UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Tesis de Licenciatura

Puntos de Heegner

Daniel Kohen

Director: Ariel Martín Pacetti

Fecha de Presentación: Marzo 2013

Agradecimientos

A mis viejos por bancarme y principalmente por aguantarme. A mi familia.

A Meli por acompañarme en todas, soportarme y quererme. Gracias por este año maravilloso , me hacés muy bien y te amo muchísimo. No se que haría sin vos.

A la OMA por haberme ayudado a encontrar mi lugar en el mundo. En especial a Flora, Patricia y Beto.

A Ariel por guiarme en el camino de la teoría de números y de la tesis; tomarse el trabajo de leerla y aportar cosas que me ayudaron un montón. Un placer trabajar con alguien que sabe tanto y siempre está dispuesto a enseñar y a contar cosas copadas con la mejor onda.

A Fernando y Teresa, el jurado, por sus correcciones que ayudaron a mejorar el trabajo.

A todos los del seminario de teoría de números por hacerme sentir cómodo y compartir grandes momentos, ya sea de matemática o comiendo una bondiola y hablando de fútbol.

A Charly y a Maxi por haber sido mis referentes durante la carrera. Gracias por siempre responder mis dudas existenciales acerca de la matemática y la facultad y haberme acercado a la teoría de números.

A todos los profesores que tuve durante la carrera en especial a: Malena, Mariela, Ariel, Fernando, Daniel y Julián.

A la infinita ayuda que me dieron Mariano y Andrea.

A todos los jtp y ayudantes que tuve, en especial a: Marce, Nico, Mariano, Maxi, Seba, Julieta, Román, Chris, Jonathan

A la Escuela Argentina Modelo y a la Escuela Técnica ORT por darme la posibilidad de hacer un trabajo hermoso y mantenerme en contacto con las olimpiadas.

A la ANCEFN por otorgarme una beca que me ayudó mucho durante la carrera.

A la UBA por la beca estímulo.

A Nacho y a Juanjo por ser grandes amigos y estar siempre ahí.

A Julián E, Julián H, Javier y Taurus por compartir un gran viaje y una gran experiencia.

A todos los compañeros de viaje en la UMA.

A todos mis compañeros de cursada, en especial a Diego, Maxi, Euge, Fransisco, Ezequiel, Matías, Julián, Pablo B.

A todos mis amigos y gente maravillosa que conocí en la OMA y en su mayoría tengo la suerte de verlos día a día en la facu, en especial a Matías, Mariano y Franco.

A todos mis amigos con los que comparto grandes momentos tanto dentro como fuera de la facu. En especial a Meli,Nacho,Nati,Belén, Diego, Santi, Cami, Vale, Jero,

Maxi,Sofi, Rafa, Fede, Pablo H.

A todos los miembros de que la sigan pipeteando por dejarme jugar en su equipo y deleitarme con su buen fútbol mientras pego patadas. A toda la hinchada que nos banca los trapos. También a todo el equipo e hinchada de los Borbotones.

A TODOS los que hacen que la facu sea mi segundo hogar. Compartiendo un café, una charla sobre matemática o de fútbol , una mesa de estudio o un partido de Tute. O simplemente por estar ahí y hacerme sentir bien.

Gracias! :)

Introducción

Un problema de suma importancia para la teoría de números clásica y moderna es el de poder determinar el conjunto de soluciones racionales de una ecuación con coeficientes racionales. Un ejemplo de este problema es la determinación de las ternas pitagóricas, que se pueden pensar como soluciones racionales, o sea puntos cuyas ambas coordenadas son racionales, en la circunferencia unitaria o soluciones enteras de la ecuación $x^2 + y^2 = z^2$. Las curvas pueden clasificarse por un invariante llamado el género. La circunferencia es una curva de género 0, y a partir de un punto racional, es fácil encontrar todos ellos por el método de la tangente.

Más generalmente, un resultado de Hasse-Minkowski nos dice que uno puede determinar si cualquier curva de género 0 (por ejemplo las cónicas) tiene alguna solución entera fijándose si tiene solución módulo todos los primos y una solución real. Además, si la curva tiene una solución racional, automáticamente tiene infinitas, pudiéndose parametrizar todas ellas.

En el otro extremo, se encuentran las curvas de género ≥ 2. Faltings demostró que estas curvas siempre tienen finitos puntos racionales aunque no se conoce un método general para calcular efectivamente estos puntos, y tampoco se sabe si un tal proceso existe o no.

El caso que nos interesa en este trabajo es el caso intermedio de curvas de género 1. Dada una curva de género 1, no se conoce un método que pueda decidir si tiene un punto racional o no (aunque existen algoritmos que funcionan en muchos casos).Una curva elíptica es una curva de género 1 con un punto racional distinguido. Estas curvas tienen una estructura de grupo abeliano y el teorema de Mordelll-Weil nos dice que dicho grupo es finitamente generado. La parte de torsión de la curva se puede calcular usando el teorema de Nagell-Lutz. El problema más interesante es como calcular el *rango* de la curva, esto es la cantidad de puntos linealmente independientes sobre $\mathbb{Z}$. Claramente esto implica el poder calcular todos los puntos racionales de la curva. Siguiendo la filosofía de Hasse-Minkowski, que nos dice que si una forma cuadrática tiene soluciones locales entonces se pueden "pegar"para obtener una solución global uno podría esperar que esto valga en contextos más generales. Lamentablemente este teorema no es cierto para género mayor que 1, sin embargo los principios locales - globales aparecen de otras maneras.

En el caso de las curvas elípticas existe una conjetura, de Birch y Swinnerton-Dyer que relaciona el rango de la curva elíptica con el orden de anulación de una función de variable compleja en su centro de simetría. Esta función se obtiene multiplicando factores para cada primo y estos factores tienen que ver con la cantidad de soluciones módulo p de la curva. O sea, lo que estamos diciendo es que la infor-

mación local (contar puntos módulo p) pegada de cierta forma debería darnos una información global (el rango de la curva). Esta conjetura todavía está abierta pero gracias a resultados de Gross-Zagier y Kolyvagin (entre otros) se puede probar para ciertos casos particulares. La idea de la demostración es utilizar los llamados *puntos de Heegner* que dan lugar al título del presente trabajo y sobre los que discutiremos varios aspectos. Estos puntos proveen una teoría rica que no sólo nos permite resolver esta maravillosa conjetura para una gran cantidad de casos sino que también para esos casos nos da un algoritmo efectivo para calcular todos los puntos de la curva elíptica. Además los puntos tienen otras aplicaciones, por ejemplo relacionadas con el antiguo problema de los números congruentes que consiste en determinar que valores enteros puede tomar el área de un triángulo rectángulo con lados de longitud racional.

En la secciones 1, 2 y 3 explicaremos los preliminares necesarios acerca de curvas elípticas, L-series y formas modulares. Estos conceptos no son solo centrales en nuestro trabajo sino que también forman una parte destacada del desarrollo de la teoría de números moderna, famosos por ser una pieza clave en la resolución del último teorema de Fermat.

En la sección 4, la central de este trabajo, se explica que son los puntos de Heegner, sus propiedades teóricas y también como se usan para calcular puntos racionales mediante ejemplos explícitos.

Por último en la sección 5 se cuentan las distintas generalizaciones (conocidas y por conocer) que tienen estos puntos a contextos más generales y se plantean problemas abiertos respecto a los mismos que formarán parte del estudio e investigación durante el transcurso del doctorado.

Índice

1. Curvas Elípticas

1.1. Definiciones y ley de grupo

Una curva elíptica sobre un cuerpo K es un curva proyectiva suave de género 1 con un punto racional distinguido. Por el teorema de Riemann-Roch una tal curva se puede escribir en una ecuación de Weierstrass de la forma

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

con $a_i \in K$ y $\Delta \neq 0$. Si la característica de K es distinta de 2 y 3 se puede llevar la ecuación a la forma más sencila

$$y^2 = x^3 + ax + b,$$

$a, b \in K$ y $\Delta = -2^4(4a^3 + 27b^2) \neq 0$.

Dada E/K una curva elíptica definimos su j-invariante como

$$j(E) = \frac{-1728(4a)^3}{\Delta}.$$

Es fácil ver que dos curvas elípticas son isomorfas sobre $\bar{K}$ si y sólo si sus j-invariantes coinciden. Además, dado $j \in K$, podemos encontrar una curva con coeficientes en K con ese invariante.

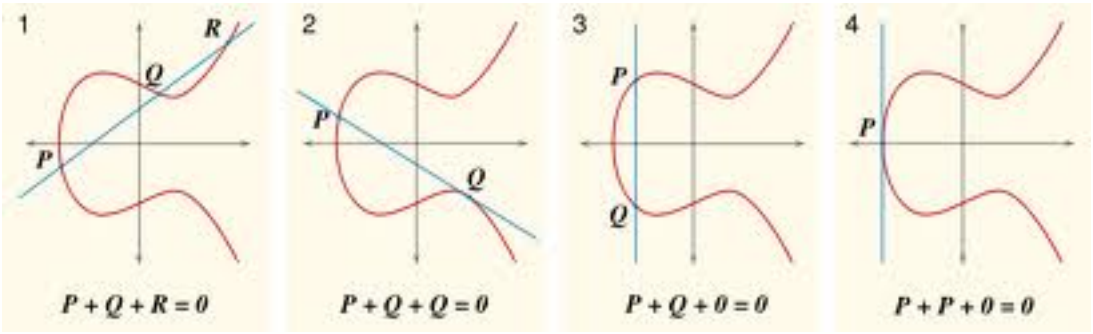
Para las definiciones y propiedades básicas de estos hechos se puede consultar [17] (III.1).

Tomemos una ecuación de Weierstrass como arriba; si la miramos en el plano proyectivo (homogeneizando respecto de z) vemos que en $z = 0$ tenemos un único punto, que llameremos punto del infinito, que es el $O = [0 : 1 : 0]$. Este será nuestro punto racional distinguido en la curva elíptica. La ventaja de trabajar con una curva elíptica es que los puntos de la curva tienen una estructura de grupo, que se obtiene de la manera siguiente: Sean $P, Q \in E$ y sea L la recta que los une (consideramos la tangente en P si ocurre que $P = Q$). Por Bezout esta recta corta a la cúbica en un tercer punto, digamos R. Análogamente la recta que pasa por R y O corta a la cúbica en un tercer punto, que llamaremos $P \oplus Q$. Como estamos pidiendo que tres puntos colineales sumen O, sabiendo que dos de esos puntos tienen coordenadas en K el tercero también las tendrá. En efecto, sean P_1, P_2 dos puntos de la curva elíptica definidos sobre K, y sea L la recta que los une que corta a la cúbica en un tercer punto P_3. Sea

$$L : y = \lambda x + v,$$

donde claramente x, v, λ están definidos sobre K. Llamando a $P_i = (x_i, y_i)$ tenemos entonces que si evaluamos la ecuación de la curva elíptica en $(x, \lambda x + v)$ nos queda de la forma $c(x - x_1)(x - x_2)(x - x_3)$. Finalmente igualando los coeficientes en x^2 y en x^3 se obtiene que $c = -1$ y que $x_3 = \lambda^2 + a_1\lambda + a_2 - x_1 - x_2$ y por lo tanto el punto P_3 está definido sobre K como queríamos.

Se puede ver que este proceso dota a los puntos de la curva elíptica de una estructura de grupo abeliano, y podemos dar fórmulas explícitas para sumar puntos en la curva. Para más detalles se puede consultar [17] (III.2) ó [12] (III.4).



1.2. Estructura analítica

Sea ahora $E/\mathbb{C}$ una curva elíptica. A la curva E se le puede asociar un retículo $\Lambda \subset \mathbb{C}$ de forma que los puntos complejos de la curva están en biyección con los puntos de $\mathbb{C}/\Lambda$. Todo retículo de $\mathbb{C}$ se puede escribir de la forma

$$\langle \omega_1, \omega_2 \rangle_{\mathbb{Z}}$$

donde ω_1, ω_2 son $\mathbb{R}$ - linealmente independientes.

Si llamamos $\wp_\Lambda$ a la función $\wp$ de Weierstrass asociada al retículo Λ dada por

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right),$$

entonces se tiene que las funciones Λ periódicas $\wp_\Lambda(z)$ y $\wp'_\Lambda(z)$ satisfacen la siguiente relación algebraica

$$E : y^2 = x^3 - g_2 x - g_3,$$

donde

$$x = \wp_\Lambda(z), y = \wp'_\Lambda(z),$$

$$g_2 = 60 \sum_{\lambda \in \Lambda - 0} \frac{1}{\lambda^4},$$

$$g_3 = 140 \sum_{\lambda \in \Lambda - 0} \frac{1}{\lambda^6},$$

y la aplicación $\Phi_w(z) = (\rho_\Lambda(z), \rho'_\Lambda(z))$ nos da un isomorfismo (de grupos y de variedades analíticas) entre $\mathbb{C}/\Lambda$ y la curva elíptica E.

El libro [13] (cap. I) realiza el estudio acerca de las curvas elípticas desde este punto de vista y es una buena referencia para estos resultados. También están explicados en [17] (cap.VI).

1.3. Isogenías

Sean E_1, E_2 dos curvas elípticas. Una isogenía es un morfismo de curvas algebraicas

$$\phi : E_1 \longrightarrow E_2,$$

tal que $\Phi(O) = O$. Si dos curvas están relacionadas por una isogenía se dicen que son isógenas. Una isogenía es o bien constante (en cuyo caso $\phi \equiv 0$ y se dice que es trivial) o es no constante y es un morfismo finito de curvas. En este último caso, uno tiene la inyección usual de cuerpos de funciones

$$\phi^* : \bar{K}(E_2) \longrightarrow \bar{K}(E_1).$$

Se dice que una isogenía tiene grado n, es separable, puramente inseparable, etc, si la correspondiente extensión de cuerpos goza tal propiedad.

Un ejemplo es la isogenía multiplicar por m que se define, si $m > 0$, como

$$[m] : E \longrightarrow E, \qquad [m](P) = P + P + \cdots + P \ (m \text{ veces}).$$

Se puede ver que estas isogenías son no triviales. Podemos mirar el núcleo de estas isogenías y definir el subgrupo de puntos de m-torsión como sigue:

$$E[m] = \{P \in E : [m]P = O\}.$$

También podemos definir el grupo de torsión como

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

Vamos a destacar una serie de resultados útiles acerca de las isogenías. Para las demostraciones se puede consultar [17] (III.4 y III.6).

