Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Tesis de Licenciatura

Formas Modulares y el Problema de los Números Congruentes

Santiago Agustín Ramírez

Director: Nicolás Sirolli

Marzo 2019

Agradecimientos

A mi familia, mis viejos, mis hermanos, mis abuelos, por cuidarme y quererme desde chico.

A mis amigos de la infancia y del colegio, a Fede, Lauta, Pilu, Ian, Delfi, Ludmi, Hernán, Luz, Maru, Tefi, Tomás, Nacho, Mariano, Vale, Mechi, por todos los años de amistad.

A mis amigos de la facultad, Jaz, Darío, Juan, Jaquie, Gonza, Martín, Pablito, Billy, Uli, Mati, Gastón, Mai, Alejo, Juampi, Agus, por hacer que las horas de estudio y cursada en la facultad fueran tan llevaderos.

A mis docentes del secundario, a Juan Pablo Muszkatz, Maxi Camporino, Fede Felguer y Gustavo Krimker por enseñarme a pensar y disfrutar la matemática, y a Yoshi, Mati, Diego, Cynthia, Valeria, por enseñarme lo que es la ciencia.

A mis profesores de la facultad Leandro Vendramín, Jonathan Barmak, Daniel Carando, Teresa Krick, Mariano Suarez-Álvarez, Pablo Ferrari, Gabriel Larotonda, por haberme dado una formación de excelencia y al jurado Miguel Walsh y Fernando Cukierman por habrse tomado el trabajo de leer la tesis.

A Nico, por darme la oportunidad de hacer esta tesis con él, ayudarme cuándo no podía avanzar con algo, por todos sus comentarios tanto matemáticos, como de redacción o de LaTeX y su apoyo general en este trabajo.

A ellas y todas las demás personas de las que me estoy olvidando y que me apoyaron, acompañaron y enseñaron en la matemática y la vida, gracias.

Índice general

Introducción

Las denominadas L-series son ciertas series de Dirichlet, i.e. series de la forma $\sum_{n=1}^{\infty} a_n n^{-s}$, que aparecen en la teoría de números. La más famosa de estas es la función ζ de Riemann:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Su conexión con la teoría de números ya empezó a ser clara con Euler a mediados del 1700, quien demostró que admite el desarrollo como producto infinito sobre los primos $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$, calculó sus valores en los naturales pares y mostró como de sus propiedades analíticas alrededor de $s = 1$, concretamente de la divergencia en este punto, se puede deducir la infinitud de los números primos. Aunque esto último parezca no ser más que una aplicación simpática pero innecesariamente complicada, es el principio de una teoría sumamente profunda.

En 1837 Dirichlet extendió el método utilizado por Euler para demostrar el siguiente resultado:

Teorema (Dirichlet, 1837)**.** *Dados $a, d \in \mathbb{N}$, coprimos hay infinitos primos de la forma $a + kd$ con $k \in \mathbb{N}$, i.e. hay infinitos primos congruentes a a módulo d.*

Para demostrarlo se consideran las series $L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$, donde χ es un caracter módulo d, y al igual que en la demostración de Euler se estudia su comportamiento en $s = 1$. La demostración del producto de Euler para la ζ de Riemann depende únicamente de la multiplicatividad de los coeficientes de la serie, y se extiende por lo tanto a las L-series que consideró Dirichlet. Esta propiedad común es una de las prototípicas de las L-series en la teoría de números.

Tanto en el caso de Euler como en el de Dirichlet analizando el comportamiento de esta L-serie se obtiene información aún más precisa sobre como se distribuyen los primos que estamos considerando que su mera infinitud. Por ejemplo, las demostraciones de Euler y Dirichlet permiten concluir que las series $\sum_p p^{-1}$, con la suma sobre todos los primos ó todos los primos congruentes a a módulo d, divergen.

En 1859 Riemann publicó el que probablemente sea uno sus trabajos de mayor impacto [Rie59]; en este demostró algunas de las propiedades más importantes de la función ζ, que servirían como prototipo para muchas generalizaciones, y conjeturó otras. Concretamente demostró que la función ζ, en principio definida por una serie que converge sólo si $\Re(s) > 1$, admite una continuación analítica a una función meromorfa

en todo $\mathbb{C}$ con un único polo simple en $s = 1$, y que esta función satisface la ecuación funcional:

$$\Lambda(s) = \Lambda(1 - s),$$

donde la función Λ es la denominada *función ζ completada*, que está definida como $\Lambda(s) = \frac{1}{2}\pi^{-\frac{s}{2}} s(s-1)\Gamma(\frac{s}{2})\zeta(s)$. Del análisis que hace de la función ζ obtiene una expresión explícita para la función de contar primos en términos de los ceros de la función y ζ, y hace una de las conjeturas más importantes de la matemática moderna:

Conjetura (Hipótesis de Riemann)**.** *Los ceros de la función ζ son ó bien números pares negativos ó tienen parte real igual a $1/2$.*

La importancia de esta conjetura es que, junto con las fórmulas explícitas, permite obtener de manera bastante precisa el comportamiento asintótico de los primos.

En el siglo XX los métodos de L-series se extendieron aún más en la teoría de números y se comenzaron a asociar series de Dirichlet a una multitud de objetos de interés aritmético: las funciones zeta de Dedekind asociadas a cuerpos de números, las funciones L de Artin asociadas a representaciones de Galois y las L series de Hasse-Weil asociadas a variedades abelianas. De manera análoga a los resultados clásicos, se busca relacionar las propiedades anlíticas de las funciones definidas por estas series con propiedades aritméticas de los objetos a los que están asociados. Sin embargo, el compartamiento analítico de estas series es en general bastante difícil de entender, y las propiedades prototípicas que mencionamos antes, la continuación analítica, ecuación funcional e hipótesis de Riemann, son en muchos casos conjeturales.

A principios del siglo XX se obtuvieron resultados sobre las propiedades aritméticas de los coeficientes de series asociadas a ciertas funciones analíticas del semiplano superior, las denominadas *formas modulares*. Para demostrar parte de las conjeturas de Ramanujan sobre la función τ, Mordell usó técnicas analíticas que luego Hecke desarrollaría en la teoría de Hecke para formas modulares. Esta teoría permite asociar a ciertas formas modulares, denominadas autoformas, series de Dirichlet que admiten un producto de Euler y cuyo comportamiento analítico se puede estudiar con herramientas de la teoría de formas modulares. A lo largo de siglo XX comenzaron a surgir conjeturas que buscaban vincular de manera teórica las formas modulares, o funciones más generales llamadas formas automorfas, con los objetos aritméticos que mencionamos antes, de forma que las series L asociadas a estos coincidan con las provenientes de la teoría de Hecke. De esta forma se podrían usar las herramientas analíticas de la teoría de formas automorfas para enteder los objetos aritméticos.

En esta tesis vamos a mostrar como estas herramientas analíticas permiten resolver problemas de teoría de números en un caso particular. Vamos a tomar como ejemplo el problema de la clasificación de números congruentes resuelto, por lo menos en parte, por Tunnell en [Tun83]. En el primer capítulo vamos a plantear este problema y ver como se puede entender en términos de la L-serie de Hasse-Weil de una curva elíptica. En el segundo y tercer capítulo vamos a desarrollar la teoría formas modulares necesaria para entender la resolución de este problema. El segundo capítulo está dedicado a la

teoría más clásica de formas modulares de peso entero, incluyendo la teoría de Hecke. Por otro lado, en el tercer capítulo vamos a tratar la teoría moderna de formas de peso medio entero iniciada por Shimura. Finalmente en el cuarto capítulo vamos a explicar como las herramientas desarrolladas en los capítulos anteriores permite obtener el resultado de Tunnell.

Capítulo 1

Curvas elípticas

1.1. El problema de los números congruentes

Nuestro objetivo va a ser obtener una descripción, en parte conjetural, de los denominados números congruentes.

Definición 1.1.1. Decimos que $d \in \mathbb{Q}^\times$ es un *número congruente* si existe un triángulo rectángulo con todos sus lados racionales que tiene área d, i.e. si existen numeros racionales $a, b, c \in \mathbb{Q}^\times$ tales que $a^2 + b^2 = c^2$ y $ab/2 = d$.

El problema de clasificar los números congruentes tiene bastante antigüedad ya sea en la forma en que lo enunciamos o en los términos dados por el siguiente resultado:

Proposición 1.1.2. *Un número racional d es congruente si y sólo si existe un número racional q tal que los números $q - d$, q y $q + d$ son cuadrados.*

Demostración. Si d es un número congruente y a, b, c son los lados del triángulo rectángulo que lo tiene como área, podemos tomar $q = (c/2)^2$. Entonces se verifica fácilmente que $q - d = (a - b)^2/4$ y $q + d = (a + b)^2/4$ son también cuadrados.

Recíprocamente si $q - d$, q y $q + d$ son cuadrados racionales tomando $a = \sqrt{q + d} + \sqrt{q - d}$, $b = \sqrt{q + d} - \sqrt{q - d}$ y $c = 2\sqrt{q}$ se puede verificar que estos son los lados de un triángulo rectángulo con área d. □

Decidir si un número es o no congruente es en principio un problema bastante díficil incluso para valores pequeños. En parte esto se debe a que uno no puede en principio acotar la "complejidad", en algún sentido preciso, de los lados del triángulo con área d en términos de esta. Por ejemplo, mientras que es fácil ver que 6 es un número congruente por ser el área de un triángulo de lado 3,4 y 5, el triángulo de lados racionales más sencillo con área 5 tiene lados $\frac{3}{2}$, $\frac{20}{3}$ y $\frac{41}{6}$, y con área 157 el triángulo más sencillo

fue encontrado por Zagier y tiene lados:

$$a = \frac{4113405192277161493832 03}{21666555693714761309610},$$

$$b = \frac{6803298487826435051217540}{4113405192277161493832 03},$$

$$c = \frac{2244035177043369699245575130906748631609484720 41}{8912332268928859588025535178967163570016480830}.$$

Notemos que si d es un número congruente $x^2 d$ también lo es para cualquier $x \in \mathbb{Q}^\times$, es decir que la propiedad de ser congruente sólo depende de la clase de equivalencia de d en $\mathbb{Q}^\times / (\mathbb{Q}^\times)^2$. Como cada una de estas clases de equivalencia contiene exactemente un entero positivo libre de cuadrados, la clasificación de números congruentes se puede reducir, por lo menos a nivel teórico, al caso de $d \in \mathbb{N}$ libre de cuadrados.

El primer paso para lograr esta clasificación es traducir el problema de decidir si un número d es congruente a un problema de geometría algebraica. El siguiente resultado nos da una biyección entre los triángulos rectángulos racionales con área d y los puntos racionales de una curva plana.

Teorema 1.1.3. *Dado $d \in \mathbb{N}$ se tiene la siguiente biyección de conjuntos:*

$$\left\{(a,b,c) \in (\mathbb{Q}^\times)^3 \,:\, a^2 + b^2 = c^2 \wedge \frac{ab}{2} = d\right\} \longleftrightarrow \left\{(x,y) \in \mathbb{Q}^2 \,:\, y^2 = x^3 - d^2 x \wedge y \neq 0\right\};$$

$$(a,b,c) \longmapsto \left(\frac{bd}{c-a}, \frac{2d^2}{c-a}\right)$$

$$\left(\frac{x^2-d^2}{y}, \frac{2dx}{y}, \frac{x^2+d^2}{y}\right) \longmapsto (x,y).$$

Demostración. Sean A el conjunto de la izquierda y B el conjunto de la derecha. Supongamos primero $(a,b,c) \in A$ y observemos que como $b^2 = c^2 - a^2$ se tiene:

$$\begin{aligned}
\frac{b^2}{(c-a)^2} - 1 &= \frac{1}{(c-a)^2}(b^2 - c^2 + 2ac - a^2) \\
&= \frac{1}{(c-a)^2}(c^2 - a^2 - c^2 + 2ac - a^2) \\
&= \frac{1}{(c-a)^2}(2a(c-a)) \\
&= \frac{2a}{c-a}.
\end{aligned}$$

Tomando $x = \frac{db}{c-a}$ e $y = \frac{2d^2}{c-a}$ y usando la identidad anterior y que $ab = 2d$ obtenemos:

$$\begin{aligned} x^3 - d^2x &= \left(\frac{db}{c-a}\right)^3 - d^2\frac{db}{c-a} = d^3\frac{b}{c-a}\left(\frac{b^2}{(c-a)^2} - 1\right) \\ &= \frac{d^3b}{c-a}\cdot\frac{2a}{c-a} = \frac{4d^4}{(c-a)^2} = y^2. \end{aligned}$$

Es decir que la primera aplicación está bien definida. Si calculamos la composición con la segunda función obtenemos:

$$\begin{aligned} \frac{x^2-d^2}{y} &= \left(\frac{d^2b^2}{(c-a)^2} - d^2\right)\frac{c-a}{2d^2} = \left(\frac{b^2}{(c-a)^2} - 1\right)\frac{d^2(c-a)}{2d^2} \\ &= \frac{2a}{c-a}\cdot\frac{c-a}{2} = a, \end{aligned}$$

$$\frac{2dx}{y} = \frac{2d\cdot db}{c-a}\cdot\frac{c-a}{2d^2} = b,$$

$$\begin{aligned} \frac{x^2+d^2}{y} &= \left(\frac{d^2b^2}{(c-a)^2} + d^2\right)\frac{c-a}{2d^2} = \left(\frac{b^2}{(c-a)^2} + 1\right)\frac{d^2(c-a)}{2d^2} \\ &= (b^2 + (c-a)^2)\frac{1}{(c-a)^2}\cdot\frac{c-a}{2} \\ &= (c^2 - a^2 + c^2 + a^2 - 2ac)\frac{1}{2(c-a)} \\ &= (2c(c-a))\frac{1}{2(c-a)} = c. \end{aligned}$$

Suponiendo ahora $(x, y) \in B$ tenemos que:

$$\frac{x^2-d^2}{y}\cdot\frac{2dx}{y} = 2d\frac{x^3-d^2x}{y^2} = 2d$$

y

$$\begin{aligned} \left(\frac{x^2-d^2}{y}\right)^2 + \left(\frac{2dx}{y}\right)^2 &= \frac{x^4 - 2d^2x^+d^4 + 4d^2x^2}{y^2} \\ &= \frac{x^4 + 2d^2x^2 + d^4}{y^2} = \left(\frac{x^2+d^2}{y}\right)^2. \end{aligned}$$

Es decir que la segunda función está bien definida. Antes de calcular la composición observemos primero que:

$$c - a = \frac{x^2+d^2}{y} - \frac{x^2-d^2}{y} = \frac{2d^2}{y}.$$

Luego componiendo con la primer aplicación:

$$\frac{bd}{c-a} = \frac{2d^2x}{y} \cdot \frac{y}{2d^2} = x,$$

$$\frac{2d^2}{c-a} = 2d^2 \frac{y}{2d^2} = y.$$

□

1.2. Curvas elípticas

Para trabajar con el subconjunto de $\mathbb{Q}^2$ que aparece en el último resultado vamos a introducir algo de lenguaje de geometría algebraica.

Definición 1.2.1. Una *curva plana* E sobre un cuerpo K va a ser, para nosotros, una ecuación polinomial en dos variables con coeficientes en K. Dada una curva plana podemos considerar sus puntos sobre cualquier extensión L/K, que es el conjunto de puntos de L^2 que satisfacen la ecuación; vamos a notar $E(L)$ a este conjunto.

El subconjunto del plano que aparece en el teorema anterior es entonces el conjunto de puntos en $\mathbb{Q}$ con segunda coordenada no nula de la siguiente curva:

$$E^d : y^2 = x^3 - d^2x.$$

Por razones técnicas resulta importante considerar también las soluciones proyectivas de las ecuaciones:

Definición 1.2.2. Dado un cuerpo K definimos el plano proyectivo como el cociente: $\mathbb{P}(K) = \left(K^3 \setminus \{(0,0,0)\}\right) / \sim$, donde la relación $\sim$ identifica puntos que difieren en un múltiplo escalar.

Si P es un polinomio homogéneo en tres variables con coeficientes en K, el conjunto de puntos de $\mathbb{P}(K)$ en donde P se anula está bien definido. Si P es un polinomio en dos variables consideramos su *polinomio homogeneizado*, $\tilde{P}(x,y,z) = z^{\deg(P)}P(\frac{x}{z}, \frac{y}{z})$.

Cuando E es una curva plana sobre K definimos entonces sus *puntos proyectivos* en L, que notamos $\tilde{E}(L)$, como las raíces en el plano proyectivo a la ecuación homogeneizada.

Observemos que si E es una curva plana todo punto $(x,y) \in E(L)$ se corresponde con el punto $(x,y,1) \in \tilde{E}(L)$. Además de estos puntos, $\tilde{E}(L)$ contiene los denominados *puntos en el infinito*, que son los de la forma $(x,y,0)$.

En nuestros casos las curvas E^d tienen coeficientes enteros, lo que nos permite considerarlas también como curvas definidas sobre $\mathbb{Z}/p\mathbb{Z}$ para todo primo p. Vamos a notar entonces $E^d(\mathbb{Z}/p\mathbb{Z})$ y $\tilde{E}^d(\mathbb{Z}/p\mathbb{Z})$ a los puntos de las curvas sobre estos cuerpos.

Definición 1.2.3. Si K es un cuerpo de característica distinta de 2 y $f \in K[X]$ es un polinomio de grado 3, sin raíces múltiples en ninguna extensión L/K, decimos que la curva plana $E : y^2 = f(x)$ es una *curva elíptica* sobre K.

Cuando la característica de K es dos la definición de curva elíptica requiere considerar ecuaciones algo más complicadas. Nuestras curvas E^d son entonces curvas elípticas sobre $\mathbb{Q}$. Más aún, tenemos:

Lema 1.2.4. *Si $p \nmid 2d$, entonces E^d define una curva elíptica sobre $\mathbb{Z}/p\mathbb{Z}$.*

Demostración. Reduciendo $f(x) = x^3 - d^2x = x(x-d)(x+d)$ módulo p, vemos que este polinomio sigue teniendo todas sus raíces simples siempre que $d \not\equiv -d \pmod{p}$, i.e. siempre que $p \neq 2$, y $p \nmid d$. □

Otra observación importante es que las curvas elípticas contienen un único punto en el infinito, al que vamos a denotar **O**:

Lema 1.2.5. *Si $E : y^2 = f(x)$ es una curva elíptica entonces su único punto proyectivo (x, y, z) con $z = 0$ es $(0, 1, 0)$.*

Demostración. Si $f(x) = ax^3 + bx^2 + cx + d$ entonces la ecuación homogeneizada es:

$$y^2z = ax^3 + bx^2z + cxz^2 + dz^3,$$

y poniendo $z = 0$ obtenemos $ax^3 = 0$, de donde se deduce inmediatamente lo que queremos. □

Dados dos puntos de una curva elíptica podemos obtener otro de manera geométrica. Si trazamos la recta que pasa por estos dos puntos, como la curva está definida por una ecuación de grado 3, uno esperaría que esta recta intersecte a la curva en un tercer punto. Esta idea permite definir en una curva elíptica una estructura de grupo: dados dos puntos distintos, si la recta que pasa por estos interseca a la curva en un tercer punto (x, y), definimos su suma como el punto $(x, -y)$. En general la recta va a intersecar a la curva en tres puntos *contados con multiplicidad* en el plano proyectivo, por lo que la descripción anterior no es enteramente satisfactoria. Definimos entonces la estructura de grupo en los puntos proyectivos de una curva elíptica de la siguiente manera:

Definición 1.2.6. Dada E una curva elíptica sobre K, y $P_1, P_2 \in \tilde{E}(L)$, con $P_i = (a_i, b_i, 1)$ definimos su suma $P_1 + P_2$ como:

1. Si alguno de los dos puntos es **O**, entonces definimos la suma como el otro de los dos puntos.

2. Cuando P_1 es distinto de P_2 consideramos la recta que pasa por estos dos puntos, parametrizada como $P(t) = (a_1, b_1, 1) + t(a_2 - a_1, b_2 - b_1, 0)$. Denotando $F(x, y) = f(x) - y^2$, consideramos el polinomio $g(t) = F \circ P(t)$, que tiene como ceros a 0 y a 1. Si $a_1 = a_2$, y entonces $b_1 \neq b_2$, g resulta un polinomio cuadrático en t, 0 y 1 son sus únicas raíces, y definimos $P_1 + P_2 = \mathbf{O}$. Si a_1 y a_2 no son iguales g resulta un polinomio de grado tres; como tiene dos raíces se factoriza completamente como $g(t) = t(t-1)(t-\lambda)$, y si $P(\lambda) = (a_3, b_3, 1)$ definimos $P_1 + P_2 = (a_3, -b_3, 1)$.

3. Si $P_1 = P_2$ consideramos la recta parametrizada $P(t) = (a_1, b_1, 1) + t(2b_1, f'(a_1), 0)$, y el polinomio $g(t) = F \circ P(t)$. En este caso tenemos que 0 es raíz de g; calculando su derivada vemos que de hecho es doble. En el caso tengamos $b_1 = 0$ tenemos que el polinomio es cuadrático y por lo tanto su única raíz es 0; en este caso tomamos $P_1 + P_2 = \mathbf{O}$. Si $b \neq 0$ g es de grado 3 y lo podemos factorizar como $g(t) = t^2(t - \lambda)$; si $P(\lambda) = (a_3, b_3, 1)$ definimos igual que antes $P_1 + P_2 = (a_3, -b_3, 1)$.

Es claro que la definición que hicimos para la suma es simétrica, tiene neutro $\mathbf{O}$, y todo elemento tiene un inverso: $(a, b) + (a, -b) = \mathbf{O}$. Para terminar de ver que esto define una estructura de grupo abeliano queda ver la asociatividad de esta suma. Una demostración elemental de este hecho como consecuencia del teorema de Cayley-Bacharach se puede ver en [ST94, Capítulo 1]. En consecuencia tenemos el siguiente teorema:

Teorema 1.2.7. *Si E es una curva elíptica sobre K, entonces $\tilde{E}(L)$ es un grupo abeliano para toda extensión L/K.*

Más aún, de nuestra descripción para la fórmula de adición, se ve que dada una curva elíptica podemos despejar el λ que aparece en la definición como una función racional de las componentes de los puntos P_1 y P_2, y por lo tanto las coordenadas de $P_1 + P_2$ también son de ésta forma. Esto quiere decir que las curvas elípticas son lo que se conoce como un *grupo algebráico*. Estas funciones racionales son expresiones en los coeficientes de la ecuación de la curva E que se pueden encontrar explícitamente. Una observación inmediata de la definición es que los puntos de orden 2 son precisamente los que tienen segunda coordenada 0.

En el caso de que la curva E está definida sobre $\mathbb{Q}$, como es el caso de las curvas E^d que nos interesan, se puede decir más sobre la estructura de este grupo. Concretamente se tienen el siguiente resultado de Mordell:

Teorema 1.2.8 (Mordell)**.** *Si E es una curva elíptica sobre $\mathbb{Q}$ entonces $\tilde{E}(\mathbb{Q})$ es un grupo finitamente generado.*

Definición 1.2.9. Dada una curva elíptica E definida sobre $\mathbb{Q}$ tenemos por el teorema de Mordell que $E(\mathbb{Q}) = E_{\text{tor}}(\mathbb{Q}) \oplus \mathbb{Z}^k$, con $E_{\text{tor}}(\mathbb{Q})$ un grupo finito. Definimos el *rango* de $E(\mathbb{Q})$ como k.

El resultado anterior se demuestra como vía un resultado de descenso. Concretamente se tiene el siguiente enunciado general:

Teorema 1.2.10 (Teorema del descenso)**.** *Sea G un grupo conmutativo tal que existe una función $h : G \to [0, \infty)$ que cumple:*

1. *Los conjuntos $\{P \in G : h(P) < M\}$ son finitos.*
2. *Para cada $P_0 \in G$, existe $\kappa_0 > 0$ tal que:*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \qquad \forall P \in G.$$

3. *Existe* $\kappa > 0$ *tal que:*

$$h(2P) \geq 4h(P) - \kappa \qquad \forall P \in G.$$

Si existe $m \in \mathbb{N}$ *tal que* $G/(mG)$ *es finito entonces* G *es finitamente generado.*

Una demostración completa de este resultado, y del teorema de Mordell, se puede ver en [ST94, Capítulo 3]. La función h que se tiene en nuestro caso es esencialmente el máximo de los denominadores y numeradores que aparecen en las coordenadas del punto, esta denominada *altura* es lo que da la noción de complejidad que mencionabamos al principio del capítulo. Ver que esta función satisface las hipótesis del enunciado es relativamente directo; la mayor dificultad de la demostración está en probar que $G/(2G)$ resulta un grupo finito cuando G es el grupo de puntos racionales de una curva elíptica.

