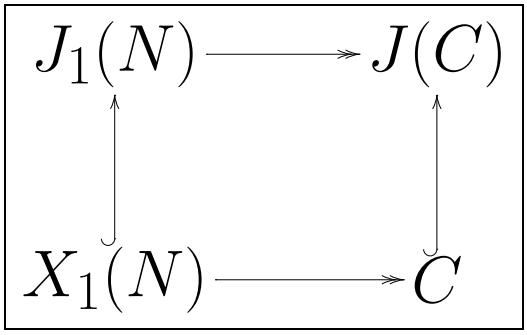
Curvas Hiperelípticas Modulares



Enrique González Jiménez

Curvas Hiperelípticas Modulares

Memoria presentada para
optar al grado de
Doctor en Matemáticas

por

Enrique González Jiménez

Departament de Matemàtiques
Universitat Autònoma de Barcelona

2001

CERTIFICO que la presente memoria ha sido realizada bajo mi dirección por Enrique González Jiménez.

Barcelona, Diciembre de 2001.

Fdo: Dr. Josep González i Rovira.

A Ana,
y a mi familia.

"El buen cristiano deberá guardarse de los matemáticos y de todos aquellos que practican la predicción sacrílega, particularmente cuando proclaman la verdad. Porque existe el peligro de que esta gente aliada con el diablo, puede cegar las almas de los hombres y atraparlos en las redes del infierno."

De genesi ad Litteram 2, XVIII, 37

Índice General

Índice de Tablas

Introducción

Las integrales elípticas fueron objeto de atención de importantes matemáticos y físicos del siglo XIX. Esto llevó al estudio de las curvas elípticas y, posteriormente, al de las curvas modulares. Las propiedades aritméticas de las curvas modulares han situado a éstas en un puesto destacado en el campo de la Teoría de Números.

Así, Yutaka Taniyama [Tan55] enunció, en el año 1955, una importante conjetura que relacionaba las curvas modulares y las curvas elípticas definidas sobre $\mathbb{Q}$. Más tarde, Goro Shimura precisó el enunciado de esta conjetura que, sin embargo, sólo llegó a ser ampliamente conocida tras su publicación en un artículo de André Weil en 1967 [Wei67]. Dicha conjetura, conocida como *Conjetura de Shimura-Taniyama-Weil*, establecía:

"Para toda curva elíptica E definida sobre $\mathbb{Q}$ de conductor geométrico N, existe un morfismo no constante $\pi : X_0(N) \to E$ definido sobre $\mathbb{Q}$."

Equivalentemente, esta conjetura afirma que existe una forma modular de peso 2 de $\Gamma_0(N)$ tal que las funciones L asociadas a la forma modular y a la curva elíptica coinciden. Así, la información aritmético-geométrica almacenada en la función L de la curva elíptica se puede obtener a partir de la forma modular correspondiente.

Esta conjetura ha sido de gran importancia en el desarrollo de la moderna Teoría de Números y, más concretamente, en la Geometría Aritmética. La constatación de que ésta implicaba el *Último teorema de Fermat* proporcionó un impulso notable para conseguir su demostración. Andrew Wiles [Wil95], con la ayuda de Richard Taylor [TW95], demostró esta conjetura para el caso semiestable, condición suficiente para probar el último teorema de Fermat como había demostrado Kenneth Ribet [Rib90]. Este resultado mostraba la

potencia de las curvas modulares en la resolución de problemas diofánticos. Recientemente, esta conjetura ha sido demostrada en su totalidad por Christophe Breuil, Brian Conrad, Fred Diamond y Richard Taylor [BCDT01].

Una vez demostrada la conjetura de Shimura-Taniyama-Weil, parece natural determinar otras familias de curvas que sean *modulares*, entendida la modularidad de una curva como la propiedad de admitir un recubrimiento desde alguna curva modular $X_1(N)$. Éste es el punto de partida de esta tesis. Más concretamente, nuestro objetivo es el estudio de las curvas hiperelípticas que son modulares. El interés suscitado por dichas curvas aparece por varias razones. En primer lugar, las curvas hiperelípticas son la generalización natural de las curvas elípticas para género mayor que 1, ya que están caracterizadas por el hecho de admitir morfismos de grado 2 sobre la recta proyectiva. En segundo lugar, dichas curvas han sido ampliamente estudiadas y conocemos muchas de sus propiedades; en particular, las curvas hiperelípticas son descritas por ecuaciones explícitas de la forma $y^2 = F(x)$, donde F es un polinomio de grado mayor que 4 sin raíces múltiples. Por último, el interés en las curvas hiperelípticas definidas sobre cuerpos finitos de género pequeño ha aumentado considerablemente desde que son consideradas para usos criptográficos. En este sentido, son de especial interés aquéllas que se obtienen como reducción de curvas hiperelípticas definidas sobre $\mathbb{Q}$ cuya jacobiana es modular. Esto es debido a que la congruencia de Eichler-Shimura permite el uso de un método propio para el recuento del número de puntos sobre un cuerpo finito, basado en la acción de los operadores de Hecke sobre las diferenciales regulares.

El estudio y la obtención de ecuaciones de curvas modulares que son hiperelípticas han sido realizados por diferentes autores. Andrew P. Ogg [Ogg74] determinó qué curvas modulares $X_0(N)$ son hiperelípticas. En concreto, demostró que los únicos valores posibles son $N = 22, 23, 26, 28, 29, 30, 31, 33, 37, 39, 40, 41, 46, 47, 48, 50, 59$ y 71. Ecuaciones para todas estas curvas fueron calculadas por Josep González [Gon91]. Jean-François Mestre [Mes81] demostró que $N = 13, 16$ y 18 son los únicos valores para los que la curva modular $X_1(N)$ es hiperelíptica y Markus A.Reichert [Rei84] calculó ecuaciones para estas curvas. Más tarde, Noburo Ishii y Fumiyuki Momose [IM91] demostraron que ningún subrecubrimiento propio de $X_1(N) \to X_0(N)$ es hiperelíptico. Desde un punto de vista un poco más general, Yuji Hasegawa y Ki-ichiro Hashimoto ([HH96], [Has97]) determinaron algunos cocientes modulares hiperelípticos y ecuaciones para éstos. Concretamente, determinaron los valores de N para los cuales las curvas $X_0^*(N) := X_0(N)/B(N)$, donde $B(N)$ denota el

grupo de involuciones de Atkin-Lehner, son hiperelípticas. Por último, Yuji Hasegawa y Masahiro Furumoto ([FH99], [Has95]) determinaron y calcularon ecuaciones para todas las curvas hiperelípticas obtenidas como cocientes de $X_0(N)$ por subgrupos propios de $B(N)$.