Teorema 1.1. *Si ϕ una isogenía separable entonces $\#ker\phi = deg\phi$ y la extensión de cuerpos inducida por la isogenía es Galois.*

Teorema 1.2. *Sea E una curva elíptica y sea Φ un subgrupo finito de E. Entonces existe una única curva elíptica E' y una isogenía separable*

$$\phi : E \longrightarrow E',$$

tal que $ker\phi = \Phi$.

Teorema 1.3 (Isogenía Dual)**.** *Dada $\phi : E_1 \longrightarrow E_2$ una isogenía no constante de grado m existe una única isogenía (llamada isogenía dual)*

$$\hat{\phi} : E_2 \longrightarrow E_1,$$

tal que

$$\hat{\phi} \circ \phi = [m].$$

Además se tiene que $[m] = [\hat{m}]$ y que $deg\,[m] = m^2$.

Como coralario uno obtiene lo siguiente:

Corolario 1.4. *Sea K algebraicamente cerrado. Si $car(K) = 0$ o $car(K)$ coprima con m entonces se tiene que*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Demostración. Sabemos que $[m]$ tiene grado m^2 y luego en las condiciones del corolario nos queda que la isogenía es separable. Luego por lo visto antes

$$\#E\,[m] = \#ker\phi = m^2,$$

y más aún para todo $d \mid m$ se tiene que

$$\#E\,[d] = d^2.$$

Por el teorema de estructura para grupos abelianos finitos aplicado a $E\,[m]$, escribiéndolo como producto de subgrupos cíclicos se ve rápidamente que la única posibilidad es la que buscamos.

□

Volvamos a la estructura analítica por un momento y tratemos de entender como son las isogenías en ese caso.

Teorema 1.5. *Sean $E_1 = \mathbb{C}/\Lambda_1, E_2 = \mathbb{C}/\Lambda_2$ dos curvas elípticas. Entonces tenemos*

1. *La función*

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \mapsto \{\phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2 : \phi(0) = 0, \phi \text{ holomorfa}\}$$

   dada por mandar

$$\alpha \longrightarrow \phi_\alpha$$

   donde

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2, z \longrightarrow \alpha z (mod \Lambda_2),$$

   es una biyección.

2. *La inclusión natural de $\{$isogenías $\phi : E_1 \longrightarrow E_2\}$ en*

$$\{\phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2 : \phi(0) = 0, \phi \text{ holomorfa}\}$$

   es una biyección.

Demostración. La idea es levantar las funciones holomorfas a $\mathbb{C}$ que es el revestimiento universal de $\mathbb{C}/\Lambda$. Para la demostración ver [17] (VI.4).

□

Observación 1.6. Podemos definir $End(E) = \{\phi : E \longrightarrow E \text{ isogenías}\}$ y se tiene que si $E \cong \mathbb{C}/\Lambda$ entonces

$$End(E) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$$

Siguiendo estas ideas se pueden obtener demostraciones sencillas de algunos hechos de curvas elípticas sobre $\mathbb{C}$ y usando el principio de Lefschetz que dice que hacer geometría algebraica en $\mathbb{C}$ y en un cuerpo de K de característica 0 algebraicamente cerrado es lo mismo (más precisamente nos da una equivalencia de categorías), uno puede probar tales afirmaciones para los cuerpos mencionados recién. Por ejemplo es trivial ver que

$$E[m] \cong (\mathbb{C}/\Lambda)[m] \cong \frac{1}{m}\Lambda/\Lambda \cong (\mathbb{Z}/m\mathbb{Z})^2.$$

También tenemos el siguiente resultado, que juega un rol crucial en este trabajo.

Teorema 1.7. *Sea E una curva elíptica sobre $\mathbb{C}$ entonces*

1. *$End(E) \cong \mathbb{Z}$, ó*

2. $End(E) \cong \mathcal{O}$ donde $\mathcal{O}$ es un orden en un cuerpo cuadrático imaginario.

Observación 1.8. Un orden en un cuerpo cuadrático K es un subanillo de $\mathcal{O}_K$ (el anillo de enteros de K), de rango 2 como $\mathbb{Z}$- módulo, Si $\mathcal{O}_K = \mathbb{Z}[\alpha]$ existe un entero c, llamado conductor del orden tal que $\mathcal{O} = \mathbb{Z}[c\alpha]$.

Demostración. Sea $E \cong \mathbb{C}/\Lambda$ con $\Lambda = \langle \omega_1, \omega_2 \rangle$. Sabemos por la observación 8 que

$$End(E) = \{\alpha : \alpha\Lambda \subset \Lambda\}.$$

Entonces, podemos cambiar a Λ por un retículo homotético de la forma $\mathbb{Z}+\tau\mathbb{Z}$ donde $\tau = \omega_1/\omega_2$. Como Λ es un retículo $\tau \notin \mathbb{R}$ pues sino esto nos diría que ω_1 y ω_2 son $\mathbb{R}$-linealmente dependientes, lo que es absurdo. Sea α tal que

$$\{\alpha(\mathbb{Z} + \tau\mathbb{Z}) \subset \mathbb{Z} + \tau\mathbb{Z}\}.$$

Eso quiere decir que existen enteros a, b, c, d tales que

$$\alpha = a + b\tau, \alpha\tau = c + d\tau.$$

Eliminando τ obtenemos la siguiente ecuación

$$\alpha^2 - (a + d)\alpha + ad - bc = 0.$$

Luego $End(E)$ es una extensión entera de $\mathbb{Z}$. Si suponemos que es más grande que $\mathbb{Z}$ entonces tomando un $\alpha \notin \mathbb{Z}$ tenemos que $b \neq 0$; eliminando ahora a α tenemos

$$b\tau^2 + (a - d)\tau - c = 0,$$

por lo tanto $\mathbb{Q}(\tau)$ es un cuerpo cuadrático imaginario y como $End(E)$ está metido ahí y es entero sobre $\mathbb{Z}$ se sigue que

$$End(E) \cong \mathcal{O},$$

como queríamos probar.

□

Cuando ocurre el caso 2 se dice que la curva elíptica tiene multiplicación compleja por $\mathcal{O}$.

1.4. El teorema de Mordellll-Weil

Sea E/K una curva elíptica sobre un cuerpo de números K (es decir una extensión finita de $\mathbb{Q}$). Entonces se tiene el siguiente teorema.

Teorema 1.9. *(Mordellll-Weil): $E(K)$ es finitamente generado, i.e.*

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}.$$

El número $r \geq 0$ se llama el rango de la curva elíptica sobre K y $E(K)_{tors}$ es el subgrupo finito de torsión.

La demostración tiene dos ingredientes principales:

- La existencia de una altura $h : E(K) \longrightarrow \mathbb{R}$ satisfaciendo
  1. Para todo $Q \in E(K)$ existe una constante C_Q que depende sólo de Q y una constante C que depende sólo de la la curva tal que
  $$h(P+Q) \leq 2h(P) + C_Q,$$
  y
  $$h(mP) \geq m^2 h(P) + C,$$
  para todo $P \in E(K)$
  2. Para todo $B > 0$
  $$\{P : h(P) < B\},$$
  es finito.
- (Teorema débil de Mordellll-Weil): Para todo n entero, el grupo $E(K)/nE(K)$ es finito.

Estas dos piezas se conectan con el siguiente lema para dar la demostración del teorema de Mordellll-Weil.

Lema 1.10. *(Descenso de Fermat) Sea G un grupo abeliano equipado con una altura que cumple las propiedades mencionadas arriba. Asumamos que para algún $n > 1$ el grupo G/nG es finito. Entonces G es finitamente generado.*

La demostración del teorema débil empieza con la observación que es trivialmente cierto para cualquier clausura algebraica de K, ya que en ese caso multiplicar por n es suryectivo. Tenemos la siguiente sucesión exacta

$$0 \longrightarrow E[n](\bar{K}) \longrightarrow E(\bar{K}) \xrightarrow{n} E(\bar{K}) \longrightarrow 0.$$

Tenemos que también es una sucesión exacta de módulos equipada con la acción continua de $G_K = Gal(\bar{K}/K)$. Tomando cohomología se tiene la siguiente sucesión exacta larga de cohomología:

$$0 \longrightarrow E[n](K) \longrightarrow E(K) \xrightarrow{n} E(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K, E) \xrightarrow{n} H^1(K, E),$$

de la cual se puede extraer la llamada suceción exacta de descenso

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K, E)[n] \longrightarrow 0.$$

Para cada lugar (primo) ya sea finito o infinito v podemos pensar a K metido en la completación K_v y ese embbeding se extiende a uno de $\bar{K}$ en $\bar{K_v}$. Luego se induce una inclusión $G_{K_v} \subset G_K$ y la sucesión exacta de descenso tiene su versión local como se puede apreciar en el siguiente diagrama conmutativo:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\delta} & H^1(K, E[n]) & \longrightarrow & H^1(K, E)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K_v)/nE(K_v) & \xrightarrow{\delta} & H^1(K_v, E[n]) & \longrightarrow & H^1(K_v, E)[n] & \longrightarrow & 0
\end{array}$$

en donde del diagrama de arriba al de abajo tenemos las flechas verticales que corresponden a las restricciones. Del diagrama nos surge una flecha

$$H^1(K, E[n]) \xrightarrow{\delta_v} H^1(K_v, E)[n].$$

Como

$$\delta(E(K)/nE(K)) \subset ker(\delta_v),$$

para todo v, tenemos que $E(K)/nE(K)$ está contenido en el grupo de Selmer, que se define como sigue:

- El n-grupo de Selmer de E/K, denotado $Sel_n(E/K)$, es el conjunto de clases $c \in H^1(K, E[n])$ que satisfacen $\delta_v(c) = 0$ para todo v primo de K.

Lo que queremos probar es consecuencia del siguiente resultado general

Proposición 1.11. *El grupo $Sel_n(E/K)$ es finito.*

Una pregunta a la que apuntamos responder es la siguiente: Dada una curva elíptica sobre un cuerpo de números K, ¿existe un algoritmo para

1. determinar si $E(K)$ es infinito?

2. hallar el rango de la curva elíptica?

3. encontrar un sistema de generadores de $E(K)/E(K)_{tors}$?

Para consultar las versiones más accesibles de este teorema se puede consultar [10] (cap. III) ó [12] (cap. IV). También se puede ver [5] (I.2) y[17] (cap. VIII).

Observación 1.12. Si bien el problema de calcular el rango y hallar generadores es díficil, el problema de encontrar todos los puntos de torsión es sencillo. Se tiene el siguiente resultado, cuya demostración se puede consultar en [10] (II.5).

Teorema 1.13 (Nagell-Lutz). *Sea E una curva elíptica con coeficientes enteros de la forma*

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

y sea D el discriminante del polinomio $f(x)$. Sea $P = (w, z)$ un punto de torsión. Entonces $w, z \in \mathbb{Z}$ y $z = 0$ (en cuyo caso tiene orden 2) ó $z^2 \mid D$. Por lo tanto hay un algoritmo eficiente para calcular la torsión.

1.5. Ejemplos

Los siguientes 3 ejemplos nos servirán a lo largo de la tesis, para ilustrar los distintos conceptos que vayamos aplicando. Los datos de las curvas elípticas son extraídos de las tablas de Cremona, que se pueden consultar online en [3].

A **Curva 11a1.**

$E : y^2 + y = x^3 - x^2 - 10x - 20$,

Discriminante $= \Delta = -11^5$,

j-invariante $= j = \frac{-122023936}{161051}$,

Rango $= r = 0$,

Cantidad de puntos de torsión $= t = 5$.

B **Curva 37a1.**

$E : y^2 + y = x^3 - x$,

Discriminante $= \Delta = 37$,

j-invariante $= j = \frac{110592}{37}$,

Rango $= r = 1$,

Cantidad de puntos de torsión $= t = 1$.

C **Curva 225a1.**

$E : y^2 + y = x^3 - 1$,

Discriminante $= \Delta = -3^3 5^2$,

j-invariante $= j = 0$,

Rango $= r = 1$,

Cantidad de puntos de torsión $= t = 1$.

2. L- series

2.1. Definiciones

Supongamos que $K = \mathbb{Q}$. Se sabe que para cada curva elíptica existe una ecuación de Weierstrass minimal, que cumple que todos sus coeficientes son enteros y ademas Δ es lo más chico posible entre todos las posibles ecuaciones con coeficientes enteros para esa curva. (Por ejemplo ver [12] (VIII.1) y [17] (VII.1)). Si p es un primo que no divide al discriminante, entonces la clase de isomorfismo de la curva reducida módulo p no depende de la elección de la ecuación minimal y uno puede definir N_p como la cantidad de puntos de la curva $E(\mathbb{F}_p)$. En este caso se dice que la curva tiene buena reducción en p. Un resultado muy importante de Hasse muestra que uno tiene un cierto control de estos números. Mas precisamente, si escribimos

$$N_p = p + 1 - a_p,$$

entonces

$$|a_p| \leq 2\sqrt{p}.$$

Este resultado se puede consultar en [12] (X.3) ó [17] (V.1).

Vamos a extender la defincón de los a_p para los primos de mala reducción módulo p. (que en este caso también se obtienen contando puntos módulo p, ver por ejemplo [12] (III.5)).

Tenemos 3 tipos:

1. Reducción aditiva: Esto ocurre si la curva reducida tiene una cúspide. Ponemos $a_p = 0$.

2. Reducción multiplicativa, caso split: La curva reducida tiene un nodo, y las pendientes de las rectas tangentes están definidas sobre $\mathbb{F}_p$. Ponemos $a_p = 1$.

3. Reducción multiplicativa, caso non-split: La curva reducida tiene un nodo pero las tangentes no están definidas sobre $\mathbb{F}_p$ pero si lo están sobre una extensión cuadrática de $\mathbb{F}_p$. Ponemos $a_p = -1$.

Otro número importante es el conductor N de la curva elíptica. Cumple que

- $ord_p(N) = 0$ si y sólo si p tiene buena reducción.
- $ord_p(N) = 1$ si y sólo si p tiene reducción multiplicativa .
- $ord_p(N) = 2$ si p tiene reducción aditiva y $p > 3$.

- Si $p = 2, 3$ y hay reducción aditiva hay un algoritmo de Tate que permite calcular este número.

Estamos en condiciones de definir la función L asociada a la curva elíptica en forma de producto de Euler de la siguiente forma:

$$L(E,s) = \prod_{p\nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - a_p p^{-s})^{-1} =: \sum a_n n^{-s}.$$

Esto nos define los a_n cuando n no es primo.