Cabe destacar que el resultado anterior no da un método efectivo para encontrar generadores del grupo o acotar la altura de los mismos, y entender el rango de una curva elíptica es un problema díficil. La parte de torsión de la curva elíptica por otro lado está bien entendida: hay algoritmos que permiten calcularla y pertenece a un conjunto finito de grupos posibles; este es un resultado de Mazur. En nuestro caso particular la torsión de $E^d(\mathbb{Q})$ puede entenderse con métodos bastante sencillos. Para esto demostramos primero el siguiente lema:

Lema 1.2.11. *Si* $p \nmid 2d$ *y* $p \equiv 3 \pmod 4$, *entonces* $\tilde{E}^d(\mathbb{Z}/p\mathbb{Z})$ *tiene* $p+1$ *elementos.*

Demostración. Por cada $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0, \pm d\}$ para el cual $f(x)$ es un cuadrado módulo p obtenemos dos puntos de $E^d(\mathbb{Z}/p\mathbb{Z})$, uno por cada solución de $y^2 = f(x)$. Por otro lado como f es impar, $f(x)$ es un cuadrado si y sólo si $f(-x)$ no lo es, ya que $p \equiv 3 \pmod 4$ implica que -1 no es un cuadrado. Es decir que la mitad de estos $p-3$ elementos se corresponde con dos puntos de la curva, y la otra mitad no se corresponde con ninguno.

Si $x \in \{0, \pm d\}$ por otro lado tenemos que $f(x) = 0$ y hay un único punto de la curva cuya primera coordenada es x. Esto nos da otros tres puntos de la curva y junto $textbfO$ suman $p+1$ puntos en total. □

Teorema 1.2.12. *Los únicos puntos de torsión de* $E^d(\mathbb{Q}) : y^2 = x^3 - d^2x$ *sobre* $\mathbb{Q}$ *son* $\mathbf{O}, (0,0,1)$ *y* $(\pm d, 0, 1)$, *i.e. el neutro* $\mathbf{O}$ *y los puntos afines que cumplen* $y = 0$.

A continuación damos un bosquejo de la demostración; una referencia donde se puede encontrar esta demostración en detalle es [Kob93, Sección 1.9].

Demostración. Vamos a definir una función $\phi_p : \tilde{E}^d(\mathbb{Q}) \to \tilde{E}^d(\mathbb{Z}/p\mathbb{Z})$ para cada primo p. Este morfismo es esencialmente la reducción módulo p, pero para poder darle sentido a esto primero hay que observar algún detalle. Dado un punto $(a,b,c) \in \mathbb{P}^2(\mathbb{Q})$ hay una única terna de enteros coprimos, a menos de signo, (a',b',c') que define el mismo elemento que (a,b,c) en $\mathbb{P}^2(\mathbb{Q})$. Como p no puede dividir a los tres elemntos simultáneamente esta terna define un elemento $([a'],[b'],[c']) \in \mathbb{P}^2(\mathbb{Z}/p\mathbb{Z})$, definimos entonces $\phi_p((a,b,c)) = ([a'],[b'],[c'])$.

Cuando $p \nmid 2d$, la reducción de E^d módulo p resulta también una curva elíptica, Lema 1.2.4, y en estos casos la aplicación que definimos resulta un morfismo de grupos, i.e. $\phi_p(P_1+P_2) = \phi_p(P_1)+\phi_p(P_2)$. Cuando $P_1 = P_2$, $P_1 \neq P_2$ y $\phi_p(P_1) \neq \phi_p(P_1)$ ó alguno de los dos puntos es $\mathbf{O}$, esto se deduce de que la suma se expresa como funciones racionales de los puntos. Como la curva tiene los mismos coeficientes módulo p, estas funciones racionales tienen las mismas expresiones sobre $\mathbb{Q}$ y sobre $\mathbb{Z}/p\mathbb{Z}$. Se puede verificar que esto sigue valiendo en los restantes casos.

Dados dos puntos P_1, P_2 de $E^d(\mathbb{Q})$ tomamos $\tilde{P}_i = (a_i, b_i, c_i)$, $i = 1, 2$, las ternas de enteros que usamos para definir la función ϕ_p. Se puede ver entonces que P_1 y P_2 tienen la misma imágen por la aplicación ϕ_p si y sólo p divide a todas las componentes del producto cruz $\tilde{P}_1 \times \tilde{P}_2$. Como el subgrupo de torsión de $E^d(\mathbb{Q})$ es finito por el teorema de Mordell, podemos considerar N el mínimo común múltiplo de todas las componentes de los productos cruz de todos los pares de puntos de torsión de $E^d(\mathbb{Q})$. Si p no divide a N ni a $2d$, esto nos dice que ϕ_p es un morfismo inyectivo de $E^d_{\text{tor}}(\mathbb{Q})$ en $E^d(\mathbb{Z}/\mathbb{Z})$. Pero en particular esto nos dice que para todo primo $p \equiv 3 \pmod 4$ mayor que N y que $2d$, el orden de la torsión de $E^d(\mathbb{Q})$ debe dividir a $p+1$, el orden de la curva módulo p.

Para poder terminar la demostración basta observar que orden de $E^d_{\text{tor}}(\mathbb{Q})$ es un divisor de 4. En efecto supongamos que q es un primo distinto de 2 que divide al orden de $E^d_{\text{tor}}(\mathbb{Q})$. Por el teorema de Dirichlet existen infinitos primos p que satisfacen simultáneamente $p+1 \equiv 0 \pmod 4$ y $p \equiv 0 \pmod q$. Tomando un primo p que satisface esto y es mayor que N vemos que el orden de $E^d_{\text{tor}}(\mathbb{Q})$ debe dividir $p+1$, lo que es absurdo porque q no divide a este número. □

Habiendo caracterizado la torsión de los puntos racionales de las curvas E^d vemos que se tiene la siguiente caracterización de los números congruentes:

Corolario 1.2.13. *Un entero positivo d es congruente si y sólo si $E^d(\mathbb{Q})$ tiene rango positivo.*

Demostración. Por el Teorema 1.1.3, d es un número congruente si y sólo si $E^d(\mathbb{Q})$ tiene puntos (x, y) con $y \neq 0$. Ahora los de $E^d(\mathbb{Q})$ puntos con segunda coordenada nula, concretamente $(\pm d, 0)$ y $(0, 0)$, de son, por el teorema anterior, precisamente los puntos de torsión de esta curva. Es decir que $E^d(\mathbb{Q})$ tiene puntos con segunda coordenada no nula si y sólo si tiene rango positivo. □

1.3. L-serie de una curva elíptica

Hasta ahora vimos que el problema de decidir si un número d libre de cuadrados es congruente es equvialente a ver si la curva $E^d(\mathbb{Q})$ tiene rango postivo. El siguiente paso es traducir este problema en uno analítico. Para esto necesitamos definir las L-series asociadas al curvas elípticas E^d.

Definición 1.3.1. Para cada curva elíptica E^d y cada primo p que no divide a $2d$ denotamos $a_p = a_p(E^d) = p - |E^d(\mathbb{Z}/pZ)|$. La *$L$-serie* asociada a esta curva elíptica es la serie

de Dirichlet:

$$L(E^d, s) = \prod_{p \nmid 2d} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \tag{1.3.1}$$

Cada una de los factores de el producto se denomina el *factor local en el primo* p.

Observación 1.3.2. A una curva elíptica E en general se le puede asignar un número entero, su *conductor* $N(E)$. Este número satisface que los primos que lo dividen son precisamente los primos para los que la curva E módulo p no es una curva elíptica, se dice que E tiene *mala reducción* en estos primos; los restantes primos se dicen de *buena reducción*. Para los primos de buena reducción se definen los factores locales en términos de la cantidad de soluciones módulo p como lo definimos para las curvas E^d. Para los primos de mala reducción por otro lado se definen los coeficientes a_p de otro modo; en el caso de las curvas E^d estos resultan ser 0. La forma general de la L-serie de una curva E elíptica es:

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

Como cada uno de los factores locales es una función racional en p^{-s}, lo podemos desarrollar como serie de potencias en esta variable, y luego desarrollando el producto infinito (1.3.1) se ve que $L(E^d, s)$ es efectivamente una serie de Dirichlet. Esto quiere decir que tiene un desarrollo, por lo menos formal, de la forma: $L(E^d, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$. Para la cantidad de soluciones de una curva elíptica módulo p se tienen las denominadas cotas de Hasse, que aseguran que $|a_p| \leq 2\sqrt{p}$, de donde se deduce que la L-serie de una curva elíptica converge de manera uniforme sobre compactos cuando $\Re(s) > 3/2$, por lo que en esta región la serie define una función holomorfa.

Definición 1.3.3. Sean E una curva elíptica sobre $\mathbb{Q}$, definida por la ecuación: $y^2 = f(x)$, y D un entero. El *twist cuadrático* de E, es la curva E^D definida por la ecuación $Dy^2 = f(x)$.

Si $f(x) = x^3 + ax^2 + bx + c$, podemos hacer el cambio de variables $\tilde{y} = y/D$, $\tilde{x} = Dx$, para obtener que la ecuación del twist cuadrático de E por D es equivalente a $\tilde{y}^2 = x^3 + D^3ax^2 + D^2bx + Dc$, por lo que es también una curva elíptica. Más aún, este cambio de variables sigue siendo válido para las curvas módulo p, cuando p es un primo que no divide a D. Nuestras curvas E^d son entonces isomorfas, sobre $\mathbb{Q}$ y módulo p para todo primo que no divide a $2d$, a los twists cuadráticos de la curva $E = E^1$ definida por la ecuación $y^2 = x^3 - x$. En particular, estas curvas tienen las mismas L-series.

Veamos ahora como se relacionan las L-series de una curva elíptica y de sus twists.

Proposición 1.3.4. *Sean E una curva elíptica, D un entero positivo y p un primo que no lo divide. Se tiene que:*

$$a_p(E^D) = a_p(E) \left(\frac{D}{p}\right),$$

donde $\left(\frac{m}{n}\right)$ es el símbolo de Kronecker, la extensión del símbolo de Lagrange a $\mathbb{Z}$.

Demostración. Tomemos $y^2 = f(x)$ la ecuación de E. Observemos primero que podemos dar una expresión explícita para la camtidad de soluciones de una curva elíptica módulo p. Si $x \in \mathbb{Z}/p\mathbb{Z}$, entonces la cantidad de puntos de $E(\mathbb{Z}/p\mathbb{Z})$ que tienen a x como primera coordenada es 1 si $f(x) = 0$, 2 si $f(x)$ es un cuadrado no nulo y 0 si $f(x)$ no es un cuadrado. En cualquier caso hay exactamente $\left(\frac{f(x)}{p}\right) + 1$ puntos cuya primera coordenada es x. Luego:

$$|E(\mathbb{Z}/p\mathbb{Z})| = \sum_x \left(\left(\frac{f(x)}{p}\right) + 1\right) = p + \sum_x \left(\frac{f(x)}{p}\right).$$

Por otro lado el mismo argumento aplicado al twist nos dice que la cantidad de soluciones con primera coordenada igual a x depende de si $f(x)D^{-1}$, o equivalentemente $f(x)D$, es un cuadrado módulo p. Tenemos entonces:

$$|E^D(\mathbb{Z}/p\mathbb{Z})| = \sum_x \left(\left(\frac{f(x)D}{p}\right) + 1\right) = p + \sum_x \left(\frac{f(x)D}{p}\right).$$

Para verificar que $a_p(E)\left(\frac{D}{p}\right) = a_p(E^D)$ basta ver que:

$$\left(\frac{D}{p}\right)|E(\mathbb{Z}/p\mathbb{Z})| - |E^D(\mathbb{Z}/p\mathbb{Z})| = \left(\left(\frac{D}{p}\right) - 1\right)p.$$

Desarrollando el lado izquierdo obtenemos:

$$\begin{aligned}\left(\frac{D}{p}\right)|E(\mathbb{Z}/p\mathbb{Z})| - |E^D(\mathbb{Z}/p\mathbb{Z})| &= \left(\frac{D}{p}\right)(p + \sum_x \left(\frac{f(x)}{p}\right)) - p + \sum_x \left(\frac{f(x)D}{p}\right) \\ &= \left(\left(\frac{D}{P} - 1\right)\right)p + \sum_x \left(\frac{D}{p}\right)\left(\frac{f(x)}{p}\right) - \left(\frac{Df(x)}{p}\right) \\ &= \left(\left(\frac{D}{p}\right) - 1\right)p.\end{aligned}$$

□

Lema 1.3.5. *Sea $P(X) = 1 - a_pX + pX^2 \in \mathbb{Q}[X]$ y $\sum_{k=0}^{\infty} b_kX^k$ su inversa en $\mathbb{Q}[[X]]$. Entonces los coeficientes b_k están definidos por la recurrencia:*

$$b_0 = 1 \quad ; \quad b_1 = a_p \quad ; \quad b_{k+1} = b_ka_p - pa_{k-1}.$$

Demostración. Sea $S(X)$ la serie cuyos coeficientes están dados por la recurrencia ante-

rior. Calculemos entonces el producto:

$$\begin{aligned} S(X)P(X) &= S(X)(1 - a_pX + pX^2) = S(x) - a_pXS(X) + pX^2S(X) \\ &= \sum_{k=0}^{\infty} b_kX^k - \sum_{k=0}^{\infty} a_pb_kX^{k+1} + \sum_{k=0}^{\infty} pb_kX^{k+2} \\ &= \sum_{k=0}^{\infty} b_kX^k - \sum_{k=1}^{\infty} a_pb_{k-1}X^k + \sum_{k=2}^{\infty} pb_{k-2}X^k \\ &= b_0 + (b_1 - a_pb_0)X + \sum_{k=2}^{\infty} (b_k - a_pb_{k-1} + pb_{k-2})\, X^k \\ &= 1. \end{aligned}$$

□

Proposición 1.3.6. *Si* $L(E^1, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, *entonces* $L(E^d, s) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \frac{a_n}{n^s}$.

Demostración. Sea $b_n = \left(\frac{d}{n}\right) a_n$. Si p es un primo que divide a $2d$ entonces $b_p^k = 0$. Si $p = 2$ esto es porque $a_n = 0$, y si $p \neq 2$ es porque el símbolo de Jacobi es 0. Por otro lado si p es un primo que no divide a $2d$ usando la recurrencia para los coeficientes a_n tenemos:

$$\begin{aligned} \left(\frac{d}{p^{k+1}}\right) a_{p^{k+1}} &= \left(\frac{d}{p^{k+1}}\right) a_{p^k} a_p - \left(\frac{d}{p^{k+1}}\right) p a_{p^{k-1}} \\ &= \left(\left(\frac{d}{p^k}\right) a_{p^k}\right) \left(\left(\frac{d}{p}\right) a_p\right) - \left(\frac{d}{p}\right)^2 p \left(\left(\frac{d}{p^{k-1}}\right) a_{p^{k-1}}\right) \\ &= \left(\left(\frac{d}{p^k}\right) a_{p^k}\right) \left(\left(\frac{d}{p}\right) a_p\right) - p \left(\left(\frac{d}{p^{k-1}}\right) a_{p^{k-1}}\right), \end{aligned}$$

es decir:

$$b_{p^k+1} = b_{p^k} b_p - p b_{p^k-1}.$$

Esto nos dice que los coeficientes b_{p^k} satisfacen las recurrencias del lema previo, y como además son multiplicativos tenemos, por la Proposición 1.3.4:

$$\sum_{n=1}^{\infty} \frac{b_n}{n^s} = \prod_{p \nmid 2d} \frac{1}{1 - b_p p^s + p^{1-2s}} = \prod_{p \nmid 2d} \frac{1}{1 - \left(\frac{d}{p}\right) a_p p^s + p^{1-2s}} = L(E^d, s).$$

□

Como dijimos antes se puede ver que las L-series asociadas a curvas elípticas convergen de manera absoluta y uniforme sobre compactos del semiplano $\Re(s) > 3/2$, y definen entonces funciones holomorfas en este dominio. Haciendo una analogía con la función zeta de Riemann a uno le gustaría que estas series L admitan una extensión

analítica a funciones, por lo menos meromorfas, en todo $\mathbb{C}$, y que estas extensiones satisfagan alguna ecuación funcional. Como dijimos en la introducción obtener este tipo de resultados suele ser difícil. En el próximo capítulo vamos a introducir las formas modulares, a las que vamos a asociar series de Dirichlet satisfacen estas propiedades, y nos van a permitir obtener estas propiadedes para las L-series de curvas elípticas.

Capítulo 2

Formas modulares de peso entero

2.1. El grupo modular y el semiplano de Poincaré

Definición 2.1.1. El grupo $\mathrm{SL}_2(\mathbb{Z})$ se denomina el *grupo modular*. Notamos $\mathrm{PSL}_2(\mathbb{Z})$ al cociente del grupo modular por su centro, concretamente $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm \mathrm{Id}\}$.

El algoritmo de división nos permite entender la estructura del grupo modular, como podemos ver en los siguientes resultados.

Proposición 2.1.2. $\mathrm{SL}_2(\mathbb{Z})$ *está generado por las siguientes dos matrices:*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Demostración. Notemos que se tienen las siguientes identidades:

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \qquad T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix},$$

$$, S^2 = -\mathrm{Id}, \qquad S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}.$$

Tomemos entonces $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Vamos a probar por inducción en el valor absoluto de c que γ pertenece al subgrupo generado por S y T. Si $c = 0$ se tiene que $ad = 1$, y por lo tanto $a = d = \pm 1$. Es decir que $\gamma = \pm T^n$ para algún $n \in \mathbb{Z}$ y esto nos asegura lo que queremos.

En caso contrario, por el algoritmo de división existen $q \in \mathbb{Z}$ y $0 \leq r < |c|$ tales que $a = qc + r$. Entonces aplicando las identidades que notamos al principio tenemos que:

$$ST^{-q}\gamma = S \begin{pmatrix} a - qc & b - qd \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ r & b - qd \end{pmatrix}.$$

Como el valor absoluto r es menor que el de c, esta matriz se escribe como productos de S, T o sus inversos y despejando obtenemos que γ se encuentra entonces en el subgrupo generado por estas matrices. □

Observación 2.1.3. El proceso inductivo de la demostración anterior está esencialmente aplicando el algoritmo de Euclides a a y c para obtener una matriz que en la esquina superior derecha tiene a su máximo común divisor. Como γ pertenece al grupo modular a y c deben ser coprimos y por lo tanto obtenemos finalmente una potencia de T, a menos del signo.

Observación 2.1.4. Consideremos las matrices S y ST. Se puede verificar fácilmente que $(ST)^3 = -\mathrm{Id}$, y ya observamos que $S^2 = -\mathrm{Id}$. Del resultado anterior se deduce que estas dos matrices de orden finito generan el grupo modular. Más aún se puede probar que lo generan de manera casi libre. Concretamente el morfismo $\phi : C_2 * C_3 \to \mathrm{PSL}_2(\mathbb{Z})$, definido por $\phi((x_1, 1)) = [S]$ y $\phi((1, x_2)) = [T]$, donde x_1 y x_2 son los generadores C_2 y C_3 respectivamente, es un isomorfismo.

Definición 2.1.5. Dado $n \in \mathbb{N}$ el *subgrupo de congruencia principal de nivel* n se define como:

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

Decimos que un subgrupo $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ es un *subgrupo de congruencia* si contiene algún subgrupo de congruencia principal, y el mínimo n tal que $\Gamma(n) < \Gamma$ se denomina el *nivel* de Γ. Introducimos la siguiente notación para ciertos subgrupos de especial importancia:

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{n} \right\},$$
$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod{n}, c \equiv 0 \pmod{n} \right\}.$$

Si notamos $\pi_n : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ al morfismo de reducción módulo n, entonces $\Gamma(n)$ es el núcleo de π_n, $\Gamma_0(n)$ es la preimagen de las matrices triangulares superiores, y $\Gamma_1(n)$ es la preimagen de las matrices estrictamente triangulares superiores. En particular esto nos asegura que $\Gamma(n)$, $\Gamma_0(n)$ y $\Gamma_1(n)$ son efectivamente subgrupos de $\mathrm{SL}_2(\mathbb{Z})$. Más aún como $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ es un grupo finito podemos afirmar que estos subgrupos, y en general todos los subgrupos de congruencia, tienen índice finito en el grupo modular.

Para poder calcular los índices de estos subgrupos vamos a intentar entender mejor los morfismos π_n y los grupos $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Lema 2.1.6. *El morfismo $\pi_n : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ es sobreyectivo.*

Demostración. Sea $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ tal que $\det(\gamma) = ad - bc \equiv 1 \pmod{n}$. Observemos que esto nos asegura que el máximo común divisor de los conjuntos $\{c, d, n\}$ es uno. Escribimos $c = \tilde{c}(c : n)$, tenemos que en particular $(\tilde{c} : n) = 1$ y podemos tomar entonces x un inverso multiplicativo de n módulo $\tilde{c}$. Entonces consideramos $d' = d + (1 - d)xn$. Es claro que $d' \equiv 1 \pmod{n}$, y en particular d' y $\tilde{c}$ son coprimos. Ahora si p es un primo que divide tanto a d' como a $c = \tilde{c}(c : n)$, debe ser que entonces

$p|(c:n)$, pero de la expresión que tenemos para d' es claro que esto implica que p divide a todos los elementos de $\{c, d, n\}$, lo que es absurdo. Es decir que d' y c son coprimos. Tenemos entonces que para todo $k, l \in \mathbb{Z}$ vale:

$$\begin{pmatrix} a+kn & b+ln \\ c & d' \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{n}.$$

Buscamos entonces una matriz de esta forma con determinante 1, es decir que satisfaga la ecuación:

$$d'(a+kn) - c(b+ln) = (d'a - cb) + n(d'k - cl) = 1.$$

Ahora como $d'a - cb \equiv 1 \pmod{n}$ existe $t \in \mathbb{Z}$ tal que $(d'a - cb) + tn = 1$. Y como $(d' : c) = 1$ existen k y l tales que $d'k - cl = t$, y esto es exactemente lo que buscamos. □

Observación 2.1.7. El resultado anterior nos permite dar otra descripción de los subgrupos de congruencia. Como $\Gamma(n) = \ker(\pi_n)$ los subgrupos de $\mathrm{SL}_2(\mathbb{Z})$ que contienen a $\Gamma(n)$ son precisamente las preimágenes de los subgrupos de $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. Pero por el resultado anterior tenemos que, más aún, hay una correspondencia uno a uno entre ambas coas.

Lema 2.1.8. *El orden de* $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ *es* $n^3 \prod_{p|n} \left(1 - \frac{1}{p^2}\right)$.

Demostración. Primero notemos que el teorema chino del resto tenemos un isomorfismo: $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \simeq \prod_{p|n} \mathrm{SL}_2\left(\mathbb{Z}/p^{\nu_p(n)}\mathbb{Z}\right)$, por lo que alcanza con demostrar el enunciado suponiendo que $n = p^\alpha$ para algún primo p. Procedemos entonces por inducción en α.

Si α es 1, $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, y la cantidad de elementos de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ se puede conseguir contando la cantidad de bases ordenadas de $(\mathbb{Z}/p\mathbb{Z})^2$. Para el primer elemento de una base podemos elegir cualquier elemento no nulo del espacio y para el segundo cualquiera que no se encuentre en el generado por el primero. Por lo tanto tenemos:

$$\begin{aligned} |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| &= (p^2-1)(p^2-p) \\ &= p^3\left(1 - \frac{1}{p^2}\right)(p-1). \end{aligned}$$

Por otro lado la función $\gamma \mapsto \left(\begin{smallmatrix} k & 0 \\ 0 & 1 \end{smallmatrix}\right)\gamma$ da una biyección entre $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ y las matrices de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ con determinante k. Como hay exactamente $p-1$ posibles determinantes tenemos que $|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})| = p^3\left(1 - \frac{1}{p^2}\right)$ como queríamos.

Si $\alpha > 1$, consideramos el morfismo $\phi : \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^{\alpha-1}\mathbb{Z})$ de reducción módulo $p^{\alpha-1}$. Como $\pi_{p^{\alpha-1}}$ se factoriza por este morfismo, ϕ debe ser también suryectivo y por lo tanto tenemos que $|\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z})| = |\ker(\phi)||\mathrm{SL}_2(\mathbb{Z}/p^{\alpha-1}\mathbb{Z})|$. Tenemos que calcular entonces el orden del núcleo de ϕ. Si $\gamma \in \ker(\phi)$, entonces tenemos que:

$$\gamma = \begin{pmatrix} 1 + k_1 p^{\alpha-1} & k_2 p^{\alpha-1} \\ k_3 p^{\alpha-1} & 1 + k_4 p^{\alpha-1} \end{pmatrix}, \qquad 0 \le k_i < p.$$

Observemos que en tal caso $\det(\gamma) \equiv 1 + (k_1 + k_4) \pmod{p^\alpha}$. Luego para que γ tenga determinante 1 la única condición es $k_1 + k_4 \equiv 0 \pmod{p}$, y por lo tanto hay p^3 elementos en el núcleo de ϕ. Luego de la hipótesis inductiva se deduce lo que buscamos. □

Como corolario de estos resultados podemos obtener los índices de los grupos de congruencia que definimos antes en $\mathrm{SL}_2(\mathbb{Z})$:

Proposición 2.1.9. *Si $n \in \mathbb{N}$ entonces:*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(n)] = n^3 \prod_{p|n} \left(1 - \frac{1}{p^2}\right),$$
$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(n)] = n^2 \prod_{p|n} \left(1 - \frac{1}{p^2}\right),$$
$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n)] = n \prod_{p|n} \left(1 + \frac{1}{p}\right).$$

Demostración. Como $\Gamma(n)$ es el núcleo de π_n y este morfismo es suryectivo, el índice de $\Gamma(n)$ en $\mathrm{SL}_2(\mathbb{Z})$ coincide con el orden del cociente, que ya calculamos y es exactamente lo queremos.

