba del caso con torcimiento extra para reducir el número de candidatos a 99.

Cuarta criba. Por último, utilizamos la sexta criba del caso con torcimiento extra. Aquí tenemos cuatro candidatos que tienen curvas $\mathbb{Q}$-isomorfas. Por lo tanto, sólo falta determinar la forma nueva correcta. De este modo, concluimos con sólo 96 candidatos.

4.1.3 Búsqueda

En este apartado mostraremos el método utilizado para encontrar la forma nueva asociada a los candidatos que han pasado todas las cribas. Para conseguir esto, primero determinaremos el nivel N y el carácter ε de la correspondiente forma nueva. Después, de todas las formas nuevas en $S_2(N, \varepsilon)$ buscaremos aquellas que los primeros M'_{n_0} coeficientes de las correspondientes q-expansiones coincidan con los de nuestro candidato.

En cuanto al nivel, sabemos que $N = \sqrt{\mathcal{N}_{\mathbb{Q}}(J(C))}$. Sea $N = 2^k M$ con M un entero positivo impar. Calculamos la parte impar del conductor geométrico, M, utilizando el programa de `genus2reduction` de Q. Liu. El algoritmo descrito en [Liu94] también nos permitiría calcular la parte par del conductor geométrico de la jacobiana de cualquier curva de género 2 definida sobre $\mathbb{Q}$. Pero como este algoritmo es bastante complicado, hemos optado por utilizar otro método, basado en un resultado de A. Brumer que acota el conductor geométrico de una variedad abeliana de tipo GL_2. Lo enunciaremos sólo para el caso de una variedad abeliana modular asociada a una forma nueva.

Proposición 4.7. *Sea $f \in S_2(N, \varepsilon)$ una forma nueva. Pongamos*

$$s_p = \left\lceil \frac{r_p}{2} - 1 - \frac{1}{p-1} \right\rceil ,$$

donde $r_p = \mathrm{ord}_p(N)$ y $\lceil x \rceil = \min\{z \in \mathbb{Z} \,|\, z \geq x\}$, y por ζ la raíz p^{s_p} primitiva de la unidad. Entonces

(i) Si $p = 2$, se tiene $\mathbb{Q}(\varepsilon, \zeta + \zeta^{-1}) \subseteq K_f$.

(ii) Si $p \neq 2$, se tiene $\mathbb{Q}(\varepsilon, \zeta^2) \subseteq K_f$.

Demostración: Ver teorema 5.5 de [Bru95]. □

Por lo tanto, fijado un entero impar M, para cada cuerpo cuadrático $\mathbb{Q}(\sqrt{d})$ sólo hay un número finito de posibles valores de k para los que existe una forma nueva f de nivel $N = 2^k M$ tal que $K_f = \mathbb{Q}(\sqrt{d})$.

De entre los candidatos que han pasado todas las cribas, distinguiremos los siguientes casos:

(i) *Caso $\varepsilon = 1$ sin torcimiento extra*:

- Si $n_0 = 2$, entonces $2 \nmid N$ y, por tanto, el conductor geométrico de $J(C)$ puede ser calculado con el programa `genus2reduction`.
- Si $n_0 = 3$, utilizaremos la cota de Brumer para calcular la parte par del conductor geométrico de $J(C)$.

(ii) *Caso* ord $\varepsilon \leq 2$ *con torcimiento extra*: En este caso, todas las curvas C que hemos obtenido tienen una involución no hiperelíptica definida sobre un cuerpo cuadrático K. Así, el cálculo del conductor geométrico

de $J(C)$ se hará de la manera descrita a continuación. Calculamos una curva elíptica E definida sobre K tal que $J(C) \overset{K}{\sim} E^2$. Entonces, por la propiedad universal de la restricción de escalares de Weil (ver [Mil72]), $J(C)$ es $\mathbb{Q}$-isógena a $\mathrm{Res}_{K/\mathbb{Q}}(E)$, es decir,

$$J(C) \overset{\mathbb{Q}}{\sim} \mathrm{Res}_{K/\mathbb{Q}}(E).$$

Aplicando la fórmula de Milne (ver [Mil72]) para $\mathrm{Res}_{K/\mathbb{Q}}(E)$, obtenemos:

$$\mathcal{N}_{\mathbb{Q}}(J(C)) = \mathcal{N}_{\mathbb{Q}}(\mathrm{Res}_{K/\mathbb{Q}}(E)) = N_{K/\mathbb{Q}}(\mathcal{N}_K(E)) \cdot d_{K/\mathbb{Q}}^2\,,$$

donde $d_{K/\mathbb{Q}}$ denota el discriminante de $K/\mathbb{Q}$. Nótese que si $\operatorname{ord}\varepsilon = 2$, se tiene que el cuerpo K es real y el carácter ε es el carácter asociado a este cuerpo cuadrático K.