Nuestro enfoque es más general, ya que estamos interesados en el estudio y determinación computacional de las curvas hiperelípticas C definidas sobre $\mathbb{Q}$ que son modulares, en el sentido de que exista un morfismo no constante $\pi : X_1(N) \to C$ definido sobre $\mathbb{Q}$. El estudio de curvas de género mayor que 1 definidas sobre $\mathbb{Q}$ (no necesariamente hiperelípticas) que son modulares presenta diferencias notables respecto del caso de curvas elípticas definidas sobre $\mathbb{Q}$, ya que estas últimas se identifican con sus jacobianas y, además, como variedades abelianas son $\mathbb{Q}$-simples. Así, para una curva modular C sobre $\mathbb{Q}$ de género 1 siempre existe un morfismo no constante $\pi : X_1(N) \to C$ tal que el correspondiente morfismo entre las jacobianas factoriza a través de la parte nueva de la jacobiana de $X_1(N)$. No obstante, esta condición no puede garantizarse para curvas de género mayor que 1. Llamaremos curvas *modulares nuevas de nivel* N a aquéllas que satisfacen dicha condición. Esta familia de curvas contiene a todas las curvas elípticas definidas sobre $\mathbb{Q}$ y nuestro estudio se restringirá a las curvas modulares nuevas que son hiperelípticas.

A diferencia del caso elíptico y de manera sorprendente, el conjunto de curvas hiperelípticas modulares nuevas es finito, tal como se demuestra en esta tesis. Tras haber obtenido este inesperado resultado, nuestro objetivo se ha encaminado a la determinación de estas curvas, es decir, a encontrar ecuaciones y los correspondientes morfismos que las hacen modulares. Para ello, hemos acotado sus géneros y encontrado condiciones sobre los niveles correspondientes. Creando paquetes computacionales, que recogían los resultados teóricos demostrados, y utilizando propiedades de las curvas modulares y de las curvas hiperelípticas, hemos conseguido probar que solamente existen 213 de tales curvas con género 2 y encontrado ecuaciones para cada una de ellas. Para el caso de género mayor que 2, hemos calculado 75 de tales curvas y presentamos evidencias numéricas que sugieren que éstas son todas las curvas hiperelípticas modulares nuevas.

La memoria se ha organizado en siete capítulos. Los dos primeros se dedican a recopilar resultados conocidos y fijar notaciones acerca de las curvas modulares e hiperelípticas. Los cinco capítulos restantes contienen nuestras aportaciones originales y se dividen en dos partes bien diferenciadas. La primera parte consta del capítulo 3 y en ella se recogen los resultados teóricos

más importantes de este trabajo. El resto de capítulos tiene un claro contenido computacional destinado a materializar y completar los resultados obtenidos en el capítulo 3.

El capítulo 1 está dedicado a las curvas modulares que se obtienen como subrecubrimientos de $X_1(N) \to X_0(N)$. En él, se presenta un resumen de resultados conocidos acerca de estas curvas, los cuales serán utilizados posteriormente. De manera especial, se abarca la teoría de formas nuevas, la acción del grupo de automorfismos formado por los operadores diamante y las involuciones de Weil sobre éstas y la descomposición de las jacobianas de tales curvas, tanto sobre $\mathbb{Q}$ como sobre $\overline{\mathbb{Q}}$.

En el capítulo 2 se presenta un resumen sobre curvas hiperelípticas. Se trata con especial interés los resultados relativos a las ecuaciones de la forma $y^2 = F(x)$, donde F es un polinomio sin raíces múltiples, para el caso en el cual el cuerpo de definición no es algebraicamente cerrado. Además, se muestran resultados concernientes a isomorfismos e involuciones de éstas.

El capítulo 3 es el núcleo teórico de la memoria. En primer lugar, se introducen los principales objetos de estudio, esto es, las curvas que son recubiertas por alguna curva modular $X_1(N)$ y que, aún a riesgo de confusión, seguiremos llamando *curvas modulares*. Definimos las nociones de curva modular *nueva* y *primitiva*. A continuación, se estudian las curvas hiperelípticas modulares nuevas definidas sobre $\mathbb{Q}$. Obtenemos resultados que nos permitirán determinar y calcular de manera efectiva ecuaciones para estas curvas. Terminamos el capítulo demostrando el resultado teórico principal de este trabajo, que nos asegura que solamente hay un número finito de curvas hiperelípticas modulares nuevas definidas sobre $\mathbb{Q}$, salvo $\mathbb{Q}$-isomorfismo, toda ellas de género menor o igual que 10.

En el capítulo 4 calculamos todas las curvas modulares nuevas definidas sobre $\mathbb{Q}$ de género 2. Para ello, utilizando los resultados teóricos obtenidos en el capítulo 3 se han elaborado programas en MATHEMATICA y GP-PARI, que han estado trabajando durante más de doce meses de forma ininterrumpida. Posteriormente, utilizando propiedades de las curvas hiperelípticas y modulares, hemos podido establecer criterios para cribar las soluciones correctas de entre las proporcionadas por el programa. Finalmente, demostramos que el total de estas curvas es 213.

El capítulo 5 está dedicado al cálculo del resto de curvas hiperelípticas modulares nuevas definidas sobre $\mathbb{Q}$. Para ello, mejoramos algunos de los re-

sultados obtenidos en el capítulo 3. En concreto, damos restricciones sobre los posibles niveles y géneros de estas curvas. Con estos resultados, elaboramos un programa en MAGMA que nos permite reconocer si en un cierto nivel N existen curvas hiperelípticas modulares nuevas y, en tal caso, determinarlas. Con este programa, hemos calculado todas estas curvas para el caso de género mayor que 2 y nivel menor que uno dado. Por último, mostramos evidencias numéricas que nos permiten conjeturar que las curvas hiperelípticas modulares nuevas definidas sobre $\mathbb{Q}$ que aparecen en esta tesis completan el conjunto de tales curvas.

Todas las ecuaciones de las curvas hiperelípticas modulares nuevas definidas sobre $\mathbb{Q}$ aquí calculadas se muestran en el capítulo 6. También se presentan ecuaciones de las $\mathbb{Q}$-curvas cocientes de las curvas modulares nuevas de género 2 cuando sus jacobianas son $\mathbb{Q}$-simples y no $\overline{\mathbb{Q}}$-simples.

Por último, en el capítulo 7 mostramos ejemplos de curvas modulares no nuevas. Estas curvas se han obtenido a partir de algunas de las curvas que aparecen en el capítulo 6, utilizando coincidencias que hemos detectado cuando en un mismo nivel aparecen varias curvas hiperelípticas nuevas. Estos ejemplos nos permiten mostrar el mayor abanico de situaciones que presentan las curvas modulares con género mayor que 1 en relación al caso elíptico.