Notemos que $\phi : \Gamma_1(n) \to \mathbb{Z}/n\mathbb{Z}$, definido por $\phi\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) = b$ es un morfismo de grupos suryectivo; más aún su núcleo es precisamente $\Gamma(n)$. Esto nos dice que $[\Gamma_1(n) : \Gamma(n)] = n$. Pero entonces aplicando el teorema de Lagrange tenemos que:

$$\begin{aligned}
[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] &= [\mathrm{SL}_2(Z) : \Gamma(n)][\Gamma_1(n) : \Gamma(n)]^{-1} \\
&= n^3 \prod_{p|n} \left(1 - \frac{1}{p^2}\right) n^{-1} \\
&= n^2 \prod_{p|n} \left(1 - \frac{1}{p^2}\right)
\end{aligned}$$

Por último para $\Gamma_0(n)$ consideramos el morfismo $\psi : \Gamma_0(n) \to (\mathbb{Z}/n\mathbb{Z})^\times$ definido por $\psi\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) = d$. Este morfismo es suryectivo y tiene núcleo precisamente $\Gamma_1(n)$. Por lo tanto $[\Gamma_0(n) : \Gamma_1(n)] = \varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$. Al igual que antes aplicando el teorema de lagrange podemos despejar el índice de $\Gamma_0(n)$:

$$\begin{aligned}
[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] &= [\mathrm{SL}_2(Z) : \Gamma_1(n)][\Gamma_0(n) : \Gamma_1(n)]^{-1} \\
&= \left(n^2 \prod_{p|n} \left(1 - \frac{1}{p^2}\right)\right) \left(n \prod_{p|n} \left(1 - \frac{1}{p}\right)\right)^{-1} \\
&= n \prod_{p|n} \left(1 + \frac{1}{p}\right)
\end{aligned}$$

□

Definición 2.1.10. El *semiplano de Poincaré* ó *semiplano superior* es el subconjunto de números complejos con parte imaginaria estrictamente positiva, i.e. $\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. El *semiplano de Poincaré extendido* se define como $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$. Los racionales junto con $i\infty$ se denominanan las *cúspides*. Denotamos $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, y consideramos $\mathcal{H}^* \subset \hat{\mathbb{C}}$ identificando $i\infty$ e ∞.

El grupo $\mathrm{GL}_2(\mathbb{C})$ actúa en $\hat{\mathbb{C}}$ por homografías, es decir $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z = \frac{az+b}{cz+d}$; las matrices que actúan trivialmente son precisamente las matrices escalares y por lo tanto esta acción factoriza por una acción de $\mathrm{PGL}_2(\mathbb{C})$. Esta acción se restringe a una de $\mathrm{GL}_2(\mathbb{R})$ en $\mathcal{H}$ y por lo tanto a una acción de $\mathrm{SL}_2(\mathbb{Z})$. Más aún la acción de SL_2 se extiende a una en el semiplano de Poincaré extendido.

Definición 2.1.11. Dado un grupo subgrupo discreto $\Gamma < \mathrm{GL}_2(\mathbb{R})$ un *dominio fundamental* para Γ es un subconjunto cerrado, conexo y con interior conexo $\mathcal{F} \subset \mathcal{H}$ que contiene por lo menos un representante de cada órbita de la acción de Γ, no tiene dos puntos interiores en una misma órbita, y cuyo borde es una unión de finitas curvas suaves.

Teorema 2.1.12. *El conjunto* $\mathcal{F} = \{z \in \mathcal{H} : -1/2 \leq \Re(z) \leq 1/2, |z| \geq 1\}$ *es un dominio fundamental para el grupo modular.*

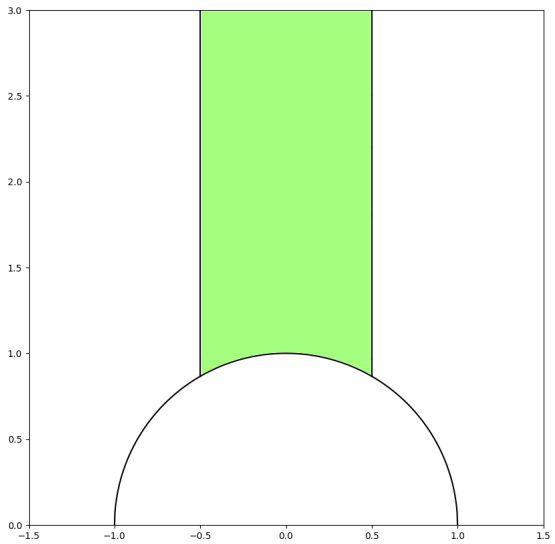

Figura 2.1: El dominio fundamental $\mathcal{F}$.

Demostración. Es claro que $\mathcal{F}$ es cerrado, conexo y con interior conexo. Más aún el borde de $\mathcal{F}$ es la unión de dos semirrectas y un arco de circunferencia. Esto quiere decir que las condiciones topológicas para que sea un dominio fundamental se satisfacen. Dado

$z \in \mathcal{H}$, se tiene que para cada $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ vale:

$$\begin{aligned} \gamma z = \frac{az+b}{cz+d} &= \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2} \\ &= \frac{ac|z|^2 + adz + bc\bar{z} + bd}{|cz+d|^2} \end{aligned}$$

y tomando la parte imaginaria:

$$\begin{aligned} \Im(\gamma z) &= \frac{\Im(adz + bc\bar{z})}{|cz+d|^2} \\ &= \frac{(ad-bc)\Im(z)}{|cz+d|^2} \\ &= \frac{\Im(z)}{|cz+d|^2} \end{aligned} \tag{2.1.1}$$

Si $|cz+d| \leq 1$ entonces $|\Im(cz+d)| \leq 1$, i.e. $|c\Im(z)| \leq 1$, es decir que hay sólo finitos posibles valores de c para los cuales $|cz+d|$ puede ser menor o igual a 1. Más aún una vez fijado c sólo hay finitos valores de d para los cuales se cumple la desigualdad. El conjunto de los pares (c,d) coprimos tales que $|cz+d| \leq 1$ es finito y no vacío, ya que el par $(0,1)$ siempre satisface estas condiciones. En particular de la ecuación (2.1.1) podemos concluir que existe $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ que hace que la parte imaginaria de γz sea maxima.Tomemos un tal γ, y supongamos además que $-1/2 \leq \Re(\gamma z) \leq 1/2$. Esto lo podemos suponer ya que en otro caso se puede reemplazar γ por una potencia apropiada T, pues $T^n z = z + n$. Afirmamos que $\gamma z \in \mathcal{F}$. En caso contrario tendríamos $|\gamma z| < 1$. Por otro lado $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \gamma z = -(\gamma z)^{-1}$ está en la órbita de z, y tomando $\gamma z = x+iy$ tenemos que $-(\gamma z)^{-1} = \frac{x-iy}{|x+iy|}$. Luego $\Im(\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \gamma z) = \frac{y}{|x+iy|} > y$, lo que contradice la maximalidad de γz.

Tenemos entonces que todos los puntos de $\mathcal{H}$ están en la órbita de un punto de $\mathcal{F}$. Tomemos ahora $z, w \in \mathcal{F}^{\mathrm{o}}$ y supongamos $\Im(z) \leq \Im(w)$. Observemos que como $z \in \mathcal{F}^{\mathrm{o}}$, tiene que valer que $\Im(z) = \sqrt{|z|^2 - \Re(z)^2} > \sqrt{1-(1/2)^2} = \sqrt{3}/2$. Ahora si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ y $\gamma z = w$, nuevamente por la ecuación (2.1.1) tiene que valer que $|cz+d| \leq 1$ y por lo tanto $|c\Im(z)| < 1$, que junto con la observación anterior nos dice que $|c| \leq 2/\sqrt{3}$, i.e. $c \in \{-1, 0, 1\}$.

Si $c = 0$ entonces $\gamma = \left(\begin{smallmatrix} \pm 1 & b \\ 0 & \pm 1 \end{smallmatrix}\right)$, y en cualquier caso γ actúa como una traslación por un número entero. Como z y w son puntos interiores $|\Re(w-z)| < 1$. Por lo tanto la única posibilidad en este caso es $\gamma = \pm \mathrm{Id}$ y $w = z$.

Resta verificar que sucede si $c = \pm 1$. Notemos que como $(-\gamma)z = \gamma z$, de modo que podemos suponer $c = 1$. Escribiendo $z = x + iy$, tenemos que:

$$1 \geq |z+d|^2 = (x+d)^2 + y^2 > (x+d)^2 + \frac{3}{4}$$

Y por lo tanto $|x+d| < 1/2$. Como d es entero y $|x| < 1/2$, por ser z un punto interior, tiene que valer que $d = 0$. Pero entonces $|cz+d| = |z| \leq 1$, y z no puede ser entonces interior. $\square$

A partir de un dominio fundamental para $\mathrm{SL}_2(\mathbb{Z})$ el siguiente resultado permite dar dominios fundamentales para cualquier subgrupo de índice finito $\Gamma < \mathrm{SL}_2(\mathbb{Z})$, a partir de un conjunto suficientemente bueno de representantes para sus coclases. En particular nos permite construir dominios fundamentales para los subgrupos de congruencia. Antes observemos que se tiene lo siguiente:

Lema 2.1.13. *Sea $\mathcal{F}$ es un dominio fundamental para Γ. Si $z \in \mathcal{F}^{\mathrm{o}}$ y $\gamma \in \Gamma$ son tales que $\gamma z = z$, entonces $\gamma = \pm \mathrm{Id}$.*

Demostración. Como γ actúa de manera continua podemos tomar U entorno abierto de z tal que $\gamma U \subset \mathcal{F}^{\mathrm{o}}$. Ahora como $\mathcal{F}$ es un dominio fundamental tiene que valer que γ actúa como la identidad en U. Como la acción de Γ en $\mathcal{H}$ es analítica, por el principio de identidad γ debe actuar como la identidad en todo $\mathcal{H}$ y por lo tanto $\gamma = \pm \mathrm{Id}$. □

Teorema 2.1.14. *Sea $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ un subgrupo de índice finito que contiene a $\{\pm \mathrm{Id}\}$. Si $\mathcal{F}$ es un dominio fundamental para $\mathrm{SL}_2(\mathbb{Z})$ y $g_1, \ldots, g_r$ dan un conjunto completo de representantes para las coclases de Γ en $\mathrm{SL}_2(\mathbb{Z})$, tales que $\mathcal{D} = \cup_{i=1}^{r} g_i^{-1}\mathcal{F}$ tiene interior conexo, entonces $\mathcal{D}$ es un dominio fundamental para Γ.*

Demostración. Como cada g_i actúa en $\mathcal{H}$ por difeomorfismos, el borde de cada $g_i^{-1}\mathcal{F}$ va a ser unión de finitas curvas suaves, y luego lo mismo sucede con el borde de $\mathcal{D}$. Similarmente se verifican las restantes condiciones topológicas.

Para ver que cualquier $z \in \mathcal{H}$ está en la Γ-órbita de un elemento de $\mathcal{D}$ observemos que como $\mathcal{F}$ es un dominio fundamental existe $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\gamma z \in \mathcal{D}$. Existen entonces $\gamma_1 \in \Gamma$ y $1 \leq k \leq r$ tales que $g_k\gamma_1 = \gamma$. Entonces:

$$g_k\gamma_1 z = \gamma z \in \mathcal{F},$$
$$\gamma_1 z \in g_k^{-1}\mathcal{F} \subset \mathcal{D}.$$

Es decir que z está en la Γ-órbita de un punto de $\mathcal{D}$.

Supongamos ahora que $z \in \mathcal{D}^{\mathrm{o}}$ y $\gamma \in \Gamma$ son tales que $\gamma z \in \mathcal{D}^{\mathrm{o}}$. Como γ actúa de manera continua existe U entorno abierto de z tal que $\gamma U \subset \mathcal{D}^{\mathrm{o}}$. Tomemos g_l de entre los representantes el que hace que $g_l z \in \mathcal{F}$. Si $V = g_l U \cap \mathcal{F}^{\mathrm{o}}$ entonces para cada $x \in V$ se tiene que $(\gamma g_l^{-1})x \in \gamma g_i^{-1} V \subset \gamma U \subset \mathcal{D}$. Por otro lado tomando j tal que $(\gamma g_l^{-1})x \in g_j^{-1}\mathcal{F}$ tenemos que $g_j\gamma g_l^{-1}x$ y x son dos puntos $\mathrm{SL}_2(\mathbb{Z})$-equivalentes de $\mathcal{F}^{\mathrm{o}}$, y por lo tanto $g_j\gamma g_l^{-1} = \pm \mathrm{Id}$. Entonces:

$$g_l\Gamma = g_j\gamma\Gamma = g_j\Gamma.$$

Es decir que $g_j = g_l$, luego $g_i\gamma g_i^{-1} = \pm \mathrm{Id}$, y despejando obtenemos que $\gamma = \pm \mathrm{Id}$ y por lo tanto $\gamma z = z$. □

Para analizar la acción del grupo modular en las cúspides es conveniente cambiar la topología de $\mathcal{H}^*$ de la usual. Para definir la topología vamos a dar una base local de abiertos $\mathcal{B}_x$ para cada punto $x \in \mathcal{H}^*$. Si $x \in \mathcal{H}$ entonces $\mathcal{B}_x$ consiste de las bolas abiertas centradas en x y con radio menor que $\Im(x)$. Si $x = i\infty$, $\mathcal{B}_{i\infty}$ esta formada por

los semiplanos $S_r = \{z \in \mathcal{H} : \Im(z) > r\} \cup \{i\infty\}$. Por último si $x \in \mathbb{Q}$, $\mathcal{B}_x$ consta de los subconjuntos $S_r = \{z \in \mathcal{H} : |z - (x + ir)| < r\} \cup \{x\}$, i.e. un elemento de $\mathcal{B}_x$ es la unión de x con una bola tangente a la recta real en x.

Con esta topología $\mathcal{H}^*$ resulta un espacio Hausdorff. Más aún si consideramos la base dada por la unión de todas estas bases locales, como las homografías preservan las circunferencias generalizadas $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ aplica un elemento de esta base en otro. Es decir que la acción del grupo modular en $\mathcal{H}^*$ es por homeomorfismos.

Proposición 2.1.15. *Todas las cúspides son* $\mathrm{SL}_2(\mathbb{Z})$*-equivalentes.*

Demostración. Sea $x = \frac{p}{q} \in \mathbb{Q}$ con $(p : q) = 1$. Alcanza con encontrar $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\gamma x = i\infty$. Como p y q son coprimos existen $r, s \in \mathbb{Z}$ tales que $pr + sq = 1$. Entonces tomando $\gamma = \left(\begin{smallmatrix} r & s \\ -q & p \end{smallmatrix}\right)$, entonces $\gamma x = i\infty$. □

Proposición 2.1.16. *Si* $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ *es un subgrupo de índice finito, el número de clases de equivalencia de cúspides bajo la acción de* Γ *esta acotado por el índice de* Γ, $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$.

Demostración. Sea $g_1, \ldots, g_r$, con $r = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$, una familia de representantes para las coclases a derecha de Γ. Entonces $\mathrm{SL}_2(\mathbb{Z}) = \cup_{i=1}^{r} \Gamma g_i$. Ahora por el lema anterior tenemos que el conjunto de todas las cúspides es $\mathrm{SL}_2(\mathbb{Z})i\infty = \cup_{i=1}^{r} \Gamma g_i i\infty$, y como cada $\Gamma(g_i i\infty)$ es una órbita, la cantidad total de órbitas distintas tiene que ser menor o igual a r. □

Observación 2.1.17. Notemos que el resultado anterior nos da, si conocemos una familia de representantes para las coclases, un conjunto finito de cúspides que cubre todas las clases de equivalencia de cúspides, posiblemente con repeticiones.

2.2. Formas Modulares

Definición 2.2.1. Sean $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$, $z \in \mathcal{H}$. Definimos el *factor de automorfía* $j(\gamma, z) = cz + d$.

Para cada $k \in \mathbb{N}$ y $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ definimos *operador slash* $-|\gamma$ en el espacio de fuciones $f : \mathcal{H} \to \mathbb{C}$, definido por $f|\gamma(z) = \det(\gamma)^{k/2} j(\gamma, z)^{-k} f(\gamma z)$.

Proposición 2.2.2. *Sean* $z \in \mathcal{H}$ *y* $\gamma_1, \gamma_2 \in \mathrm{GL}_2^+(\mathbb{R})$. *Se tiene que* j *satisface la siguiente condición de cociclo:*

$$j(\gamma_1\gamma_2, z) = j(\gamma_1, \gamma_2 z) j(\gamma_2, z).$$

Más aún, dada $f : \mathcal{H} \to \mathbb{C}$ *se tiene que* $f|\gamma_1\gamma_2 = (f|\gamma_1)|\gamma_2$, *i.e. la aplicación* $\gamma \mapsto -|\gamma$ *define una acción de* $\mathrm{GL}_2^+(\mathbb{R})$ *en el espacio de funciones holomorfas en* $\mathcal{H}$.

Demostración. Escribiendo $\gamma_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$, para $i = 1, 2$, se tiene que:

$$\gamma_1\gamma_2 = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix} \qquad \text{y} \qquad \gamma_2 z = \frac{a_2 z + b_2}{c_2 z + d_2}.$$

Luego:

$$\begin{aligned} j(\gamma_1, \gamma_2 z) j(\gamma_2, z) &= \left(c_1 \frac{a_2 z + b_2}{c_2 z + d_2} + d_1 \right) (c_2 z + d_2) \\ &= (c_1(a_2 z + b_2) + d_1(c_2 z + d_2)) \\ &= ((c_1 a_2 + d_1 c_2) z + (c_1 b_2 + d_1 d_2)) = j(\gamma_1 \gamma_2, z). \end{aligned}$$

Que la aplicación $\gamma \mapsto -|\gamma$ defina una acción se deduce ahora de que j satisface la relación de cociclo:

$$\begin{aligned} (f|\gamma_1)|\gamma_2(z) &= \det(\gamma_2)^{k/2} j(\gamma_2, z)^{-k} f|\gamma_1(\gamma_2 z) \\ &= \det(\gamma_2)^{k/2} j(\gamma_2, z)^{-k} \det(\gamma_1)^{k/2} j(\gamma_1, \gamma_2 z)^{-k} f(\gamma_1 \gamma_2 z) \\ &= \det(\gamma_1 \gamma_2)^{k/2} j(\gamma_1 \gamma_2, z)^{-k} f(\gamma_1 \gamma_2 z) \\ &= f|\gamma_1 \gamma_2(z). \end{aligned}$$

□

Definición 2.2.3. Una función $f : \mathcal{H} \to \mathbb{C}$ se dice una *forma modular de peso* k para un subgrupo de congruencia Γ si satisface:

1. f es analítica en $\mathcal{H}$.
2. $f|\gamma = f$ para toda matriz $\gamma \in \Gamma$, donde el operador $|\gamma$ es el definido para el entero k.
3. $f|\gamma$ está acotada en cada semiplano $\{z \in \mathcal{H} : \Im(z) > r\}$ para $r > 0$ para toda matriz $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Notamos $M_k(\Gamma)$ al espacio de fomas modulares de peso k para Γ.

Observación 2.2.4. En principio los items 2 y 3 involucran infinitas condiciones. Sin embargo como los operadores $-|\gamma$ definen una acción para verificar el item 2 alcanza con verificarlo para un conjunto de generadores de Γ. Por otro lado, se puede ver que alcanza con ver que el item 3 vale para un conjunto de representantes de las coclases o, más aún, en un conjunto de representantes de las cúspides, que son finitos por la Proposición 2.1.16.

Si f es una forma modular de peso k para el subgrupo Γ y $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ entonces $f|\gamma$ es una forma modular de peso k para el subgrupo $\gamma^{-1}\Gamma\gamma$.

Si el subgrupo Γ contiene la matriz $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ entonces toda forma modular es periódica de período 1, pues $f|T(z) = f(z+1)$. En particular esto vale si Γ es $\mathrm{SL}_2(\mathbb{Z})$, $\Gamma_0(n)$ ó $\Gamma_1(n)$. En el caso de que Γ sea un subgrupo de congruencia de nivel n, $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ pertenece a Γ y por lo tanto tanto f es una función periódica de período n.

Nuestro principal interés está en estudiar formas modulares para $\Gamma_0(N)$. Este subgrupo contiene a las matriz $-\mathrm{Id}$, por lo que para simplificar los argumentos a partir de ahora cuando nos refiramos a un grupo de congruencia vamos a suponer que el mismo contiene esta matriz.

Lema 2.2.5. *Dada $f : \mathcal{H} \to \mathbb{C}$ analítica y periódica de período 1, existe una única función analítica $g : D \setminus \{0\} \to \mathbb{C}$ tal que $g(e^{2\pi iz}) = f(z)$, donde $D = \{z \in \mathbb{C} : |z| < 1\}$ es el disco unitario.*

Demostración. Dado $q \in D \setminus \{0\}$ podemos tomar $U \subset D \setminus \{0\}$ una bola centrada en q. Como U es simplemente conexo y no contiene al cero podemos tomar $\log : U \to \mathbb{C}$ una rama del logaritmo tal que $e^{2\pi i \log(\tilde{q})} = \tilde{q}$ para todo $\tilde{q}$ en U. Luego en U tenemos que $g = f \circ \exp \circ \log$, con $\exp(z) = e^{2\pi iz}$ y por lo tanto g resulta analítica en U al ser composición de funciones analíticas. □

A partir de este momento vamos a notar q a un punto del disco D, y dada una forma modular f de período 1 vamos a notar también $f(q) = g(q)$ con g la función del lema anterior, salvo que sea necesario hacer la distinción entre ambas funciones. i.e. estamos tomando $q = e^{2\pi iz}$ si q no es 0, y pensamos a las formas modulares como funciones con dominio tanto en el disco D como en el semiplano $\mathcal{H}$.

Supongamos que f es una forma modular de peso k para un grupo de congruencia Γ tal que la matriz T pertenece a todos los subgrupos conjugados de Γ. En particular sabemos que f es periódica de período 1 y por el lema anterior podemos pensar a $f|\gamma$ como una función analítica $f|\gamma : D \setminus \{0\} \to \mathbb{C}$. Como la función exponencial aplica el semiplano $\{z \in \mathcal{H} : \Im(z) > r\}$ en el disco pinchado $\{q \in D : 0 < |q| < e^{-r}\}$ la tercera condición de la definición de las formas modulares nos asegura que $f|\gamma$ está acotada en un entorno de la singularidad aislada $q = 0$, y por lo tanto la función $f|\gamma$ se extiende de manera única a una función en el disco.

En el caso de que no todos los conjugados de Γ contengan a T podemos tomar g definida en el disco pinchado tal que $g(e^{2\pi iz/n}) = f(z)$; en estos casos notamos $q^{1/n}$ a la variable en el disco. Tenemos igual que antes que la condición de crecimiento en la definición de modularidad nos asegura que estas funciones se extienden a una función analítica en el disco entero.

Definición 2.2.6. Dada una forma modular f de peso k para un grupo Γ que contiene a T, definimos su *desarrollo de Fourier* ó su *q-expansión* como el desarrollo de Taylor de la f en el disco:

$$f(q) = \sum_{n=0}^{\infty} a_n(f) q^n.$$

Una forma modular f se dice *cuspidal* si $\lim_{r \to +\infty} f|\gamma(z + ir) = 0$ para toda $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Denotamos $S_k(\Gamma)$ al espacio de formas cuspidales de peso k para Γ.

Por la observación anterior, en el caso de que todos los subgrupos conjugados de Γ contengan a T, esto es equivalente a que el desarrollo de Fourier de cada $f|\gamma$ tenga $a_0(f|\gamma) = 0$. En el caso en que Γ o alguno de sus conjugados no contenga la matriz T podemos obtener una interpretación similar desarrollando f como una serie de potencias en $q^{1/N}$.

Observación 2.2.7. Si f es una forma cuspidal de período 1, entonces $|f(z)| = O(|q|) = O(e^{-y})$, con $z = x + iy$. Es decir que las formas cuspidales tienden rápido a 0 cuándo z tiende a $i\infty$.

Ejemplos 2.2.8.

1. Las series de Eisenstein son unos de los ejemplos prototípicos de formas modulares. Estas son series de la forma:

$$G_k(z) \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(mz+n)^k},$$

donde la suma es sobre los pares de enteros no ambos nulos y que posiblemente satisfacen ciertas relaciones de congruencia. Los coeficientes de Fourier de estas series, apropiadamente normalizadas, dan funciones de sumas de divisores.