(iii) *Caso* $\operatorname{ord}\varepsilon > 2$: En este caso, las curvas que han pasado todas las cribas provienen de una forma nueva sin multiplicación compleja, ya que los cocientes de estas curvas por sus involuciones no hiperelípticas proporcionan curvas elípticas sin multiplicación compleja. El cuerpo de definición de cada involución no hiperelíptica de C ha de ser igual al cuerpo fijo por los torcimientos extras de f, al que denotaremos por L_C. Por lo tanto, L_C es el cuerpo fijo por ε, ya que W_N está definida sobre dicho cuerpo. Este hecho determina ε salvo conjugación por Galois. Para calcular el nivel utilizaremos el programa `genus2reduction` para la parte impar del conductor geométrico de $J(C)$ y para calcular la parte par utilizaremos las cotas de Brumer y el hecho de que el conductor del carácter de ε divide al nivel.

4.1.4 Comprobación

En el primer paso dado para encontrar todas las curvas modulares nuevas de género 2 con jacobiana $\mathbb{Q}$-simple hemos obtenido un total de 3168 candidatos. Después del proceso de criba, hemos obtenido que sólo hay 149 candidatos como posibles soluciones a nuestro problema. En el proceso de búsqueda hemos encontrado para cada candidato $(F(X), \{a_n\}_{2\le n\le M'_{n_0}}, k, d)$ una forma nueva $f \in S_2(N,\varepsilon)$ tal que

$$f = q + \sum_{n=2}^{M'_{n_0}} a_n\, q^n + O(q^{M'_{n_0}+1}), \qquad K_f = \mathbb{Q}(\sqrt{d}) \quad \text{y} \quad \operatorname{ord}\varepsilon = k.$$

El último paso que falta por realizar es comprobar que estos candidatos son realmente soluciones a nuestro problema. Para ello, utilizaremos la proposición 3.6, que a continuación reproducimos adaptada al caso que estamos estudiando.

Criterio 4.1. *Sean* $f = \sum_{n\geq 1} a_n\, q^n \in S_2(N,\varepsilon)$ *una forma nueva normalizada tal que* $K_f = \mathbb{Q}(\sqrt{d})$*, con* d *libre de cuadrados y* σ *el automorfismo no trivial de* $\mathrm{Gal}(K_f/\mathbb{Q})$*. Denotamos por* $g_{N,\varepsilon}$ *el género de* $X(N,\varepsilon)$*. Definamos*

$$h_1 = \frac{f + {}^{\sigma}f}{2}, \quad h_2 = \frac{f - {}^{\sigma}f}{2B_{n_0}\sqrt{d}}, \quad x = \frac{h_1}{h_2} \;\; e \;\; y = \frac{q\,dx/dq}{h_2},$$

donde recordamos que $n_0 = \min\{n \in \mathbb{Z} : a_n \notin \mathbb{Z}\}$ *y* $a_n = A_n + B_n\sqrt{d}$*. Si existe* $F[X] \in \mathbb{Q}[X]$ *de grado* 5 *ó* 6 *sin raíces repetidas tal que*

$$y^2 - F(x) = O(q^{c_{N,\varepsilon}}) \quad con \quad c_{N,\varepsilon} = 6(2g_{N,\varepsilon} - 2) + 1\,,$$

entonces la curva definida por $C : y^2 = F(x)$ *es modular nueva de nivel* N*, de género* 2 *y* $J(C) \overset{\mathbb{Q}}{\sim} A_f$*.*

Utilizando este criterio hemos comprobado que todos los 149 candidatos son soluciones a nuestro problema. Para realizar esta comprobación hemos necesitado las q-expansiones de cada una de las formas nuevas hasta el coeficiente necesario para cumplirse el criterio anterior. Esto ha sido posible principalmente gracias al programa `Hecke` [Ste] de W. A. Stein, tanto en su versión `C++` como en la implementada en Magma [BCP97]. También hemos usado el paquete *Modular Symbols* implementado por J. Quer en Mathematica y recibido la ayuda de W. A. Stein y de M. Müller para determinar los coeficientes en algunos casos en los que nuestros ordenadores no eran suficientemente potentes.