2.2. La conjetura de Birch y Swinnerton-Dyer

La conjetura de Birch y Swinnerton-Dyer (BSD) es una de las conjeturas abiertas más importantes en la teoría de números. Vamos a motivarla de la siguiente forma: Si el rango de la curva elíptica fuera grande, esto debería verse reflejado en el hecho que los números N_p sean más grandes que $p + 1$ en promedio. En cambio si los números fueran más chicos que $p + 1$ uno esperaría que el rango sea pequeño. Más precisamente se tiene la siguiente conjetura.

Conjetura 2.1. (BSD-versión 1): Existe una constante C_E que depende sólo de E tal que

$$\prod_{p<X} \frac{N_p}{p} \approx C_E(logX)^r,$$

donde $\approx$ significa que el cociente entre el miembro izquierdo y el derecho tiende a 1 cuando $X \longrightarrow \infty$ y r es el rango de la curva $E(\mathbb{Q})$.

Esto es un ejemplo del principio local-global en teoría de números, ya que a partir de información local (contar puntos módulo p) estamos obteniendo un resultado global como lo es el rango de la curva elíptica.

Tratemos de conectar esta conjetura con el objeto que definimos anteriormente, la L-serie asociada a la curva elíptica. Evaluando formalmente en $s = 1$ nos queda que

$$L(E,1) = \prod \frac{p}{N_p},$$

donde N_p es el cardinal de los puntos no singulares de $E(\mathbb{F}_p)$. De todos modos no podemos hacer esta cuenta pues el producto de Euler en principio converge en $Re(s) > \frac{3}{2}$. Para poder evaluar en $s = 1$ habría que tratar de extender analíticamente la función.

Conjetura 2.2. (Birch y Swinnerton-Dyer (BSD)) La función $L(E, s)$ se extiende a una función entera en todo $\mathbb{C}$ y se tiene que el rango de la curva elíptica es igual al orden de anulación de $L(E, s)$ en $s = 1$. En particular la curva tiene finitos puntos racionales si y sólo si $L(E, 1) \neq 0$.

En vista de responder esta conjetura nombramos estos dos resultados que son cruciales en intentar entender y demostrar la conjetura BSD. El primer resultado importante es debido a Taylor-Wiles, en su famoso trabajo que termina de resolver el último teorema de Fermat.

Teorema 2.3. *(Taylor-Wiles): $L(E, s)$ se extiende de forma entera a todo $\mathbb{C}$ y satisface la ecuación funcional*

$$\Lambda(E, s) = \text{signo}(E)\Lambda(E, 2 - s),$$

donde signo$(E) = \pm 1$*, se llama el* signo *de E,*

$$\Lambda(E, s) = (2\pi)^{-s}\Gamma(s)N^{s/2}L(E, s),$$

y

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt.$$

El siguiente resultado, clave en éste trabajo, trata de responder la conjetura BDS, al menos para un caso particular. Más sobre esté teorema será tratado en este trabajo más adelante.

Teorema 2.4. *(Gross,Zagier,Kolyvagin): Sea E una curva elíptica sobre $\mathbb{Q}$. Si*

$$ord_{s=1}L(E, s) \leq 1,$$

entonces el rango de E coincide con $ord_{s=1}L(E, s)$ y hay un método eficiente para calcular los puntos racionales de la curva.

2.3. Twists cuadráticos

Sea $E : y^2 = x^3 + ax^2 + bx + c = f(x)$ una curva elíptica sobre $\mathbb{Q}$. Sea D un entero, definimos el twist E^D como la curva elíptica dada por la ecuación

$$Dy^2 = x^3 + ax^2 + bx + c,$$

que puede ser llevada mediante un cambio de coordenadas a la ecuacíon en forma de Weierstrass

$$y^2 = x^3 + Dax^2 + D^2bx + D^3c.$$

Básicamente el twist cuadrático es una curva que es isomorfa a la original sobre el cuerpo $\mathbb{Q}(\sqrt{D})$. Se puede dar una fórmula para el twist cuadrático de la ecuación de Weierstass más general o proceder como el método que se mostrará más adelante en la sección de ejemplos.

Sea ahora K un cuerpo cuadrático de discriminante D. Definimos el twist de la curva elíptica E por K como el twist por el discriminante D del cuerpo K (un tal D se llama discriminante fundamental). Más precisamente tenemos que si $K = \mathbb{Q}[\sqrt{d}]$ (con d libre de cuadrados) entonces los discriminantes fundamentales son:

- $D = d$ si $d \equiv 1$ mód 4
- $D = 4d$ si $d \equiv 2, 3$ mód 4

Sea K un cuerpo cuadrático de discriminante D. Sea v un ideal y sea $|v|$ su norma. Si $E/\mathbb{Q}$ es una curva elíptica de conductor N, podemos pensarla que está definida sobre K y definir

$$L(E/K, s) = \prod_v L_v(E/K, s)$$

donde los factores locales vienen dados por

$$L_v(E/K, s) = (1 - a_{|v|}|v|^{-s} + |v|^{1-2s})^{-1}$$

si $v \nmid N$ y

$$L_v(E/K, s) = (1 - a_{|v|}|v|^{-s})^{-1}$$

si $v \mid N$.

Esta fórmula es la análoga a la que definimos antes para una curva elíptica sobre $\mathbb{Q}$.

Proposición 2.5. *Si K es un cuerpo cuadrático tenemos la siguiente fórmula:*

$$L(E/K, s) = L(E, s)L(E^D, s)$$

donde E^D es el twist cuadrático de E sobre K.

Demostración. Tenemos las siguientes ecuaciones de las curvas, como en la introducción previa a esta proposición:

$$E : y^2 = x^3 + ax^2 + bx + c = f(x),$$

$$E^D : Dy^2 = x^3 + ax^2 + bx + c.$$

Llamemos a_p a los números que nos sirven para formas las L -series como antes, y llamemos b_p a los correspondientes números para E^D.

Sea $p \nmid DN$, entonces ambas curvas tienen buena reducción en p, por lo tanto para calcular a_p y b_p vamos a contar la cantidad de soluciones de las curvas módulo p, digamos que E tiene N_p puntos y que su twist cuadrático tiene M_p puntos. Veamos dos casos

- p se parte como producto de dos primos en K, ie $\left(\frac{D}{p}\right) = 1$ (D es un cuadrado módulo p):

  En ese caso fijado un valor de x existe una solución módulo p en un caso si y sólo si existe en el otro, ya que lo que necesitamos en ambos casos es que $f(x)$ sea un cuadrado o que sea D por un cuadrado; al ser D un cuadrado no nulo módulo p éstas nociones son equivalentes. Luego tenemos $a_p = b_p$. Pero si nos fijamos el primo p se parte como producto de dos primos y por la definición dada arriba cada uno de estos primos contribuye a L-serie asociada a la curva mirada con coeficientes en K con un factor igual al correspondiente que contribuyen el factor local de E ó E^D en p. (observar que como se parte $|p| = p$).

- p es inerte (o sea sigue siendo primo) en K, ie $\left(\frac{D}{p}\right) = -1$ (D no es un cuadrado módulo p):

  En ese caso observemos que cada ecuación tiene por un lado un punto en el infinito. Por otro lado, si fijo un valor x_0 entonces tenemos tres posibilidades

  1. $f(x_0) = 0$ mód p. Entonces cada ecuación tiene un único valor de y que funciona. En conjunto forman dos soluciones.
  2. $f(x_0) \neq 0$ mód p. En ese caso exactamente una de las dos ecuaciones tiene dos soluciones módulo p (si $f(x)$ es un cuadrado será la primera, en caso contrario será la segunda).

Entonces como x puede tomar p valores tenemos que

$$N_p + M_p = 1 + 1 + p + p.$$

Recordando que

$$a_p = p + 1 - N_p, b_p = p + 1 - M_p,$$

concluimos que

$$a_p + b_p = 0.$$

Cuando multiplicamos los inversos de los correspondientes factores locales obtenemos (usando la relación expuesta arriba)

$$(1 - a_p p^{-s} + p^{1-2s})(1 - b_p p^{-s} + p^{1-2s}) = 1 + 2p^{1-2s} + p^{2-4s} + (a_p)(b_p)p^{-2s}.$$

Ahora recordando la definición de la L-serie asociada a la curva mirada sobre K, y como en este caso $|p| = p^2$, tenemos que el inverso del factor local es

$$1 - a_{p^2} p^{-2s} + p^{2-4s}.$$

Por último recordando que podemos calcular a_{p^2} en términos de a_p como

$$a_{p^2} = {a_p}^2 - 2p,$$

se ve que las dos expresiones que queremos resultan iguales.

Ahora si $p \mid ND$ se puede chequear, con un poco más de cuidado, que también vale la igualdad que queremos. □

2.4. Ejemplos

A Como el discriminante es solamente divisible por el primo 11, el resto de los primos no contribuyen al conductor. Veamos que tipo de reducción tiene la curva módulo 11 para poder calcular el conductor. Mirando la ecuación vemos que el punto $(3, 5)$ es el único punto singular de la curva reducida. Haciendo el desarrollo de Taylor para la parte de y alrededor de 5 y alrededor de 3 para la parte de x obtenemos la ecuación

$$(y-5)^2 = (x-3)^3 + 8(x-3)^2,$$

que corresponde claramente a un nodo. Por lo tanto la curva tiene reducción multiplicativa, y como 8 no es un cuadrado módulo 11 la reducción es del tipo non-split (luego $a_{11} = -1$). Por lo visto recién concluímos que el conductor de la curva es 11.

Ahora calculemos, por ejemplo el a_5. Para ello contamos la cantidad de puntos de la curva módulo 5 (ya que la curva tiene reducción buena). Vemos que tenemos 8 soluciones, más el punto del infinito, por lo tanto $N_5 = 9$ y $a_5 = 5 + 1 - 9 = -3$. Observar que $3 = |a_5| \leq 2\sqrt{5}$ verificando la cota de Hasse en este ejemplo.

Para terminar el ejemplo calculemos el twist cuadrático de la curva por el cuerpo cuadrático $\mathbb{Q}(\sqrt{-7})$ cuyo discriminante es -7. El problema es que esta curva no está en la forma que supusimos para definir el twist cuadrático en la sección 2,3. Lo que vamos a hacer es mediante un cambio de coordenadas llevarla a la forma deseada y luego twistearla. Ahora nos aparece el problema de que la ecuación no es minimal, más precisamente no es minimal en el primo 2. Pero si desahcemos el cambio de variables que hicimos si obtenemos una ecuación minimal. Veamos como hacer esto para este caso:

Multiplicamos la ecuación por 2^6 y realizamos el cambio de coordenadas $y' = 8y + 4$, $x' = 4x$ y obtenemos la ecuación

$$y'^2 = x'^3 - 4x'^2 - 160x' - 1264.$$

Ahora twisteamos por -7 y llevándola a un ecuación de Weierstrass obtenemos la ecuación

$$y''^2 = x''^3 - 4(-7)x''^2 - 160(-7^2)x'' + -1264(-7^3).$$

Poniendo ahora (deshaciendo el cambio de variables del principio)

$$y = \frac{y'' - 4}{8}, x = \frac{x''}{4},$$

y dividiendo todo por 2^6 btenemos la ecuación

$$y^2 + y = x^3 + 7x^2 - 490x + 6744.$$

Esta ecuación es un modelo minimal de la curva, mediante el cambio de variables $x \longrightarrow x-2$ obtenemos otra ecuación en modelo minimal que corresponde a la curva $539d2$ de acuerdo a las tablas de Cremona. Esta curva tiene conductor $539 = 7^2 11$ y rango 1.

B Como en el caso anterior, es fácil ver que la curva tiene conductor 37. Podemos calcular el twist de la curva por -3 y obtenemos, del mismo modo que antes, la curva $33d1$ de rango 0.

C El discriminante de esta curva es divisible sólo por los primos 3 y 5. En el primo 5 uno chequea que el punto singular módulo 5 es el $(0, 2)$ y la ecuación se puede reescribir módulo 5 como

$$(y-2)^2 = x^3,$$

Por lo que claramente hay una cúspide. Eso implica que la potencia de 5 que aparece en el conductor es 2 y que $a_5 = 0$. Por último uno puede chequear que 3 tiene reducción aditiva también y para calcular cuanto aporta al conductor hay que usar el algoritmo de Tate. El conductor es $225 = 3^2 5^2$.

Si twisteamos a la curva por -11 obtenemos la curva 27225b1, de rango 0.

3. Formas Modulares

3.1. Generalidades

Sea $\mathcal{H}$ el semiplano complejo superior (o semiplano de Poincaré). El grupo $\mathrm{SL}_2(\mathbb{R})$ actúa en él de la forma

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

Sea Γ un subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ de índice finito. Decimos que una función

$$f : \mathcal{H} \longrightarrow \mathbb{C}$$

holomorfa es una forma modular de peso k para Γ si cumple:

1. $f(\gamma\tau) = (c\tau + d)^k f(\tau)$, para toda $\gamma \in \Gamma$.
2. Para toda $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ existe un número natural h tal que la función

   $$f\mid_\gamma(\tau) =: (c\tau + d)^{-k} f(\gamma\tau)$$

   admite una expansión de Fourier de la forma

   $$\sum_{n=0}^{\infty} a_n^\gamma q^{n/h}$$

   con $q = e^{2\pi i\tau}$.

El entero h se llama el ancho de la cúspide $\gamma^{-1}\infty = \frac{-d}{c}$ y la expresión $\sum_{n=0}^{\infty} a_n^\gamma q^{n/h}$ sólo depende de $\gamma^{-1}\infty = \frac{-d}{c}$ salvo multiplicar a $q^{1/h}$ por una raiz h-ésima de la unidad y se llama la expansión de Fourier de f en la cúspide $\frac{-d}{c}$

Una forma modular que satisface que $a_0^\gamma = 0$ para todo γ se llama una forma cuspidal, y al espacio vectorial de todas las formas cuspidales de peso k para Γ lo denotamos $S_k(\Gamma)$. Este espacio resulta de dimensión finita como $\mathbb{C}$- espacio vectorial.

En nuestro caso particular estamos interesados en el caso $k = 2$ y

$$\Gamma = \Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \text{ mód } (N) \right\}.$$

Esto resulta un órden en el algebra $M_2(\mathbb{R})$ y se llama el orden de Eichler o subgrupo de congruencia de Hecke de nivel N y al espacio de las formas cuspidales para tal grupo lo dentoamos $S_2(N)$. El cociente $\mathcal{H}/\Gamma_0(N)$ hereda una estructura

de superficie de Riemann. Si $N \geq 3$ resulta útil compactificarlo agregándole finitas cúspides, que se corresponden con las $\Gamma_0(N)$-órbitas de $\mathbb{P}^1(\mathbb{Q})$. Uno le puede dar una estrctura topológica y compleja. Para referencias consultar [6] (cap. 2).