2. A una forma cuadrática Q en $2k$ variables se le puede asignar la serie θ:

$$\Theta_Q(z) = \sum_{x\in\mathbb{Z}^{2n}} q^{Q(x)},$$

que va a ser en general una forma modular de peso k y cuyos coeficientes de Fourier dan la cantidad de maneras en que la forma cuadrática representa a un número.

3. Si tomamos $\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n)$, la función η de Dedekind, los productos de la forma $\prod_{d|N} \eta(dz)^{r_d}$, con $r_d \in \mathbb{Z}$, resultan formas modulares siempre que los r_d satisfagan ciertas relacions (ver [Ono04, Teorema 1.64] para un enunciado preciso).

Observación 2.2.9. Notemos que si $f \in M_{k_1}(\Gamma)$ y $g \in M_{k_2}(\Gamma)$ entonces $fg \in M_{k_1+k_2}(\Gamma)$; más aún si alguna de las dos funciones es cuspidal el producto también lo es. Es decir que el espacio generado por las formas modulares $\bigoplus_{k=0}^{\infty} M_k(\Gamma)$ es un álgebra graduada y $\bigoplus_{k=0}^{\infty} S_k(\Gamma)$ es un ideal homogéneo.

Lema 2.2.10. *Si Γ es un subgrupo de congruencia y k es un entero impar entonces $M_k(\Gamma) = \{0\}$.*

Demostración. Si f es una forma en $M_k(\Gamma)$ para todo $z \in \mathcal{H}$ se tiene:

$$f(z) = f|-\mathrm{Id}(z) = (-1)^k f((-\mathrm{Id})z) = -f(z)$$

Y por lo tanto $f(z) = 0$ para todo z. □

Teorema 2.2.11 (Fórmula de Valencia para $\mathrm{SL}_2(\mathbb{Z})$)**.** *Sea $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ no nula. Entonces vale la siguiente igualdad:*

$$v_{i\infty}(f) + \frac{v_i(f)}{2} + \frac{v_\rho(f)}{3} + \sum_{\substack{z\in\mathcal{F}\\ z\neq i,\rho\rho^2}}{}' v_z(f) = \frac{k}{12}$$

Donde $v_z(f)$ es el orden de anulación de f en z y la prima en la sumatoria nota que si z y z' son $\mathrm{SL}_2(\mathbb{Z})$-equivalentes entonces sólo sumamos uno de los términos.

Demostración. Supongamos primero que f no tiene ceros en $\partial\mathcal{F}$. En tal caso consideramos la curva γ_t que recorre el segmento que une ρ con $\frac{1}{2}+it$, luego el segmento que une este punto con $\frac{-1}{2}+it$, luego el segmento que une este con ρ^2 y finalmente el arco de la circunferencia con radio y centro 0 que une a ρ^2 con ρ. Luego la integral de la función $\frac{f'}{f}$ a lo largo de γ_t es igual a la suma de los ordenes de anulación de f en los puntos que rodea la curva, por el teorema de los residuos. Cómo f es holomorfa en el disco sólo puede tener finitos ceros en un dominio fundamental. Por lo tanto tomando t suficientemente grande podemos asegurar que la curva γ_t encierra todos los ceros de f en $\mathcal{H}$. Tenemos entonces:

$$\frac{1}{2\pi i}\int_{\gamma_t}\frac{f'}{f}dz=\sum_{z\in\mathcal{F}}v_z(f). \tag{2.2.1}$$

Ahora, como f es periódica, las integrales sobre las rectas laterales de γ_t se cancelan. Por otro lado haciendo el cambio de variable $q=e^{2\pi iz}$, la recta superior del dominio de integración se convierte en una circunferencia, en sentido horario, que encierra al 0 y a ningún otro cero de f. Notando $\tilde{f}(e^{2\pi iz})=f(z)$, tenemos que:

$$\begin{aligned}\frac{d}{dq}\tilde{f}(q)&=\tilde{f}'(e^{2\pi iz})e^{2\pi iz}2\pi iz=f'(z),\\ \frac{1}{2\pi i}\int\frac{\tilde{f}'(q)}{\tilde{f}(q)}dq&=\frac{1}{2\pi i}\int\frac{f'(z)e^{2\pi iz}2\pi iz}{f(z)e^{2\pi iz}2\pi iz}dz=\frac{1}{2\pi i}\int\frac{f'(z)}{f(z)}dz.\end{aligned}$$

De modo que la integral a lo largo del segmento superior coincide con la integral alrededor de la circunferencia en el disco. Nuevamente por el teorema de residuos esta integral coincide con menos el orden de anulación de f en $i\infty$.

Resta analizar lo que sucede con la integral sobre el arco de circunferencia. Para esto separamos la integral en la que va de ρ^2 a i y la que va de i a ρ. La aplicación $z\mapsto -1/z$ una de estas en la otra invirtiendo la orientación. Aplicando el cambio de variables $\tilde{z}=-1/z$ tenemos entonces que:

$$\frac{1}{2\pi i}\int_{\rho^2}^{i}\frac{f'(z)}{f(z)}dz=\frac{1}{2\pi i}\int_{\rho}^{i}\frac{f'(\tilde{z})}{f(\tilde{z})}d\tilde{z}.$$

Como f es una forma modular $f(\tilde{z})=z^kf(z)$, y derivando término a término se obtenemos que:

$$\begin{aligned}f'(\tilde{z})\frac{1}{z^2}&=kz^{k-1}f(z)+z^kf'(z),\\ \frac{f'(\tilde{z})}{f(\tilde{z})}&=kz^{k+1}\frac{f(z)}{z^kf(z)}+z^{k+2}\frac{f'(z)}{z^kf(z)}\\ &=kz+z^2\frac{f'(z)}{f(z)}.\end{aligned}$$

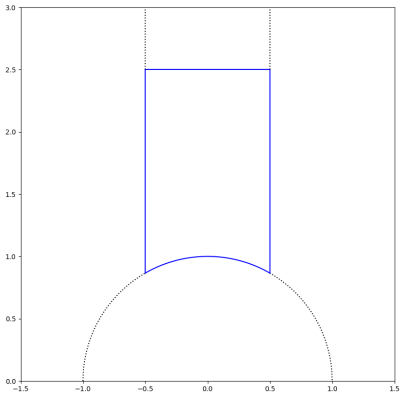

Figura 2.2: La curva γ_t en azul.

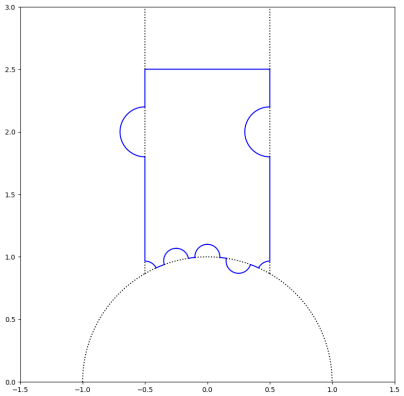

Figura 2.3: La curva γ_t modificada.

Aplicando el teorema de cambio de variables tenemos entonces:

$$\begin{aligned}\frac{1}{2\pi i}\int_{\rho^2}^{\rho}\frac{f'(z)}{f(z)}dz &= \frac{1}{2\pi i}\left(\int_{\rho^2}^{i}\frac{f'(z)}{f(z)}dz + \int_{i}^{\rho}\frac{f'(z)}{f(z)}dz\right)\\ &= \frac{1}{2\pi i}\left(\int_{\rho}^{i}\left(\frac{k}{z}+\frac{f'(z)}{f(z)}\right)dz + \int_{i}^{\rho}\frac{f'(z)}{f(z)}dz\right)\\ &= \frac{1}{2\pi i}\int_{\rho}^{i}\frac{k}{z}dz\\ &= \frac{k}{2\pi i}\left(\frac{\pi}{2}-\frac{\pi}{6}\right) = \frac{k}{12}.\end{aligned}$$

Por lo tanto obtenemos para la integral sobre γ_t el valor:

$$\frac{1}{2\pi i}\int_{\gamma_t}\frac{f'(z)}{f(z)}dz = \frac{k}{12} - v_{i\infty}(f) \tag{2.2.2}$$

y junto con (2.2.1) concluimos que:

$$\frac{k}{12} = v_{i\infty}(z) + \sum_{z\in\mathcal{F}} v_z(f).$$

que es lo que buscabamos en el caso de que f no se anule en ningún punto de $\partial\mathcal{F}$.

En el caso en que f tenga un cero $z \in \partial\mathcal{F}$ que no es i, ρ ó ρ^2 podemos modificar la curva sobre la que integramos usando arcos de circunferencia suficientemente chicos alrededor de z y $z+1$ en el caso de que $|\Re(z)| = 1/2$, ó de z y $-1/z$ en el caso de que $|z| = 1$, y el argumento anterior sigue siendo válido. Cuándo hay un cero en i, ρ o ρ^2 nuevamente modificamos la curva con pequeños arcos de circunferencia, como se ve en la Figura 2.3. En este caso los arcos que tomamos no nos permiten usar el mismo argumento de antes, por lo que aportan términos adicionales, pero haciendo tender a cero el radio de estas circunferencias y aplicando el teorema de residuos obtenemos

términos de la forma $\frac{\theta v_z(f)}{2\pi}$ con θ el ángulo que tienden los arcos en el límite. En el caso de $z = i$ se tiene $\theta = \pi$ y si $z = \rho$ y ρ^2 obtenemos un término con $\theta = \frac{\pi}{3}$ por cada uno de estos dos ceros, y esto da precisamente los coeficientes del enunciado. □

Observación 2.2.12. La demostración anterior sigue siendo válida si f fuera meromorfa en $\mathcal{H}$ y la función que define en el disco tiene un polo en 0. En este caso la fórmula de valencia sigue valiendo, pero puede tener términos negativos.

Teorema 2.2.13 (Cotas de Sturm)**.** *Sea Γ un subgrupo de congruencia. Si $f \in M_k(\Gamma)$ y $v_{i\infty}(f) > \frac{k[\mathrm{SL}_2(\mathbb{Z}):\Gamma]}{12}$ entonces $f \equiv 0$.*

Demostración. Supongamos primero $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Si f no fuera nula debería en este caso satisfacer la fórmula de valencia y entonces tendríamos:

$$\frac{k}{12} = v_{i\infty}(f) + \frac{v_i(f)}{2} + \frac{v_\rho(f)}{3} + \sum_{\substack{z\in\mathcal{F}\\ z\neq i,\rho\rho^2}}{}' v_z(f) \geq v_{i\infty}(f) > \frac{k}{12}$$

lo que es absurdo, y por lo tanto f debe ser nula.

Si ahora Γ no es el grupo modular notamos $r = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. Tomamos γ_i un conjunto de representantes para las coclases de Γ en $\mathrm{SL}_2(\mathbb{Z})$ y definimos $\tilde{f} = \prod_i f|\gamma_i$. Afirmamos que $\tilde{f}$ es una forma modular para $\mathrm{SL}_2(\mathbb{Z})$ de peso kr. En efecto, si $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ podemos tomar $\alpha_i \in \Gamma$ y σ una permutación tales que $\gamma_i\gamma = \alpha_i\gamma_{\sigma(i)}$ y entonces se tiene:

$$\begin{aligned}
\tilde{f}(\gamma z) &= \prod_i f|\gamma_i(\gamma z) = \prod_i j(\gamma_i, \gamma z)^{-k} f(\gamma_i\gamma z)\\
&= \prod_i j(\gamma_i\gamma, z)^{-k} j(\gamma, z)^k f(\alpha_i\gamma_{\sigma(i)} z)\\
&= \prod_i j(\alpha_i\gamma_{\sigma(i)}, z)^{-k} j(\gamma, z)^k f(\alpha_i\gamma_{\sigma(i)} z)\\
&= \prod_i j(\alpha_i\gamma_{\sigma(i)}, z)^{-k} j(\gamma, z)^k j(\alpha_i, \gamma_{\sigma(i)} z)^k f(\gamma_{\sigma(i)} z)\\
&= \prod_i j(\alpha_i\gamma_{\sigma(i)}, z)^{-k} j(\gamma, z)^k j(\alpha_i\gamma_{\sigma(i)}, z)^k j(\gamma_{\sigma(i)}, z)^{-k} f(\gamma_{\sigma(i)} z)\\
&= j(\gamma, z)^{kr} \prod_i j(\gamma_{\sigma(i)}, z)^{-k} f(\gamma_{\sigma(i)} z)\\
&= j(\gamma, z)^{kr} \tilde{f}(z).
\end{aligned}$$

Aplicando el resultado para $\mathrm{SL}_2(\mathbb{Z})$ vemos que si $v_{i\infty}(\tilde{f}) > \frac{k[\mathrm{SL}_2(\mathbb{Z}):\Gamma]}{12}$ entonces $\tilde{f} \equiv 0$, y esto implica por la definición de $\tilde{f}$ que la función original debe ser la función 0. Por otro lado como f es uno de los factores de $\tilde{f}$ debe valer que $v_{i\infty}(f) \leq v_{i\infty}(\tilde{f})$, de donde se deduce lo que queremos. □

Corolario 2.2.14. *Si Γ es un subgrupo de congruencia entonces $M_k(\Gamma)$ tiene dimensión finita.*

Demostración. Consideremos la función $\phi : M_k(\gamma) \to \mathbb{C}^{\lfloor kr/12 \rfloor}$, con $r = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$, que aplica f en el vector que tiene sus primeros kr coeficientes de Fourier. Entonces por el teorema anterior si $\phi(f) = 0$, la función f es la función 0. Luego $\dim(M_k(\Gamma)) \leq \frac{kr}{12}$, y en particular es finita. □

Corolario 2.2.15. $M_2(\mathrm{SL}_2(\mathbb{Z})) = 0$.

Demostración. Si tuvieramos $f \in M_2(\mathrm{SL}_2(\mathbb{Z}))$ no nula entonces por la fórmula de valencia tendríamos:

$$v_{i\infty}(f) + \frac{v_i(f)}{2} + \frac{v_\rho(f)}{3} + \sum_{\substack{z \in \mathcal{F} \\ z \neq i, \rho\rho^2}}{}' v_z(f) = \frac{1}{6}.$$

Pero si cualquiera de los términos del lado izquierdo fuera no nulo sería mayor a $1/6$ y por lo tanto no puede valer la igualdad; luego no puede existir tal f. □

2.3. Operadores de Hecke

Definición 2.3.1. Dados $n, N \in \mathbb{N}$, $S < (\mathbb{Z}/N\mathbb{Z})^\times$ un subgrupo y un ideal $I \in \mathbb{Z}$, definimos el conjunto de matrices:

$$X_n(N, S, I) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad - bc = n; N|c; [a] \in S; b \in I \right\}.$$

En lo que resta de esta sección vamos a suponer que tenemos un sistema N, S, I fijo y entonces $X_n = X_n(N, S, I)$ o que no estamos usando ninguno de estos sistemas y en este caso simplemente tenemos $X_n = \{\gamma \in M_2(\mathbb{Z}) : \det(\gamma) = n\}$. Notemos que con esta convención $X_1 = \mathrm{SL}_2(\mathbb{Z})$ en el caso en que nos estamos usando ninguno de estos sistemas, y $X_1(N, \{1\}, N\mathbb{Z}) = \Gamma(N)$, $X_1(N, \{1\}, \mathbb{Z}) = \Gamma_1(N)$ y $X_1(N, (\mathbb{Z}/N\mathbb{Z})^\times, \mathbb{Z}) = \Gamma_0(N)$

Proposición 2.3.2. *Se tienen las inclusiones de conjuntos:*

$$X_n X_m \subset X_{nm},$$

y además X_1 es un subgrupo de congruencia de $\mathrm{SL}_2(\mathbb{Z})$*. En particular X_1 actúa por multiplicación a ambos lados en todos los X_n.*

Demostración. Cuando X_1 es $\mathrm{SL}_2(\mathbb{Z})$ no hay nada que hacer. Supongamos entonces que tenemos $N \in \mathbb{N}$, $S < (\mathbb{Z}/N\mathbb{Z})^\times$ un subgrupo e $I < \mathbb{Z}$ un ideal. Dados $\gamma_1 = \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right) \in X_n$ y $\gamma_2 = \left(\begin{smallmatrix} a_2 & b_2 \\ c_2 & d_2 \end{smallmatrix}\right) \in X_m$, queremos ver entonces que:

$$\gamma_1\gamma_2 = \begin{pmatrix} a_1a_2 + b_1c_1 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix} \quad \in X_{nm}.$$

En particular como $c_1 \equiv c_2 \equiv 0 \pmod{N}$ tenemos que:

$$\begin{aligned} a_1a_2 + b_1c_1 &\equiv a_1a_2 \pmod{N}, \\ c_1a_2 + d_1c_2 &\equiv 0 \pmod{N}, \\ c_1b_2 + d_1d_2 &\equiv d_1d_2 \pmod{N}. \end{aligned}$$

Como las clases de a_1 y a_2 pertenecen al subgrupo S, de estas ecuaciones se deduce que también la clase de $a_1a_2 + b_1c_1$ pertenece a este subgrupo. Por último como b_1 y b_2 pertenecen al ideal I se tiene que $a_1b_2 + b_1d_2 \in I$.

Ya que acabamos de probar que $X_1X_1 \subset X_1$, para poder concluir que X_1 es un grupo basta ver que el inverso de un elemento $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in X_1$ pertenece efectivamente a X_1. Supongamos entonces que $\gamma \left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) = \mathrm{Id}$. Como N divide a c se tiene que $0 = cw + dy \equiv dy \pmod{N}$, y como d es coprimo con N por pertenecer a S debe valer que $N|y$. Luego tenemos que $1 = aw + by \equiv aw \pmod{N}$ y como a pertenece a S concluimos que $w \in S$, y de manera análoga se obtiene que $z \in S$.

Finalmente tenemos que, como $0 = ax + bz \in I$ y $b \in I$, entonces $ax \in I$. Como $(a : b) = 1$ porque γ tiene determinante 1, si $ax \in I$ es porque necesariamente $x \in I$. Por lo tanto podemos concluir que $\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) \in X_1$ como queríamos demostrar. □

Proposición 2.3.3. *La acción de X_1 en X_m tiene finitas órbitas.*

Demostración. Supongamos que $X_1 = \mathrm{SL}_2(\mathbb{Z})$. En este caso afirmamos que se tiene:

$$X_m = \coprod_{\substack{ad=m \\ d>0}} \coprod_{0 \le b < d} \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}. \tag{2.3.1}$$

Veamos primero que la unión es disjunta. Para esto supongamos que tenemos:

$$\begin{pmatrix} w & x \\ y & z \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} \tilde{a} & \tilde{b} \\ 0 & \tilde{d} \end{pmatrix},$$

con las matrices en los conjuntos apropiados. En particular tenemos que $ya = 0$, y como $ad = m$ tiene que valer $y = 0$. Luego tenemos que $wz = 1$ y por lo tanto $w = z = \pm 1$, pero como $zd = \tilde{d}$ y tanto d como $\tilde{d}$ son positivos $w = z = 1$, y en consecuencia se tiene que $d = \tilde{d}$ y $a = \tilde{a}$ también. Por último tenemos:

$$\tilde{b} = b + xd \equiv b \pmod{d},$$

y como $0 \le b, \tilde{b} < d$ debe valer $b = \tilde{b}$, i.e. $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = \begin{pmatrix} \tilde{a} & \tilde{b} \\ 0 & \tilde{d} \end{pmatrix}$.

Que el lado derecho de (2.3.1) está incluido en el lado izquierdo es claro. Sea entonces $\gamma \in X_m$. Repitiendo el argumento que hicimos en la Proposición 2.1.2 podemos aplicar el algoritmo de Euclides multiplicando por potencias apropiadas de las matrices S y T a izquierda para obtener que existe $P \in \mathrm{SL}_2(\mathbb{Z})$ tal que:

$$P\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Es claro que $ad = m$ porque P tiene deteminante 1. Por otro lado multiplicando a izquierda por $-\mathrm{Id}$ podemos suponer que $a, d > 0$ y multiplicando por una potencia apropiada de T podemos conseguir que b esté en el rango que buscamos. Con esto terminamos de probar el caso $X_1 = \mathrm{SL}_2(\mathbb{Z})$; más aún obtuvimos representantes concretos para las órbitas.

Si ahora X_1 es arbitrario, llamamos $Y_m = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \det(\gamma) = m\}$ y tomamos $\gamma_1, \ldots, \gamma_r \in \mathrm{SL}_2(\mathbb{Z})$ representantes de las coclases de $X_1 \backslash \mathrm{SL}_2(\mathbb{Z})$. Entonces si $y_1, \ldots, y_k$ son representantes de las órbitas de Y_m por la acción del grupo modular, que ya vimos que son finitas, entonces tenemos:

$$Y_m = \coprod_{j=1}^{k} \mathrm{SL}_2(\mathbb{Z}) y_j = \coprod_{j=1}^{k} \coprod_{i=1}^{r} X_1 \gamma_i y_j.$$

Es decir que la acción de X_1 en Y_m tiene finitas órbitas. Como $X_m \subset Y_m$ es un subconjunto X_1-invariante las órbitas de este también son finitas, pues son un subconjunto de las de Y_m. □

Definición 2.3.4. Dado $n \in \mathbb{N}$ definimos el *operador de Hecke* T_n en $M_k(X_1)$ como:

$$T_n(f) = n^{\frac{k}{2}-1} \sum_{\alpha \in X_1 \backslash X_m} f|\alpha.$$

Proposición 2.3.5. *Si $f \in M_k(X_1)$ entonces $T_n(f) \in M_k(X_1)$.*

Demostración. Basta observar que si $\gamma \in X_1$ entonces la multiplicación a derecha por γ permuta las órbitas de $X_1 \backslash X_m$. Luego:

$$\begin{aligned} T_n(f)|\gamma &= n^{\frac{k}{2}-1} \sum_{\alpha \in X_1 \backslash X_m} f|(\alpha\gamma) \\ &= n^{\frac{k}{2}-1} \sum_{\alpha \in X_1 \backslash X_m} f|\alpha = T_n(f) \end{aligned}$$

□

La proposición anterior nos dice que los operadores de Hecke son endomorfismos de los espacios de formas modulares, y podemos entonces considerar sus autovectores. En particular nos van a interesar los autovectores simultáneos de estos operadores.

Definición 2.3.6. Una forma modular $f \in M_k(\Gamma)$ se dice una *autoforma* si es un autovector para todos los operadores de Hecke.

Los coeficientes de las autoformas satisfacen propiedades de multiplicativadad. En particular nos va interesar estudiar estas propiedades en el caso de $M_k(\Gamma_1(N))$. Para poder analizar estas propiedades vamos a necesitar conocer representantes para las órbitas de X_n.

Proposición 2.3.7. *Si $X_1 = \Gamma_1(N)$, i.e. $S = \{1\}$ e $I = \mathbb{Z}$, se tiene que:*

$$X_n = \coprod_{\substack{ad=m \\ d>0 \\ (a:N)=1}} \coprod_{0 \le b < d} \Gamma_1 \left(\sigma_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right),$$

donde $\sigma_a \in \mathrm{SL}_2(\mathbb{Z})$ es tal que $\sigma_a \equiv \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right) \pmod N$.

Demostración. Como $\sigma_a \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \equiv \begin{pmatrix} 1 & a^{-1}b \\ 0 & a^{-1}d \end{pmatrix} \pmod N$, el lado derecho está incluido en X_n. Veamos ahora que la unión es efectivamente disjunta. Supongamos entonces que existen $\gamma \in \Gamma_1(N)$, a_i, b_i, d_i, con $i = 1, 2$ y las restricciones de la unión, tales que $\gamma \sigma_{a_1} \left(\begin{smallmatrix} a_1 & b_1 \\ 0 & d_1 \end{smallmatrix}\right) = \sigma_{a_2} \left(\begin{smallmatrix} a_2 & b_2 \\ 0 & d_2 \end{smallmatrix}\right)$. En particular tenemos que:

$$\begin{aligned} \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}^{-1} &= \frac{1}{a_2 d_2} \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} d_2 & -b_2 \\ 0 & a_2 \end{pmatrix} \\ &= \frac{1}{a_2 d_2} \begin{pmatrix} a_1 d_2 & a_2 b_1 - a_1 b_2 \\ 0 & d_1 a_2 \end{pmatrix} \\ &= \begin{pmatrix} \frac{a_1}{a_2} & \frac{a_2 b_1 - a_1 b_2}{a_2 d_2} \\ 0 & \frac{d_1}{d_2} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}). \end{aligned}$$

Por como elegimos los elementos de las matrices es inmediato de esto que $a_1 = a_2$ y $d_1 = d_2$, ya que $\frac{a_1 d_1}{a_2 d_2} = 1$. Y entonces tenemos que $a_2 d_2 | a_2 b_1 - a_1 b_2 = a_2(b_1 - b_2)$, i.e. $d_2 | b_1 - b_2$. Nuevamente por como elegimos los elementos de las matrices esto implica que $b_1 = b_2$.