Los resultados obtenidos en el capítulo 4 para el caso en el cual la jacobiana es $\mathbb{Q}$-simple están recogidos en el artículo conjunto con Josep González títulado *"Modular curves of genus* 2*"*, que ha sido aceptado para su publicación en Mathematics of Computation. La mayor parte del resto de resultados forman parte de un trabajo conjunto con Matthew H. Baker y Bjorn Poonen sobre curvas modulares, no necesariamente hiperelípticas, y que contiene resultados de finitud más generales. La prepublicación conjunta con Matthew H. Baker, Josep González y Bjorn Poonen lleva por título *"Finiteness results for modular curves of genus at least* 2*"* y será sometida próximamente para su publicación.

En esta tesis hemos traducido al castellano los términos anglófonos utilizados usualmente en la literatura de formas modulares. Así, hemos utilizado los términos *forma parabólica*, *forma propia*, *forma nueva* y *torcimiento* para hacer referencia a los términos *cusp form*, *eigenform*, *newform* y *twist* respectivamente. Aunque hemos seguido utilizando la notación habitual en este contexto, esto es, $S_2(N)^{\mathrm{new}}, S_2(N)^{\mathrm{old}}, J_1(N)^{\mathrm{new}}$ y $J_1(N)^{\mathrm{old}}$.

Para concluir esta introducción, quisiera expresar mis agradecimientos a todos aquellos que han colaborado de forma directa o indirecta en la realización de esta memoria.

En primer lugar y muy especialmente a Ana, por el apoyo y el ánimo que en todo momento me ha ofrecido. Sin ella esta *aventura* en Barcelona no hubiera sido posible.

A mis padres, por los valores que me han inculcado. Si algo bueno puedo llegar a tener, se lo debo a ellos. Por supuesto también a mi hermano, porque él, al igual que mi familia, siempre ha estado cuando le he necesitado.

A los compañeros que comparten conmigo el día a día. De forma especial a los que además me han ayudado en esta memoria: Biel, Javi, Jorge, Julio, Ramón,.... No quisiera dejar de mencionar, también, a mis amigos de Madrid.

Al *Seminari de Teoria de Nombres de Barcelona*, en especial a Enric Nart por darme la oportunidad de realizar este trabajo en Barcelona, y a Jordi Quer y Joan-Carles Lario por estar dispuestos a responder a mis preguntas en cualquier momento. A la parte *jove i no tan jove* que forma parte del $\mathrm{STNB}_{\mathrm{Jove}}$, con los que tanto he aprendido.

Quisiera agradecer a William A. Stein y Michael Müller por la ayuda desinteresada que me han ofrecido, y a Bjorn Poonen por sus observaciones.

Por último, a Josep González, por la aportación de sus geniales ideas para la resolución de los problemas que han ido surgiendo durante la realización de esta tesis. El optimismo que desprende a su alrededor ha hecho que esta tarea haya sido menos ardua. A él le estoy profundamente agradecido.

Barcelona, Diciembre de 2001.

Capítulo 1

Curvas modulares

En este capítulo presentamos un resumen de resultados conocidos sobre las curvas modulares que serán usados en esta tesis. Las principales referencias utilizadas para este resumen han sido [Shi71a], [DDT94] y [Roh97]. En ellas se encuentran la mayoría de las demostraciones de los resultados que enunciaremos a lo largo de este capítulo.

1.1 Curvas modulares

Sea $\mathbb{H} = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$ el semiplano superior de Poincaré. El grupo modular $\mathrm{SL}_2(\mathbb{Z})$ actua en $\mathbb{H}$ mediante transformaciones lineales fraccionarias. Se define el *grupo principal de congruencias de nivel* N como

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; b \equiv c \equiv 0 \pmod{N}, a \equiv 1 \pmod{N} \right\}.$$

Un subgrupo Γ de $\mathrm{SL}_2(\mathbb{Z})$ se dice que es un *subgrupo de congruencias de nivel* N si contiene a $\Gamma(N)$.

Si Γ es un subgrupo de congruencias, denotamos por Y_Γ la superficie de Riemann no compacta $\Gamma\backslash\mathbb{H}$. Para compactificar Y_Γ es suficiente con añadir el conjunto finito de las órbitas de los elementos de $\mathbb{P}^1(\mathbb{Q})$ bajo Γ. Los elementos que pertenecen a este conjunto son llamados *puntas*. A la única punta que hay en el infinito se la denota por $i\infty$. Denotamos por X_Γ dicha compactificación y sea $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, con lo que $X_\Gamma = \Gamma\backslash\mathbb{H}^*$. La superficie de Riemann X_Γ es

compacta y, por lo tanto, es una curva algebraica sobre $\mathbb{C}$ que recibe el nombre de *curva modular asociada a* Γ.

En nuestro caso, estamos interesados en las curvas modulares asociadas a los subgrupos de congruencias de nivel N siguientes:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \;\middle|\; a \equiv 1 \pmod{N} \right\}.$$

Como es habitual, denotaremos a estas curvas por $X_0(N)$ y $X_1(N)$ respectivamente. El grupo $\Gamma_1(N)$ es un subgrupo normal de $\Gamma_0(N)$ y el cociente $\Gamma_0(N)/\Gamma_1(N)$ es isomorfo a $(\mathbb{Z}/N\mathbb{Z})^*$. Cada subgrupo Δ de $(\mathbb{Z}/N\mathbb{Z})^*$ determina el subgrupo de congruencias de nivel N:

$$\Gamma(N,\Delta) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \;\middle|\; d \pmod{N} \in \Delta \right\},$$

que tiene asociada una curva modular que denotamos por $X(N,\Delta)$. Además, cualquier grupo Γ que cumpla $\Gamma_1(N) \subset \Gamma \subset \Gamma_0(N)$ es de la forma $\Gamma(N,\Delta)$ para algún subgrupo Δ de $(\mathbb{Z}/N\mathbb{Z})^*$. Sabemos por [Shi71a] que $X(N,\Delta)$ tiene un modelo definido sobre $\mathbb{Q}$. Estas curvas son todas las curvas intermedias entre $X_1(N)$ y $X_0(N)$ y admiten la siguiente interpretación de móduli:

Los puntos en $Y(N,\Delta) = Y_{\Gamma(N,\Delta)}$ pueden ser interpretados como curvas elípticas sobre $\mathbb{C}$ con una estructura extra "de nivel N" . Más precisamente, los puntos en $\Gamma(N,\Delta)$ parametrizan clases de isomorfismos de pares de la forma $(E, A = \Delta.P)$, donde E es una curva elíptica definida sobre $\mathbb{C}$ y A es el subconjunto de los puntos de E de orden N obtenidos multiplicando un punto $P \in E(\mathbb{C})$, de orden N, por el subgrupo Δ de $(\mathbb{Z}/N\,\mathbb{Z})^*$.