Por lo tanto, hemos obtenido el siguiente resultado.

Teorema 4.8. *Salvo* $\mathbb{Q}$*-isomorfismos, hay exactamente* 149 *curvas modulares nuevas de género* 2 *con jacobianas* $\mathbb{Q}$*-simples. De éstas, sólo* 96 *tienen jacobiana* $\overline{\mathbb{Q}}$*-simple.*

Las ecuaciones hiperelípticas de estas 149 curvas modulares nuevas aparecen en las tablas 6.1 y 6.2, así como las clases de $\mathbb{Q}$-isogenia de las correspondientes jacobianas.

4.2 Con jacobiana no $\mathbb{Q}$-simple

En esta sección vamos a calcular todas las curvas modulares nuevas de género 2 cuyas jacobianas no son $\mathbb{Q}$-simples. Si C es una curva con estas condiciones, se tiene que existen dos formas nuevas $f_i \in S_2(N, \varepsilon_i)$, $i = 1, 2$, tales que

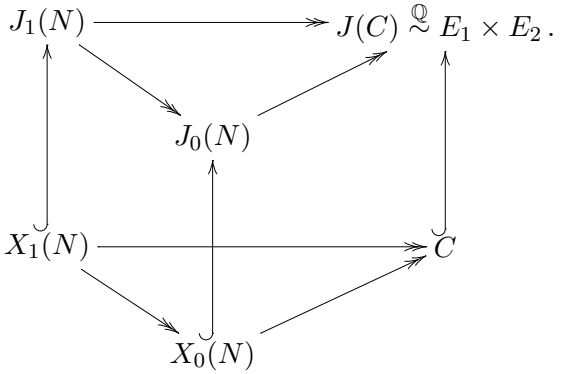
$$J(C) \overset{\mathbb{Q}}{\sim} A_{f_1} \times A_{f_2}.$$

Ahora, como $\dim J(C) = 2$, se tiene que A_{f_1} y A_{f_2} son curvas elípticas sobre $\mathbb{Q}$ y las denotaremos por E_1 y E_2. Así, para $i = 1, 2$ se tendrá $\varepsilon_i = 1$ y $K_{f_i} = \mathbb{Q}$. En consecuencia, tenemos que

$$J(C) \overset{\mathbb{Q}}{\sim} E_1 \times E_2,$$

de modo que $\mathcal{N}_{\mathbb{Q}}(E_i) = N$ para $i = 1, 2$, y E_1 no es $\mathbb{Q}$-isógena a E_2.

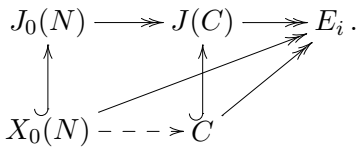
Así, si C es una curva modular nueva de nivel N y género 2 con jacobiana no $\mathbb{Q}$-simple, tendremos que el siguiente diagrama es conmutativo



Observación 4.2. Sea C una curva de género 2 definida sobre $\mathbb{Q}$ tal que $J(C)$ es $\mathbb{Q}$-isógena al producto de dos curvas elípticas E_1 y E_2 definidas sobre $\mathbb{Q}$. Entonces $J(C)$ es una variedad abeliana modular primitiva de nivel

$$N = \operatorname{mcm}(\mathcal{N}_{\mathbb{Q}}(E_1), \mathcal{N}_{\mathbb{Q}}(E_2)),$$

que da lugar al siguiente diagrama conmutativo para $i = 1, 2$:



Obsérvese que el morfismo que está en línea discontinua entre $X_0(N)$ y C no tiene por qué existir, ya que la modularidad de $J(C)$ no comporta la modularidad de C. Además, $J(C)$ es nueva si y sólo si $\mathcal{N}_{\mathbb{Q}}(E_1) = \mathcal{N}_{\mathbb{Q}}(E_2)$ y E_1 no es $\mathbb{Q}$-isógena a E_2.