Resta ver ahora que X_n está contenido en la unión. Sea $\gamma = \left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) \in X_n$, y elegimos g, h coprimos tales que $gw + hy = 0$. Eligiendo e, f tales que $eh - fg = 1$ conseguimos una matriz $\alpha = \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\alpha\gamma$ es triangular superior, es decir que tenemos $\alpha\gamma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, y multiplicando por una potencia apropiada de T y por $-\mathrm{Id}$ podemos suponer que esta matriz satisface $a > 0$ y $0 \le b < d$. Reduciendo módulo N obtenemos que se tiene que cumplir:

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & z \end{pmatrix} \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \pmod N.$$

Es decir que $e \equiv a \pmod N$ y $g \equiv 0 \pmod N$, y por lo tanto $h \equiv a^{-1} \pmod N$. Esto nos asegura que $\alpha^{-1}\sigma_a^{-1} \in \Gamma_1(N)$, i.e. $\gamma = (\alpha^{-1}\sigma_a^{-1})\sigma_a \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ y por lo tanto X_m está incluído en el lado derecho de la igualdad. □

Corolario 2.3.8. *Si $(n : N) = 1$ entonces y $f \in M_k(\Gamma_1(N))$ entonces:*

$$T_n(f) = n^{\frac{k}{4}-1} \sum_{\substack{ad=n \\ a>0}} \sum_{b=0}^{d-1} f | \left(\sigma_a \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \right).$$

Nos gustaría convertir esta descripción de los operadores de Hecke en una en términos de los coeficientes del desarrollo de Fourier de las formas modulares. De la descripción anterior no es claro que vayamos a poder hacer esto. Lo que vamos a hacer es descomponer el espacio de $M_k(\Gamma_1(N))$ en términos de espacios de formas modulares para $\Gamma_0(N)$ donde sí podemos encontrar a partir del resultado anterior una descripción como la que nos interesa. Para esto necesitamos formas modulares sobre $\Gamma_0(N)$ un poco más generales.

Definición 2.3.9. Sean $\chi : \mathbb{Z} \to \mathbb{C}$ un caracter de Dirichlet módulo $N \in \mathbb{N}$ y $k \in \mathbb{N}$ definimos las formas modulares sobre $\Gamma_0(N)$ de peso k y caracter χ, como las funciones holomorfas $f : \mathcal{H} \to \mathbb{C}$, que satisfacen la condición de crecimiento en las cúspides y tales que:

$$f|\gamma(z) = \chi(d)f \qquad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Denotamos $M_k(\Gamma_0(N), \chi)$ el espacio de estas formas modulares.

Consideremos la extensión del caracter a $\chi : \Gamma_0(N) \to \mathbb{C}; \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \chi(d)$. Para que pueda haber elementos no triviales en $M_k(\Gamma_0(N), \chi)$ necesitamos que esta extensión sea multiplicativa, pues tenemos si f está en este espacio tenemos:

$$\chi(\gamma_1\gamma_2)f = f|\gamma_1\gamma_2 = (\chi(\gamma_1)f)|\gamma_2 = \chi(\gamma_1)\chi(\gamma_2)f$$

Lema 2.3.10. *Extendiendo χ a una función de $\Gamma_0(N)$ de la manera anterior se tiene:*

$$\chi(\gamma_1\gamma_2) = \chi(\gamma_1)\chi(\gamma_2) \qquad \forall \gamma_1, \gamma_2 \in \Gamma_0(N).$$

Demostración. Escribiendo $\gamma_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ tenemos:

$$\chi(\gamma_1\gamma_2) = \chi(c_1b_2 + d_1d_2) = \chi(d_1d_2) = \chi(d_1)\chi(d_2) = \chi(\gamma_1)\chi(\gamma_2),$$

donde la segunda igualdad se deduce de que χ es un caracter módulo N y $N|c_1$. □

Observemos que el núcleo de la extensión de χ a $\Gamma_0(N)$ contiene a $\Gamma_1(N)$ para cualquier caracter. Tenemos entonces la inclusión de $M_k(\Gamma_0(N), \chi) \subset M_k(\Gamma_1(N))$. Más estos subespacios van a dar una descomposicón de $M_k(\Gamma_1(N))$ como una suma directa.

Lema 2.3.11. *1. El conjunto de caracteres de Dirichlet módulo N forma un grupo abeliano de orden $\phi(N)$.*

2. Para $d \in \mathbb{Z}$ fijo se tiene:

$$\sum_{\chi} \chi(d) = \begin{cases} \phi(N) & \text{si } d \equiv 1 \pmod{N}, \\ 0 & \text{si } d \not\equiv 1 \pmod{N}, \end{cases}$$

donde la suma es sobre todos los caracteres de Dirichlet χ módulo N.

3. *Para un caracter χ módulo N fijo se tiene:*

$$\sum_d \chi(d) = \begin{cases} \phi(N) & \text{si } \chi \equiv 1, \\ 0 & \text{si } \chi \not\equiv 1, \end{cases}$$

donde la suma es sobra todas las clases residuales $d \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Demostración. 1. Es inmediato del resultado de la estructura de grupo de $(\mathbb{Z}/n\mathbb{Z})^\times$.

2. Si $d = 1$ es inmediato. Si $d \neq 1$, podemos tomar χ_0 un caracter tal que $\chi_0(d) \neq 1$. Tenemos entonces:

$$\sum_\chi \chi(d) = \sum_\chi (\chi \cdot \chi_0)(d) = \chi_0(d) \sum_\chi \chi(d),$$

ya que multiplicar por χ_0 va a simplemente permutar los caracteres. Como $\chi_0(d)$ es distinto de 1 esto implica necesariamente que la suma es 0.

3. Análogamente al punto anterior, si χ es el caracter trivial el resultado es inmediato. En caso contrario existe d_0 en las unidades módulo N tal que $\chi(d_0) \neq 1$. Entonces como multiplicar por d_0 simplemente permuta las unidades módulo N:

$$\sum_d \chi(d) = \sum_d \chi(d_0 d) = \sum_d \chi(d_0)\chi(d) = \chi(d_0) \sum_d \chi(d),$$

y como $\chi(d_0) \neq 1$ la suma debe necesariamente anularse.

□

Observación 2.3.12. El resultado anterior no es más que un caso particular de las relaciones de ortogonalidad de la tabla de caracteres de un grupo finito.

Teorema 2.3.13. *Se tiene la siguiente descomposición en suma directa:*

$$M_k(\Gamma_1(N)) = \bigoplus_\chi M_k(\Gamma_0(N), \chi),$$

donde la suma es sobre todos los caracteres χ módulo N.

Demostración. Ya observamos antes que el lado derecho de la igualdad está incluído en lado izquierdo. Para ver la otra inclusión elegimos para cada d en las unidades módulo N una matriz en $\Gamma_0(N)$ de la forma $\left(\begin{smallmatrix} * & * \\ * & d \end{smallmatrix}\right)$. Dada $f \in M_k(\Gamma_1(N))$ consideramos para cada caracter χ modulo N la función definida por:

$$f_\chi = \frac{1}{\phi(N)} \sum_d \overline{\chi(d)} f|\gamma_d.$$

Notemos primero que esta función está bien definida independientemente de la elección que hayamos hecho de γ_d. En efecto si tenemos dos elecciones distintas $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ y $\left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & d \end{smallmatrix}\right)$ tenemos que módulo N vale:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & d \end{pmatrix}^{-1} \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} d & -\tilde{b} \\ 0 & \tilde{a} \end{pmatrix} \equiv \begin{pmatrix} ad & * \\ 0 & \tilde{a}d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \quad (\text{mód } N).$$

Por lo tanto las dos posibles elecciones difieren en multiplicar a derecha por una matriz de $\Gamma_1(N)$ y esto no afecta la definición. Afirmamos que $f_\chi \in M_k(\Gamma_0(N), \chi)$. Dada $\gamma = \left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) \in \Gamma_0(N)$ tenemos:

$$\begin{aligned} f_\chi|\gamma &= \frac{1}{\phi(N)} \sum_d \overline{\chi(d)} f|(\gamma_d \gamma) = \frac{1}{\phi(N)} \sum_d \overline{\chi(d)} f|\gamma_{dz} \\ &= \frac{1}{\phi(N)} \sum_d \chi(z)\overline{\chi(dz)} f|\gamma_{dz} = \chi(z) f_\chi. \end{aligned}$$

Para concluir la inclusión que queremos basta sumar sobre todos los caracteres para obtener:

$$\sum_\chi f_\chi = \sum_\chi \left(\frac{1}{\phi(N)} \sum_d \overline{\chi(d)} f|\gamma_d \right) = \frac{1}{\phi(N)} \sum_d \left(f|\gamma_d \sum_\chi \overline{\chi(d)} \right),$$

y por el Lema 2.3.11 la suma interior es $\phi(N)$ cuando $d = 1$ y 0 en otro caso. De modo que toda la suma sobre todos los caracteres nos devuelve la forma modular original y por lo tanto f pertenece al lado derecho de la igualdad que queremos demostrar.

Resta sólo ver que la suma es efectivamente directa. Dada $f \in M_k(\Gamma_0(N), \psi)$ tenemos que:

$$\begin{aligned} f_\chi &= \frac{1}{\phi(N)} \sum_d \overline{\chi(d)} f|\gamma_d = \frac{1}{\phi(N)} \sum_d \overline{\chi(d)} \psi(d) f \\ &= \frac{1}{\phi(N)} f \sum_d \left(\overline{\chi}\psi\right)(d), \end{aligned}$$

y nuevamente por el Lema 2.3.11 la suma interna es $\phi(N)$ si $\chi = \psi$ y 0 en otro caso. Es decir que $f|\chi = f$ si $\psi = \chi$ y 0 en otro caso. La suma debe entonces ser directa pues si $f \in \left(\bigoplus_{\chi \neq \psi} M_k(\Gamma_0(N), \chi)\right) \cap M_k(\Gamma_0(N), \psi)$, entonces $f = f_\psi = 0$. □

Observación 2.3.14. En la demostración anterior estamos viendo que los operadores de promedio $f \mapsto f_\psi$ son proyectores a $M_k(\Gamma_0(N), \psi)$ con núcleo $\bigoplus_{\chi \neq \psi} M_k(\Gamma_0(N), \chi)$.

En la Proposición 2.3.7 encontramos representantes de matrices que nos permiten describir los operadores de Hecke para $\Gamma_1(N)$ como:

$$T_n(f) = n^{\frac{k}{2}-1} \sum_{\substack{ad=n \\ a>0 \\ (a:N)=1}} \sum_{0 \leq b < d} f|\sigma_a \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right).$$

En el caso en que $f \in M_k(\Gamma_0(N), \chi)$, tenemos que $f|\sigma_a = \chi(a)f$. Más aún como $\chi(a) = 0$ si $(a : N) \neq 1$ podemos reescribir la escripción anterior como:

$$T_n(f) = n^{\frac{k}{2}-1} \sum_{\substack{ad=n \\ a>0}} \sum_{0 \leq b < d} \chi(a) f|\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right). \tag{2.3.2}$$

Esto nos permite encontrar las expresiones que buscábamos para la acción de los operadores de Hecke sobre los coeficientes:

Teorema 2.3.15. *Sea $f \in M_k(\Gamma_0(N), \chi)$. Escribiendo $f(z) = \sum_{m=0}^{\infty} a(m)q^m$ y $T_n(f)(z) = \sum_{m=0}^{\infty} b(m)q^m$ se tiene que:*

$$b(m) = \sum_{a|(m:n)} \chi(a)a^{k-1}a(mn/a^2).$$

En particular cuando $n = p$ es un número primo tenemos:

$$b(m) = a(mp) + \chi(p)p^{k-1}a(m/p),$$

donde estamos tomando $a(m/p) = 0$ si $p \nmid m$.

Demostración. Por la (2.3.2) tenemos que:

$$\begin{aligned}
T_n(f) &= n^{\frac{k}{2}-1} \sum_{\substack{ad=n \\ a>0}} \left(\chi(a) \sum_{0 \leq b < d} n^{\frac{k}{2}} d^{-k} f\left(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) z\right) \right) \\
&= n^{k-1} \sum_{\substack{ad=n \\ a>0}} \left(\chi(a) \sum_{m=0}^{\infty} \sum_{0 \leq b < d} a(m)(\frac{n}{a})^{-k} \exp(2\pi i m(az+b)/d) \right) \\
&= n^{-1} \sum_{\substack{ad=n \\ a>0}} \left(\chi(a)a^k \sum_{m=0}^{\infty} \sum_{0 \leq b < d} a(m) \exp(2\pi i z m a/d) \exp(2\pi i m b/d) \right) \\
&= n^{-1} \sum_{\substack{ad=n \\ a>0}} \left(\chi(a)a^k \sum_{m=0}^{\infty} \left(a(m)q^{ma/d} \sum_{0 \leq b < d} \exp(2\pi i m b/d) \right) \right).
\end{aligned}$$

Notemos que la suma interna de la última línea es una geométrica con razón una raíz de la unidad. Por lo tanto obtenemos que es 0 si $d \nmid m$, y la razón es distinta de uno, y d

cuándo $d|m$. Luego:

$$\begin{aligned} T_n(f) &= n^{-1} \sum_{\substack{ad=n \\ a>0}} \left(\chi(a) a^k \sum_{\substack{m\geq 0 \\ d|m}} a(m) d q^{ma/d} \right) \\ &= \sum_{\substack{m\geq 0 \\ d|m}} \sum_{\substack{ad=n \\ a>0}} \chi(a) a^{k-1} a(m) q^{ma/d} \\ &= \sum_{m\geq 0} \sum_{\substack{ad=n \\ a>0}} \chi(a) a^{k-1} a(md) q^{ma}. \end{aligned}$$

Observemos que si $(m : n) = 1$ no hay ningún término con q^n, i.e. $b(m) = 0$. En caso contrario hay un término con exponente q^m por cada divisor común a entre m y n y el coeficiente de este término es $\chi(a)a^{k-1}a(md/a) = \chi(a)a^{k-1}a(mn/a^2)$, de modo que podemos escribir:

$$b(n) = \sum_{\substack{a|(m:n) \\ a>0}} \chi(a) a^{k-1} a(mn/a^2).$$

□

Corolario 2.3.16. *Si $(m : n) = 1$ entonces $T_m T_n = T_{mn}$ y, en particular, los operadores T_m y T_n conmutan.*

Demostración. Dada $f \in M_k(\Gamma_0(N), \chi)$ escribimos $f(z) = \sum_{l\geq 0} a(l)q^l$, $T_n(f) = \sum_{l\geq 0} b(l)q^l$ y $T_{mn}(f) = \sum_{l\geq 0} c(l)q^l$. Tenemos entonces que:

$$c(l) = \sum_{\substack{a|(l:mn) \\ a>0}} \chi(a) a^{k-1} a(lmn/a^2).$$

Ahora como m y n son coprimos los divisores de mn se escriben como producto de divisores de m y n por separado. Es decir que podemos escribir la suma como:

$$\begin{aligned} c(l) &= \sum_{\substack{a|(l:m) \\ a>0}} \left(\sum_{\substack{\tilde{a}|(l:n) \\ \tilde{a}>0}} \chi(a\tilde{a})(a\tilde{a})^{k-1} a(mnl/(a\tilde{a})^2) \right) \\ &= \sum_{\substack{a|(l:m) \\ a>0}} \left(\chi(a) a^{k-1} \sum_{\substack{\tilde{a}|(lm/a^2:n) \\ \tilde{a}>0}} \chi(\tilde{a}) \tilde{a}^{k-1} a(mnl/(a\tilde{a})^2) \right) \\ &= \sum_{\substack{a|(l:m) \\ a>0}} \chi(a) a^{k-1} b(ml/a^2), \end{aligned}$$

y esto es precisamente el coeficiente de q^l en $T_m(T_n(f))$, como queríamos. □

El resultado anterior nos dice que la aplicación $n \mapsto T_n$ es multiplicativa. No es sin embargo completamente multiplicativa, concretamente se tiene el siguiente resultado:

Corolario 2.3.17. *Sea p un número primo y $f \in M_k(\Gamma_0(N), \chi)$, con $f(z) = \sum_{n\geq 0} a(n)q^n$. Se tiene:*

1. *Si $p|N$: $T_{p^l} = T_p^l$.*
2. *Si $p \nmid N$: $T_{p^{l+1}} = T_{p^l}T_p - \chi(p)pT_{p^{l-1}}$.*

Demostración. 1. Aplicando la ecuación (2.3.2) tenemos:

$$T_{p^l}(f) = p^{l(\frac{k}{2}-1)} \sum_{m=0}^{l} \sum_{0\leq b<p^{l-m}} \chi(p^m) f| \left(\begin{smallmatrix} p^m & b \\ 0 & p^{l-m} \end{smallmatrix}\right).$$

Ahora como $p|N$ tenemos que $\chi(p) = 0$ y por lo tanto todos los términos de la suma exterior salvo el primero se anulan y tenemos:

$$\begin{aligned} T_{p^l}(f) &= p^{l(\frac{k}{2}-1)} \sum_{0\leq b<p^l} f| \begin{pmatrix} 1 & b \\ 0 & p^l \end{pmatrix} = p^{l(\frac{k}{2}-1)} \sum_{0\leq b<p^{l-1}} \sum_{c=0}^{p-1} f| \begin{pmatrix} 1 & cp^{l-1}+b \\ 0 & p^l \end{pmatrix} \\ &= p^{l(\frac{k}{2}-1)} \sum_{0\leq b<p^{l-1}} \sum_{c=0}^{p-1} f| \begin{pmatrix} 1 & c \\ 0 & p \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & p^{l-1} \end{pmatrix} \\ &= p^{(l-1)(\frac{k}{2}-1)} \sum_{0\leq b<p^{l-1}} \left(p^{\frac{k}{2}-1} \sum_{c=0}^{p-1} f| \begin{pmatrix} 1 & c \\ 0 & p \end{pmatrix} \right) \Bigg| \begin{pmatrix} 1 & b \\ 0 & p^{l-1} \end{pmatrix} \\ &= T_{p^{l-1}}(T_p(f)). \end{aligned}$$

Es decir que tenemos $T_{p^l} = T_{p^{l-1}}T_p$ y por inducción se sigue lo que queremos.

2. Dada $f \in M_k(\Gamma_0, \chi)$ usamos la ecuación (2.3.2) para escribir $T_{p^l}T_p(f)$:

$$\begin{aligned} T_{p^l}T_p(f) &= \sum_{j=0}^{l} \sum_{b=0}^{p^j-1} \chi(p)^{l-j} T_p(f) \Bigg| \begin{pmatrix} p^{l-j} & b \\ 0 & p^j \end{pmatrix} \\ &= \sum_{j=0}^{l} \sum_{b=0}^{p^j-1} \chi(p)^{l-j} \left(\sum_{c=0}^{p-1} f \Bigg| \begin{pmatrix} 1 & c \\ 0 & p \end{pmatrix} + \chi(p) f \Bigg| \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right) \Bigg| \begin{pmatrix} p^{l-j} & b \\ 0 & p^j \end{pmatrix} \\ &= \sum_{j=0}^{l} \sum_{b=0}^{p^j-1} \sum_{c=0}^{p-1} \chi(p)^{l-j} f \Bigg| \begin{pmatrix} p^{l-j} & p^j c+b \\ 0 & p^{j+1} \end{pmatrix} \\ &\quad + \sum_{j=0}^{l} \sum_{b=0}^{p^j-1} \chi(p)^{l+1-j} f \Bigg| \begin{pmatrix} p^{l+1-j} & bp \\ 0 & p^j \end{pmatrix}. \end{aligned}$$

Para el primero de estos dos últimos términos notemos que las dos sumas interiores se pueden reemplazar por una única suma ya que cuando b y c recorren esos límites $p^j c + b$ va de 0 a $p^{j+1} - 1$. En la segunda suma podemos separar el término $j = 0$ y en los demás térmnos podemos factorizar la matriz que aparece como $\left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)\left(\begin{smallmatrix} p^{l-j} & b \\ 0 & p^{j-1} \end{smallmatrix}\right)$, y como el operador slash de la primera de estas matrices actúa trivialmente tenemos:

$$T_{p^l}T_p(f) = \sum_{j=0}^{l}\sum_{b=0}^{p^{j+1}-1} \chi(p)^{l-j} f\left|\begin{pmatrix} p^{l-j} & b \\ 0 & p^{j+1} \end{pmatrix}\right. + \chi(p)^{l+1} f\left|\begin{pmatrix} p^{l+1}0 & \\ 0 & 1 \end{pmatrix}\right. + \sum_{j=1}^{l}\sum_{b=0}^{p^j-1} \chi(p)^{l+1-j} f\left|\begin{pmatrix} p^{l-j} & b \\ 0 & p^{j-1} \end{pmatrix}\right..$$

Ahora observemos que la primera suma difiere de T_p^{l+1} precisamente en el término que separamos de la segunda. Por otro lado el operador slash de la última serie depende sólo de la clase de congruencia de b módulo p^{j-1}; luego podemos reemplazar la suma interior por p veces la suma con b recorriendo los números de 0 a $p^{j-1} - 1$. Es decir que tenemos:

$$\begin{aligned} T_{p^l}T_p(f) &= T_{p^{l+1}} + \sum_{j=1}^{l}\sum_{b=0}^{p^{j-1}-1} p\chi(p)^{l+1-j} f\left|\begin{pmatrix} p^{l-j} & b \\ 0 & p^{j-1} \end{pmatrix}\right. \\ &= T_{p^{l+1}} + p\chi(p)\sum_{j=1}^{l}\sum_{b=0}^{p^{j-1}-1} \chi(p)^{l-j} f\left|\begin{pmatrix} p^{l-j} & b \\ 0 & p^{j-1} \end{pmatrix}\right.. \end{aligned}$$

Por último notemos que haciendo un cambio de índice en la última suma se convierte en la expresión para $T_{p^{l-1}}$. De modo que tenemos que:

$$T_{p^l}T_p(f) = T_{p^{l+1}} + \chi(p)pT_{p^{l-1}}$$

como queríamos demostrar.

□

En particular de este resultado se deduce por inducción que T_{p^l} es siempre un polinomio en T_p, y junto con el resultado anterior obtenemos:

Corolario 2.3.18. *El álgebra generada por los operadores de Hecke en $M_k(\Gamma_0(N), \chi)$ es un álgebra conmutativa.*

Lema 2.3.19. *Si $f \in M_k(\Gamma_0(N), \chi)$ es una autoforma no nula y $a(n) \in \mathbb{C}$ son sus coeficientes de Fourier, entonces $a(1) \neq 0$.*

Demostración. Consideremos λ_m el autovalor de f asociado a T_m. Calculando el coeficiente $b(1)$ de q en $T_m(f)$ tenemos que:

$$\lambda_m a(1) = b(1) = \chi(1)a^{1-1}a(m1/1^2) = a(m).$$

Luego si $a(1)$ fuera cero todos los coeficientes de f se anularían. □

Definición 2.3.20. Decimos que una autoforma está *normalizada* si el coeficiente de q en su desarrollo de Fourier es 1.

En la demostración del lema anterior se puede ver que en una autoforma normalizada sus coeficientes de Fourier son precisamente los autovalores de los correspondientes operadores de Hecke.

Corolario 2.3.21. *Sea $f \in M_k(\Gamma_0(N), \chi)$ una autoforma normalizada con $a(n)$ sus coeficientes de Fourier.*

1. *Si $(m : n) = 1$ entonces $a(mn) = a(m)a(n)$.*
2. *Si p es primo y $p|N$ entonces $a(p^l) = a(p)^l$.*
3. *Si p es primo y $p \nmid N$ entonces $a(p^l) = a(p)a(p^{l-1}) - \chi(p)p^{k-1}a(p^{l-2})$ si $l \geq 2$.*

Demostración. Por lo que observamos antes los coeficientes de la serie son precisamente los autovalores de los operadores de Hecke. Luego aplicando el Corolario 2.3.16 tenemos que:

$$a(mn)f = T_{mn}f = T_mT_n(f) = T_m(a(n)f) = a(n)a(m)f.$$

Análogamente aplicando el Corolario 2.3.17, vemos que si $p|N$:

$$a(p^l)f = T_{p^l}(f) = T_p^l(f) = a(p)^l f,$$

y si $p \nmid N$:

$$a(p^l)f = T_{p^l}(f) = (T_{p^{l-1}}T_p + \chi(p)pT_{p^{l-2}}(f) = (a(p)a(p^{l-1}) + \chi(p)pa(p^{l-2}))f.$$

Asumiendo entonces que f es no nula tenemos lo que queremos. □

Los resultados anteriores nos dan las propiedades de mutliplicativadad de los coeficientes de las autoformas, y estos se van a corresponder con los productos de Euler de las L-series asociadas a estas. Como el álgebra de los operadores de Hecke es conmutativa en caso de que cada uno fuera diagonalizable existirían bases de autoformas en los espacios de formas modulares. Para poder justificar esto buscamos un producto interno respecto al cual los operadores resulten autoadjuntos.

Definición 2.3.22. Dadas $f \in M_k(\Gamma)$ y $g \in S_k(\Gamma)$ definimos el *producto de Petersson* entre estas como:

$$\langle f, g\rangle = \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]} \int\int_{\mathcal{D}} y^{k-2} f(z) \cdot \overline{g(z)} dxdy,$$

donde $\mathcal{D}$ es un dominio fundamental para Γ.