Así, en el caso particular en que $\Delta = (\mathbb{Z}/N\mathbb{Z})^*$, $\Delta.P$ es el subconjunto de todos los generadores del grupo cíclico de orden N generado por P y obtenemos la curva $X_0(N)$. Habitualmente $Y_0(N)$ se describe de forma equivalente, interpretando los puntos de $Y_0(N)$ como clases de isomorfismos de pares (E, C), donde E es una curva elíptica y C un subgrupo cíclico de orden N.

Para el caso $\Delta = \{1\}$, obtenemos la curva $X_1(N)$ y la interpretación de móduli de $Y_1(N)$ es la habitual. Es decir, $Y_1(N)$ parametriza clases de isomorfismos de pares (E, P) donde E es una curva elíptica y P un punto de orden exactamente N.

Otro ejemplo de interés se obtiene considerando un carácter de Dirichlet ε módulo N. En este caso, denotamos por $\Gamma(N,\varepsilon)$, resp. $X(N,\varepsilon)$, al grupo $\Gamma(N,\ker\varepsilon)$, resp. a la curva $X(N,\ker\varepsilon)$.

1.2 Automorfismos de curvas modulares

Sea Γ un grupo de congruencias de nivel N y X_Γ la curva modular asociada. El grupo $\mathrm{PSL}_2(\mathbb{R})$ es el grupo de automorfismos de $\mathbb{H}$. Por lo tanto, si denotamos por Γ^* el normalizador de Γ en $\mathrm{PSL}_2(\mathbb{R})$, el grupo $B(\Gamma)=\Gamma^*/\overline{\Gamma}$, con $\overline{\Gamma}=\Gamma/(\Gamma\cap\{\pm1\})$, proporciona un subgrupo de $\mathrm{Aut}(X_\Gamma)$. Este grupo se ha estudiado en profundidad para el caso en el cual $\Gamma=\Gamma(N,\Delta)$, donde Δ es un subgrupo de $(\mathbb{Z}/N\mathbb{Z})^*$ y X_Γ de género mayor que 1. Recuérdese que toda curva de género mayor que 1 tiene un número finito de automorfismos.

El grupo de automorfismos de $X_0(N)$ ha sido determinado por M. A. Kenku y F. Momose en [KM88] excepto para $N=63$, caso que concluyó N. D. Elkies en [Elk90]. Para un entero N libre de cuadrados y un subgrupo propio Δ de $(\mathbb{Z}/N\mathbb{Z})^*$, el grupo de automorfismos de $X(N,\Delta)$ ha sido determinado por F. Momose y S. Yamada [MY01]. Por último, F. Momose [Mom01] ha determinado el grupo de automorfismos de $X_1(N)$.

A partir de ahora, vamos a centrarnos en ciertos subgrupos de los automorfismos de estas curvas.

Para cada entero positivo M tal que $M|N$ y $(M,N/M)=1$, toda matriz de la forma

$$W(M;a,b,c,d)=\begin{pmatrix} Ma & b \\ Nc & Md\end{pmatrix} \text{ con } a,b,c,d\in\mathbb{Z} \text{ y } \det(W(M;a,b,c,d))=M,$$

pertenece al normalizador de $\Gamma_1(N)$ y también al de $\Gamma_0(N)$, y proporciona sendos automorfismos de $X_1(N)$ y de $X_0(N)$. El automorfismo obtenido en $X_1(N)$ depende únicamente de $d \pmod{N/M}$ y $c \pmod{M}$, mientras que el obtenido en $X_0(N)$ es independiente de los valores a,b,c,d. Cuando tomamos $M=1$, los automorfismos obtenidos en $X_1(N)$ sólo dependen de $d\in(\mathbb{Z}/NZ)^*$; éstos son denotados por $\langle d\rangle$ y llamados *diamantes*. Nótese que las matrices $W(1;a,b,c,d)$ pertenecen a $\Gamma_0(N)$ y, en consecuencia, proporcionan la identidad en $X_0(N)$.

Para un tal M, fijamos la matriz $W(M;a,b,c,d)$ con las condiciones

$$a\equiv 1 \pmod{N/M} \qquad \text{y} \qquad c\equiv 1 \pmod{M}.$$

De acuerdo con Atkin y Li [AL78], denotamos por W_M al correspondiente automorfismo en $X_1(N)$. En $X_0(N)$, dicha matriz define una involución llamada *involución de Atkin-Lehner*, que también denotaremos por W_M. En general, tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} X_1(N) & \xrightarrow{W_M\langle d\rangle} & X_1(N) \\ \downarrow & & \downarrow \\ X_0(N) & \xrightarrow{W_M} & X_0(N)\,. \end{array}$$

En el caso particular $M = N$, el automorfismo W_N es una involución que actúa tanto en $X_1(N)$ como en $X_0(N)$, cuya acción proviene de la acción de la matriz

$$\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$$

en el semiplano superior de Poincaré. Esta involución actuando en $X_1(N)$ es conocida con el nombre de *involución de Weil* y como *involución de Fricke* cuando actúa en $X_0(N)$. Su relación con los diamantes viene dada por:

$$\langle d\rangle W_N = W_N \langle d\rangle^{-1}\,.$$

1.3 Formas parabólicas de peso 2

Sea Γ un grupo de congruencias de nivel N y X_Γ la correspondiente curva modular. Si f es una función meromorfa de $\mathbb{H}$ se define

$$f|_\gamma(z) = (\det\gamma)(cz+d)^{-2} f(\gamma z), \quad \text{para } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \text{ y } \det\gamma > 0\,.$$

Sea $f(z)\,dz$ una forma diferencial de X_Γ. Utilizando las igualdades

$$f(\gamma z)d(\gamma z) = f(z)dz \qquad \text{y} \qquad d(\gamma z) = (\det\gamma)(cz+d)^{-2}dz,$$

obtenemos

$$f|_\gamma = f, \qquad \text{para toda } \gamma \in \Gamma.$$

Además, la meromorfía de la forma diferencial implica que $f(z)$ es meromorfa en $\mathbb{H}$ y en las puntas de Γ. Sea M el menor entero positivo tal que Γ contiene la

traslación por M. Entonces podemos tomar $q = e^{2\pi iz/M}$ como uniformizante en la punta $i\infty$ y obtener así

$$f(z)\,dz = f(q)\frac{M}{2\pi i}\frac{dq}{q}.$$

Si además la forma es holomorfa, entonces f es holomorfa en cada una de las puntas y se anula en todas ellas. Esto justifica la siguiente definición.

Definición 1.1. Una *forma parabólica de peso* 2 *en* Γ es una función en $\mathbb{H}$ tal que

(i) f es holomorfa en $\mathbb{H}$ y en las puntas de Γ,

(ii) $f|_\gamma = f$, para toda $\gamma \in \Gamma$,

(iii) f se anula en las puntas de Γ.

El conjunto de formas parabólicas de peso 2 en Γ forman un espacio vectorial complejo, denotado por $S_2(\Gamma)$. Se tiene el siguiente resultado.