Sea $X_0(N)$ la curva algebraica proyectiva sobre $\mathbb{C}$ que corresponde a la superficie de Riemann. La asignación que a cada $f \in S_2(N)$ le asigna

$$\omega_f = 2\pi i f(\tau) d\tau,$$

identifica a $S_2(N)$ con el espacio de formas diferenciales en $X_0(N)(\mathbb{C})$. Por el teorema de Riemann-Roch este espacio resulta de dimensión finita de dimensión igual al género de $X_0(N)$, y por lo tanto se pueden hallar fórmulas explícitas para calcular su dimensión. Esto se puede ver por ejemplo en [6] (III.5) o de una forma más elemental en [12] (IX.5) y [16] (VII.3).

3.2. Operadores de Hecke

El espacio vectorial $S_2(N)$ tiene un producto interno Hermitiano no degenerado, conocido como el producto de Petersson dado por

$$\langle f_1, f_2 \rangle = \int_{\mathcal{H}/\Gamma_0(N)} f_1(\tau) f_2(\bar{\tau}) dx dy.$$

Posee además una acción de ciertos operadores, llamados operadores de Hecke T_p indexados en los primos p, definidos de la siguiente forma:

$$T_p f := T_p(f) = \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{\tau + i}{p}\right) + \begin{cases} pf(p\tau) & \text{si } p \nmid N, \\ 0 & \text{si } p \mid N. \end{cases}$$

Estos operadores actúan linealmente en $S_2(N)$. Su acción en términos de las q-expansiones de Fourier es la siguiente:

$$T_p(f) = \sum_{p|n} a_n q^{n/p} + \begin{cases} p \sum a_n q^{pn} & \text{si } p \nmid N, \\ 0 & \text{si } p \mid N. \end{cases}$$

Mirando la acción en las expansiones de Fourier es inmediato verificar que los operadores de Hecke conmutan unos con otros.

Extendemos la definición de los operadores de Hecke a todos los enteros positivos igualando los coeficientes en n^{-s} en la siguiente igualdad formal de las L-series de Dirichlet

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p \nmid N} (1 - T_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N} (1 - T_p p^{-s})^{-1}.$$

Para otras definiciones de los operadores de Hecke se pueden consultar [15] (II.8) , [6] (V.2 y V.3) , [12] (IX. 6) y [16](VII. 5).

Sea $\mathbb{T}$ la subálgebra conmutativa de $End_{\mathbb{C}}(S_2(N))$ generada sobre $\mathbb{Z}$ por los operadores de Hecke T_n y sea $\mathbb{T}^0$ la generada por los operadores T_n con $(n : N) = 1$. Tenemos el siguiente resultado

Teorema 3.1. *Las álgebras de Hecke $\mathbb{T}$ y $\mathbb{T}^0$ son finitamente generadas como $\mathbb{Z}$ módulos y el rango de $\mathbb{T}$ es $g = dim_{\mathbb{C}}(S_2(N)) =$ género $X_0(N)$.*

Teorema 3.2. *$S_2(N)$ tiene una base de formas modulares con coeficientes enteros.*

Para estos resultados se puede consultar [6] (VI.5).

3.3. Formas nuevas y teoría de Atkin-Lehner

Lema 3.3. *Si T está en $\mathbb{T}^0$ entonces es autoadjunta respecto al producto de Petersson.*

Por el lema anterior más el teorema de descomposición para operadores autoadjuntos tenemos que

$$S_2(N) = \oplus_\lambda S^0_\lambda,$$

donde la suma se toma sobre todos los morfismos de $\mathbb{C}$-álgebras $\lambda : \mathbb{T}^0 \longrightarrow \mathbb{C}$, y S^0_λ es el autoespacio correspondiente en $S_2(N)$. (o sea $T_n f = \lambda(T_n) f$). Los autoespacios no son necesariamente 1-dimensionales. En cambio si ahora miramos $\lambda : \mathbb{T} \longrightarrow \mathbb{C}$ y denotamos S_λ al correspondiente autoespacio se tiene lo siguiente:

Lema 3.4. *(Multiplicidad uno) El autoespacio S_λ tiene dimensión* 1.

Demostración. Esto es por que los coeficientes de Fourier quedan determinados por $a_1(f)$ por la fórmula $a_n(f) = a_1(f)\lambda(T_n)$.

□

El problema de mirar todo el álgebra de Hecke es que, a pesar de que los autoespacios son de dimensión 1, no actúa de forma semisimple en $S_2(N)$. Sin embargo tiene un subespacio distinguido, que llamaremos el espacio de las formas nuevas que se descompone en suma directa de autoespacios de dimensión 1 para las acciones de tanto $\mathbb{T}$ como $\mathbb{T}^0$. Una forma modular en $S_2(N)$ se dice vieja si es una combinación lineal de funciones de la forma $f(d'z)$ con $f \in S_2(N/d)$ y $d' \mid d$ con $d > 1$. Al subespacio de las formas viejas lo denotamos $S_2^{old}(N)$ y el espacio de formas nuevas, o el subespacio nuevo $S_2^{new}(N)$ será el complemento ortogonal del espacio de las formas viejas respecto del producto de Petersson.

Teorema 3.5. *(Atkin-Lehner) Sea $f \in S_2^{new}(N)$ una autofunción simultánea para todo el álgebra $\mathbb{T}^0$. Sea S un conjunto finito de primos y $g \in S_2(N)$ una autofunción para todos los T_p con $p \notin S$.Si $a_p(f) = a_p(g)$ para todo $p \notin S$ entonces $g = \lambda f$ para algún $\lambda \in \mathbb{C}$.*

Para la demostración ver [21].

Corolario 3.6. *El álgebra $\mathbb{T}$ actúa de forma semisimple en $S_2^{new}(N)$ con autoespacios de dimensión 1. Entonces tenemos una descomposición ortogonal de la forma*

$$S_2(N) = S_2^{old}(N) \oplus_\lambda \mathbb{C} f_\lambda,$$

donde la suma se toma sobre todos los morfismos de $\mathbb{C}$- álgebras $\lambda : \mathbb{T} \longrightarrow \mathbb{C}$ correspondientes a los autovectores en $S_2^{new}(N)$ y $f_\lambda(\tau) = \sum_{n=1}^{\infty} \lambda(T_n) e^{2\pi i n \tau}$.

Un autovector simultáneo se llama una autofunción normalizada o una forma nueva de nivel N. Notar que cumple que $a_1(f) = 1$.

3.4. L-series asociadas a formas modulares

A una forma nueva de nivel N le podemos asignar una L-serie de la forma

$$L(f, s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

donde $a_n := a_n(f) = \lambda(T_n)$. Este función L tiene las siguientes propiedades:

1. Producto de Euler:

$$L(f, s) = \prod_{p|N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N} (1 - a_p p^{-s})^{-1}.$$

2. Representación Integral:

$$\Lambda(f, s) := (2\pi)^{-s} \Gamma(s) N^{s/2} L(f, s) = N^{s/2} \int_0^{\infty} f(it) t^{s-1} dt,$$

donde

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt.$$

3. Ecuación Funcional: En $S_2^{new}(N)$ hay una involución (llamada involución de Atkin-Lehner) ω_N definida por

$$\omega_N(f)(\tau) = \frac{-1}{N\tau^2} f\left(\frac{-1}{N\tau}\right).$$

Esta involución conmuta con los operadores de Hecke en $\mathbb{T}^0$ y por lo tanto preserva los autoespacios S_λ. Luego para cada forma nueva de nivel N se tiene que $\omega_N(f) = \epsilon f$ con $\epsilon = 1$ ó -1. Se puede ver que la ecuación funcional que satisface $L(f,s)$ es

$$\Lambda(f,s) = -\Lambda(\omega_N(f), 2-s) = -\epsilon\Lambda(f, 2-s).$$

3.5. Espacios de modulii y teoría de Eichler-Shimura

Sea $Y_0(N) = \mathcal{H}/\Gamma_0(N)$ la curva modular abierta sobre $\mathbb{Q}$. Vamos a darle una interpretación de espacio de modulii, más precisamente queremos que los puntos de la curva clasifiquen clases de isomorfismos de objetos geométricos.

Más precisamente $Y_0(N)$ clasifica pares de curvas elípticas (E, E') (módulo isomorfismo) con una isogenía cíclica $E \to E'$ de grado N. Esto es lo mismo que un par (E, C) donde E es una curva elíptica y C es un subgrupo cíclico de orden N en E (que se corresponde con el núcleo de la isogenía anterior).

Para ver este isomorfismo, a cada punto $y = (E, E')$ la asociamos un par de toros (o sea $\mathbb{C}$ módulo un retículo) relacionados por una isogenía de grado N

$$\mathbb{C}/M \to \mathbb{C}/M'.$$

Cambiando a M por una homotecia podemos suponer que $M \subset M'$ y que la isogenía está inducida por la identidad en los revestimientos de los toros.

Como M'/M es cíclico de orden N tenemos que hay una base orientada $\{\omega_1, \omega_2\}$ de M tal que $\langle \omega_1, \omega_2/N\rangle = M'$ y $\tau = \frac{\omega_1}{\omega_2} \in \mathcal{H}$. Luego la $\Gamma_0(N)$ órbita del punto $y = (\mathbb{C}/M, \mathbb{C}/M')$ está bien definida.

Para ver que esto es suryectivo, a un punto $\tau \in \mathcal{H}/\Gamma_0(N)$ le asociamos los retículos $M = \langle 1, \tau\rangle$ y $M' = \langle 1, \tau/N\rangle$. Las curvas elípticas $E = \mathbb{C}/M$ y $E' = \mathbb{C}/M'$ están relacionadas por la isogenía de grado N obvia.

También podemos considerar la curva modular $X_0(N)$, que es la compactificación de la curva modular abierta, que ahora clasifica pares de curvas elípticas generalizadas N-isógenas. Los puntos complejos de la curva modular se pueden identificar con el cociente $\mathcal{H}^*/\Gamma_0(N)$, donde $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. Los finitos puntos de $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$ se llaman las cúspides de la curva modular.

Este punto de vista nos permitirá entender varias construcciones a lo largo de la tesis.

Otro elemento importante es la ecuación modular, que es un modelo (singular) de la curva $X_0(N)$ sobre $\mathbb{Q}$. Para esto veamos que podemos definir la función

$$j : \mathcal{H} \longrightarrow \mathbb{C},$$

tal que

$$j(\tau) =: j(\mathbb{C}/\langle 1, \tau \rangle).$$

Observación 3.7. Notar que esto nos permite definir para cualquier retículo $\Lambda \subset \mathbb{C}$ la función $j(\Lambda) =: j(\mathbb{C}/\Lambda)$. Esto será usado más adelante para el caso donde Λ sea un ideal en un cuerpo cuadrático imaginario, que es fácil ver que en particular es un retículo.

Las funciones $j(\tau)$ y $j(N\tau)$ están relacionadas por una ecuación $f_N(x, y) = 0$ con coeficientes racionales que nos da un modelo de la curva. Para los detalles de construcción y las propiedad más importantes de la ecuación modular una excelente referencia es [2] (III.11.C).

Teorema 3.8 (Eichler- Shimura)**.** *Sea f una autofunción normalizada con coeficientes de Fourier enteros. Entonces existe una curva elíptica E_f sobre $\mathbb{Q}$ tal que*

$$L(f, s) = L(E_f, s).$$

Demostración. (idea):

En el modelo dado por la ecuación modular si $\tau \in \mathcal{H}/\Gamma_0(N)$ corresponde a un punto en $X_0(N)(F)$ con F un subcuerpo de $\mathbb{C}$ entonces

$$(j(\tau), j(N\tau)) \in F^2.$$

Los operadores de Hecke que actúan en $S_2(N)$ surgen geométricamente de ciertas correspondencias en $X_0(N) \times X_0(N)$. El problema es que un operador de Hecke le asocia a un punto en $X_0(N)$ varios puntos de la misma curva, con lo cual no es una función. A uno le gustaría "sumar" estos puntos, pero la curva $X_0(N)$ no posee ley de grupo y es por esto que aparece la noción de correspondencia. Estas correspondencias (denotadas por abuso de notación como T_p) están dadas por los puntos en $X_0(N) \times X_0(N)$ asociados a pares relacionados por una p-isogenía cíclica (una p isogenía cíclica que es un isomorfismo entre las estructuras de nivel N). Sea $J_0(N)$ la Jacobiana de $X_0(N)$ que es una variedad abeliana de dimensión $g = dim_{\mathbb{C}}(S_2(N)) = \text{género} X_0(N)$ definida sobre $\mathbb{Q}$. Las correspondencias dan lugar a endomorfismos de la Jacobiana

definidos sobre $\mathbb{Q}$ (porque $J_0(N)$ si tiene una estructura de grupo abeliano). Sea I_f el núcleo del morfismo $\lambda : \mathbb{T} \longrightarrow \mathbb{Z}$ asociado a f. Luego el cociente $J_0(N)/I_f J_0(N)$ es la curva elíptica deseada E_f.

La clave para mostrar la igualdad de las L-series es relacionar el coeficiente $a_p(E)$ que se obtiene contando puntos de la curva en $\mathbb{F}_p$ (o mejor aún como la traza del Frobenius en p actuando en los puntos de torsión de orden potencia de p) con el autovalor del operador de Hecke T_p. Esto se hace usando las relaciones de congruencia de Eichler-Shimura en característica p. Por ejemplo si $p \nmid N$ entonces la curva $X_0(N)$ tiene un modelo entero con buena reducción módulo p y uno tiene

$$T_p = F + F^t$$

en $X_0(N)_{\mathbb{F}_p}$, donde F es el gráfico del frobenius y F^t su transpuesta. Para más detalles de esta construcción se puede consultar [6] (VIII.7 y VIII.8) y [12] (X.11).

Resultados de Deligne y Carayol ([1]) muestran que el conductor de la curva elíptica E_f coincide con el nivel N de la forma modular nueva f.

□

La curva $X_0(N)$ se puede embeber en su jacobiana mandando un punto P a la clase del divisor de grado cero $(P)-(i\infty)$. Sea $\Phi_N : X_0(N) \longrightarrow E_f$ la parametrización modular que se obtiene componiendo el embedding de antes con la proyección que nos da Eichler-Shimura. El pullback $\Phi_N^*(\omega)$ del diferencial correspondiente a E_f es un múltiplo distinto de cero de ω_f i.e.

$$\Phi_N^*(\omega) = c2\pi i f(\tau)d\tau. \tag{1}$$

La constante c se llama constante de Manin y (conjeturalmente) se espera que sea siempre 1.