Proposición 2.3.23. *El producto de Petersson de dos formas modulares es finito.*

Demostración. Primero observemos que por el Teorema 2.1.14 podemos podemos elegir $\gamma_1, \dots, \gamma_r \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$, tales que $\mathcal{D} = \cup_{i=1}^r \gamma_i \mathcal{F}$, donde $r = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. Luego tenemos que:

$$\langle f, g \rangle = \frac{1}{r} \sum_{i=1}^{r} \int \int_{\gamma_i \mathcal{F}} y^{k-2} f(z) \cdot \overline{g(z)} dx dy$$

y aplicando el teorema de cambio de variables podemos reescribir cada una de estas integrales como una integral sobre $\mathcal{F}$. Utilizando (2.1.1) vemos como cambia y al aplicar γ_i y obtenemos entonces:

$$\begin{aligned}
\langle f, g \rangle &= \frac{1}{r} \sum_{i=1}^{r} \int \int_{\mathcal{F}} \frac{y^{k-2}}{|c_i z + d_i|^{2k-2}} f(\gamma_i z) \cdot \overline{g(\gamma_i z)} |J_i| dx dy \\
&= \frac{1}{r} \sum_{i=1}^{r} \int \int_{\mathcal{F}} \frac{y^{k-2}}{|c_i z + d_i|^{2k-4}} (c_i z + d_i)^k f|\gamma_i(z) \cdot (\overline{c_i z + d_i^k}) \overline{g|\gamma_i(z)} |J_i| dx dy \\
&= \frac{1}{r} \sum_{i=1}^{r} \int \int_{\mathcal{F}} y^{k-2} |c_i z + d_i|^4 f|\gamma_i(z) \cdot \overline{g|\gamma_i(z)} |J_i| dx dy
\end{aligned}$$

donde J_i es el jacobiano de la multiplicación por γ_i. Notando μ_i a la multiplicación por γ_i, de las ecuaciones de Cauchy-Riemann se desprende que:

$$J_i = \partial_x \Re(\mu_i) \partial_y \Im(\mu_i) - \partial_y \Re(\mu_i) \partial_x \Im(\mu_i) = \left| \frac{d\mu_i}{dz} \right|^2.$$

Por otro lado es fácil ver que $\frac{d\mu_i}{dz}(z) = (c_i z + d_i)^{-2}$, de modo que podemos reescribir el producto de Petersson como:

$$\langle f, g \rangle = \frac{1}{r} \sum_{i=1}^{r} \int \int_{\mathcal{F}} y^{k-2} f|\gamma_i(z) \cdot \overline{g|\gamma_i(z)} dx dy.$$

Por último recordemos que por la Observación 2.2.7 como g es cuspidal, $\left| g|\gamma_i(z) \right| = O\left(e^{-y/N}\right)$, y como $f|\gamma_i$ está acotada cuando z tiende a $i\infty$ cada una de estas integrales es finita. □

Proposición 2.3.24. *Sean $\Gamma_1 < \Gamma_2$ dos subgrupos de congruencia, $f \in M_k(\Gamma_2) < M_k(\Gamma_1)$ y $g \in S_k(\Gamma_2) < S_k(\Gamma_1)$. Entonces el producto de Petersson $\langle f, g \rangle_1$ como formas modulares para Γ_1 coincide con el producto de Petersson $\langle f, g \rangle_2$ como formas para Γ_2.*

Demostración. De manera análoga a como probamos el Teorema 2.1.14 podemos ver que existen $\gamma_1, \dots, \gamma_r \in \Gamma_2$, con $r = [\Gamma_2 : \Gamma_1]$, tales que $\mathcal{D}_1 = \cup_{i=1}^r \gamma_i \mathcal{D}_2$. Luego argumentando

como en el teorema anterior obtenemos:

$$\begin{aligned}\langle f,g\rangle_1 &= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_1]}\int\int_{\mathcal{D}_1} y^{k-2}f(z)\cdot\overline{g(z)}dxdy\\ &= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_2]}\frac{1}{[\Gamma_2:\Gamma_1]}\sum_{i=1}^{r}\int\int_{\mathcal{D}_2} y^{k-2}f|\gamma_i(z)\cdot\overline{g|\gamma_i(z)}dxdy\\ &= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_2]}\frac{1}{r}\sum_{i=1}^{r}\int\int_{\mathcal{D}_2} y^{k-2}f(z)\cdot\overline{g(z)}dxdy\\ &= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_2]}\int\int_{\mathcal{D}_2} y^{k-2}f(z)\cdot\overline{g(z)}dxdy = \langle f,g\rangle_2.\end{aligned}$$

□

Se puede ver (por ejemplo en [Kob93, III.5 Proposición 48] que los operadores de Hecke sobre $M_k(\Gamma_0(N),\chi)$ satisfacen $\langle T_n(f);g\rangle = \chi(n)\langle f;T_n(g)\rangle$, si n es coprimo con N. En particular los operadores $\chi(n)^{1/2}T_n$ son operadores autoadjuntos, siempre que $(N:n)=1$, y por el teorema espectral admiten una base de autovectores, y como los operadores de Hecke conmutan obtenemos entonces una base de autovectores simultáneos de todos los operadores de Hecke coprimos con el nivel. Para poder obtener una base de autoformas debemos restringirnos al espacio de las denominadas "formas nuevas".

En el espacio de formas modulares $M_k(\Gamma_1(N))$ además de los operadores de Hecke actúan también otros operadores. En la próxima sección vamos a usar la denominada *involución de Atkin-Lehner*. Tomando la matriz $w_N = \left(\begin{smallmatrix}0 & -1\\ N & 0\end{smallmatrix}\right)$ el operador de Atkin-Lehner está definido por $f\mapsto f|w_N$. Si $\gamma\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in\Gamma_0(N)$ entonces tenemos:

$$w_N\gamma w_N^{-1} = \begin{pmatrix} d & -c/N\\ -Nb & a\end{pmatrix}\in\Gamma_0(N).$$

Por lo tanto si $f\in S_k(\Gamma_0(N),\chi)$ y $g=f|w_N$ se tiene que:

$$g|\gamma(z) = f|(w_N\gamma)(z) = f|(w_N\gamma w_N^{-1}w_N)(z) = \chi(a)f|w_N(z) = \overline{\chi}(d)g(z),$$

es decir que $f\in M_k(\Gamma_0(N),\overline{\chi})$; más aún no es difícil ver que la aplicación $f\mapsto f|w_N$ conmuta con los operadores de Hecke y preserva la cuspidalidad, es decir que $f|w_N\in S_k(\Gamma_0(N),\overline{\chi}$ si f es cuspidal. Como w_N^2 es una matriz escalar el operador de Atkin-Lehner en $M_k(\Gamma_1(N)$ es una involución, y entonces los espacios $M_k(\Gamma_1(N))$ y $S_k(\Gamma_1(N))$ se descomponen como una suma directa en los autoespacios de autovalor 1 y -1 de este operador.

Además de la involución de Atkin-Lehner podemos definir los siguientes operadores, que en este caso alteran el nivel:

Definición 2.3.25. Dado un número natural m, definimos el operador U_m en las formas modulares por $U_m(f) = f|\left(\begin{smallmatrix}m & 0\\ 0 & 1\end{smallmatrix}\right)$.

Lema 2.3.26. *Si $mM|N$ se tiene que U_m aplica $M_k(\Gamma_0(M),\chi)$ en $M_k(\Gamma_0(N),\tilde{\chi})$, donde $\tilde{\chi}$ es el caracter módulo N inducido por χ.*

Demostración. Sea $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ y $f \in M_k(\Gamma_0(M),\chi)$, entonces tenemos:

$$U_m(f)|\gamma = f\left|\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = f\right|\begin{pmatrix} ma & mb \\ c & d \end{pmatrix}.$$

Como c es divisible por N, $M|(c/m)$ y podemos escribir:

$$U_m(f)|\gamma = f\left|\begin{pmatrix} a & mb \\ c/m & d \end{pmatrix}\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} = \chi(d)f\right|\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} = \chi(d)U_m(f).$$

□

Escribiendo $f(z) = \sum_{n=0}^{\infty} a_n q^n$, tenemos que $U_m(f)(z) = \sum_{n=0}^{\infty} a_n q^{nm}$. Aplicando entonces el Teorema 2.3.15 es fácil ver que U_m también conmuta con todos los operadores de Hecke.

Definición 2.3.27. Definimos el espacio de *formas viejas* $S_k^{\text{old}}(\Gamma_1(N))$ como el generado por las imágenes de todos los morfismos $U_m : S_k(\Gamma_1(M)) \to S_k(\Gamma_1(N))$, con $Mm|N$. El espacio de *formas nuevas* es $S_k^{\text{new}}(\Gamma_1(N)) = S_k^{\text{old}}(\Gamma_1(N))^{\perp}$.

Atkin y Lehner probaron que en el espacio de formas nuevas $S_k^{\text{new}}(\Gamma_1(N))$ los autoespacios comunes a todos los operadores de Hecke T_n con $(N:n) = 1$, que sabemos que descomponenen al espacio de formas porque estos son autoadjuntos, tienen dimensión 1. Como tanto los demás operadores de Hecke como la involución de Atkin-Lehner conmutan con todos los operadores anteriores deben preservar estos autoespacios comunes. Pero como tienen dimensión 1 esto quiere decir que son también autoespacios para estos operadores. Es decir que los espacios de formas nuevas admiten bases de autoformas, que además resultan autovectores para la involución de Atkin-Lehner.

2.4. L-series

A una forma modular le vamos a asignar una L-serie de la siguiente manera:

Definición 2.4.1. Dada una forma modular f con desarrollo de Fourier $\sum_{n=0}^{\infty} a_n q^n$, definimos su L-serie:

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

La definición anterior es esencialmente formal. Se puede ver que los coeficientes de Fourier de una forma modular de peso k satisfacen $a_n = O(n^{k-1+\epsilon})$ para todo $\epsilon > 0$. Esto nos permite concluir que esta L-serie converge absolutamente en el semiplano $\Re(s) > k$. Para entender mejor las propiedades analíticas de esta serie de Dirichlet vamos a introducir un operador integral y ver que la serie $L(f,s)$ se puede obtener aplicando dicho operador a la forma f.

Definición 2.4.2. Dada una función $f : \mathbb{R}_{>}0 \to \mathbb{C}$, definimos su *transformada de Mellin*, como:

$$\mathcal{M}\{f\}(s) = \int_0^\infty f(t)t^{s-1}dt.$$

En general la transformada de Mellin de una función f está bien definida en una franja de la forma $a < \Re(s) < b$, para ciertos a y b que dependen del comportamiento asintótico de $f(t)$ cuando t tiende a 0 y a ∞. Usando el teorema de diferenciación bajo el signo de la integral se ve que define de hecho una función holomorfa en esta región.

Lema 2.4.3. *Si consideramos la función $g(t) = e^{-2\pi nt}$, con $n \in \mathbb{N}$, entoces tenemos que:*

$$\mathcal{M}\{g\}(s) = \frac{\Gamma(s)}{(2\pi)^s n^s}, \quad \Re(s) > 0.$$

Demostración. Simplemente haciendo el cambio de variables $\tilde{t} = 2\pi tn$ tenemos:

$$\begin{aligned}\mathcal{M}\{g\}(s) &= \int_0^\infty e^{-2\pi tn}t^{s-1} = \int_0^\infty e^{\tilde{t}}(\frac{\tilde{t}}{2\pi n})^{s-1}\frac{d\tilde{t}}{2\pi n} \\ &= \frac{1}{(2\pi)^s n^s}\int_0^\infty e^{-t}t^{s-1}dt = \frac{\Gamma(s)}{(2\pi)^s n^s}.\end{aligned}$$

□

De el resultado anterior podemos obtener la L-serie de una forma modular en términos de su transformada de Mellin como:

Proposición 2.4.4. *Si f es una forma cuspidal tomando $g : \mathbb{R} \to \mathbb{C}$ definida por $g(t) = f(it)$ tenemos:*

$$\mathcal{M}\{g\}(s) = \frac{\Gamma(s)}{(2\pi)^s}L(f, s),$$

donde la serie de Dirichlet converge absolutamente.

Demostración.

$$\begin{aligned}\mathcal{M}\{g\}(s) &= \int_0^\infty \sum_{n=1}^\infty a_n e^{-2\pi nt}t^{s-1}dt = \sum_{n=1}^\infty \int_0^\infty a_n e^{-2\pi nt}t^{s-1}dt \\ &= \sum_{n=1}^\infty \frac{\Gamma(s)a_n}{(2\pi)^s n^s} = \frac{\Gamma(s)}{(2\pi)^s}L(f, s).\end{aligned}$$

Donde la segunda igualdad está justificada por la convergencia absoluta de la serie de Dirichlet. □

En el caso de que f no sea cuspidal podemos considerar la transformada de Mellin de $g(t) = f(it) - a_0$. Usando esta descripción de la L-serie podemos obtener los resultados de continuación analítica y ecuación funcional:

Teorema 2.4.5. *Sean $f \in S_k(\Gamma_1(N))$ y $g = f|w_N$ la involución de Atkin-Lehner aplicada a f, entonces las L-series completadas:*

$$\Lambda_f(s) = \frac{\sqrt{N}^s}{(2\pi)^s}\Gamma(s)L(f,s), \qquad \Lambda_g(s) = \frac{\sqrt{N}^s}{(2\pi)^s}\Gamma(s)L(g,s),$$

se extienden a funciones holomorfas en todo $\mathbb{C}$ y satisfacen la ecuación funcional:

$$\Lambda_f(s) = i^k\Lambda_g(k-s).$$

Demostración. Cuando $\Re(s) > k$ la L-serie converge absolutamente y tenemos:

$$\begin{aligned}\frac{\Gamma(s)}{(2\pi)^s}L(g,s) &= \int_0^\infty g(it)t^{s-1}dt = \int_0^1 g(it)t^{s-1}dt + \int_1^\infty g(it)t^{s-1}dt \\ &= N^{-k/2}i^{-k}\int_0^1 f(\frac{i}{Nt})t^{s-k-1}dt + \int_1^\infty g(it)t^{s-1}dt.\end{aligned}$$

Haciendo un cambio de variables en la primera de las dos integrales:

$$\begin{aligned}\frac{\Gamma(s)}{(2\pi)^s}L(g,s) &= N^{-k/2}i^{-k}\int_{1/N}^\infty N^{1-s}f(it)t^{k-s-1}dt + \int_1^\infty g(it)t^{s-1}dt \\ &= N^{k/2-s}i^{-k}\int_{1/N}^\infty f(it)t^{k-s-1}dt + \int_1^\infty g(it)t^{s-1}dt.\end{aligned}$$

Ahora por la Observación 2.2.7 ambas de estas integrales están bien definidas para todo s y definen funciones holomorfas por el teorema de diferenciación bajo el signo de la integral. Esto demuestra que Λ_g se extiende una función entera, y lo mismo sucede con Λ_f.

Para ver la ecuación funcional realizamos el mismo cambio de variable de antes pero sin separar la integral en dos términos:

$$\begin{aligned}\frac{\Gamma(s)}{(2\pi)^s}L(g,s) &= \int_0^\infty g(it)t^{s-1}dt = i^{-k}N^{-k/2}\int_0^\infty f(\frac{i}{tN})t^{s-k-1}dt \\ &= i^{-k}N^{-k/2}\int_0^\infty f(it)t^{k-1-s}N^{k-s}dt = i^{-k}N^{k/2-s}\int_0^\infty f(it)t^{k-s-1}dt \\ &= i^{-k}N^{k/2-s}\frac{\Gamma(k-s)}{(2\pi)^{k-s}}L(f,k-s),\end{aligned}$$

y multiplicando a ambos lados de la ecuación por $N^{s/2}$ obtenemos la ecuación funcional. □

Recordemos que, por ser una involución, el operador de Atkin-Lehner descompone al espacio de formas modulares en sus autoespacios de autovalor 1 y -1. Aplicando el resultado anterior al caso particular de un autovector para Atkin-Lehner, y en particular para una autoforma nueva se tiene:

Corolario 2.4.6. *Si $f \in S_k(\Gamma_1(N))$ es un autovector de autovalor $\omega = \pm 1$ para la involución de Atkin-Lehner y $\Lambda_f(s)$ es su L-serie completada se tiene:*

$$\Lambda_f(s) = \omega i^k \Lambda_f(k-s).$$

En el caso en que la forma f no sea cuspidal se tiene un resultado similar. En este caso la extensión anlítica que se obtienen son funciones meromorfas que tienen únicamente dos polos simples, en $s = 0$ y $s = k$, cuyos residuos son los coeficientes que acompañan a q^0 en los desarrollos de Fourier de las formas f y g. Para poder describir un resulta converso a a este introducimos el *twist* de una forma modular:

Teorema 2.4.7. *Sean $f \in M_k(\Gamma_0(N), \chi)$, m el conductor de χ y ψ un caracter primitivo módulo r. Si el desarrollo de Fourier de f está dado por:*

$$f(z) = \sum_{n=0}^{\infty} a_n q^n,$$

entonces el twist de f por ψ, definido por:

$$f \otimes \psi(z) = \sum_{n=0}^{\infty} a_n \psi(n) q^n,$$

es una forma modular para $\Gamma_0(\tilde{N})$ de caracter $\chi\psi^2$, donde $\tilde{N} = mcm(N, mr, r^2)$.

Demostración. Sea $\tau(\overline{\psi}) = \sum_{l=0}^{r} \overline{\psi(l)} e^{2\pi i l/r}$, la suma de Gauss del caracter $\overline{\psi}$. No es difícil ver que:

$$\tau(\overline{\psi})\psi(n) = \sum_{l=1}^{r} \overline{\psi(l)} e^{2\pi i l n/r}.$$

Usando esta identidad tenemos:

$$\tau(\overline{\psi}) f \otimes \psi = \sum_{l=1}^{r} \overline{\psi(l)} f| \left(\begin{smallmatrix} 1 & l/r \\ 0 & 1 \end{smallmatrix}\right). \tag{2.4.1}$$

Dada una matriz $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\tilde{N})$, se tiene:

$$\begin{pmatrix} 1 & l/r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -d^2 l/r \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} a & * \\ 0 & d \end{pmatrix} \pmod{m}$$

y la matriz de la izquierda se encuentra en $\Gamma_0(\tilde{N})$, de modo que como $f \in M_k(\Gamma_0(\tilde{N}), \chi)$:

$$\sum_{l=1}^{r} \overline{\psi(l)} f| \left(\begin{smallmatrix} 1 & l/r \\ 0 & 1 \end{smallmatrix}\right) \gamma = \sum_{l=1}^{r} \overline{\psi(l)} \chi(d) f| \left(\begin{smallmatrix} 1 & d^2 l/r \\ 0 & 1 \end{smallmatrix}\right).$$

Como d es coprimo con $\tilde{N}$, cuando l recorre todas las clases residuales módulo r, d^2l también lo hace y podemos reescribir la última suma para obtener:

$$\tau(\overline{\psi})f\otimes\psi|\gamma=\chi(d)\sum_{l=1}^{r}\psi(d^2)\overline{\psi(l)}f|\begin{pmatrix}1 & l/r\\ 0 & 1\end{pmatrix}=\chi(d)\psi(d)^2\tau(\overline{\psi})f\otimes\psi.$$

Como ψ es un caracter primitivo módulo r, la suma de Gauss no es nula, de donde se deduce que $f\otimes\psi$ satisface la condición de modularidad. Por otro lado de (2.4.1) es claro que el twist satisface la condición de holomorfía y de crecimiento también, y es por lo tanto una forma modular. □

Dada una serie de Dirichlet $\sum_{n=1}^{\infty}\frac{a_n}{n^s}$, los resultados anteriores nos dicen que si sus coeficientes son los coeficientes de una forma modular, entonces esta serie y todos sus twists $\sum_{n=1}^{\infty}\frac{a_n\chi(n)}{n^s}$, con χ un caracter de Dirichlet, admiten una extensión meromorfa a todo el plano complejo y satisfacen una ecuación funcional. Estas propiedades junto con algunas más nos aseguran de hecho que los coeficientes de la L-serie sean los de una forma modular:

Teorema 2.4.8 (Teorema Converso de Weil)**.** *Sean:*

$$f(z)=\sum_{n=0}^{\infty}a_nq^n\qquad\qquad g(z)=\sum_{n=0}^{\infty}b_nq^n$$

series de Fourier con $a_n,b_n=O(n^\alpha)$, para algún $\alpha\geq 0$, $k\in 2\mathbb{N}$ y χ un caracter primitivo módulo N. Más aún supongamos que las L-series completadas:

$$\Lambda_f(s)=\frac{\sqrt{N}^s}{(2\pi)^s}\Gamma(s)L(f,s)\qquad\qquad\Lambda_g(s)=\frac{\sqrt{N}^s}{(2\pi)^s}\Gamma(s)L(g,s),$$

admiten una continuación meromorfa a todo $\mathbb{C}$ con:

$$\Lambda_f(s)+\frac{a_0}{s}+\frac{b_0i^k}{k-s}\qquad y\qquad\Lambda_g(s)+\frac{b_0}{s}+\frac{a_0i^k}{k-s},$$

enteras y acotadas en franjas verticales y satisfacen la ecuación funcional $\Lambda_f(s)=i^k\Lambda_g(k-s)$. Existe una familia finita de primos R, que depende sólo de N, tal que si todas las L-series completadas:

$$\Lambda_f(s,\psi)=\frac{\sqrt{\tilde{N}}^s}{(2\pi)^s}\Gamma(s)\sum_{n=1}^{\infty}\frac{a_n\psi(n)}{n^s},$$
$$\Lambda_g(s,\psi)=\frac{\sqrt{\tilde{N}}^s}{(2\pi)^s}\Gamma(s)\sum_{n=1}^{\infty}\frac{b_n\psi(n)}{n^s},$$

donde ψ es un caracter primitivo módulo $r\in R$, y $\tilde{N}=Nr^2$, satisfacen la ecuación funcional:

$$\Lambda_f(s,\psi)=w(\psi)i^k\Lambda_g(k-s,\overline{\psi}),$$

donde $w(\psi)$ es un número complejo que depende de ψ y χ, entonces $f\in M_k(\Gamma_0(N),\chi)$, $g\in M_k(\Gamma_0(N),\overline{\chi}$ y $g=f|w_N$.

2.5. Modularidad de curvas elípticas

Cuando tomamos $f \in S_k(\Gamma_0(N), \chi)$ una autoforma normalizada el Corolario 2.3.21 nos dice que sus coeficientes satisfacen ciertas relaciones de multiplicatividad y esto junto con el Lema 1.3.5 nos permite obtener el siguiente producto de Euler para la L-serie de esta forma modular:

Proposición 2.5.1. *Sea $f \in S_k(\Gamma_0(N), \chi)$ una autoforma, y sea $\sum_{n=1}^{\infty} a_n q^n$ su desarrollo de Fourier. Entonces se tiene:*

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

Comparando los factores de este producto de Euler con los que aparecen en la definición de la L-serie asociada a una curva elíptica general (Observación 1.3.2), podemos ver que los factores locales de ambos tipos de L-series son esencialmente los mismos. Más precisamente la L serie de una autoforma de peso 2, caracter trivial y nivel N, admite el mismo tipo de factorización que la L-serie de una curva elíptica de conductor N, lo que nos lleva a hacer la definición:

Definición 2.5.2. Decimos que una curva elíptica E es *modular* si existe una forma modular f tal que:

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

La teoría de Eichler-Shimura permite asociar a una autoforma nueva normalizada de nivel N y con todos sus autovalores enteros una curva elíptica, más precisamente una clase de isogenía de curvas elípticas, de conductor N, de manera que que comparten la misma L-serie. La curva E^1 resulta tener conductor 32. Las curvas de conductor 32 están clasificadas y hay cuatro clases de isomorfismo. Más aún estas cuatro curvas están en la misma clase de isogenía y por lo tanto tienen todas la misma L-serie.

Por otro lado la dimensión del espacio $S_k(\Gamma_0(32))$ también está calculada y es 1, i.e. existe una única autoforma normalizada de nivel 32 y caracter trivial. Su L-serie se corresponde con la de una curva elíptica de conductor 32, y como todas estas comparten su L-serie tiene que valer que la L-serie de la curva elíptica E^1 debe coincidir con la de la única autoforma ϕ de nivel 32 y caracter trivial.

Las curvas E^d que nos interesan están dadas como twists de la curva E^1 por el caracter χ_d. Ahora por el Teorema 2.4.7 los twists $\phi \otimes \chi_d$ son también formas modulares. Por la Proposición 1.3.6 las L-series de estos twists de ϕ coinciden con las L-series de las curvas E^d. Tenemos entonces que todas las curvas E^d son modulares, y por lo tanto sus L-series admiten una continuación analítica que satisface una ecuación funcional.