Proposición 1.1. *La aplicación*

$$\begin{array}{ccc} S_2(\Gamma) & \longrightarrow & H^0(X_\Gamma, \Omega^1) \\ f(z) & \mapsto & 2\pi i f(z)\,dz \end{array}$$

es un isomorfismo de $\mathbb{C}$*-espacios vectoriales.*

A partir de ahora, nos centraremos en el grupo de congruencias $\Gamma_1(N)$. En este caso, denotaremos por $S_2(N)$ a $S_2(\Gamma_1(N))$ y forma parabólica de nivel N significará forma parabólica de peso 2 para $\Gamma_1(N)$. Toda función $f \in \mathbb{C}(X_1(N))$ o $f \in S_2(N)$ es periódica de periodo 1 y tiene un desarrollo de Fourier convergente para todo $z \in \mathbb{H}$:

$$f(z) = \sum_{n\geq 1} a_n\, e^{2\pi inz}.$$

Normalmente escribiremos

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

donde $q = e^{2\pi iz}$. A este desarrollo de Fourier se le conoce con el nombre de *q-expansión de f*.

En todo lo que sigue, $X_1(N)$ denota una curva definida sobre $\mathbb{Q}$ que queda determinada, salvo $\mathbb{Q}$-isomorfismo, por la condición de que el cuerpo $\mathbb{Q}(X_1(N))$ es el subcuerpo de $\mathbb{C}(X_1(N))$ cuyas funciones tienen q-expansiones racionales. En particular, $H^0(X_1(N), \Omega^1_{X_1(N)_{/\mathbb{Q}}})$ es el $\mathbb{Q}$-espacio vectorial de las diferenciales $f(q)dq/q$ con f variando entre las formas parabólicas de nivel N con q-expansiones racionales. Los diamantes $\langle d\rangle$, resp. las involuciones de Atkin-Lehner, son automorfismos de $X_1(N)$, resp. de $X_0(N)$, definidos sobre $\mathbb{Q}$, ya que dejan estable $\mathbb{Q}(X_1(N))$, resp. $\mathbb{Q}(X_0(N))$. Sin embargo, la involución W_N actuando en $X_1(N)$ está definida sobre el cuerpo ciclotómico $\mathbb{Q}(\zeta_N)$, donde ζ_N es una raíz N-ésima primitiva de la unidad. De hecho, se cumple

$$^{\tau_d}W_N = W_N \langle d\rangle \quad \text{para todo } d \in (\mathbb{Z}/N\mathbb{Z})^*, \tag{1.1}$$

donde $\tau_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ con $\tau_d : \zeta_N \mapsto \zeta_N^d$.

Los automorfismos W_M y $\langle d\rangle$ de $X_1(N)$ proporcionan automorfismos de $S_2(N)$, cuya acción denotaremos por $W_M\, f$ y $\langle d\rangle\, f$ respectivamente. Sea ε un carácter de Dirichlet módulo N, se denota por $S_2(N,\varepsilon)$ al subespacio vectorial complejo de $S_2(N)$ formado por las formas parabólicas de nivel N tales que $\langle d\rangle\, f = \varepsilon(d)\, f$ para todo diamante $\langle d\rangle$. Los elementos de $S_2(N,\varepsilon)$ reciben el nombre de formas parabólicas de carácter ε. Es fácil comprobar que si $S_2(N,\varepsilon) \neq \{0\}$, entonces ε es par, es decir, $\varepsilon(-1) = 1$; equivalentemente, el cuerpo fijo por ε, $\overline{\mathbb{Q}}^{\ker\varepsilon}$, es un cuerpo de números totalmente real. Además, se tiene la siguiente descomposición

$$S_2(N) = \bigoplus_{\varepsilon:(\mathbb{Z}/N\mathbb{Z})^*\to\mathbb{C}^*} S_2(N,\varepsilon).$$

Si Δ es un subgrupo de $(\mathbb{Z}/N\mathbb{Z})^*$, entonces se tiene

$$S_2(\Gamma(N,\Delta)) = \bigoplus_{\Delta\subset\ker\varepsilon} S_2(N,\varepsilon).$$

Obsérvese que para el caso de carácter trivial, es decir $\varepsilon = 1$, se tiene que $S_2(N,1)$ es igual a $S_2(\Gamma_0(N))$, mientras que si $\varepsilon \neq 1$, entonces $S_2(\Gamma(N,\varepsilon))$ es distinto de $S_2(N,\varepsilon)$. En concreto, por la anterior igualdad se tiene

$$S_2(\Gamma(N,\varepsilon)) = \bigoplus_{n=1}^{\mathrm{ord}\,\varepsilon} S_2(N,\varepsilon^n).$$

Notemos que la involución de Weil W_N es un automorfismo de $X(N,\varepsilon)$, pero en este caso W_N está definida sobre $\overline{\mathbb{Q}}^{\ker\varepsilon}$ debido a (1.1).

1.4 Operadores de Hecke y formas propias

Sea p un primo, se define el *operador de Hecke* T_p *actuando en* $S_2(N)$ mediante la fórmula

$$(T_p\, f)(z) = \frac{1}{p}\sum_{k=0}^{p-1} f\left(\frac{z+k}{p}\right) + p\langle p\rangle f(pz)\,,$$

si $p\not| N$, o bien por

$$(T_p\, f)(z) = \frac{1}{p}\sum_{k=0}^{p-1} f\left(\frac{z+k}{p}\right)$$

si $p|N$.

En el espacio $S_2(N,\varepsilon)$ la fórmula del operador T_p está dada en términos de la q-expansión de $f=\sum_{n\geq 1} a_n\, q^n$, mediante

$$T_p\, f = \sum_{n\geq 1,\, p|n} a_n\, q^{n/p} + p\varepsilon(p)\sum_{n\geq 1} a_n\, q^{pn}. \tag{1.2}$$

La definición de operador de Hecke se extiende a cualquier entero positivo n. Si $n=p^k$, a través de la siguiente fórmula de recurrencia

$$T_{p^k} = \begin{cases} T_p\, T_{p^{k-1}} - \langle p\rangle p\, T_{p^{k-2}} & \text{si } p\not| N,\\ T_p^k & \text{si } p|N.\end{cases}$$

Si $n=\prod_{i=1}^k p_i^{e_i}$ es la factorización en primos de n, de forma multiplicativa, es decir $T_n=\prod_{i=1}^k T_{p_i^{e_i}}$. Para $n=1$, se define $T_1=1$.