Para propósitos computacionales la siguiente descripción de la parametrización modular es bastante útil pues nos da un algoritmo para calcular explícitamente la parametrización modular.

Proposición 3.9. *Sea Λ_{E_f} el retículo asociado a E_f y sea c la constante de Manin de E_f. Sea $\Phi_w : \mathbb{C}/\Lambda_{E_f} \longrightarrow E_f(\mathbb{C})$. Entonces $\Phi_N(\tau) = \Phi_w(z_\tau)$ donde $z_\tau = c\int_{i\infty}^{\tau} 2\pi i f(z)dz = c\sum_{n=1}^{\infty} \frac{a_n}{n} q^n$ con $q = e^{2\pi i \tau}$.*

Demostración. Por la definción del mapa de Abel-Jacobi y la proyección $J_0(N) \longrightarrow E_f$ se tiene que la imagen del divisor $(\tau) - (i\infty)$ es

$$\Phi_w\left(\int_{\Phi_N(i\infty)}^{\Phi_N(\tau)} \omega\right) = \Phi_w\left(\int_{i\infty}^{\tau} \Phi_N^*(\omega)\right)$$

por la fórmula de cambio de variables y por (1) obtenemos el resultado. □

3.6. Teorema de Wiles

Teorema 3.10. *(Wiles et al) Sea E una curva elíptica sobre $\mathbb{Q}$ de conductor N. Luego existe una forma nueva $f \in S_2(N)$ tal que $L(f,s) = L(E,s)$ y además E es isógena a la curva E_f obtenida mediante f por la construcción de Eichler-Shimura*

Nota 3.11. Wiles de manera conjunta con Taylor demostraron este teorema para curvas semiestables (es decir con buena reducción o reducción multiplicativa en todos los primos). Luego Breuil-Conrad-Diamond-Taylor generalizaron los resultados a todas las curvas elípticas.

Corolario 3.12. *La función $L(E,s)$ tiene una continuación analítica a todo el plano complejo y una representación integral de la forma*

$$\Lambda(f,s) := (2\pi)^{-s}\Gamma(s)L(f,s) = \int_0^\infty f(it)t^{s-1}dt,$$

para alguna forma modular en $S_2(N)$ con lo cual satisface una ecuación funcional como en (teorema 2.3).

Recordar que $-\epsilon$ es el signo de la ecuacíon funcional asociada a una forma nueva. Si una curva elíptica tiene asociada una tal f definimos signo$(E) = -\epsilon$. Observar que $L(E,s)$ se anula con orden par (respectivamente impar) en $s = 1$ si signo$(E) = 1$ (respectivamente signo$(E) = -1$).

Por último como corolario también obtuvimos la uniformización compleja

$$\Phi_N : \mathcal{H}^*/\Gamma_0(N) \longrightarrow E(\mathbb{C}),$$

que se obtiene componiendo la aplicación que ya teníamos con la isogenía racional entre E_f y E. Esta uniformización va a jugar un papel crucial en la sección siguiente ya que nos va a permitir calcular computacionalmente cierto puntos algebraicos en curvas elípticas.

4. Puntos de Heegner

4.1. Multiplicación Compleja

Recordemos que podemos pensar a una curva elíptica sobre $\mathbb{C}$ de la forma $\mathbb{C}/\Lambda$, y con esta identificación el anillo de endomorfismos de la curva elíptica se asocia con $\{\alpha \in \mathbb{C}/\alpha\Lambda \subseteq \Lambda\}$. Este anillo es o bien $\mathbb{Z}$ o un orden $\mathcal{O}$ en un cuerpo cuadrático imaginario. Cuando el anillo de endomorfismos es más grande que los enteros, es decir es un orden $\mathcal{O}$ en un cuerpo cuadrático imaginario, decimos que la curva elíptica tiene multiplicación compleja por $\mathcal{O}$. Definamos el grupo de clases (o grupo de Picard) del orden $\mathcal{O}$ como el cociente entre los $\mathcal{O}$-ideales fraccionales inversibles (o propios) módulo los $\mathcal{O}$-ideales fraccionales inversibles principales. Lo notamos $Pic(\mathcal{O})$.

Es fácil ver que dos retículos (en $\mathbb{C}$) son homotéticos si y sólo si tienen el mismo j- invariante, luego se obtiene de manera muy sencilla una biyección entre $Pic(\mathcal{O})$ y clases de homotecias de retículos con anillo de multiplicación $\mathcal{O}$ y esto es lo mismo que curvas elípticas con multiplicación compleja por $\mathcal{O}$ módulo isomorfismos. A priori estas curvas elípticas están definidas sobre los complejos, pero en realidad están definidas sobre una extensión finita de $\mathbb{Q}$. Mas aún,

Teorema 4.1 (Multiplicación Compleja)**.** *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático imaginario K y sea $\mathfrak{a}$ un $\mathcal{O}$-ideal propio. Entonces $j(\mathfrak{a})$ es un entero algebraico y $K(j(\mathfrak{a}))$ es el cuerpo de clases de $\mathcal{O}$. Además para todo $\mathfrak{s}$ ideal propio de $\mathcal{O}_K$ cuyo símbolo de Artin es σ tenemos que $\sigma(j(\mathfrak{a})) = j((\mathfrak{s}^{-1} \cap \mathcal{O})\mathfrak{a})$.*

Para explicar un poco este teorema vamos a recordar un par de conceptos. Las definiciones que siguen y la demostración de la primer parte del teorema se puede consultar en [2](XI) . Otra referencia, en donde tambíen se demuestra la segunda parte del teorema es [11] (IV). Esta demostración es más bien analítica. Una demostración más algebraica se puede consultar en [18](II).

Dado un cuerpo de números K, un módulo en K es un producto formal

$$m = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}},$$

donde vale que

- $n_{\mathfrak{p}} \geq 0$ y a lo sumo finitos son distintos de cero.
- $n_{\mathfrak{p}} = 0$ si $\mathfrak{p}$ es un primo infinito complejo (i.e una inmersión de K que no es real).

- $n_{\mathfrak{p}} \leq 1$ si $\mathfrak{p}$ es un primo infinito real (i.e una inmersión real de K).

El módulo m se puede escribir de la forma $m_0 m_\infty$, donde m_0 es un $\mathcal{O}_K$ ideal y m_∞ es el producto de distintos primos del infinito reales. En nuestro caso de interés, que es cuando K es un cuerpo cuadrático imaginario, no aparece la parte del infinito. Dado un módulo m podemos considerar $I_K(m)$ como el grupo de $\mathcal{O}_K$ ideales fraccionarios de norma coprima con m (i.e de norma coprima con m_0). Ahora consideremos $P_{K,1}(m)$ como el subgrupo de $I_K(m)$ generado por los ideales principales de la forma $\alpha\mathcal{O}_K$ con $\alpha \in \mathcal{O}_K$ tal que

- $\alpha \equiv 1$ mód m_0,
- $\sigma(\alpha) > 0$ para todo primo infinito real σ que divida a m_∞.

Vale que este subgrupo tiene índice finito en $I_K(m)$.

Decimos que un subgrupo H de $I_K(m)$ es un subgrupo de congruencia para el módulo m si cumple que $P_{K,1}(m) \subset H \subset I_K(m)$. En ese caso decimos que $I_K(m)/H$ es un *grupo de clases generalizado* para m.

Por ejemplo si $\mathcal{O}$ es un orden en un cuerpo cuadrático imaginario de conductor c, entonces tomando el subgrupo de congruencia $P_{K,\mathbb{Z}}(c)$ como el generado por los ideales principales $\alpha\mathcal{O}_K$ tales $\alpha \equiv a$ mód $c\mathcal{O}_K$ con a entero coprimo con c, se puede ver que $I_K(c)/P_{K,\mathbb{Z}}(c) \cong Pic(\mathcal{O})$.

Sea L/K una extensión abeliana de cuerpos de números (o sea Galois y con grupo de Galois abeliano). Sea m un módulo divisible por todos los primos que ramifican en la extensión L/K. Sabemos que para cada primo $\mathfrak{p}$ que no ramifica existe un único $\sigma \in Gal(L/K)$, llamado Frobenius, que verifica que

$$\sigma(\alpha) \equiv \alpha^{N\mathfrak{p}} \text{ mód } \mathfrak{B},$$

para todo $\alpha \in \mathcal{O}_L$ donde $\mathfrak{B}$ es cualquier primo de L arriba de $\mathfrak{p}$ (funciona cualquiera pues la extensión es abeliana). Para ver las definiciones y propiedades usadas se puede consultar [14], capítulos (3 y 4)

A esta aplicación se la llama símbolo de Artin, y se nota $\left(\frac{L/K}{\mathfrak{p}}\right) \in Gal(L/K)$. Extendiendo multiplicativamente se obtiene un morfismo, llamado mapa de Artin

$$\Phi_m : I_K(m) \longrightarrow Gal(L/K).$$

Se tienen los siguientes resultados, cuyas demostraciones se pueden ver en [9] capítulo V.

Teorema 4.2. *Sea $K \subset L$ una extensión abeliana. Existe un módulo $\mathfrak{f} = \mathfrak{f}(L/K)$ tal que*

1. *Un primo de K ramifica en L si y sólo si divide a $\mathfrak{f}$.*
2. *Sea m un módulo divisible por todos los primos de K que ramifican en L. Entonces $ker(\Phi_m)$ es un subgrupo de congruencia para m si y sólo si $\mathfrak{f} \mid m$.*

Un tal $\mathfrak{f}$ se llama el conductor de la extensión

Teorema 4.3. *Sea m un módulo para K y H un subgrupo de congruencia para m. Entonces existe una única extensión abeliana L de K tal que los primos que ramifican en L dividen a m y tal que $ker(\Phi_m) = H$.*

Además, como se puede ver que el mapa de artin es suryectivo se tiene

$$I_K(m)/H \cong Gal(L/K).$$

El caso que nos interesa principalmente es cuando $\mathcal{O}$ es un orden en un cuerpo cuadrático imaginario de conductor c. Tomando como antes el subgrupo de congruencia $P_{K,\mathbb{Z}}(c)$ se tiene que existe una extensión L/K abeliana (llamada el cuerpo de clases de $\mathcal{O}$) que cumple las propiedades del teorema anterior. En particular se tiene

$$Pic(\mathcal{O}) \cong Gal(L/K).$$

Cuando $c = 1$, o sea cuando $\mathcal{O} = \mathcal{O}_K$, la extensión que obtenemos se llama el cuerpo de clases de Hilbert y es la máxima extensión abeliana no ramificada de K.

Además por la descripción de los teoremas para el caso donde K es un cuerpo cuadrático imaginario obtenemos una familia de ordenes que van creciendo. Más precisamente para cada c natural tenemos el orden $\mathcal{O}_c$ de conductor c y tenemos que

$$\mathcal{O}_c \subset \mathcal{O}_{c'} \iff c \mid c'.$$

Por último, para la demostración del teorema como está explicada en [2] (Teorema 11.1, capítulo 11) juega un rol crucial la ecuación modular mencionada en el capítulo 3 de este trabajo. En dicho libro se deduce la ecuación y sus propiedades más importantes.

Para la demostración de la segunda parte del teorema que se puede consultar en [11] la clave es, en vez de estudiar las propiedades de la función j, es estudiar la función modular Δ y usando argumentos similares a los usados para la función j uno llega al resultado deseado.

4.2. Puntos de Heegner

Definición 4.4. Los **puntos de Heegner** son los puntos en $Y_0(N)$ que clasifican pares de curvas elípticas N isógenas y que tienen el mismo anillo de endomorfismos $\mathcal{O}$ módulo isomorfismos.

Si $y = (E, E')$ es un punto de Heegner con mutliplicación compleja por $\mathcal{O}$ entonces tiene asociado dos retículos que son $\mathcal{O}$-módulos proyectivos de rango 1. Cambiándolos por homotecias podemos asumir que $M = \mathfrak{a}$ y $M' = \mathfrak{b}$, con $\mathfrak{a}, \mathfrak{b}$ dos $\mathcal{O}$-submódulos inversibles de K con $\mathfrak{a} \subset \mathfrak{b}$. El ideal $\mathfrak{n} = \mathfrak{a}\mathfrak{b}^{-1}$, es un $\mathcal{O}$-ideal propio (inversible) de cociente cíclico $\mathcal{O}/\mathfrak{n}$ de orden N. Recíprocamente si un tal ideal existe, construimos puntos de Heegner con anillo de endomorfismos $\mathcal{O}$ como sigue:

Sea $\mathfrak{a}$ un $\mathcal{O}$-submódulo inversible y sea $[\mathfrak{a}]$ su clase en $Pic(\mathcal{O})$. Sea $\mathfrak{n}$ un ideal con cociente cíclico de orden N, y pongamos $E = \mathbb{C}/\mathfrak{a}$ y $E' = \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$. Estas curvas están relacionadas por la isogenía obvia cuyo núcleo es isomorfo a

$$\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}.$$

Entonces hemos encontrado un punto en la curva modular abierta. Como las curvas E y E' sólo dependen de la clase de $\mathfrak{a}$ en el grupo de Picard hemos probado:

Proposición 4.5. *Fijado el orden $\mathcal{O}$, y una vez elegido el ideal $\mathfrak{n}$, los puntos de Heegner con anillo de endomorfismos $\mathcal{O}$ están en correspondencia con $Pic(\mathcal{O})$.*

Luego recordando que hemos hecho una elección de tanto el orden como del ideal, podemos notar a un punto de Heegner y mediante una terna de la forma

$$y = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]).$$

Tenemos la siguiente proposición:

Proposición 4.6. *Sea $\mathcal{O}$ un orden de discriminante D y sea $N \in \mathbb{N}$. Las siguientes son equivalentes:*

1. *Existe un punto de Heegner en $X_0(N)$ con anillo de endomorfismos $\mathcal{O}$.*
2. *Existe un ideal $\mathfrak{n}$ de $\mathcal{O}$ de norma N y tal que $\mathcal{O}/\mathfrak{n}$ es cíclico.*
3. *Existen B, C enteros con $mcd(B, C, N) = 1$ tales que*

$$D = B^2 - 4NC.$$

Demostración. La equivalencia $1 \iff 2$ la probamos más arriba. La equivalencia $2 \iff 3$ es consecuencia de la teoría de formas cuadráticas binarias, y se puede consultar en [2] (VII.B). □

De ahora en más supongamos que $mcd(c, N) = 1$ donde c es el conductor del orden $\mathcal{O}$. Entonces la condición 3 de la proposición anterior (y por lo tanto todas) es equivalente al hecho de que D sea un cuadrado módulo $4N$. En efecto escribiendo $D = d.c^2$ donde d es el discriminante del cuerpo K, si D es un cuadrado módulo $4N$ entonces existen B, C tales que

$$D = B^2 - 4NC.$$

Si p es un primo que divide a $mcd(B, C, N)$ entonces como $(c, N) = 1$ se ve fácilmente que $p^2 \mid d$, y como d es un discriminante fundamental se sigue que $p = 2$. Pero en ese caso se tiene fácilmente que

$$D \equiv 8, 12 \text{ mód } 16,$$

mientras que

$$B^2 - 4NC \equiv 0, 4 \text{ mód } 16,$$

lo que es absurdo y termina de probar nuestra afirmación.