El proceso que vamos a seguir en el caso que estamos tratando será muy parecido al caso anterior, es decir, cuando la jacobiana es $\mathbb{Q}$-simple.

Sea (C, π) una curva modular nueva de nivel N y de género 2 con jacobiana no $\mathbb{Q}$-simple. Entonces, como hemos visto antes, existen dos formas nuevas normalizadas f_1 y f_2 de $S_2(N, 1)$ con q-expansiones

$$f_1 = \sum_{n\geq 1} a_n\, q^n \qquad \text{y} \qquad f_2 = \sum_{n\geq 1} b_n\, q^n\,,$$

tales que $a_n, b_n \in \mathbb{Z}$ para todo n. Además, se tiene la igualdad

$$\pi^*(H^0(C, \Omega^1)) = \left\langle f_1(q)\frac{dq}{q}, f_2(q)\frac{dq}{q} \right\rangle.$$

El lema 3.4 y la proposición 3.5 aplicados a este caso establece el siguiente resultado, análogo a la proposición 4.2.

Proposición 4.9. *Sea $P = \pi(i\infty)$ y definamos*

$$h_1 = \frac{b_{n_0} f_1 - a_{n_0} f_2}{b_{n_0} - a_{n_0}} \qquad y \qquad h_2 = \frac{f_1 - f_2}{a_{n_0} - b_{n_0}}\,,$$

donde $n_0 = \min\{n \in \mathbb{Z} : a_n \neq b_n\}$. Entonces las funciones de $X_0(N)$ definidas por

$$x = \frac{h_1}{h_2} \qquad e \qquad y = \frac{q\, dx/dq}{h_2}\,,$$

satisfacen la ecuación $y^2 = F(x)$, con $F(X) \in \mathbb{Q}[X]$ sin raíces múltiples, de modo que:

(i) Si $P \notin \mathrm{Wei}(C)$ entonces $n_0 = 2$, en cuyo caso F es de grado 6 y $4 \nmid N$.

(ii) Si $P \in \mathrm{Wei}(C)$ entonces $n_0 = 3$, en cuyo caso F es de grado 5 y $9 \nmid N$.

Para facilitar los cálculos, el siguiente resultado, análogo a la proposición 4.3, nos será de gran utilidad.

Proposición 4.10. *Si $P \in \mathrm{Wei}(C)$, se tiene que $a_{2n} = 0$ para todo $n \geq 1$ y, en particular, $4 \mid N$.*

Demostración: Supongamos que $P \in \mathrm{Wei}(C)$. Sabemos que las funciones x e y, como en la anterior proposición, satisfacen $y^2 = F(x)$ para un polinomio de grado 5 sin raíces repetidas. Para construir F empezamos igualando los coeficientes de y^2 y x^5 de menor grado. Así, obtenemos

$$y^2 - x^5 = -4\, b_2\, q^{-9} + O(q^{-8}).$$

Como $\mathrm{ord}_{i\infty}\, x = 2$, se tiene que $b_2 = 0$ y, por lo tanto, $a_2 = 0$. Denotemos por ε el carácter trivial módulo N. Ahora, igualando los coeficientes de q^{-8} tenemos que

$$y^2 - \left(x^5 + 3\frac{a_5 - b_5}{a_3 - b_3}\, x^4\right) = 12\, \varepsilon(2) q^{-7} + O(q^{-6})\,,$$

de donde deducimos que $\varepsilon(2) = 0$. Así, hemos visto que $a_2 = b_2 = \varepsilon(2) = 0$ lo que implica, por las relaciones de recurrencia de los coeficientes de la q-expansión de una forma nueva normalizada, que $a_{2n} = b_{2n} = 0$ para $n \geq 1$. Para demostrar que $4|N$ basta con observar que si $p|N$ y $a_p = 0$, entonces $p^2|N$. □

4.2.1 Cálculo de candidatos.

Para calcular las curvas modulares nuevas de género 2 cuyas jacobianas son $\mathbb{Q}$-simples, hemos implementado en MATHEMATICA dos programas dependiendo de si $n_0 = 2$ ó $n_0 = 3$. Estos son completamente similares a los programas expuestos para el caso $\mathbb{Q}$-simple. Sin embargo, para clarificar las diferencias, hemos optado por poner todos los pasos de los programas.