De la definición se deduce

$$T_{n\,m} = T_n\, T_m \qquad \text{si } (n,m)=1.$$

Además, conmutan entre sí, con los operadores diamante y satisfacen la siguiente igualdad de series de Dirichlet formales

$$\sum_{n=1}^{\infty} T_n\, n^{-s} = \prod_p (1 - T_p\, p^{-s} + \langle p\rangle p^{1-2s})^{-1}.$$

Se denota por $\mathbb{T}_N$ al subanillo de $\mathrm{End}_{\mathbb{C}}(S_2(N))$ generado por todos los operadores de Hecke y recibe el nombre de *álgebra de Hecke de nivel* N. Nótese que $\mathbb{T}_N$ contiene los operadores diamante.

Definición 1.2. Sea $f \in S_2(N)$, $f \neq 0$, diremos que f es una *forma propia* si es un vector propio para todos los operadores de Hecke, es decir, cuando $Tf = \lambda(T)f$ para un cierto $\lambda(T) \in \mathbb{C}$ y para todo $T \in \mathbb{T}_N$.

Proposición 1.2. *Si $f(q) = \sum_{n\geq 1} a_n\, q^n$ es una forma propia, entonces existe un carácter de Dirichlet ε módulo N tal que $f \in S_2(N, \varepsilon)$. Además, $a_1 \neq 0$ y a_n/a_1 es el autovalor de f bajo la acción de T_n.*

Una forma propia se dirá *normalizada* si $a_1 = 1$. En tal caso, $T_n\, f = a_n\, f$ para todo $n \geq 1$.

Si $f(q) = \sum_{n\geq 1} a_n\, q^n \in S_2(N)$ es una forma propia normalizada de carácter ε, se tiene

(i) $a_{m\,n} = a_m a_n$ si $(m, n) = 1$.

(ii) $a_{p^k} = a_{p^{k-1}}\, a_p - p\,\varepsilon(p) a_{p^{k-2}}$ para todo primo p.

(iii) $\overline{a_p} = \overline{\varepsilon}(p) a_p$ para todo primo $p \nmid N$, donde $\overline{\ }$ denota la conjugación compleja.

1.5 Formas nuevas

En esta sección resumiremos los principales resultados de la teoría de formas nuevas. Ésta fue desarrollada por Atkin-Lehner [AL70], Miyake [Miy71] y Li [Li75].

En el espacio $S_2(N)$ tenemos el *producto escalar de Petersson* que está definido por

$$\langle f, g\rangle = \int_{\mathcal{F}} f(z)\overline{g}(z)\, dx\, dy,$$

donde $z = x + yi$ y $\mathcal{F}$ es un dominio fundamental de $Y_1(N)$.

Sean M un entero positivo tal que $M|N$ y d un divisor positivo de N/M. El automorfismo de $\mathbb{H}$ definido por $z \mapsto d\,z$ define un morfismo no constante $t_{M,d} : X_1(N) \to X_1(M)$, que proporciona un monomorfismo de $S_2(M)$ en

$S_2(N)$, $f(q) \mapsto f(q^d)$, el cual envia $S_2(M,\varepsilon)$ a un subespacio de $S_2(N,\varepsilon)$, y que commuta con los operadores de Hecke T_p cuando $p \not| N$. Introducimos el siguiente subespacio vectorial de $S_2(N)$:

$$S_2(N)^{\text{old}} = \langle f(q^d) \,:\, f \in S_2(M) \text{ con } M|N,\ M \neq N \text{ y } d|N/M \rangle_{\mathbb{C}}\,.$$

Al subespacio de $S_2(N)$ ortogonal a $S_2(N)^{\text{old}}$ con respecto al producto escalar de Petersson se le denota por $S_2(N)^{\text{new}}$. Así, tenemos la siguiente descomposición:

$$S_2(N) = S_2(N)^{\text{old}} \perp S_2(N)^{\text{new}}.$$

Análogamente, se denota por $S_2(N,\varepsilon)^{\text{new}}$ al espacio $S_2(N)^{\text{new}} \cap S_2(N,\varepsilon)$.

Definición 1.3. Sea $f \in S_2(N)$. Diremos que f es una *forma nueva de nivel* N si es una forma propia y $f \in S_2(N)^{\text{new}}$.

De hecho, se tiene la siguiente igualdad

$$S_2(N) = \bigoplus_{M|N} \bigoplus_{d|N/M} t_{M,d}(S_2(M)^{\text{new}}).$$

Dos de los principales resultados de la teoría de formas nuevas son los siguientes.

Teorema 1.3. *El conjunto de las formas nuevas normalizadas de nivel N forman una base de $S_2(N)^{\text{new}}$.*

Teorema 1.4. *Sean $f = \sum_{n\geq 1} a_n q^n$ y $g = \sum_{n\geq 1} b_n q^n$ formas nuevas normalizadas de $S_2(N)$ y $S_2(M)$ respectivamente. Si $a_p = b_p$ para casi todo primo p, entonces $N = M$ y $f = g$.*

Los siguientes resultados, que serán de gran importancia en el resto de la tesis, nos proporcionan información de los coeficientes de la q-expansión de una forma nueva normalizada.

Teorema 1.5. *Sea $f(q) = \sum_{n\geq 1} a_n\, q^n$ una forma nueva normalizada de nivel N y carácter ε. Denotaremos por $K_f = \mathbb{Q}(\{a_n\}_{n\geq 1})$ al cuerpo de los coeficientes de la q-expansión de f. Entonces, K_f es un cuerpo de números y $a_n \in \mathcal{O}_{K_f}$, el anillo de enteros de K. Además K_f es totalmente real si $\varepsilon = 1$, mientras que si $\varepsilon \neq 1$, K_f es una extensión cuadrática imaginaria de un cuerpo totalmente real.*

La demostración del anterior resultado se puede encontrar en [Shi71a] y [Shi72].

Teorema 1.6. *Sea $f(q) = \sum_{n\geq 1} a_n\, q^n$ una forma nueva normalizada de nivel N y carácter ε. Entonces*

$$|a_n| \leq \sigma_0(n)\sqrt{n},$$

donde $\sigma_0(n)$ denota el número de divisores de n. Además, si p es un primo tal que $p|N$, se tiene

$$|a_p| = \begin{cases} 0 & \text{si } p^2|N \text{ y } \mathfrak{f}_\varepsilon \,|\, N/p, \\ \sqrt{p} & \text{si } \mathfrak{f}_\varepsilon \not| N/p, \\ 1 & \text{si } p^2 \not| N \text{ y } \mathfrak{f}_\varepsilon \,|\, N/p, \end{cases}$$

donde $\mathfrak{f}_\varepsilon$ denota el conductor de ε. En particular, si ε es trivial, $a_p \in \{0, \pm 1\}$.

La primera parte del teorema es un caso particular de la conjetura de Ramanujan-Petersson, que fue probada por P. Deligne ([Del71], [Del74]) como una consecuencia de su demostración de la hipótesis de Riemann para variedades sobre cuerpos finitos. Para el caso particular de n primo, dicha desigualdad recibe el nombre de *desigualdad de Weil*. La segunda parte del teorema se puede encontrar en [DS74].