Hagamos una suposición más, que es que $mcd(d, N) = 1$. En ese caso tenemos que si $p \mid N$ entonces $\left(\frac{D}{p}\right) = 1$ y esto quiere decir que el ideal (p) se parte como producto de dos primos en el cuerpo cuadrático K.

Definición 4.7. Decimos que K satisface la **hipótesis de Heegner** respecto de N si $(d, N) = 1$ y D es un cuadrado módulo $4N$. Equivalentemente todo $p \mid N$ se parte en K.

4.3. Órdenes en álgebras de matrices

Sea $M_2(\mathbb{Z})$ el álgebra de matrices de 2×2. Dado un $\tau \in \mathcal{H}$ definimos el orden

$$\mathcal{O}_\tau = \{\gamma \in M_2(\mathbb{Z}) \mid det\gamma \neq 0, \gamma\tau = \tau\} \cup \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

Es claro que $\mathcal{O}_\tau$ es un orden, y este orden se puede ver como las matrices en $M_2(\mathbb{Z})$ que tienen a $\begin{pmatrix} \tau \\ 1 \end{pmatrix}$ y $\begin{pmatrix} \bar{\tau} \\ 1 \end{pmatrix}$ como autovectores (digamos con autovalores λ y $\bar{\lambda}$). Luego tenemos una aplicación (inyectiva) natural que a cada matriz en el orden le

asocia $\lambda\left(\text{el autovalor correspondiente al vector columna } \begin{pmatrix} \tau \\ 1 \end{pmatrix}\right)$. De esta descripción resulta evidente que $\mathcal{O}_\tau$ es un subanillo conmutativo de $M_2(\mathbb{Z})$.

Esto nos permite ver a $\mathcal{O}_\tau$ como un subanillo (discreto) de $\mathbb{C}$, y además se ve fácilmente que el orden es isomorfo al anillo de endomofismos de la curva elíptica $\mathbb{C}/\langle 1, \tau\rangle$.

Si $\mathcal{O}$ es un orden en un cuerpo cuadrático imaginario definimos

$$CM(\mathcal{O}) = \{\tau \in \mathcal{H}/\operatorname{SL}_2(\mathbb{Z}) : \mathcal{O}_\tau = \mathcal{O}\}.$$

Sea N un entero positivo fijo, y sea $M_0(N)$ el anillo de las matrices de 2×2 con coeficientes enteros que son triangulares superiores módulo N. El grupo de unidades de determinante 1 de este anillo es precisamente $\Gamma_0(N)$. Dado $\tau \in \mathcal{H}$ definimos el orden asociado (relativo al nivel N) como:

$$\mathcal{O}_\tau^{(N)} = \{\gamma \in M_0(N) : \gamma\tau = \tau\} \cup \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

Se ve fácilmente que $\mathcal{O}_\tau^{(N)} = \mathcal{O}_\tau \cap \mathcal{O}_{N\tau}$ (pensados como subanillos de $\mathbb{C}$). Tenemos el siguiente teorema, clave para nuestro interés:

Teorema 4.8. *Sea $\tau \in \mathcal{H} \cap K$ y sea $\mathcal{O} = \mathcal{O}_\tau^{(N)}$ su orden asociado en $M_0(N)$ y sea H/K el cuerpo de clases asociado a ese orden. Entonces $\Phi_N(\tau) \in E(H)$.*

Demostración. Sabemos por el teorema anterior que tanto $j(\tau)$ y $j(N\tau)$ pertenecen al cuerpo de clases H asociado a $\mathcal{O}_\tau \cap \mathcal{O}_{N\tau}$ (la correspondencia entre ordenes y extensiones revierte las inclusiones). Luego $\Phi_N(\tau)$ es la imagen de un punto de $X_0(N)(H)$ (con coordenadas $(j(\tau), j(N\tau))$ dadas por el modelo de la curva modular dado por el polinomio modular de orden N). Pero entonces $\Phi_N(\tau) \in E(H)$ porque la función $X_0(N) \to E$ inducida por Φ_N es una función entre curvas algebraicas definidas sobre $\mathbb{Q}$. □

Podemos definir como antes

$$CM_N(\mathcal{O}) = \{\tau \in \mathcal{H}/\Gamma_0(N) \text{ tal que } \mathcal{O}_\tau^{(N)} = \mathcal{O}\}.$$

Proposición 4.9. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático K que satisface la hipótesis de Heegner respecto de N. Entonces existe un punto de Heegner cuyo orden asociado $\mathcal{O}^{(N)}$ es igual a $\mathcal{O}$.*

Demostración. Supongamos que

$$\mathcal{O} = \langle 1, \omega \rangle .$$

Como en un orden siempre tenemos a la matriz identidad, bastará encontrar una matriz que se comporte como ω, más precisamente una matriz $M \in M_0(N)$ que cumpla que

$$M^2 - \text{Traza}(\omega)M + \text{Norma}(\omega) = 0$$

y esto es claramente equivalente a encontrar una matriz que cumpla que

$$\text{Traza}(M) = \text{Traza}(\omega), \det(M) = \text{Norma}(\omega).$$

Afirmo que esto es equivalente a que el orden cumpla la hipótesis de Heegner. En efecto sea

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

con $N \mid \gamma$. Separemos en dos casos:

- $d \equiv 2, 3$ mód 4 por lo tanto $\omega = c\sqrt{d}$ y $D = 4dc^2$. En ese caso $\text{Traza}(\omega) = 0$ y $\text{Norma}(\omega) = -dc^2$.

  Luego queremos que $\alpha + \delta = 0$ y $\alpha\delta - \beta\gamma = -d.c^2$. Entonces ponemos $\delta = -\alpha$ y queremos que

  $$dc^2 = \alpha^2 + \beta\gamma.$$

  Multiplicando la ecuación por 4, vemos que

  $$D = (2\alpha)^2 + 4\beta N\gamma',$$

  con $N\gamma' = \gamma$ y éste sistema se puede resolver por la condicion 3 de la existencia de los puntos de Heegner.

- $d \equiv 1$ mód 4 por lo tanto $\omega = c(\frac{1+\sqrt{d}}{2})$ y $D = dc^2$. En ese caso $\text{Traza}(\omega) = 1$ y $\text{Norma}(\omega) = (\frac{1-d}{4})c^2$.

  Luego queremos que $\alpha + \delta = 1$ y $\alpha\delta - \beta\gamma = (\frac{1-d}{4})c^2$. Entonces ponemos $\delta = -\alpha + 1$ y queremos que

  $$\left(\frac{d-1}{4}\right) c^2 = \alpha^2 - \alpha + \beta\gamma.$$

Como antes, multiplicamos la ecuación por 4, y sumamos uno a cada miembro y obtenemos

$$D = (2\alpha - 1)^2 + 4\beta\gamma,$$

que de vuelta es equivalente a la existencia de puntos de Heegner.

Por último, una vez que ya construimos la matriz M, y por lo tanto el orden que buscábamos, basta tomar un $\tau \in \mathcal{H}$ tal que $M\tau = \tau$.

□

4.4. Acción del grupo de Galois y los operadores de Hecke sobre los puntos de Heegner

Resulta evidente que tenemos la siguiente fórmula (de acuerdo al teorema fundamental de la multiplicación compleja):

$$\sigma((\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])) = (\mathcal{O}, \mathfrak{n}, [s^{-1}\mathfrak{a}]).$$

Claramente, la acción de la conjugación compleja τ actúa de la siguiente forma

$$\tau(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \tau\mathfrak{n}, [\tau\mathfrak{a}])$$

Además si denotamos por w_N a la involución canónica, tenemos que

$$w_N(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \bar{\mathfrak{n}}, [\mathfrak{a}\mathfrak{n}^{-1}]).$$

También las correspondencias de Hecke T_p para primos $p \nmid N$ actúan en los puntos de Heegner de K de conductor coprimo con N (permitiendo cambiar el orden dentro de $\mathcal{O}_K$) de la siguiente manera

$$T_p(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = \sum_{\frac{\mathfrak{a}}{\mathfrak{b}} \cong \mathbb{Z}/p} (\mathcal{O}_b, \mathfrak{n}_\mathfrak{b}, [\mathfrak{b}]),$$

donde

$$\mathcal{O}_\mathfrak{b} = \mathrm{End}(\mathfrak{b}),$$
$$\mathfrak{n}_\mathfrak{b} = \mathfrak{n}\mathcal{O}_b \cap \mathcal{O}_b,$$

y la suma se realiza sobre los $p + 1$ subretículos $\mathfrak{b}$ de $\mathfrak{a}$ de índice p. Estos resultados se pueden ver en [7].

4.5. Condiciones de Compatibilidad y sistemas de Heegner

Fijemos N (que será el conductor de la curva elíptica) y sea K un cuerpo cuadrático imaginario satisfaciendo la hipótesis de Heegner. Si vamos tomando conductores c coprimos con N obtenemos una familia de órdenes crecientes en donde hay inclusiones (mencionadas en la sección 4.1). Luego los puntos de Heegner en cada uno de éstos vienen acompañanados por ciertas relaciones de compatiibilidad, formando un sistema de puntos. Más precisamente sea $\mathcal{O}_n$ el orden de conductor n en K. Sea $\tau \in CM(\mathcal{O}_n)$; el punto $\Phi_N(\tau)$ se llama un punto de Heegner de conductor n. Consideremos $E(H_n)$ donde H_n es el cuerpo de clases asociado a $\mathcal{O}_n$, y llamamos a $HP(n) \subset E(H_n)$ al conjunto de puntos de Heegner de conductor n. Se tiene lo siguiente:

Teorema 4.10. *Sea n un entero y l un primo, ambos coprimos con N. Sea P_{nl} un punto en $HP(nl)$. Entonces existen $P_n \in HP(n)$ y (si $l \mid n$) $P_{n/l} \in HP(n/l)$ tales que se satisfacen las siguientes condiciones de compatibilidad*

$$\text{Traza}_{H_{nl}/H_n}(P_{nl}) = \begin{cases} a_l P_n & \text{si } l \text{ es inerte en } K \text{ y } l \nmid n. \\ (a_l - \sigma_\lambda - \sigma_\lambda^{-1})P_n & \text{si } l = \lambda\bar{\lambda} \text{ se parte en } K \text{ y } l \nmid n. \\ (a_l - \sigma_\lambda)P_n & \text{si } l = \lambda^2 \text{ ramifica en } K. \\ (a_l P_n - P_{n/l}) & \text{si } l \mid n. \end{cases}$$

Donde $a_l = l + 1 - N_l$ como en la sección 1,5.

La demostración se puede consultar [7] y [8].

Proposición 4.11. *Sea $\tau \in Gal(H/\mathbb{Q})$ la conjugación compleja. Luego existe $\sigma \in Gal(H/K)$ tal que*

$$\tau P_n \equiv -\,\text{signo}(E, \mathbb{Q})\sigma P_n \quad (\text{mód } E(H)_{tors}).$$

Demostración. Sea x un punto de Heegner en $X_0(N)(H)$ tal que $\Phi_n(x) = P_n$. Por lo visto en la Sección 3.3 tenemos que existe un $\sigma \in Gal(H/K)$ tal que

$$\tau x = \omega_N(\sigma x)$$

Ahora, en $J_0(N)$ tenemos la siguiente igualdad

$$\tau\,(x - \infty) = \omega_N\,(\sigma x - \infty) + (\omega_N \infty - \infty)$$

Ahora, aplicando la parametrización modular y recordando que ω_N actúa por $-\text{signo}(E,\mathbb{Q})$ y que $\omega_N\infty$ corresponde a la cúspide 0, que mediante la parametrización modular va a parar a un punto de torsión obtenemos el resultado que queríamos.

□

Definición 4.12. Un *sistema de Heegner* asociado a (E,K) es una colección de puntos $P_n \in HP(n)$ indexados por n coprimos con N que satisfacen las condiciones de compatibilidad de la proposición anterior más el comportamiento bajo las reflexiones mencionado antes. Si alguno de los puntos no es de torsión decimos que el sistema es no trivial.

Teorema 4.13. *Si (E,K) satisface la hipótesis de Heegner hay un sistema de Heegner no trivial asociado a (E,K)*

Demostración. La unión de los puntos $CM(n)$ es infinita en $\mathcal{H}$ siempre y cuando se satisfaga la hipótesis de Heegner que garantiza que los $CM(n)$ no son vacíos. La imagen de estos puntos en $E(\mathbb{C})$ es infinita. Sea H_∞ la unión de todos los cuerpos de clases de conductor coprimo con N. Veamos que $E(H_\infty)$ tiene torsión finita.

Un primo que es inerte en K se parte completamente o ramifica en todos los cuerpos de clases. Luego el cuerpo resiudal en H_∞ de un tal primo q es el cuerpo $\mathbb{F}_{q^2}$. Como la torsión coprima con q se puede meter inyectivamente en $E(\mathbb{F}_{q^2})$ se sigue que todo el grupo de torsión se mete en $E(\mathbb{F}_{q^2}) \oplus E(\mathbb{F}_{p^2})$, donde p,q son dos primos distintos inertes en K. □

Definición 4.14. Sea $E/\mathbb{Q}$ una curva elíptica. Sea K una extensión cuadrática de $\mathbb{Q}$. Luego podemos pensar a E/K y como vimos en la proposición 2.5, se tiene que

$$L(E/K,s) = L(E/\mathbb{Q},s)L(E^D/\mathbb{Q},s)$$

Como tanto E como E^D son modulares por el teorema 3.10 y la observación 3.12 se tiene que las respectivas L-series satisfacen una cierta ecuación funcional. Luego $L(E/K,s)$ tiene una ecuación funcional y su signo, $\text{signo}(E,K)$, será el producto de los signos de las L-series de E y E^D.