(1) Introducimos las expresiones formales

$$f_1 = q + a_2\, q^2 + \cdots + a_{M_{n_0}}\, q^{M_{n_0}} + O(q^{M_{n_0}+1}),$$
$$f_2 = q + b_2\, q^2 + \cdots + b_{M_{n_0}}\, q^{M_{n_0}} + O(q^{M_{n_0}+1}),$$

que representan dos formas nuevas normalizadas asociadas a dos curvas elípticas, donde M_{n_0} es igual que en el caso de jacobiana $\mathbb{Q}$-simple.

Denotamos por ε el carácter trivial módulo N. Por las leyes de recurrencia, para $n \leq M_{n_0}$ los valores a_n y b_n dependen de a_p y b_p para p primo tal que $p \leq 13$ si $n_0 = 2$ ó $p \leq 19$ si $n_0 = 3$ y también dependen de $\varepsilon(2)$ y $\varepsilon(3)$. Además, por la proposición 4.10, imponemos la condición adicional de que $a_2 = \varepsilon(2) = 0$ cuando $n_0 = 3$.

(2) Calculamos x e y como en la proposición 4.9.

(3) Calculamos el polinomio

$$F_{n_0}(X) = \sum_{i=0}^{n_0} A_{n_0,i}\, X^i$$

tal que $y^2 - F_{n_0}(x) = O(q)$.

(4) Calculamos el polinomio en q

$$y^2 - F_{n_0}(x) = \sum_{m=1}^{8} Q_{n_0,m}(\{a_n\}_{2\leq n\leq M_{n_0}})\, q^m$$

y obtenemos que $Q_{n_0,1}, \ldots, Q_{n_0,8} \in \mathbb{Z}[a_2, \ldots, a_{M_{n_0}}]$.

Para p primo, sólo consideraremos los valores a_p y b_p que pertenecen al conjunto S_p que a continuación describimos:

- Caso $p \neq 2, 3$:
$$S_p = \{(a,b) \in \mathbb{Z}^2 \,|\, |a|, |b| \leq 2\sqrt{p}\}.$$
- Caso $p = 2$:
  - Si $n_0 = 2$:
$$S_2 = \begin{cases} \{\pm(1,-1)\} & \text{si } \varepsilon(2) = 0, \\ \{(a,b) \,|\, a,b \in \{\pm 2, \pm 1, 0\}\,,\ a \neq b\} & \text{si } \varepsilon(2) = 1. \end{cases}$$
  - Si $n_0 = 3$:
$$S_2 = \{(0,0)\}.$$

- Caso $p = 3$:
  - Si $n_0 = 2$:

$$S_3 = \begin{cases} \{(a,b) \,|\, a,b \in \{\pm 1, 0\}\} & \text{si } \varepsilon(3) = 0, \\ \{(a,b) \,|\, a,b \in \{\pm 3, \pm 2, \pm 1, 0\}\} & \text{si } \varepsilon(3) = 1. \end{cases}$$

  - Si $n_0 = 3$:

$$S_3 = \begin{cases} \{\pm(1,-1)\} & \text{si } \varepsilon(3) = 0, \\ \{(a,b) \,|\, a,b \in \{\pm 3, \pm 2, \pm 1, 0\}\,,\, a \neq b\} & \text{si } \varepsilon(3) = 1. \end{cases}$$

Los polinomios $F_{n_0}, Q_{n_0,1}, \ldots, Q_{n_0,8}$ que hemos obtenido anteriormente los traducimos al lenguaje de GP-PARI. Aquí elaboramos un algoritmo, similar al caso de jacobiana $\mathbb{Q}$-simple, para calcular un conjunto de candidatos para el caso de jacobiana no $\mathbb{Q}$-simple. Este conjunto está formado por elementos de la forma $(F(X), \{(a_n, b_n)\}_{2 \leq n \leq M_{n_0}}, \varepsilon(2), \varepsilon(3))$ tales que la curva de género 2 definida por $C : Y^2 = F(X)$ es candidata a ser una curva modular nueva de género 2 y tal que $J(C)$ es $\mathbb{Q}$-isógena a $A_{f_1} \times A_{f_2}$, donde f_1 y f_2 son candidatas a ser formas nuevas con q-expansiones de la forma

$$f_1 = q + a_2\, q^2 + \cdots + a_{M_{n_0}}\, q^{M_{n_0}} + O(q^{M_{n_0}+1}),$$
$$f_2 = q + b_2\, q^2 + \cdots + b_{M_{n_0}}\, q^{M_{n_0}} + O(q^{M_{n_0}+1}).$$