Teorema 1.7. *Sea $f(q) = \sum_{n\geq 1} a_n\, q^n$ una forma nueva normalizada de nivel N y carácter ε. Entonces*

$$L(f,s) = \prod_{p \text{ primo}} (1 - a_p p^{-s} + \varepsilon(p) p^{1-2s})^{-1},$$

donde $L(f,s) = \sum_{n\geq 1} a_n\, n^{-s}$ denota la función L asociada a f.

Si $f(q) = \sum_{n\geq 1} a_n\, q^n \in S_2(N,\varepsilon)$ es una forma nueva normalizada y χ un carácter de Dirichlet módulo N, denotaremos por f_χ a la forma parabólica (cf. [AL78]) de carácter $\varepsilon\chi^2$ y cuya q-expansión es de la forma

$$f_\chi(q) = \sum_{n\geq 1} \chi(p) a_p\, q^n.$$

Denotaremos por $f \otimes \chi$ a la única forma nueva normalizada de carácter $\varepsilon\chi^2$ (cf. [Rib77]) cuya q-expansión es de la forma $(f\otimes\chi)(q) = \sum_{n\geq 1} b_n\, q^n$ con

$b_p = \chi(p)a_p$ para casi todo primo p. De hecho, se tiene que $b_p = \chi(p)a_p$ para todo primo que no divide al conductor de χ.

Cada automorfismo W_M proporciona un isomorfismo (cf. [AL78]) entre los espacios vectoriales $S_2(N,\varepsilon)^{\text{new}}$ y $S_2(N,\overline{\varepsilon}_M\varepsilon_{N/M})^{\text{new}}$, donde ε_M y $\varepsilon_{N/M}$ denotan respectivamente los caracteres de Dirichlet de módulos M y N/M, tales que $\varepsilon = \varepsilon_M\varepsilon_{N/M}$. Además, se tiene

$$W_M f = \lambda_M(f)\cdot f\otimes\overline{\varepsilon}_M, \qquad \text{con } |\lambda_M(f)| = 1,$$

$f\otimes\overline{\varepsilon}_M \in S_2(N,\overline{\varepsilon}_M\varepsilon_{N/M})^{\text{new}}$ y su q-expansión es de la forma

$$(f\otimes\overline{\varepsilon}_M)(q) = \sum_{n\geq 0} b_n q^n, \text{ con } b(p) = \begin{cases} \overline{\varepsilon}_M(p)a_p & \text{si } p\nmid M,\\ \overline{\varepsilon}_{N/M}(p)\overline{a_p} & \text{si } p|M.\end{cases}$$

Definición 1.4. Sea $f\in S_2(N,\varepsilon)$ una forma nueva normalizada. Un *torcimiento interno de* f es un par (σ,χ), donde $\sigma\in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ y $\chi\neq 1$ es un carácter de Dirichlet módulo N, tal que

$${}^{\sigma}f = f\otimes\chi.$$

Se dice que una forma f tiene *multiplicación compleja* si tiene un torcimiento interno (σ,χ) con $\sigma = \mathrm{id}$. En este caso, χ és el carácter asociado a un cuerpo cuadrático imaginario (cf. [Rib77]). Diremos que (σ,χ) es un *torcimiento extra* de f si σ es no trivial. Cuando el cáracter ε es trivial los caracteres de los torcimientos internos són cuadráticos (cf. [Rib80]) y si $\varepsilon\neq 1$ entonces f tiene el torcimiento extra formado por la conjugación compleja y ε^{-1}.

1.6 Las jacobianas de las curvas modulares

En esta sección mostramos la descomposición de la jacobiana de $X_1(N)$, $J_1(N)$, sobre $\mathbb{Q}$ y también sobre $\overline{\mathbb{Q}}$. En primer lugar, notamos que cada operador de Hecke T_n define una correspondencia de $X_1(N)$ y, por lo tanto, un endormorfismo de $J_1(N)$ que está definido sobre $\mathbb{Q}$. Omitimos la descripción de la acción de T_n como correspondencia, ya que ésta no será utilizada posteriormente. El siguiente resultado desempeña un papel importante en la teoría de curvas modulares.

Teorema 1.8 (La congruencia de Eichler-Shimura). *Si p es un primo entero tal que $p \nmid N$, entonces p es un primo de buena reducción para $X_1(N)$ y además*

$$\widetilde{T_p} = \mathrm{Frob}_p + \widetilde{\langle p \rangle}\widehat{\mathrm{Frob}}_p = \mathrm{Frob}_p + \widetilde{\langle p \rangle} p \,\mathrm{Frob}_p^{-1},$$

donde $\widetilde{T_p}$, resp. $\widetilde{\langle p \rangle}$, denota la reducción del endomorfismo T_p, resp. $\langle p \rangle$, módulo p, Frob_p el endomorfismo de Frobenius módulo p y $\widehat{\mathrm{Frob}}_p$ su dual.

H.M. Eichler [Eic54] demostró que este resultado era cierto para todo primo $p \nmid N$ excepto para un número finito en el caso de la jacobiana de $X_0(N)$, $J_0(N)$. G. Shimura [Shi58] lo generalizó para $J_1(N)$ y, finalmente, J. Igusa [Igu59] demostró su validez para todo primo que no divide a N.

En segundo lugar, hacemos una breve introducción de la construcción de G. Shimura (ver capítulo 7 de [Shi71a] y [Shi73]) para asociar a una forma nueva f (o, más bien, a la órbita de f bajo $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) una variedad abeliana A_f. Sea $f \in S_2(N)$ una forma nueva normalizada. Consideramos el homomorfismo de anillos $\lambda_f : \mathbb{T}_N \to \mathbb{C}$ tal que $Tf = \lambda_f(T) f$ para $T \in \mathbb{T}_N$. Sea $\mathbb{I}_f = \ker(\lambda_f)$ y definamos

$$\mathbb{T}_f = \mathbb{T}_N / \mathbb{I}_f.$$

Si $f(q) = \sum_{n \geq 1} a_n \, q^n \in S_2(N, \varepsilon)$, entonces λ_f induce un isomorfismo

$$\begin{array}{rcl} \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T}_f & \to & K_f\,, \\ T_p + \mathbb{I}_f & \mapsto & a_p\,, \\ \langle d \rangle + \mathbb{I}_f & \mapsto & \varepsilon(d)\,. \end{array}$$

La imagén $\mathbb{I}_f \, J_1(N)$ es una subvariedad abeliana de $J_1(N)$ que es estable bajo $\mathbb{T}_N$ y está definida sobre $\mathbb{Q}$.