Luego podemos enunciar la siguiente conjetura:

Conjetura 4.15. Si $\text{signo}(E,K) = -1$ entonces tenemos un sistema de Heegner no trivial asociado a (E,K).

Definimos $S_{E,K}$ como el conjunto de lugares del infinito o lugares donde la curva tiene reducción split multiplicativa.

Definición 4.16. Si E/K es una curva elíptica, decimos que es *semiestable* si todo primo de K tiene reduccíon buena o multiplicativa.

En particular, si E/K es semiestable, el conductor de E es libre de cuadrados.

Proposición 4.17. *Si E/K es semiestable y modular, entonces*

$$\text{signo}(E,K) = (-1)^{|S_{E,K}|}.$$

Esto sale escribiendo al signo como producto de signos locales y viendo que contribuye con -1 en los casos mencionados.

En el caso de K un cuerpo cuadrático imaginario que satisface la hipótesis de Heegner respecto de E (es decir de $N = cond(E)$) tenemos que $S_{E.K}$ consiste del lugar del infinito y de los primos donde la curva tiene reducción split multiplicativa, pero como estos primos dividen necesariamente al conductor tenemos que se parten en K y vienen de a pares entonces el signo da -1 y la construcción de los puntos de Heegner responde la conjetura para este caso especial.

4.6. Teorema de Gross-Zagier-Kolyvagin

En esta sección enunciamos los teoremas más importantes que sirve para probar el teorema de Gross-Zagier-Kolyvagin, enunciado en el capítulo 2.

Sea $E/\mathbb{Q}$ una curva elíptica y sea K un cuerpo cuadrático imaginario que satisface la hipótesis de Heegner respecto de E; sea $\{P_n\} = \{\Phi_n(\tau_n)\}$ un sistema de Heegner. Sea

$$P_K = traza_{H_1/K}(P_1) \in E(K)$$

la traza de un punto de Heegner de conductor 1 sobre el cuerpo de clases de Hilbert de K. Más generalmente, sea χ un caracter del cuerpo de clases de conductor n y definimos

$$P_n^\chi = \sum_{\sigma \in Gal(H_n/K)} \bar{\chi}(\sigma) P_n^\sigma \in E(H_n) \otimes \mathbb{C}$$

Teorema 4.18 (Gross-Zagier-Zhang)**.** *: Sea $\langle , \rangle_n$ la altura canónica de Nerón-Tate en $E(H_n)$ extendida por linearidad al pairing en $E(H_n) \otimes \mathbb{C}$. Entonces:*

1. $\langle P_K, P_K \rangle =^\cdot L'(E/K, 1)$ *y*
2. $\langle P_n^\chi, P_n^{\bar{\chi}} \rangle =^\cdot L'(E/K, \chi, 1)$ *donde $=^\cdot$ significa igualdad salvo multiplicar un factor distinto de cero que en prinipcio puede hacerse explícito.*

Para la primer parte ver [20]. La segunda parte se puede ver en [23].

Observación 4.19. La consecuencia de este teorema es que el punto de Heegner P_K no es de torsión y sólo $L'(E/K, 1) \neq 0$.

Teorema 4.20 (Kolyvagin)**.** *: Sea $\{P_n\}_n$ un sistema de Heegner asociado a (E, K). Si P_K no es de torsión entonces vale:*

El grupo de Mordellll-Weil $E(K)$ es de rango 1, y entonces P_K genera un subgrupo de índice finito.

Para lo demostración ver [5] capítulo 10 o [7].

Teorema 4.21 (Gross-Zagier-Kolyvagin)**.** *Sea $E/\mathbb{Q}$ una curva elíptica y*

$$ord_{s=1}L(E, s) \leq 1$$

entonces $rank(E(\mathbb{Q})) = ord_{s=1}L(E, s)$.

Demostración. Idea: si signo$(E) = -1$ por un resultado de Waldspurger ([19]) entonces existen infinitos caracteres de Dirichlet cuadráticos ϵ tales que:

1. $\epsilon(l) = 1$ si $l \mid N$;
2. $\epsilon(-1) = -1$
3. $L(E, \epsilon, 1) \neq 0$.

Las dos primeras hipótesis garantizan que el cuerpo K cumpla la hipótesis de Heegner. Sabemos que

$$L(E/K, s) = L(E, s)L(E, \epsilon, s).$$

Como K satisface la hipótesis de Heegner vimos que el orden de anulación de $L(E/K, s)$ en $s = 1$ es impar. Como estamos en el caso que se cumple la tercera condición se tiene que $L(E/K, 1) = 0$ y $L'(E/K, 1) \neq 0$.

Si en cambio tomamos signo$(E) = 1$, por paridad tenemos que $L(E, \epsilon, 1) = 0$. Además unos resultados analíticos ([4] y [22]) nos muestran que hay infinitos caracteres que satisfacen 1., 2. y $L'(E, \epsilon, 1) \neq 0$.

En ambos casos construimos un cuerpo K que satisface la hipótesis de Heegner respecto de E y tal que $ord_{s=1}L(E/K, s) = 1$. Luego tomemos un sistema de Heegner asociado a K. Por Gross-Zagier tenemos que P_K no es de torsión, y por Kolyvagin esto nos dice que $rank(E(K)) = 1$. Por la proposición 4.10 tenemos que P_K pertenece a $E(\mathbb{Q})$ modulo torsión si y sólo si signo$(E) = -1$, por lo tanto el rango de $E(\mathbb{Q})$ coincide con el orden de anulación de la L-serie. □

4.7. Ejemplos

Cálculo de puntos de Heegner

- Consideremos el orden maximal (anillo de enteros) $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ de la extensión cuadrática $K = \mathbb{Q}(\sqrt{-7})$,que tiene como discriminante -7 y número de clases 1. Tenemos que $\left(\frac{-7}{11}\right) = 1$ ($2^2 \equiv -7$ mód 11). Por lo tanto 11 se parte en el cuerpo K y tenemos que el orden cumple la hipótesis de Heegner. Como en la proposición 4.9 encontramos que la matriz en $M_0(11)$ que cumple el rol de $\frac{1+\sqrt{-7}}{2}$, es

$$\begin{pmatrix} -4 & -2 \\ 11 & 5 \end{pmatrix}.$$

Su punto fijo es el

$$\tau = \frac{-9+\sqrt{-7}}{22}.$$

Ponemos $q = e^{2\pi i\tau}$ y calculamos la imagen de $z = \sum_{n=1}^{1000} \frac{a_n}{n} q^n$ por la uniformización de Weierstrass como en la proposicíon 3.9 utilizando Pari/GP. Sabemos que el punto obtenido debe tener coordenadas en el cuerpo de clases de K, que al tener número de clases 1 es él mismo. Por lo tanto buscando un número que aproxime al obtenido numéricamente en ese cuerpo encontramos el punto:

$$P = (x, y) = \left(\frac{1-\sqrt{-7}}{2}, -2 - 2\sqrt{-7}\right).$$

Por último, reemplazando en la ecuación de la curva elíptica vemos que en efecto este punto satisface la ecuación. Por último, tomando la traza de P sobre $\mathbb{Q}$ en la curva elíptica obtenemos el punto

$$P + \bar{P} = (16, -61).$$

Como la curva tiene rango 0 este debe ser un punto de torsión, y de hecho tiene orden 5.

Si llamamos E^{-7} al twist cuadrático de la curva por -7, tiene rango 1, y tenemos la factorización

$$L(E/K, s) = L(E, s)L(E^{-7}, s).$$

Esta cuenta refleja la demostración del teorema de Gross-Zagier-Kolyvagin. Por ejemplo, sabemos que P va a tener orden infinito en $E(K)$.

- Veamos ahora un ejemplo donde el grupo de clases no es trivial. Sea $K = \mathbb{Q}(\sqrt{-6})$ cuyo anilo de enteros es $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ y su discriminante -24. Tiene número de clases 2. Luego, cuando hagamos la cuenta como en el ejemplo anterior los puntos van a estar definidos, no sobre K, sino sobre su cuerpo de clases de Hilbert H.

  Este orden cumple la hipótesis de Heegner ya que $\left(\frac{-24}{11}\right) = 1$. El truco para este caso, para calcular los distintos puntos de Heegner asociados a los representantes del grupo de clase, es pensarlo como elemento del grupo de las formas cuadráticas primitivas, definidas positivas de discriminante -24. Como estas formas van a representar al 11 (pues se satisface la condición de Heegner) se las puede llevar a respectivas formas equivalentes con A múltiplo de 11 (ver [2] (VII.B)).

  Dos de tales formas no equivalentes son:

$$11x^2 + 8xy + 2y^2,$$

$$22x^2 + 8xy + y^2.$$

  De acuerdo con la correspondencia dada en [2], una forma cuadrática de la forma $Ax^2 + Bxy + Cy^2$ se corresponde al punto $\frac{-B+\sqrt{D}}{2A} \in \mathcal{H}$.

  En este caso obtenemos los puntos

$$\tau_1 = \frac{-4+\sqrt{-6}}{11}, \qquad \tau_2 = \frac{-4+\sqrt{-6}}{22}.$$

  Finalmente, calculamos, al igual que en el ejemplo anterior usando Pari/GP los puntos

$$\Phi_{11}(\tau_i), i = 1, 2$$

  y obtenemos aproximadamente

$$P = \Phi_{11}(\tau_1) + \Phi_{11}(\tau_2) = (-2 - \sqrt{-6}, 5) \in E(K).$$

  También se puede calcular

$$P + \bar{P} = (5, -6),$$

que al igual que antes será un punto de torsión de la curva.

- Tomemos $K = \mathbb{Q}(\sqrt{-3})$ y $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ el anillo de enteros, que tiene número de clases 1.

  Cumple la hipótesis de Heegner ya que $\left(\frac{-3}{37}\right) = 1$ (o sea que 37 se parte en $\mathcal{O}_K$). Ahora encontramos la matriz en $M_0(37)$ como antes:

$$\begin{pmatrix} -10 & -3 \\ 37 & 11 \end{pmatrix}.$$

  El punto fijo por este orden es $\tau = \frac{-21+\sqrt{-3}}{74}$. Usando Pari/GP como antes obtenemos (aproximadamente) el punto

$$P = (-1, 0).$$

  Vemos reemplazando en la ecuación, que de verdad está en la curva. Además este punto tiene orden infinito, resultado esperable de acuerdo a Gross-Zagier-Kolyvagin ya que nuestra curva tiene rango (analítico) 1.

  Se puede ver que $-3(0,0) = P$, donde $(0,0)$ es un generador del grupo de Mordelll-Weil.

  Por último si llamamos E^{-3} al twist cuadrático de la curva por -3, tiene rango 0, y obtenemos

$$L(E/K, s) = L(E, s)L(E^{-3}, s).$$

  El lado izquierdo tiene orden de anulación exactamente 1 en $s = 1$, y P será un elemento de orden infinito en $E(K)$ de acuerdo al Teorema 4.21.

- Tomemos $K = \mathbb{Q}(\sqrt{-11})$ y $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ el anillo de enteros, que tiene número de clases 1.

  Cumple la hipótesis de Heegner ya que $\left(\frac{-11}{3}\right) = 1$ y $\left(\frac{-11}{5}\right) = 1$ (o sea que todo primo que divide al conductor se parte en $\mathcal{O}_K$). Ahora encontramos la matriz en $M_0(225)$ como antes:

$$\begin{pmatrix} -33 & -5 \\ 225 & 34 \end{pmatrix}.$$

  El punto fijo por este orden es $\tau = \frac{-67+\sqrt{-11}}{450}$. Haciendo exactamente lo mismo que en el ejemplo anterior con Pari/GP obtenemos (aproximadamente) el punto

$$P = (-1, 0).$$

Este punto debe tener orden infinito por Teorema 4.21. No es un generador del grupo, pero si cumple que $2(1,1) = P$, donde $(1,1)$ es un generador del grupo de puntos racionales de la curva elíptica.

Si llamamos E^{-11} al twist cuadrático de la curva por -11, tiene rango 0, y tenemos

$$L(E/K, s) = L(E, s)L(E^{-11}, s).$$

De vuelta, como antes, tenemos que el lado izquierdo tiene orden de anulación exactamente 1 en $s = 1$ y P tiene orden infinito en $E(K)$.

5. Construcción de puntos de Heegner en otras curvas

Sea $E/\mathbb{Q}$ una curva elíptica de conductor N y K un cuerpo cuadrático imaginario tal que signo$(E,K) = -1$. El objetivo de este capítulo es el de poder producir un sistema de Heegner, en condiciones donde todavía no sabemos hacerlo. Por ejemplo supongamos que $N = pq$ donde p y q son dos primos inertes en K. Entonces tenemos que $S(E,K) = \{p, q, \infty\}$ y por la Proposición 4.17 el signo es -1. Sin embargo, al no satisfacerse la hipótesis de Heegner los posibles órdenes de Eichler que construyamos no nos van a servir. Otro caso que conviene tener en mente es que pasa si $N = p^2$ donde p es un primo que no ramifica en K. En ese caso se puede ver que signo$(E,K) = -1$ sin importar como se factorice el primo en K. Entonces apuntamos a construir puntos de Heegner, aún cuando el primo sea inerte, en cuyo caso no podremos usar los órdenes de Eichler.

Supongamos por el resto del capítulo que $disc(K)$ y N son coprimos.

5.1. Álgebras de cuaterniones y curvas de Shimura

La siguiente sección sigue a [5](IV). Si N es libre de cuadrados entonces tenemos que $S(E,K) = 2a + b + 1$ donde a son la cantidad de primos que dividen a N que se parten en K y b son la cantidad de primos que son inertes en K (el 1 corresponde al primo del infinito) . Para que signo$(E,K) = -1$ necesitamos que b sea par, es decir que la cantidad de primos inertes sea par. Luego podemos factorizar a N como $N = N^+N^-$ donde N^+ es el producto de los primos que se parten y N^- es el producto de los primos inertes, que son una cantidad par. A una tal factorización de N la llamaremos admisible.

Para buscar puntos de Heegner en estas condiciones vamos a necesitar otros ordenes que los de Eichler. Más precisamente vamos a considerar ordenes en álgebras de cuaterniones.

Recordar que un álgebra de cuaterniones B sobre $\mathbb{Q}$ es un ágebra central simple de dimensión 4. Si B es isomorfa como álgebra a $M_2(\mathbb{Q})$ se dice que es split. Si B es un álgebra de cuaterniones y v es un primo de $\mathbb{Q}$ (ya sea finito o infinito), denotando por $\mathbb{Q}_v$ la completación de $\mathbb{Q}$ respecto a ese primo, podemos construir

$$B_v =: B \otimes_{\mathbb{Q}} \mathbb{Q}_v.$$

Decimos que v se parte (resp. ramifica) si B_v es un álgebra de cuaterniones split sobre $\mathbb{Q}_v$ (resp no es split).