Los pasos de este algoritmo son los siguientes:

Algoritmo: Fijados: n_0 y los valores $\varepsilon(2), \varepsilon(3)$:
ENTRADA: $\{(a_p, b_p) \,|\, p < M_{n_0}$ con p primo y $(a_p, b_p) \in S_p \times S_p\}$.
PASO 1: Calculamos a_n, b_n con $n \leq M_{n_0}$ utilizando la ley de recurrencia.
PASO 2: Sustituimos $\{(a_n, b_n)\}_{2 \leq n \leq M_{n_0}}\}$ en $F = F_{n_0}, Q_{n_0,1}, \ldots, Q_{n_0,8}$.
SALIDA: Si $Q_{n_0,1}(\{a_n\}_{2 \leq n \leq M_{n_0}}) = \cdots = Q_{n_0,8}(\{a_n\}_{2 \leq n \leq M_{n_0}}) = 0$ y F no tiene raíces múltiples, el algoritmo devuelve $(F(X), \{(a_n, b_n)\}_{2 \leq n \leq M_{n_0}}, \varepsilon(2), \varepsilon(3))$.

No hemos aplicado el algoritmo a todas las posibles entradas (aproximadamente un total de $2 \cdot 10^{15}$) ya que (a_{n_0}, b_{n_0}) y (b_{n_0}, a_{n_0}) dan la misma solución, sino que sólo lo hemos hecho para una de ellas. Con esta restricción, el cálculo ha tardado unos 6 meses de cálculo en un PIII 800MHz.

Tras este cálculo hemos obtenido un total de 891 candidatos, 41 si $n_0 = 2$ y 850 si $n_0 = 3$.

4.2.2 Criterios de eliminación

En esta sección estableceremos cribas para eliminar los candidatos que no corresponden a curvas modulares nuevas de género 2 con jacobiana no $\mathbb{Q}$-simple. Como antes, estas cribas están basadas en propiedades de formas modulares y de curvas hiperelípticas.

Criba del conductor geométrico. Sea C una curva modular nueva de género 2 de nivel N, entonces $\mathcal{N}_{\mathbb{Q}}(J(C)) = N^2$. Con el programa de Q. Liu `genus2reduction` calculamos la parte impar del conductor geométrico de la jacobiana de la curva de cada candidato. Si éste no es un cuadrado descartaremos al candidato.

Hemos separado los candidatos dependiendo de si $\varepsilon(3) = 0$ ó $\varepsilon(3) = 1$. Si un candidato ha sido obtenido cuando $\varepsilon(3) = 0$ (resp. $\varepsilon(3) \neq 0$) y finalmente 3 no divide (resp. divide) a la parte impar del conductor geométrico de la jacobiana de la curva, eliminamos ese candidato.

Tras esta criba continúan 121 candidatos. A cada uno de ellos le hemos añadido la parte impar del conductor geométrico de la jacobiana de la correspondiente curva, que denotamos por N_{liu}.

Criba de los primos que no dividen al nivel. Sea C una curva de género 2 definida sobre $\mathbb{Q}$ con jacobiana no $\mathbb{Q}$-simple. Entonces $J(C) \overset{\mathbb{Q}}{\sim} E_1 \times E_2$ para dos curvas elípticas E_1 y E_2 definidas sobre $\mathbb{Q}$. Sea p un primo tal que $p \not| \mathcal{N}_{\mathbb{Q}}(J(C))$, entonces se tiene que

$$\tilde{J}(C) \overset{\mathbb{F}_p}{\sim} \tilde{E}_1 \times \tilde{E}_2,$$

donde $\tilde{}$ representa reducción módulo p.

Si A es una variedad abeliana definida sobre $\mathbb{F}_p$, denotaremos por $Q_A(t)$ al polinomio característico del endomorfismo de Frobenius Frob_p actuando en el módulo de Tate de A. En nuestro caso tendremos

$$Q_{\tilde{J}(C)}(t) = Q_{\tilde{E}_1}(t) \cdot Q_{\tilde{E}_2}(t) = (t^2 - a_p\, t + p)(t^2 - b_p\, t + p)\,, \qquad (4.4)$$

donde a_p y b_p son los autovalores correspondientes a las formas nuevas normalizadas asociadas a E_1 y E_2 con respecto al operador de Hecke T_p.