La importancia de esto radica en la relación, en parte conjetural, de las propiedades geométricas y aritméticas de una curva elíptica E con el comportamiento de su L-serie en $s = 1$. Notemos que en principio la función $L(E,s)$ no está definida en $s = 1$, por lo que para darle sentido a estas conjeturas uno debe a priori restringirse a una clase de curvas cuya L-serie admita una extensión analítica. Concretamente a principios de los '60 Birch y Swinnerton-Dyer conjeturaron lo siguiente:

Conjetura 2.5.3 (Birch y Swinnerton-Dyer)**.** *Sea E una curva elíptica definida sobre $\mathbb{Q}$ y modular, entonces $L(E,1) \neq 0$ si y sólo si $E(\mathbb{Q})$ es finito. Más aún el rango de $E(\mathbb{Q})$ coincide con el orden de anulación de $L(E,s)$ en $s=1$.*

La anterior es de hecho una forma débil de la conjetura. En su forma más fuerte da una expresión para el primer coeficiente no nulo del desarrollo de Taylor de $L(E,s)$ alrededor de 1 en términos de invariantes geométricos de la curva E. Su forma más débil nos alcanza sin embargo para concluir lo siguiente:

Proposición 2.5.4. *Si la conjetura de Birch y Swinnerton-Dyer es cierta un entero positivo $d \in \mathbb{N}$ libre de cuadrados es congruente si y sólo si $L(E^d,1)=0$.*

Demostración. Por el Teorema 1.2.13 sabemos que d es un número congruente si y sólo si la curva E^d tiene rango positivo, y si la conjetura de Birch y Swinnerton-Dyer es cierta esto sucede si y sólo si $L(E^d,1)=0$. □

Aunque la conjetura de Birch y Swinnerton-Dyer parece todavía estar lejos de ser demostrada se tienen los siguientes resultados parciales importantes:

Teorema 2.5.5 (Coates-Wiles, 1977)**.** *Sea E una curva elíptica modular definida sobre los racionales con multiplicación compleja por el anillo de enteros de un cuerpo de números cuyo número de clase es 1. Si $L(E,1) \neq 0$ entonces $E(\mathbb{Q})$ es finito.*

El enunciado anterior usa la noción de multiplicación compleja. Dada una curva elíptica E definida sobre $\mathbb{Q}$ los endomorfismos de grupo $E(\overline{\mathbb{Q}})$ que están dadas por funciones algebraicas forman un anillo, esto es simplemente porque la estructura de grupo de esta es abeliana. Se puede ver que este anillo es o bien $\mathbb{Z}$ o un orden en una extensión cuadrática de $\mathbb{Q}$ o un álgebra de cuaterniones de $\mathbb{Q}$. Lo más usual, en algún sentido preciso, es que el anillo de endomorfismos sea $\mathbb{Z}$, en otro caso se dice que la curva tiene multiplicación compleja.

En el caso de las curvas E^d que nos interesan a nosotros se puede mostrar que el anillo de endomorfismos es $\mathbb{Z}[i]$. Concretamente la acción de i está dada por $(x,y) \mapsto (-x, iy)$. Es claro que esta acción es algebraica y tiene orden 4, se puede verificar también, por ejemplo usando fórmulas explícitas para la suma de puntos, que es de hecho un morfismo de grupos.

El resultado de Coates-Wiles es suficiente para mostrar una de las implicaciones de la proposición anterior. La otra implicación solo la podríamos asegurar en casos donde tengamos más información sobre el orden de anulación de la L-serie; por ejemplo si supieramos que el orden es exactamente 1 se puede aplicar el siguiente resultado:

Teorema 2.5.6 (Gross-Zagier, 1986)**.** *Sea una E curva elíptica modular definida sobre $\mathbb{Q}$ tal que $L(E,s)$ tiene un cero de orden 1 en $s=1$. Entonces $E(\mathbb{Q})$ tiene rango por lo menos 1.*

Taniyama y Shimura conjeturaron en los '50 que todas las curvas elípticas debían ser modulares. En 1995 Andrew Wiles [Wil95] demostró este resultado para las curvas elípticas denominadas *semiestables*. Finalmente en el 2001 luego del trabajo de múltiples autores se pudo terminar de demostrar el resultado para todas las curvas elípticas definidas sobre $\mathbb{Q}$. Es decir que se tiene:

Teorema 2.5.7 (Teorema de modularidad, Wiles et al., 2001)**.** *Toda curva elíptica definida sobre $\mathbb{Q}$ es modular.*

Este resultado nos dice que la hipótesis de modularidad en los teoremas anteriores es innecesaria, y que las L-series de todas las curvas elípticas definidas sobre $\mathbb{Q}$ admiten una extensión anlítica que satisface una ecuación funcional.

Capítulo 3

Formas modulares de peso medio entero

3.1. El grupo metapléctico

El último ingrediente necesario para atacar el problema que nos interesa son las formas modulares de peso medio entero, i.e. peso $k/2$ con k un natural impar. Siguiendo la definición que habíamos hechos para formas modulares de peso entero una de estas formas, f, debería satisfacer $f(\gamma z) = j(\gamma, z)^{k/2} f(z)$ para todo γ en algún subgrupo de congruencia Γ. La primera dificultad que nos encontramos con esta definición es como interpretar el exponente fraccionario. Uno podría elegir para cada $\gamma \in \Gamma$ una rama de la raíz de de $j(\gamma, z)$, que se puede ya que $\mathcal{H}$ es simplemente conexo y $j(\gamma, \mathcal{H})$ no contiene al cero. El problema es que en general no se puede hacer ninguna elección que haga que el factor $j(\gamma, z)$ satisfaga la relación de cociclo (Lema 2.2.2), que es lo que necesitamos para poder definir la acción del grupo en el espacio de funciones. La manera de resolver esta complicación es considerar formas modulares sobre una extensión:

Definición 3.1.1. El *grupo metapléctico* es el grupo definido por:

$$G = \left\{ (\alpha, \phi) \in \mathrm{GL}_2^+(\mathbb{Q}) \times \mathbb{C}^{\mathcal{H}} : \phi \text{ es holomorfa y } \phi(z)^2 = \pm \frac{j(\alpha, z)}{\sqrt{\det(\alpha)}} \right\},$$

con el producto de dos elementos G, $(\alpha_1, \phi_1), (\alpha_2, \phi_2)$ definido como $(\alpha_1\alpha_2, \tilde{\phi})$, donde $\tilde{\phi}(z) = \phi_1(\alpha_2 z)\phi_2(z)$. Consideramos también el subgrupo definido por las matrices con coeficientes enteros:

$$G' = \{(\alpha, \phi) \in G : \alpha \in \mathrm{SL}_2(\mathbb{Z})\}.$$

Lema 3.1.2. *El grupo metapléctico es efectivamente un grupo.*

Demostración. Verifiquemos primero que el producto está bien definido, es decir que la

función $\tilde{\phi}$ cumple la condición que queremos:

$$\begin{aligned}\tilde{\phi}(z)^2 = \phi_1(\alpha_2 z)^2\phi_2(z)^2 &= t_1\frac{j(\alpha_1,\alpha_2 z)}{\sqrt{\det(\alpha_1)}}t_2\frac{j(\alpha_2,z)}{\sqrt{\det(\alpha_2)}}\\ &= (t_1t_2)\frac{j(\alpha_1\alpha_2,z)}{\sqrt{\det(\alpha_1\alpha_2)}},\end{aligned}$$

donde t_i es el signo que aparece en la definición del grupo metapléctico. Por lo tanto el producto de dos elementos de G está efectivamente en G. Verificar la asociatividad es inmediato de la definición del producto, y para verificar la existencia de un inverso para (α,ϕ) basta con tomar (α^{-1},ϕ') con $\phi'(z) = \phi(\alpha^{-1}z)^{-1}$. Que el producto de estos dos pares da el par $(\mathrm{Id},1)$ es inmediato, solo hay que chequear que efectivamente el par que estamos tomando es un elemento de G:

$$\phi'(z)^2 = \phi(\alpha^{-1}z)^{-2} = t^{-1}\frac{\sqrt{\det(\alpha)}}{j(\alpha,\alpha^{-1}z)} = t^{-1}\frac{j(\alpha^{-1},z)}{j(\mathrm{Id},z)\sqrt{\det(\alpha^{-1})}} = t^{-1}\frac{j(\alpha^{-1},z)}{\sqrt{\det(\alpha^{-1})}}.$$

□

Observación 3.1.3. El grupo metapléctico resulta, esencialmente por definición, una extensión de $\mathrm{GL}_2^+(\mathbb{Q})$ por el grupo de raíces cuartas de la unidad. El hecho que mencionamos antes de no poder elegir ramas de la raíz cuadrada de manera compatible se corresponde con que la proyección a $\mathrm{GL}_2^+(\mathbb{Q})$ no admita secciones:

$$\begin{array}{ccccccc} 0 \to & \{\pm 1,\pm i\} & \longrightarrow & G & \longrightarrow & \mathrm{GL}_2^+(\mathbb{Q}) & \to 0\\ & t & \longmapsto & (\mathrm{Id},t) & & & \\ & & & (\alpha,\psi) & \longmapsto & \alpha & \end{array}$$

Definición 3.1.4. Dado $k\in\mathbb{N}$ y $\xi = (\alpha,\phi)\in G$ podemos definir el operador $-|\xi$ en las funciones holomorfas del semiplano superior por:

$$f|\xi(z) = f(\alpha z)\phi(z)^{-k}.$$

Observación 3.1.5. Cuando $\phi(z)^2 = j(\alpha,z)/\det(\alpha)$, i.e. el signo del par es 1, si reemplazamos el peso k por $2k$ recuperamos la Definición 2.2.1.

Si uno se restringe a $\Gamma_0(4)$ se puede definir una sección de la proyección a las matrices. Dado $d\in\mathbb{Z}$ coprimo con 4 tomamos ϵ_d dado por:

$$\epsilon_d = \begin{cases} 1 & \text{si } d\equiv 1 \pmod 4,\\ i & \text{si } d\equiv 3 \pmod 4\end{cases},$$

y para $\gamma = \left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in\Gamma_0(4)$ y $z\in\mathcal{H}$ definimos:

$$\phi(\gamma,z) = \epsilon_d\left(\frac{c}{d}\right)\sqrt{cz+d}.$$

Es claro que $\phi(\gamma,z)^2 = \pm j(\gamma,z)$. Para ver que la aplicación $\alpha \mapsto (\alpha, \phi(\alpha,-))$ es una sección, i.e. es morfismo de grupos, basta con ver ϕ satisface la ecuación de cociclo (es la misma cuenta que hicimos en el Lema 2.2.2). Vamos a dar una idea de cómo ver que esta función ϕ satisface la condición de cociclo. En principio esto se podría verificar directamente de la definición, pero esto resulta demasiado engorroso. La forma usual de demostrarlo es encontrar una función que satisfaga la condición de modularidad con este cociclo, es decir encontrar una función holomorfa $f : \mathcal{H} \to \mathbb{C}$ tal que $f(\gamma z) = \phi(\gamma,z)f(z)$ para toda $\gamma \in \Gamma_0(4)$. En tal caso la condición de cociclo se satisface ya que tenemos:

$$\phi(\gamma_1\gamma_2,z) = \frac{f(\gamma_1\gamma_2 z)}{f(z)} = \frac{f(\gamma_1\gamma_2 z)}{f(\gamma_2 z)} \cdot \frac{f(\gamma_2 z)}{f(z)} = \phi(\gamma_1,\gamma_2 z)\phi(\gamma_1,z).$$

Se considera entonces la *función θ de Jacobi*, definida por $\theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2}$. Las reglas de transformación para esta serie θ son un resultado clásico y se puede ver por ejemplo en [Kob93, Sección 3.4] como se obtiene el resultado que queremos.

Podemos considerar entonces el subgrupo $\widetilde{\Gamma}_0(4) = \{(\alpha,\phi(\alpha,-)) \in G' : \alpha \in \Gamma_0(4)\}$, y en general dado $\Gamma < \Gamma_0(4)$ vamos a denotar $\widetilde{\Gamma}$ al subgrupo de $\widetilde{\Gamma}_0(4)$ cuyos elementos tienen una matriz de Γ en su primera coordenada.

3.2. Formas modulares de peso medio entero

Para definir las formas modulares de peso medio entero vamos a restringirnos a subgrupos de congruencia $\Gamma < \Gamma_0(4)$, para los cuales tenemos una sección. Cuando definimos las formas modulares (Definición 2.2.3) impusimos tres condiciones, que sean holomorfas, que sean invariantes por la acción del grupo y una condición de crecimiento. Definimos análogamente:

Definición 3.2.1. Dado un subgrupo de congruencia $\Gamma < \Gamma_0(4)$ y $k \in \mathbb{Z}$ decimos que una función $f : \mathcal{H} \to \mathbb{C}$ es una forma modular para Γ de peso (medio entero) $k/2$ si satisface:

1. f es holomorfa en $\mathcal{H}$.
2. $f|[\gamma] = f \quad \forall \gamma \in \Gamma$, con el operador $-|[\gamma]$ el asociado a k.
3. $f|\xi$ está acotada en cada semiplano $\{z \in \mathcal{H} : \Im(z) > r\}$ para $r > 0$ y $\forall \xi \in G'$.

Notamos $G_{k/2}(\Gamma)$ al espacio de formas modulares de peso (medio entero) $k/2$ para Γ.

Notemos que cuando k es par no se recupera exactamente la definición de formas de peso entero, es decir que $M_{k/2}(\Gamma)$ no es lo mismo que $G_{k/2}(\Gamma)$ cuando k es par. Concretamente tenemos que $\phi(\gamma,z)^2 = \epsilon_d^2 j(\gamma,z) = \left(\frac{-1}{d}\right) j(\gamma,z)$, de modo que $G_{2k/2}(\Gamma) = M_k(\Gamma,\chi_{-1}^k)$ donde χ_{-1} es el caracter no trivial módulo 4.

Observación 3.2.2. Las tres familias de ejemplos que mencionamos en 2.2.8 se generalizan a familias de formas modulares de peso medio entero. Las series θ de formas cuadráticas se generalizan a formas modulares de peso medio entero cuando la forma cuadrática tiene una cantidad impar de variables; de hecho la función θ de Jacobi que consideramos antes está asociada a la forma cuadrática $Q(n) = n^2$ y es una forma modular de peso $1/2$. En la Proposición 3.3.3 damos un enunciado más preciso sobre series θ.

Obtener los desarrollos de Fourier para las formas de peso medio entero es un poco más delicado. Recordemos que si Γ es un subgrupo de congruencia existe un entero h tal que la matriz $T^h = \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ pertenece a Γ y a todos sus conjugados. Observemos también que los elementos de G' que tienen a T^h en su primera coordenada deben tener una función constante en la segunda. Tenemos entonces que para $\xi = (\gamma, \phi) \in G'$ el subgrupo conjugado $\xi^{-1}\widetilde{\Gamma}\xi$ contiene a un elemento de la forma (T^k, t) con $t \in \{\pm 1, \pm i\}$. La función $f|\xi$ satisface entonces: $f|\xi|(T^h, t)(z) = f|\xi(z)$, pues $(T^h, t) \in \xi^{-1}\widetilde{\Gamma}\xi$, es decir que $f|\xi(z) = t^k f|\xi(z + h)$. Escribiendo $t^k = \exp(2\pi i r)$, con $r \in [0, 1)$, tenemos que la función $\tilde{g}(z) = \exp(-2\pi i r z/h) g(z)$ es periódica de período h y admite entonces un desarrollo de Fourier: $\tilde{g}(z) = \sum_{k\in\mathbb{Z}} a_n q^{n/h}$, y la condición de crecimiento de las formas modulares nos asegura que este desarrollo tiene únicamente potencias positivas: esto es lo que llamamos el desarrollo de Fourier de $f|\xi$.

Definición 3.2.3. Un forma modular $f \in G_{k/2}(\Gamma)$ se dice *cuspidal* si el coeficiente de q^0 en los desarrollos de Fourier de todas las funciones $f|\xi$ con $\xi \in G'$ es 0. Vamos a denotar $S_{k/2}(\Gamma)$ al conjunto de formas cuspidales de peso $k/2$ para Γ.

Si $f \in G_{k/2}(\Gamma)$ entonces $f^2 \in M_k(\Gamma, \chi_{-1})$ y podemos aplicar las cotas de Sturm (Teorema 2.2.13) obteniendo que existe un M tal que si los primeros M coeficientes de f^2 son cero entonces f^2 es la función nula. Estos coeficientes se pueden obtener de los primeros M coeficientes de f, es decir que si los primeros M coeficientes de f son cero la función debe ser idénticamente nula. Tenemos entonces el siguiente resultado:

Proposición 3.2.4. *Los espacios de formas modulares de peso medio entero $G_{k/2}(\Gamma)$ tienen dimensión finita para todo $\Gamma < \Gamma_0(4)$.*

Cuando $N \in \mathbb{N}$ es divisible por 4 tenemos que $\Gamma_1(N) < \Gamma_0(N) < \Gamma_0(4)$ y podemos considerar entonces formas modulares de peso medio entero para $\Gamma_1(N)$ y $\Gamma_0(N)$. Dado un caracter χ módulo N podemos tomar:

$$G_{k/2}(\Gamma_0(N), \chi) = \left\{ f \in G_{k/2}(\Gamma_1(N)) : f|[\gamma](z) = \chi(d) f(z) \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\},$$

el espacio de formas modulares de peso (medio entero) $k/2$ para $\Gamma_0(N)$ con caracter χ, y

$$S_{k/2}(\Gamma_0(N), \chi) = G_{k/2}(\Gamma_0(N), \chi) \cap S_{k/2}(\Gamma_1(N), \chi),$$

el correspondiente espacio de formas cuspidales. Análogamente al Teorema 2.3.13 se puede ver:

Teorema 3.2.5. *Se tiene la siguiente descomposición como suma directa:*

$$G_{k/2}(\Gamma_1(N)) = \bigoplus_{\chi} G_{k/2}(\Gamma_0(N), \chi).$$

Este resultado se demuestra igual que en el caso de peso entero, considerando los proyectores que se obtienen de los operadores de promedio.

3.3. Operadores de Hecke para formas de peso medio entero

Recordemos que para definir los operadores de Hecke en $M_k(\Gamma_1(N))$ considerábamos los conjuntos $X_n = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \,:\, ad - bc = n, N|c, a \equiv 1 \pmod{N}\}$. Para cada $\alpha \in X_n$ vimos que el operador $f \mapsto f|\alpha$ en $M_k(\Gamma_1(N))$ sólo dependía de la coclase $\Gamma_1(N)\alpha$. Tomando una familia de representantes α_i para las coclases definíamos el operador de Hecke $T_n(f) = n^{\frac{k}{2}-1} \sum_i f|\alpha_i$.

Como $\Gamma_1(N)$ actúa a ambos lados en X_n podemos considerar también las coclases dobles $\Gamma_1(N)\beta\Gamma_1(N)$, con $\beta \in X_n$. Cada una de estas se descompone como unión disjunta de coclases a derecha $\Gamma_1(N)\beta\Gamma_1(N) = \coprod_i \Gamma_1(N)\alpha_i$. Podemos definir entonces:

$$f\big|\left[\Gamma_1(N)\beta\Gamma_1(N)\right] = \sum_i f|\alpha_1.$$

Escribiendo a X_n como unión disjunta de coclases dobles $X_n = \coprod_j \Gamma_1(N)\beta_j\Gamma_1(N)$ podemos describir los operadores de Hecke en términos de estos:

$$T_n(f) = n^{\frac{k}{2}-1} \sum_j f\big|\left[\Gamma_1(N)\beta_j\Gamma_1(N)\right].$$

Los operadores de Hecke pueden pensarse entonces como operadores que provienen de coclases dobles. Aunque en el caso de peso entero cada operador de Hecke tiene términos de varias coclases, en el caso de peso medio entero los operadores de Hecke van a estar asociados a una única coclase. Dada una doble coclase $\tilde{\Gamma}_1(N)\xi\tilde{\Gamma}_1(N)$ la escribimos como una unión disjunta de coclases a derecha $\tilde{\Gamma}_1(N)\xi_i$ y dada $f \in G_{k/2}(\Gamma_1(N))$ podemos considerar el operador:

$$f|\left[\tilde{\Gamma}_1(N)\xi\tilde{\Gamma}_1(N)\right] = \sum_i f|\xi_i.$$

Podemos definir los operadores de Hecke en $G_{k/2}(\Gamma_1(N)$ por:

$$T_m(f) = m^{\frac{k}{4}} f\big|\left[\tilde{\Gamma}_1(N)\left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right), \sqrt[4]{m}\right)\tilde{\Gamma}_1(N)\right].$$

Se puede mostrar que cuando n no es un cuadrado se tiene que el operador T_n es nulo, por lo que para formas de peso medio entero uno puede restringirse a los operadores T_{n^2}. Por otro lado al igual que en el caso de formas de peso entero cuando

n y m son coprimos se tiene que $T_n T_m = T_{nm}$, y lo operadores $T_{p^{2k}}$ pueden escribirse como polinomios en T_{p^2}. Uno puede entonces concentrarse en estudiar los operadores T_{p^2}, y como en el caso de peso entero se pueden encontrar las siguientes expresiones explícitas para la acción de estos operadores en términos de los coeficientes [Shi73, Teorema 1.7]:

Teorema 3.3.1. *Sean $f \in G_{k/2}(\Gamma_0(N), \chi)$, con k impar, y p un número primo. Tomando $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ y $T(p^2)(f)(z) = \sum_{n=0}^{\infty} b(n)q^n$, se tiene que:*

$$b(n) = a(p^2 n) + p^{\frac{k-3}{2}} \chi_1(p) \left(\frac{n}{p}\right) a(n) + \chi(p^2) p^{k-2} a(n/p^2).$$

Donde χ_1 es el caracter módulo N definido por $\chi_1(m) = \chi(m) \left(\frac{-1}{m}\right)^{(k-1)/2}$ y entendemos que $a(n/p^2) = 0$ si $p^2 \nmid n$.

La idea de la demostración es encontrar representantes para las coclases a derecha que nos permitan realizar las cuentas como en el Teorema 2.3.15. La estretagia para esto es intentar levantar los representantes en $\mathrm{GL}_2(\mathbb{Q})$ que teníamos en peso entero a elementos de G, pero esto resulta algo delicado. Primero se debe demostrar un lema que asegura que si (α_i, ϕ_i) es una familia de representantes para las coclases a derecha de $\tilde{\Gamma}_1(N)$ en la coclase doble $\tilde{\Gamma}_1(N) \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right), \sqrt[4]{m}\right) \tilde{\Gamma}_1(N)$, entonces α_i es una familia de representantes para las coclases a derecha $\Gamma_1(N)$ en la coclase doble $\Gamma_1(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right) \Gamma_1(N)$. La recíproca de esta observación sin embargo es falsa, por lo tanto dada una familia de representantes α_i para las coclases a derecha de esta última coclase doble para poder levantarlos a G necesitamos obtener además matrices γ_1^i y γ_2^i de Γ_1 tales que:

$$\alpha_i = \gamma_1^i \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix} \gamma_2^i.$$

Habiendo obtenido estas matrices y probado lema uno puede entonces ver que los elementos de la forma:

$$\tilde{\alpha}_i = (\gamma_1^i, \phi(\gamma, -)) \left(\begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix}, \sqrt[4]{m}\right) (\gamma_2^i, \phi(\gamma, -))$$

son una familia de representantes como los que queremos y ahora se puede proceder calculando explícitamente al acción.

Análogamente a lo que se tenía en el caso de peso entero podemos definir los operadores $U_m(f) = f|\left(\left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right), \sqrt[4]{m}\right)$ y el operador de Atkin-Lehner en formas de peso medio entero. Aunque no vayamos a necesitar del segundo sí vamos a necesitar el operador U_m y las propiedades del mismo que enunciamos en la siguiente proposición y cuya demostración es análoga al caso de peso entero:

Proposición 3.3.2. *Se tiene $U_m : G_{k/2}(N, \chi) \to G_{k/2}(mN, \tilde{\chi})$, donde $\tilde{\chi}(d) = \chi(d)(\frac{m}{d})$. Más aún este operador preserva las formas cuspidales. Más aún U_m conmuta con todos los operadores de Hecke.*

Más adelante vamos a necesitar también tener definidas las siguientes series θ cuya modularidad enunciamos a continuación:

Proposición 3.3.3. *Sea χ un caracter primitivo módulo k y $\nu \in \{0;1\}$ tal que $\chi(-1) = (-1)^\nu$. Definimos la función $h_\chi(z) = \frac{1}{2}\sum_{n\in\mathbb{Z}} \chi(n) n^\nu q^{n^2}$. Entonces si χ es un caracter impar, i.e. $\nu = -1$ se tiene $h_\chi \in S_{3/2}(4k^2, \tilde{\chi})$, y si χ es par $h_\chi \in G_{1/2}(4r^2, \tilde{\chi})$, donde $\tilde{\chi}(d) = \chi(d)(\frac{-1}{d})^\nu$*

Notemos que tomando χ el caracter trivial se obtiene la función θ de Jacobi, que se usa para construir el cociclo ϕ en peso medio entero. Usando el Teorema 3.3.1 es fácil verificar que resultan de hecho autoformas.