Proposición 5.1. *Sea S un conjunto finito de lugares de $\mathbb{Q}$. Luego existe un álgebra de cuaterniones ramificada precisamente en los lugares de S si y solo si el cardinal de S es par, y en ese caso el álgebra es única salvo isomorfismos.*

Un orden $\mathscr{O}$ en B es un subanillo de B que es libre de rango 4 como $\mathbb{Z}$ módulo. Un orden maximal es un orden que no está contenido propiamente en ningún otro orden. Un orden de Eichler es la intersección de dos ordenes maximales. Si $\mathscr{O}$ es un orden de Eichler, se obtiene como la intersección de dos ordenes maximales $\mathscr{O}_1$ y $\mathscr{O}_2$. Definimos el nivel de $\mathscr{O}$ como el índice de $\mathscr{O}$ en $\mathscr{O}_1$ (que es lo mismo que el índice en $\mathscr{O}_2$). Se puede probar que este índice no depende de la elección de los $\mathscr{O}_i$.

Proposición 5.2. *Si B no ramifica en el lugar del infinito, entonces cualesquiera dos ordenes maximales en B son conjugados. Del mismo modo, dos ordenes de Eichler del mismo nivel son conjugados.*

Cualquier álgebra de cuaterniones admite una representación lineal de dimensión 4 al hacer actuar B sobre si mismo por multiplicación a izquierda. Dado $b \in B$ el endomorfismo $\mathbb{Q}$-lineal correspondiente tiene un polinomio característico de la forma

$$f_b(x) = (x^2 - tx + n))^2.$$

Los enteros t y n se llaman la traza y la norma reducida de b y los denotamos por Traza(b) y Norma(b) respectivamente.

A cada factorización admisible de N le podemos asociar un subgrupo Γ_{N^+,N^-} de $\mathrm{SL}_2(\mathbb{R})$ de la manera siguiente. Tomemos el álgebra de cuaterniones B que ramifica en exactamente los primos que dividen a N^-. Este álgebra es única salvo conjugación por la Proposición 5.1. Como no ramifica en ∞ podemos fijar una identificación

$$\iota : B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R}).$$

Elijamos un orden maximal $\mathscr{O}_0$ y como el B se parte en los primos que dividen a N^+ podemos fijar una identificación

$$\eta : \mathscr{O}_0 \otimes (\mathbb{Z}/N^+\mathbb{Z}) \longrightarrow M_2(\mathbb{Z}/N^+\mathbb{Z}).$$

Sea $\mathscr{O}_{N^+}$ el subanillo de $\mathscr{O}_0$ que consiste en los x tales que $\eta(x)$ es triangular superior. El subanillo $\mathscr{O}_{N^+}$ es un orden de Eichler de nivel N^+ en B. Así como el orden maximal lo era, es único salvo conjugación de elementos de $B^\times$. Definimos

$$\Gamma_{N^+,N^-} = \iota(\mathscr{O}_{N^+}^\times).$$

Para este tipo de subgrupos de $\mathrm{SL}_2(\mathbb{R})$ se puede definir, análogamente al caso clásico, formas modulares invariantes por ellos. Las mismas tienen propiedades similares al caso clásico (operadores de Hecke, producto de Petersson y una generalización de Atkin Lehner). Sin embargo, cuando $N^- \neq 1$ uno no tiene una noción de expansión de Fourier en las cúspides porque el cociente del semiplano complejo superior por estos grupos ya es compacto. Esto hace que la teoría se vuelva más complicada.

Dada una curva elíptica de conductor N y una factorización admisible, mediante una construcción análoga a Eichler-Shimura y la correspondencia de Jacquet-Langlands uno puede construir una parametrización modular

$$\Phi'_{N^+,N^-} : Div^0_{\mathcal{H}/\Gamma_{N^+,N^-}} \longrightarrow E(\mathbb{C}).$$

Similarmente a lo hecho en el Capítulo 4, dado $\tau \in \mathcal{H}/\Gamma_{N^+,N^-}$, el orden asociado a τ es

$$\{\mathcal{O}_\tau := \gamma \in R : norm(\gamma) = 0, \iota(\gamma)(\tau) = \tau\} \cup \{0\}.$$

Podemos pensarlo como antes como un anillo discreto de $\mathbb{C}$ y es por lo tanto o $\mathbb{Z}$ o un orden en un cuerpo cuadrático imaginario.

Un punto $\tau \in \mathcal{H}/\Gamma_{N^+,N^-}$ se dice un punto de multiplicación compleja (CM) si su orden asociado es un orden en un cuerpo cuadrático imaginario. Definimos

$$CM(\mathcal{O}) = \{\tau \in \mathcal{H}/\Gamma_{N^+,N^-} : \mathcal{O}_\tau = \mathcal{O}\}.$$

Teorema 5.3 (multiplicación compleja para curvas de Shimura)**.** *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático imaginario de discriminante coprimo con N y sea H/K el cuerpo de clases asociado a $\mathcal{O}$. Entonces*

$$\Phi_{N^+,N^-}(Div^0(CM(\mathcal{O}))) \subset E(H).$$

Una pregunta interesante es la siguiente: ¿Cómo se hace para calcular numéricamente la parametrización modular en este caso? Al no tener una expansión de Fourier no podemos hacer lo mismo que con el caso clásico. Una solución parcial es usar la idea de uniformización p-ádica ([5] (V, VI). Este método no permite construir directamente los puntos globalmente, sino una aproximación p-ádica tan buena como uno quiere. Conociendo el grado de la extensión que las coordenadas de los puntos generan, se puede numéricamente calcular el polinomio minimal de ellos (que debe tener coordenadas enteras), y así poder hallarlos globalmente.

5.2. Curvas de Cartan

Ahora apuntamos a construir puntos de Heegner en el caso que $N = p^2$. Para eso introducimos *el grupo de Cartan non split*. Este es el subgrupo de $Gl_2(\mathbb{F}_p)$ dado por

$$C_{ns}(p) = \left\{ \begin{pmatrix} a & b \\ b\epsilon & a \end{pmatrix} \text{ tales que } (a,b) \neq (0,0) \right\},$$

donde ϵ es un no cuadrado en $\mathbb{F}_p$.

Dada una matriz $A \in \mathrm{SL}_2(\mathbb{Z})$, denotemos por $\bar{A}$ su reducción módulo p. Llamemos $\Gamma_{ns}(p)$ al subgrupo de $Sl_2(\mathbb{Z})$ dado por

$$\Gamma_{ns}(p) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \bar{A} \in C_{ns}(p) \cap Sl_2(\mathbb{F}_p) \right\}.$$

Luego, al igual que para $\Gamma_0(N)$ uno puede definir las curvas modulares de Cartan de la siguiente forma

$$X_{ns}(p) = \mathcal{H}^*/\Gamma_{ns}(p),$$

Sea $N = p^2$ y sea K un cuerpo cuadrático imaginario donde p es inerte (si se parte podemos usar la construcción de Heegner clásica). Vamos a hacer la misma cuenta que en el caso clásico (proposición 4.9 de este trabajo). Sea $\mathcal{O}_K$ el anillo de enteros de K.

Proposición 5.4. *Si $N = p^2$ y K es un cuerpo cuadrático imaginario donde p es interte, entonces el anillo de enteros $\mathcal{O}_K$ se mete dentro de $C_{ns}(p)$.*

Demostración. Si $\mathcal{O}_K = \langle 1, \omega \rangle$, como $1 \in C_{ns}(p)$, simplemente necesitamos encontrar una matriz con coeficientes enteros, cuya reducción módulo p caiga en $C_{ns}(p)$ y que se comporte igual que ω. Más precisamente, queremos encontrar M tal que:

- $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ con $\alpha \equiv \delta \pmod{p}$, $\beta\epsilon \equiv \gamma \pmod{p}$ y $(\alpha, \beta) \not\equiv (0,0) \pmod{p}$.
- $\mathrm{Traza}(M) = \mathrm{Traza}(\omega)$.
- $\det(M) = \mathrm{Norma}(\omega)$.

Una observación importante es que podemos elegir convenientemente en ϵ en la definición del grupo de Cartan non-split. Es fácil ver que dos elecciones distintas de los residuos no cuadráticos ϵ, ϵ' dan lugar a grupos conjugados y si encontramos una matriz para algun ϵ, conjugándola vamos a obtener una matriz que cumpla las mismas relaciones (ya que la traza y el determinante no cambian) y esté en el otro grupo de Cartan correspondiente a ϵ'.

Separemos en dos casos:

- Si $d \equiv 2,3 \pmod 4$, $\omega = \sqrt{d}$ y $D = 4d$. En este caso Traza$(\omega) = 0$ y Norma$(\omega) = -d$.

  Luego queremos que $\alpha + \delta = 0$ y $\alpha\delta - \beta\gamma = -d$. Entonces ponemos $\delta = -\alpha$ y queremos que

  $$d = \alpha^2 + \beta\gamma. \tag{2}$$

  Observemos que $\delta = -\alpha$ y $\alpha \equiv \delta \pmod p$ fuerza que $\alpha \equiv \delta \equiv 0 \pmod p$. Como buscamos elementos en $\Gamma_{ns}(p)$, debe ser $\gamma \equiv \epsilon\beta$.

  Tomemos $\alpha = \delta = 0, \beta = 1, \gamma = d$. La condición que el primo sea inerte nos dice que $\left(\frac{d}{p}\right) = -1$, con lo cual la matriz M está en el Cartan non split asociado a $\epsilon = d$.

- Si $d \equiv 1 \pmod 4$, $\omega = (\frac{1+\sqrt{d}}{2})$ y $D = d$. En ese caso Traza$(\omega) = 1$ y Norma$(\omega) = (\frac{1-d}{4})$.

  Luego queremos que $\alpha+\delta = 1$ y $\alpha\delta-\beta\gamma = (\frac{1-d}{4})$. Entonces ponemos $\delta = -\alpha+1$ y nos queda

  $$\left(\frac{d-1}{4}\right) = \alpha^2 - \alpha + \beta\gamma. \tag{3}$$

  Multiplicando por 4 y sumando 1 obtenemos

  $$d = (2\alpha - 1)^2 + 4\beta\gamma.$$

  Como $\delta = -\alpha + 1$ y $\alpha \equiv \delta \pmod p$, $2\alpha - 1 \equiv 0 \bmod p$. Como buscamos elementos en $\Gamma_{ns}(p)$, debe ser $\gamma \equiv \epsilon\beta$. Tomemos $\alpha = \frac{p-1}{2}, \beta = 1, \gamma = \frac{d-(2\alpha-1)^2}{4}$. Observemos que como $d \equiv 1 \bmod 4$, γ es entero. Además es claro que γ es un no cuadrado módulo p ya que d es un no cuadrado y $2\alpha - 1$ es múltiplo de p ; por lo tanto nos queda lo que queremos.

□

Por último, una vez que ya construimos la matriz M, y por lo tanto el orden que buscábamos, basta tomar un $\tau \in \mathcal{H}$ tal que $M\tau = \tau$.

Luego en estas curvas uno espera poder construir sistemas de Heegner cuando p sea inerte en K. Al igual que en el caso clásico, las curvas satisfacen una cierta interpretación de espacio de modulii (clasificando curvas elípticas con cierta estructura de nivel). Entonces uno puede considerar las curvas con multiplicacíon compleja y tratar de construir puntos de Heegner como antes. Para poder realizar esta construcción

necesitamos conocer una parametrización modular y poder calcular el desarrollo de Fourier. Notemos que la matriz

$$\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$$

se encuentra en $\Gamma_{ns}(p)$ y por lo tanto una forma modular para ese subgrupo va a tener una q-expansión de Fourier en términos de $q = e^{\frac{2\pi i \tau}{p}}$.

El estudio de está q-expansión y de la parametrización modular para poder calcular explícitamente los puntos de Heegner en este caso serán estudiados durante el doctorado.

Referencias

[1] H Carayol. Formes modulaires et représentations galoisiennes à valeurs dans un aneau local complet. *Contemp. Math*, 165:213–237, 1994.

[2] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.

[3] J. E. Cremona. Cremona tables of elliptic curves. `http://homepages.warwick.ac.uk/~masgaj/ftp/data/`.

[4] J. Hoffstein D. Bump, S. Friedberg. Eisenstein series on the metaplectic group and non vanishing theorems for automorphic L-functions and their derivatives. *Ann. of Math.*, 131:53–127, 1990.

[5] H. Darmon. *Rational points on modular elliptic curves*. American Mathematical Society, 2004.

[6] J. Shurman F. Diamond. *A first course in modular forms*. Springer, 2005.

[7] Benedict H. Gross. Heegner points on $X_0(N)$. *Modular Forms, edited by Rankin*, pages 87–105, 1984.

[8] Benedict H. Gross. Kolyvagin work on modular elliptic curves. *L-functions and arithmetic*, pages 235–256, 1989.

[9] Gerald J. Janusz. *Algebraic Number Fields*. Academic Pressr, 1973.

[10] John Tate Joseph H. Silverman. *Rational points of elliptic curves*. Springer, 1992.

[11] Kiran S. Kedlaya. Complex multiplication and explicit class field theory, 1996.

[12] A. Knapp. *Elliptic curves*. Princeton University Press, 1992.

[13] Neal Koblitz. *Introduction to elliptic curves and modular forms*. Springer, 1984.

[14] Daniel A. Marcus. *Number Fields*. Springer, 1977.

[15] T. Miyake. *Modular forms*. Springer, 2006.

[16] J.P. Serre. *A course in arithmetic*. Springer, 1973.

[17] Joseph H. Silverman. *Arithmetic of elliptic curves*. Springer, 1992.

[18] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer, 1994.

[19] J. L. Waldspurger. Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie. *Compositio Math.*, 54:173–242, 1985.

[20] Benedict H. Gross y D.B. Zagier. Heegner points and derivative of L series. *Invent. Math.*, 84:225–320, 1986.

[21] A. O. L Atkin y J. Lehner. Hecke operators on $\Gamma_0(m)$. *Mathematische Annalen*, 185:134–160, 1970.

[22] M.R. Murty y V.K Murty. Mean values of derivatives of modular L series. *Ann. of Math.*, 133:447–475, 1991.

[23] S. Zhang. Gross zagier formula for $Gl(2)$. *Asian J. Math*, 5:183–290, 2001.