Definición 1.5. La *variedad abeliana modular A_f asociada a f* es

$$A_f = J_1(N) / \mathbb{I}_f \, J_1(N).$$

Por construcción, tenemos un morfismo exhaustivo

$$\pi_f : J_1(N) \twoheadrightarrow A_f$$

cuyo núcleo es la variedad abeliana $\mathbb{I}_f \, J_1(N)$. Este morfismo nos proporciona información de las diferenciales regulares de A_f. En concreto, tenemos

$$\pi_f^*(H^0(A_f, \Omega^1)) = S_2(A_f) \, \frac{dq}{q},$$

donde denotamos $S_2(A_f) = \langle {}^\sigma f : \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\rangle_{\mathbb{C}}$. Además, la involución de Weil W_N y los diamantes dejan estable $S_2(A_f)$, propiedad que desempeñará un papel destacado en el capítulo 3.

El siguiente resultado muestra las principales propiedades de esta variedad abeliana.

Teorema 1.9. *Sea $f \in S_2(N)$ una forma nueva. Entonces la variedad abeliana A_f tiene las siguientes propiedades:*

(i) A_f *está definida sobre* $\mathbb{Q}$,

(ii) A_f *es* $\mathbb{Q}$*-simple,*

(iii) $\dim A_f = [K_f : \mathbb{Q}]$,

(iv) $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(A_f) = \mathbb{T}_f \simeq K_f$,

(v) A_f *sólo depende de la clase de conjugación de Galois de* f*, es decir, si* $g \in S_2(M)$ *es una forma nueva, entonces* $A_f \overset{\mathbb{Q}}{\sim} A_g$ *si y sólo si* $N = M$ *y* $g = {}^\sigma f$ *para algún* $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Utilizando la congruencia de Eichler-Shimura se obtiene el siguiente resultado.

Teorema 1.10. *Sea $f(q) = \sum_{n\geq 1} a_n\, q^n \in S_2(N, \varepsilon)$ una forma nueva y p un primo tal que $p \nmid N$. Entonces el polinomio característico del endomorfismo de Frobenius* Frob_p *actuando en el módulo de Tate de* $A_{f/\mathbb{F}_p}$ *es de la forma:*

$$\prod_{\sigma : K_f \hookrightarrow \mathbb{C}} (t^2 - {}^\sigma a_p t + p\, {}^\sigma \varepsilon(p)).$$

El siguiente resultado fue demostrado por H. Carayol [Car86] tras completar algunos trabajos de [Del71], [Iha67] y [Lan73].

Teorema 1.11. *Sea $f \in S_2(N)$ una forma nueva y denotemos por $\mathcal{N}_{\mathbb{Q}}(A_f)$ el conductor geométrico de A_f sobre $\mathbb{Q}$. Entonces,*

(i) $\mathcal{N}_{\mathbb{Q}}(A_f) = N^{\dim A_f}$,

(ii) $L(A_f, s) = \prod_{\sigma : K_f \hookrightarrow \mathbb{C}} L({}^\sigma f, s)$.

Se definen la parte vieja y nueva de $J_1(N)$ y se denotan, respectivamente, por $J_1(N)^{\text{old}}$ y $J_1(N)^{\text{new}}$, a los cocientes optimales de $J_1(N)$ definidos sobre $\mathbb{Q}$ tales que los correspondientes espacios de diferenciales regulares proporcionan los subespacios $S_2(N)^{\text{old}}dq/q$ y $S_2(N)^{\text{new}}dq/q$ respectivamente. Más concretamente, ponemos

$$J_1(N)_{\text{old}} = \sum_{M|N,\, M\neq N} \sum_{d|N/M} t^*_{M,d} J_1(M) \quad \text{y} \quad J_1(N)^{\text{new}} = J_1(N)/J_1(N)_{\text{old}}\,.$$

Si A es una subvariedad abeliana de $J_1(N)$ tal que $A + J_1(N)_{\text{old}} = J_1(N)$ y $J_1(N)_{\text{old}} \cap A$ es finito, entonces

$$J_1(N)^{\text{old}} = J_1(N)/A\,.$$

Así, $J_1(N) \overset{\mathbb{Q}}{\sim} J_1(N)^{\text{old}} \times J_1(N)^{\text{new}}$ y análogamente para $J_0(N)$.

Las variedades A_f jugarán un papel destacado en el desarrollo de esta tesis, debido a que éstas son los factores $\mathbb{Q}$-simples de $J_1(N)$, tal como se muestra en el siguiente resultado.

Teorema 1.12. *Denotemos por B_M el conjunto de clases de conjugación de Galois de formas nuevas normalizadas de nivel M. Entonces,*

$$J_1(N)^{\text{new}} \overset{\mathbb{Q}}{\sim} \prod_{f\in B_N} A_f \qquad y \qquad J_1(N) \overset{\mathbb{Q}}{\sim} \prod_{M|N} \prod_{f\in B_M} A_f{}^{\sigma_0(N/M)}\,.$$

Finalmente, damos la descripción de la descomposición de $J_1(N)$ sobre $\overline{\mathbb{Q}}$ mostrando como descomponen las variedades A_f.

Teorema 1.13. *Sea $f = \sum_{n\geq 1} a_n q^n \in S_2(N,\varepsilon)$ una forma nueva normalizada. Entonces, existe una variedad abeliana B_f, llamada bloque constituyente de f, que es $\overline{\mathbb{Q}}$-simple, isógena a todas sus conjugadas de Galois y tal que A_f es $\overline{\mathbb{Q}}$-isógena a una potencia de B_f. Además:*

(i) Si f tiene multiplicación compleja, es decir, existe un carácter de Dirichlet χ tal que $a_p = \chi(p)a_p$ para $p\nmid N$, entonces B_f es una curva elíptica con multiplicación compleja por el cuerpo fijo del carácter χ (cf. [Rib77],[Shi71b]).

(ii) Si f no tiene multiplicación compleja, entonces $\dim B_f = t[F:\mathbb{Q}]$ *donde F es el cuerpo de números $\mathbb{Q}(\{a_p^2/\varepsilon(p) : p\not| N\})$ y t es igual a* 1 *ó* 2 *dependiendo que $\mathbb{Q}\otimes\mathrm{End}(B_f)$ sea F o una álgebra de cuaterniones central sobre F (cf. [Rib80],[Mom81]). Además, el cuerpo fijo por los caracteres de los torcimientos extras es el mínimo cuerpo tal que A_f descompone completamente (cf. [GL01]).*

Observación 1.1. Se dice que una curva elíptica definida sobre $\overline{\mathbb{Q}}$ es una $\mathbb{Q}$-*curva* si es $\overline{\mathbb{Q}}$-isógena a todas sus conjugadas de Galois. Todo bloque constituyente de dimensión 1 es una $\mathbb{Q}$-curva y Ribet [Rib92] demostró que, asumiendo la conjetura 3.2.4$_?$ de Serre [Ser87], el recíproco es cierto.