Recordemos que cada candidato está formado por un vector de la forma $(F(X), \{(a_n, b_n)\}_{2\leq n\leq M_{n_0}}, \varepsilon(2), \varepsilon(3))$ junto con N_{liu}.

Eliminamos los candidatos para los cuales hay algún primo impar $p < 50$ tal que $p \not| N_{\text{liu}}$ y $Q_{\tilde{J}(C)}(t)$ no cumple la condición (4.4). Además, para el caso en el cual $p < M_{n_0}$ esta condición se ha de satisfacer con nuestros valores a_p y b_p.

Así, obtenemos que sólo 72 candidatos han pasado esta criba.

Criba de los primos que dividen al nivel. Sea $f \in S_2(N, 1)$ una forma nueva con q-expansión $\sum_{n\geq 1} a_n\, q^n$. Sea p un primo tal que $p|N$, entonces

$$a_p = \begin{cases} \pm 1 & \text{si } p^2 \not| N, \\ 0 & \text{si } p^2 | N. \end{cases} \tag{4.5}$$

Eliminamos los candidatos tales que existe un primo $p < M_{n_0}$ tal que $p|N_{\text{liu}}$ y a_p ó b_p no satisfacen la condición (4.5).

El número de candidatos que han pasado la anterior criba y que cumplen la anterior condición es 69.

En el siguiente apartado mostraremos cómo hemos de buscar las formas nuevas correspondientes a los candidatos que han pasado las cribas. Veremos que no todos los candidatos son solución al problema. En concreto, demostraremos que de los 69 candidatos, 64 corresponden a curvas modulares nuevas de género 2 y los cinco restantes candidatos, que se muestran en el último apartado de este capítulo, corresponden a curvas modulares no nuevas.

4.2.3 Búsqueda

El método utilizado para la búsqueda de las formas nuevas correspondientes a una curva modular nueva de género 2 y jacobiana no $\mathbb{Q}$-simple será similar al caso en el que la jacobiana es $\mathbb{Q}$-simple. Pero en este caso será más sencillo, ya que aquí el carácter es siempre trivial.

Para calcular el nivel, procederemos de forma análoga al caso de jacobiana $\mathbb{Q}$-simple. Calcularemos la parte impar del conductor geométrico mediante el programa `genus2reduction`. Aplicando la proposición 4.7 al caso particular de dimensión 1, obtenemos

$$\operatorname{ord}_2 \mathcal{N}_{\mathbb{Q}}(E) \leq 8,$$

donde E es una curva elíptica definida sobre $\mathbb{Q}$. Así, tenemos cotas para los niveles de las formas nuevas que buscamos. Ahora, utilizando las tablas de Cremona, tanto las que aparecen en [Cre92] como las que se pueden obtener electrónicamente vía web [Cre] o mediante MAGMA [BCP97], identificaremos el nivel de estas formas nuevas, así como la clase de $\mathbb{Q}$-isogenia de las correspondientes curvas elípticas.

De los 69 candidatos que han pasado las cribas, hemos encontrado 64 parejas de formas nuevas tales que los primeros M_{n_0} coeficientes coinciden con los datos de estos candidatos. Los cinco restantes candidatos aparecen en el último apartado de la siguiente sección.

4.2.4 Comprobación

El criterio que vamos a exponer será utilizado tanto para comprobar que una pareja de formas nuevas corresponde a un curva modular de género 2 con jacobiana no $\mathbb{Q}$-simple, como para los cinco ejemplos del último apartado de esta sección. De hecho, es simplemente la proposición 3.6 adaptada al caso actual.

Criterio 4.2. *Sean* $f_1 = \sum_{n\geq 1} a_n\, q^n$ *y* $f_2 = \sum_{n\geq 1} a_n\, q^n \in S_2(N,1)$ *dos formas parabólicas no nulas con* q*-expansiones racionales. Denotemos por* $g_0(N)$ *el género de* $X_0(N)$ *y definamos*

$$h_1 = \frac{b_{n_0}\, f_1 - a_{n_0}\, f_2}{b_{n_0} - a_{n_0}}\,, \quad h_2 = \frac{f_1 - f_2}{a_{n_0} - b_{n_0}}\,, \quad x = \frac{h_1}{h_2} \;\; e \;\; y = \frac{q\, dx/dq}{h_2}\,,$$

donde $n_0 = \min\{n \in \mathbb{Z} : a_n \neq b_n\}$*. Si existe* $F[X] \in \mathbb{Q}[X]$ *de grado* 5 *ó* 6 *sin raíces repetidas tal que*

$$y^2 - F(X) = O(q^{c_0(N)}) \quad con \quad c_0(N) = 6(2g_0(N) - 2) + 1\,,$$

entonces la curva definida por $C : y^2 = F(X)$ *es modular nueva de nivel* N *y de género* 2*.*

Utilizando el anterior criterio hemos comprobado que 64 de los candidatos son soluciones a nuestro problema. Para ello hemos tenido que calcular las q-expansiones de cada una de las formas nuevas hasta el coeficiente necesario para cumplirse el criterio anterior. Esto se ha realizado utilizando MAGMA.

Así, obtenemos el siguiente resultado.

Teorema 4.11. *Hay exactamente* 64 *curvas modulares nuevas de género* 2*, salvo* $\mathbb{Q}$*-isomorfismos, con jacobiana no* $\mathbb{Q}$*-simple.*

Las ecuaciones hiperelípticas de estas 64 curvas modulares nuevas aparecen en la tabla 6.3, así como las clases de $\mathbb{Q}$-isogenia de las curvas elípticas que aparecen en la descomposición de las jacobianas correspondientes.

Restantes casos

En este apartado expondremos las cinco curvas modulares no nuevas de género 2 que han pasado las tres cribas para el caso de jacobiana no $\mathbb{Q}$-simple, y que aparecen en la tabla siguiente. Las jacobianas de estas curvas son $\mathbb{Q}$-isógenas al producto de curvas elípticas definidas sobre $\mathbb{Q}$ con conductores geométricos distintos. Por lo tanto, son primitivas de nivel igual al mínimo común múltiplo de los niveles de ambas curvas elípticas. Denotaremos a estas curvas de género 2 mediante un subíndice que etiqueta (con la notación de Cremona) la clase de $\mathbb{Q}$-isogenia de la curva elíptica de conductor menor y un superíndice que indica la clase de $\mathbb{Q}$-isogenia de la otra curva elíptica. En estos cinco casos, el menor nivel es un divisor del mayor y, por lo tanto, estas cinco curvas son primitivas de nivel igual al mayor conductor geométrico de ambas curvas elípticas.

Tabla 4.1: Curvas modulares primitivas de género 2

C	$: y^2 = F(x)$
C_{20A}^{40A}	$: y^2 = x^5 + 3x^4 - 24x^3 + 52x^2 - 48x + 16$
C_{24A}^{48A}	$: y^2 = x^5 + 14x^3 + x$
C_{14A}^{56B}	$: y^2 = x^5 - 3x^4 + 12x^3 - 12x^2 + 16x$
C_{50B}^{100A}	$: y^2 = x^5 + 25x^2 + 20x + 4$
C_{15A}^{120B}	$: y^2 = x^5 - 3x^4 + 8x^3 - 3x^2 + x$

La tabla siguiente muestra las formas parabólicas f_1, f_2 que, como en la proposición 4.9, hay que tomar para obtener la parametrización de estas cinco curvas. Se denota por ε_2 el carácter de Dirichlet módulo 2.

C	C_{20A}^{40A}	C_{24A}^{48A}	C_{14A}^{56B}	C_{50B}^{100A}	C_{15A}^{120B}
f_1	f_{20A}	f_{24A}	$(f_{14A})_{\varepsilon_2}$	$(f_{50B})_{\varepsilon_2}$	$(f_{15A})_{\varepsilon_2}$
f_2	f_{40A}	f_{48A}	f_{56B}	f_{100A}	f_{120B}

Obsérvese que si $f = f_{14A}, f_{50B}$ ó f_{15A} y a_2 es el autovalor de la forma nueva normalizada f con respecto al operador de Hecke T_2, entonces

$$f_{\varepsilon_2}(q) = f(q) - a_2\, f(q^2) + 2\,\varepsilon_2(N)\, f(q^4).$$