Proposición 3.3.4. *Si χ no es el caracter trivial la función h_χ del lema anterior resulta una autoforma para todos los operadores de Hecke.*

Demostración. Por el Teorema 3.3.1, tomando $a(n)$ los coeficientes de h_χ y $b(n)$ los de $h_\chi|T(p^2)$, tenemos que si $p|n$:

$$\begin{aligned} b(n^2) &= a(p^2n^2) + \tilde{\chi}(p)\left(\frac{-1}{p}\right)^\lambda \left(\frac{n^2}{p}\right) p^{\lambda-1} a(n^2) \\ &= \left(\chi(p)p^\nu + \chi(p)\left(\frac{-1}{p}\right)^{\lambda+\nu} p^{\lambda-1}\right) a(n^2) \\ &= \left(\chi(p)p^\nu + \chi(p)p^{\lambda-1}\right) a(n^2), \end{aligned}$$

y si $p \nmid n$:

$$\begin{aligned} b(n^2) &= a(p^2n^2) + \tilde{\chi}(p^2)p^{k-2} a\left(\frac{n^2}{p^2}\right) \\ &= \left(\chi(p)p^\nu + \chi(p^2)\left(\frac{-1}{p^2}\right)^\nu p^{k-2-\nu}\chi(p)^{-1}\right) a(n^2) \\ &= \left(\chi(p)p^\nu + \chi(p)p^{k-2-\nu}\right) a(n^2). \end{aligned}$$

Donde $k/2$ es el peso de la forma y $\lambda = (k-1)/2$. Como $k - 2 - \nu = \lambda - 1$ obtenemos lo que buscábamos. □

3.4. Teoremas de Shimura y Waldspurger

Ahora vamos a enunciar dos resultados importantes que nos van a permitir calcular los valores centrales de las L-series que nos interesan. El primero de estos dos teoremas es la correspondencia de Shimura. Este es el resultado principal de [Shi73] y construye a partir de una forma $f \in S_{k/2}(\Gamma_0(N), \chi)$, con k impar, que es un autovector para algunos operadores de Hecke una forma $\tilde{f} \in M_{k-1}(\Gamma(\tilde{N}), \chi^2)$, para algún $\tilde{N}$, y que comparte autovalores con la forma original. En el caso de que la forma original f sea una autoforma la forma $\tilde{f}$ también lo será, y este resultado, asumiendo que f es una autoforma, es la forma usual de enunciar la correspondencia de Shimura:

Teorema 3.4.1 (Correspondencia de Shimura). *Sean k un entero impar y $f \in S_{\frac{k}{2}}(N, \chi)$ un forma cuspidal de peso medio entero. Supongamos más aún que f es una autoforma para todos los operadores de Hecke, con ω_p el autovalor asociado a T_{p^2}. Definimos la función:*

$$F(z) = \sum_{n=1}^{\infty} A(n)q^n$$

donde los coeficientes $A(n)$ están definidos como los coeficientes de la siguiente L-serie:

$$\sum_{n=1}^{\infty} A(n)n^{-s} = \prod_{p}(1 - \omega_p p^{-s} + \chi(p)^2 p^{k-2-2s})^{-1}$$

Entonces $F \in M_{k-1}(\tilde{N}, \chi^2)$, para cierto $\tilde{N}$. Más aún si $k > 5$ entonces F es cuspidal.

Shimura toma la serie de Dirichlet del teorema y muestra que esta satisface la condiciones del teorema converso de Weil (Teorema 2.4.8), de donde se deduce que la serie F define una forma modular.

Por otro lado la serie de Dirichlet está definida como un producto de Euler de manera que es inmediato que es una autoforma y que el autovalor de T_p es precisamente w_p, el autovalor de T_{p^2} para la forma original. Es decir que lo que nos está diciendo la correspondencia de Shimura es que dada una autoforma cuspidal de peso medio entero podemos encontrar una autoforma de peso entero con el mismo sistema de autovalores.

El valor de $\tilde{N}$ en el enunciado de la correspondencia se puede tomar como el máximo común divisor de los niveles N_t asociados a formas del resultado más general que demuestra Shimura. Luego de enunciar el teorema Shimura observa que cuando todos los divisores primos de N dividen al conductor del caracter $\chi(m)\left(\frac{-1}{m}\right)^{(k-1)/2}\left(\frac{t}{m}\right)$, se puede tomar $N_t = N/2$. En nuestro caso particular vamos a necesitar este resultado cuando $N = 128$ y χ es o bien el caracter trivial o el caracter $\left(\frac{2}{m}\right)$, por lo que el caracter anterior resulta siempre un símbolo de Jacobi cuyo conductor es divisible por 4. Por lo tanto en los casos que nos interesa vamos a poder tomar $\tilde{N} = N/2$.

Otra observación que tenemos que hacer es sobre la cuspidalidad. Aunque el resultado original de Shimura sólo asegura la cuspidalidad si $k > 5$ en nuestro caso vamos a necesitar asegurar que se obtiene una forma cuspidal en el caso $k = 3$. En el mismo paper Shimura conjetura lo siguiente que fue luego demostrado: en el caso de peso $3/2$ se puede asegurar la cuspidalidad siempre que la forma que estemos considerando sea ortogonal a todas las series theta h_ψ y $U_m(h_\psi)$, que definimos en la Proposición 3.3.3.

El segundo resultado es un teorema de Waldspurger. Dada una autoforma f que está en la imagen de la correspondencia de Shimura este teorema nos asegura la existencia de una función A que permite, por un lado calcular los valores centrales de ciertos twists de ψ, y por otro obtener los coeficientes de las formas de peso medio entero que se corresponden con ψ vía la correspondencia de Shimura. Concretamente se tiene el siguiente enunciado:

Teorema 3.4.2. *Sean k un entero impar, f un forma nueva de nivel divisible por 16, peso $k-1$ y caracter χ^2 que es la imágen de una forma de peso $k/2$ y caracter χ vía la aplicación de Shimura (3.4.1). Entonces existe una función $A(t)$ de los enteros libre de cuadrados en los números complejos tal que:*

1. $$A(d)^2\epsilon(\tilde{\chi},1/2) = 2(2\pi)^{(1-k)/2}\Gamma((k-1)/2)L(\psi\otimes\tilde{\chi},(k-1)/2),$$

   donde $\tilde{\chi} = \chi^{-1}\chi_{-1}^{(k-1)/2}\chi_d$, y el factor $\epsilon(\tilde{\chi},1/2)$ es el que aparece en la ecuación funcional de la L-serie del caracter.

2. *Para cada número natural N existe una lista explícita y finita de funciones $c(n)$ tales que las funciones:*
   $$\sum A(n^{sf})n^{(k-2)/4}c(n)q^n,$$
   donde n^{sf} denota al producto de los primos que dividen a n, generan el espacio de formas de peso $k/2$, nivel N y caracter χ que se corresponden con f vía la aplicación de Shimura.

En [Wal81] Waldspurger demuestra este resultado y determina explícitamente como son los posibles conjuntos de funciones c. Waldspurger da a estas funciones en terminos de una descomposición como producto sobre los primos $c = \prod_p c_p$ y describe estos factores locales. En nuestro caso vamos nos interesa calcular los twists de la forma modular ϕ asociada a la curva elíptica E, que es una forma de peso 2, caracter trivial y nivel 32. Vamos a encontrar formas de peso $3/2$, unas con caracter trivial y otras con caracter χ_2, y de nivel 128 que se corresponden con ϕ. En estos casos lo que vamos a necesitar saber es que cuando n es libre de cuadrados $c_p(n)$ es 1 si p es un primo impar y c_2 se puede tomar como cualquiera de las funciones características de las unidades módulo 8.

Capítulo 4

Clasificación de números congruentes

Recordemos que la Proposición 2.5.4 nos dice que, suponiendo la conjetura de Birch y Swinnerton-Dyer, para decidir si un número d es congruente necesitamos calcular el valor central de la L-serie $L(E^D, s)$. Sabemos también que están sociadas a las formas $\phi \otimes \chi_D$, donde ϕ es la única autoforma de nivel 32 y caracter trivial, y tiene la misma L-serie que la curva elíptica $E : y^2 = x^3 - x$. La idea es entonces buscar qué formas de peso medio entero se corresponden vía la aplicación de Shimura a la forma ϕ, y luego aplicar el resultado de Waldspurger para calcular los valores centrales de todos los Twists.

Consideremos la función g definida por:

$$g(z) = q\prod_{n=0}^{\infty}(1-q^{8n})(1-q^{16n}) = \eta(8z)\eta(16z). \tag{4.0.1}$$

Por el resultado de [Ono04, Teorema 1.64] sobre productos de la función η tenemos que $g \in S_1(\Gamma_0(128))$. Para obtener un desarrollo de esta función como una serie vamos a usar el teorema del producto triple de Jacobi:

Teorema 4.1. *Si x e y son números complejos con $|x| < 1$ e $y \neq 0$, se tiene que:*

$$\prod_{n=1}^{\infty}\left(1-x^{2n}\right)\left(1+x^{2m-1}y^2\right)\left(1+\frac{x^{2m+1}}{y^2}\right) = \sum_{n\in\mathbb{Z}} x^{n^2}y^{2n}. \tag{4.0.2}$$

Aplicando este resultado obtenemos:

Lema 4.2. *Se tiene que:*

$$g(z) = \sum_{(n,m)\in\mathbb{Z}^2}(-1)^n q^{(4m+1)^2+8n^2} \tag{4.0.3}$$

Demostración. Si en (4.0.2) tomamos $x = q^8$ e $y = i$ obtenemos:

$$\begin{aligned}\sum_{n\in\mathbb{Z}}(-1)^n q^{8n^2} &= \prod_{n=1}^{\infty}(1-q^{16n})(1-q^{16n-8})(1-q^{16n-8}) \\ &= \prod_{n=1}^{\infty}(1-q^{8n})(1-q^{8n})(1-q^{16n})^{-1}.\end{aligned}$$

Por otro lado tomando $x = q^{16}$ e $y = q^4$ obtenemos:

$$\begin{aligned}\sum_{n\in\mathbb{Z}} q^{(4m+1)^2} &= q\prod_{n=1}^{\infty}(1-q^{32n})(1+q^{32n-8})(1+q^{32n-24}) \\ &= q\prod_{n=1}^{\infty}(1-q^{16n})(1+q^{16n})(1+q^{16n+8}) \\ &= q\prod_{n=1}^{\infty}(1-q^{16n})(1+q^{8n}).\end{aligned}$$

Multiplicando ambas expresiones se obtiene el resultado que buscabamos. □

Teorema 4.3. *Las formas $g\theta_2$, $g\theta_4$, $g\theta_8$ y $g\theta_{16}$ se corresponden vía la aplicación de Shimura con la forma ϕ.*

Demostración. Consideremos primero las formas $g\theta_2$,$g\theta_8$ y $g\theta_{32}$ que son formas cuspidales de peso $3/2$, nivel 128 y caracter trivial. Por los resultados de [CO77] sabemos que el espacio en cuestión tiene dimensión 3. Desarrollando los productos podemos calcular los primeros coeficientes de sus q-series, obteniéndose:

$$\begin{aligned}g\theta_2 &= q + 2q^3 + q^9 + O(q^{10}), \\ g\theta_8 &= q + q^9 + O(q^{10}), \\ g\theta_{32} &= q - q^9 + O(q^{10}).\end{aligned}$$

Para calcular los coeficientes de estas formas usamos scripts en Sage para desarrollar las expresiones que tenemos para las series θ y la forma g. Aunque para verificar las identidades sólo se necesita conocer unos pocos coeficientes porque el espacio tiene dimensión 3, para poder calcular la acción de los operadores de Hecke usando el Teorema 3.3.1 se necesita en este caso conocer $9 \cdot 5^2 = 225$ coeficientes, por lo que hacer cálculos sin usar computadoras resulta inviable. El código que usamos para esto se puede ver en el apéndice.

Como los coeficientes de q, q^3 y q^9 de las mismas son linealmente independientes, podemos afirmar que estas son una base del espacio. Afirmamos que $2g\theta_{32} - g\theta_8$ es una autoforma para todos los operadores de Hecke T_{p^2}. En efecto las proposiciones 3.3.3 y 3.3.4 nos dicen que la función $h_{\chi_{-1}}$ es una autoforma para todos los operadores de

Hecke de caracter $(\frac{-1}{d})^2 = 1$ y nivel 64, i.e. esta forma pertenece al espacio en el que estamos. Calculando sus primeros coeficientes obtenemos:

$$h_{\chi_{-1}}(z) = q - 3q^9 + O(q^{10})$$

de modo que esta es precisamente la combinación lineal anterior.

Por otro lado, calculando la acción de T_{3^2} y T_{5^2} en $g\theta_2$ y $g\theta_8$ vemos que son autovectores ambas con autovalores $\lambda_3 = 0$ y $\lambda_5 = -2$. Como $2g\theta_{32} - g\theta_8$ tiene distintos autovalores para T_{3^2} y T_{5^2} el espacio generado por $g\theta_2$ y $g\theta_8$ debe ser ortogonal a la otra. Como esta última es una autoforma para todos los operadores de Hecke estos deben preservar el espacio generado por las primeras dos formas. Por el Lema 4.2 podemos escribir las formas como:

$$g\theta_2 = \sum_{(n,m,k)\in\mathbb{Z}^3} (-1)^n q^{(4m+1)^2+8n^2+2k^2},$$
$$g\theta_8 = \sum_{(n,m,k)\in\mathbb{Z}^3} (-1)^n q^{(4m+1)^2+8n^2+8k^2}.$$

Separando la suma de $g\theta_2$ dependiendo de si k es par o no y restando $g\theta_8$:

$$g\theta_2 - g\theta_8 = \sum_{\substack{(n,m,k)\in\mathbb{Z}^3 \\ k\equiv 1(2)}} (-1)^n q^{(4m+1)^2+8n^2+2k^2}.$$

En particular los únicos exponentes que aparecen en $g\theta_8$ son congruentes a 1 módulo 8 y los que aparecen en $g\theta_2 - g\theta 8$ son congruentes a 3 módulo 8. Del Teorema 3.3.1 se deduce que $T_{p^2}(g\theta_8)$ también tiene solo exponentes congruentes a 1 módulo 8 y $T_{p^2}(g\theta_2 - g\theta_8)$ sólo tiene exponentes congruentes a 3 módulo 8. Esto nos dice que los operadores de Hecke deben preservar los subespacios generados por cada una de estas formas y por lo tanto ambas deben ser autoformas.

Por la correspondencia de Shimura (Teorema 3.4.1) estas dos formas se corresponden con autoformas de peso 2 y nivel un divisor de 64. Más aún acabamos de ver que estas formas son ortogonales a la única serie θ de este espacio, $h_{\chi_{-1}}$, por lo que podemos asegurar que se corresponden con una forma cuspidal. Comparamos entonces los autovalores obtenidos para T_{3^2} y T_{5^2} con los posibles valores de T_3 y T_5 de las formas de peso entero de peso 2 y nivel un divisor de 64, que están tabulados y se pueden ver en [The19]. En este caso vemos que sólo tenemos la forma ϕ de nivel 32, que tiene los mismos autovalores que estas, y una autoforma de nivel 64 cuyo autovalor de T_5 es 2. Por lo tanto la única posibilidad es que ambas formas de peso medio entero se correspondan con ϕ vía la aplicación de Shimura. Por lo tanto todo el espacio generado por $g\theta_2$ y $g\theta_8$ consiste de autoformas para todos los operadores de Hecke que se corresponden con ϕ vía la aplicación de Shimura.

Consideremos ahora el caso de las formas $g\theta_1$, $g\theta_4$ y $g\theta_{16}$, que tienen nivel 128 y peso

$3/2$ igual que antes, pero caracter χ_2. Calculando sus primeros coeficientes obtenemos:

$$\begin{aligned} g\theta_1 &= q + 2q^2 + 2q^5 + O(q^6), \\ g\theta_4 &= q + 2q^5 + O(q^6), \\ g\theta_{16} &= q + O(q^6). \end{aligned}$$

Por [CO77] sabemos que en este caso también estamos trabajando con un espacio de dimensión 3 y por lo tanto estas funciones forman una base ya que son linealmente independientes. Primero notemos que $g\theta_1 - g\theta_4$ es una autoforma para todos los operadores de Hecke. En este caso no se puede encontrar una serie theta asociada a un caracter que pertenezca al espacio. Sin embargo si consideramos $\tilde{h} = U_2(h_{\chi_{-1}})$, i.e. $\tilde{h}(z) = h_{\chi_{-1}}(2z)$, obtenemos por el Lema 3.3.2 una forma de nivel 128 y caracter $\chi_2(m) = (\frac{2}{m})$ como buscamos; más aún está forma resulta también una autoforma para todos los operadores de Hecke, ya que U_2 conmuta con estos. Calculando sus primeros coeficientes tenemos:

$$\tilde{h} = q^2 + O(q^6)$$

que es precisamente $\frac{1}{2}(g\theta_1 - g\theta_4)$.

En segundo lugar observemos que las funciones $g\theta_4$ y $g\theta_{16}$ son autovectores para T_{3^2} y T_{5^2} con autovalores 0 y -2 respectivamente. Por lo tanto el subespacio generado por estas dos formas es ortogonal al generado $g\theta_1 - g\theta_4$ y en consecuencia invariante por la acción de todos los operadores de Hecke. Por otro lado aplicando el Lema 4.2 podemos escribir:

$$\begin{aligned} g\theta_{16} &= \sum_{(n,m,k)\in\mathbb{Z}^3} (-1)^n q^{(4m+1)^2+8n^2+16k^2}, \\ g\theta_4 - g\theta_{16} &= \sum_{(n,m,k)\in\mathbb{Z}^3} (-1)^n q^{(4m+1)^2+8n^2+4k^2}. \end{aligned}$$

Es decir que los únicos exponentes que aparecen con coeficiente no nulo en $g\theta_{16}$ son congruentes a 1 módulo 8, y los de $g\theta_4 - g\theta_{16}$ son congruentes a 5 módulo 8. Y luego por el Teorema 3.3.1 podemos concluir que ambas deben ser autoformas para todos los operadores de Hecke. Para concluir basta con observar que al igual que antes tenemos que por la correspondencia de Shimura, y ya que nuevamente vimos que son ortogonales a $U_2(h_{\chi_{-1}})$ que es la única serie θ del espacio, estás deben corresponderse con una forma cuspidal de peso 2 con nivel divisor de 64; y la única con un sistema de autovalores compatibles es precisamente ϕ. □

Teorema 4.4. *Sea $\beta = 2^{1/2}\pi e^{-\pi/6}\prod_n(1-e^{-2\pi n})^2$, que resulta se el período real de E, y tomemos $g\theta_2 = \sum_{n=1}^{\infty} a(n)q^n$ y $g\theta_4 = \sum_{n=1}^{\infty} b(n)q^n$. Entonces para todo $n \in \mathbb{N}$ impar y libre de cuadrados se tiene:*

$$\begin{aligned} L(E^n, 1) &= \frac{a(n)^2\beta}{4\sqrt{n}} \\ L(E^{2n}, 1) &= \frac{b(n)^2\beta}{2\sqrt{2n}}. \end{aligned}$$

Demostración. Vamos a usar la primera parte del teorema de Waldspurger (Teorema 3.4.2) para obtener los valores centrales de las L-series. Para esto necesitamos obtener información de la función A y esto lo obtendremos de la segunda parte, ya que en el teorema anterior consiguimos bases explícitas para los espacios que se corresponden con la función ϕ.

Al aplicar la primer parte del teorema de Waldspurger a la función ϕ tenemos que el factor ϵ da 1 y por lo tanto obtenemos que para t impar y libre de cuadrados:

$$A(t)^2 = 2(2\pi)^{-1} L(\phi \otimes \chi\chi_{-t}, 1). \tag{4.0.4}$$

Sin embargo a nosotros nos interesa calcular los valores de $L(E^t, 1) = L(\phi \otimes \chi_t)$. Observemos que esta L-serie difiere, en principio, de la que aparece al aplicar el teorema de Waldspurger en el factor χ_{-1}. Afirmamos que en este caso sin embargo las dos series coinciden. Esto lo podemos ver simplemente comparando los productos de Euler:

$$L(\phi \otimes \chi_{-t}, s) = \prod_{p \nmid 2t} \frac{1}{1 - a_p \left(\frac{-2t}{p}\right) p^{-s} + p^{1-2s}},$$
$$L(\phi \otimes \chi_{t}, s) = \prod_{p \nmid 2t} \frac{1}{1 - a_p \left(\frac{2t}{p}\right) p^{-s} + p^{1-2s}}.$$

Ahora el Lema 1.2.11 nos asegura que si $p \equiv 3 \pmod 4$ entonces $a_p = 0$, y $p \equiv 1 \pmod 4$ implica que -1 es un cuadrado módulo p. Tenemos entonces:

$$\begin{aligned} L(\phi \otimes \chi_{-t}, s) &= \prod_{\substack{p \nmid 2t \\ p \equiv 1 \pmod 4}} \frac{1}{1 - a_p \left(\frac{-2t}{p}\right) p^{-s} + p^{1-2s}} \prod_{\substack{p \nmid 2t \\ p \equiv 3 \pmod 4}} \frac{1}{1 + p^{1-2s}} \\ &= \prod_{\substack{p \nmid 2t \\ p \equiv 1 \pmod 4}} \frac{1}{1 - a_p \left(\frac{2t}{p}\right) p^{-s} + p^{1-2s}} \prod_{\substack{p \nmid 2t \\ p \equiv 3 \pmod 4}} \frac{1}{1 + p^{1-2s}} \\ &= L(\phi \otimes \chi_t, s). \end{aligned}$$

Tanto en el caso de caracter trivial como de caracter χ_2 el teorema de Waldspurger (Teorema 3.4.2) nos dice que el subespacio de $S_{3/2}(\Gamma_0(128), \chi)$ que se corresponde con ϕ está generado por cuatro funciones de la forma $F(q) = \sum A(n^{\text{sf}}) c(n) q^n$ con las funciones c de la forma $c(n) = n^{1/4} \prod_p c_p(n)$. En este caso los valores $c_p(n)$ son 1 cuando p es un primo impar y n es libre de cuadrados, y los posibles valores para c_2 son las funciones características de las clases de residuos impares módulo 8.

Concentrémonos ahora en el caso de caracter trivial. Sabemos que este mismo espacio está generado por las formas $g\theta_8$ y $g\theta_2 - g\theta_8$. Dónde los únicos coeficientes no nulos de la primera son congruentes a 1 módulo 8 y los de la segunda congruentes a 3 módulo 8. Más aún los coeficientes no nulos de estas son iguales al correspondiente coeficiente de $g\theta_2$. Eligiendo la función definida por tomar $c_2(n)$ la función característica de la clase residual de 1 tenemos que existe $\beta_1 \in \mathbb{C}$ tal que si n es libre de cuadrados y

congruente a 1 módulo 8:

$$\beta_1 a(n) = A(n)c(n) = A(n)n^{1/4},$$
$$a(n) = A(n)n^{1/4}\beta_1^{-1}.$$

Análogamente tomando $c_2(n)$ como la función característica de la clase de 3 obtenemos que existe un $\beta_2 \in \mathbb{C}$ tal que para n libre de cuadrados y congruente a 3 módulo 8:

$$a(n) = A(n)n^{1/4}\beta_2^{-1}.$$

En el caso de que n sea congruente a 5 ó 7 módulo 8 tenemos, tomando las funciones definidas por las correspondientes clases residuales, que $A(n) = a(n) = 0$. Luego en (4.0.4) tenemos que, como χ es trivial, la L-serie es la que se corresponde con la curva E^n, y reemplazando obtenemos:

$$a(n)^2 = \begin{cases} 0 = L(E^n, 1) & \text{si } n \equiv 5, 7 \pmod 8, \\ \beta_1^{-2} 2(2\pi)^{-1} L(E^n, 1) n^{1/2} & \text{si } n \equiv 1 \pmod 8, \\ \beta_2^{-2} 2(2\pi)^{-1} L(E^n, 1) n^{1/2} & \text{si } n \equiv 3 \pmod 8. \end{cases}.$$

Los valores de β_1 y β_2 se pueden obtener de valores ya calculados para L-series particualres. Por ejemplo en [SDB65] Birch y Swinnerton-Dyer expresan los valores centrales de estas L-series en términos de la función $\wp$ de Weierstrass. Esto les permite probar que los números $L(E^n, 1)n^{1/2}\beta^{-1}$ son racionales y calcularlos explícitamente para una gran cantidad de casos. En particular obtienen cuando $d = 1, 3$ que $L(E, 1)/\beta = 1/4$ y $L(E^3, 1)3^{-1/2}/\beta = 1$. Tenemos entonces que:

$$1 = a(1)^2 = \beta_1^{-2} 2(2\pi)^{-1} \frac{\beta}{4} \implies \beta_1^{-2} = \frac{4\pi}{\beta},$$
$$4 = a(3)^2 = \beta_2^{-2} 2(2\pi)^{-1} \beta \implies \beta_2^{-2} = \frac{4\pi}{\beta}.$$

Luego despejando obtenemos que si n es impar:

$$L(E^n, 1/2) = \frac{a(n)^2 \beta}{4\sqrt{n}},$$

que es la primera ecuación que buscábamos.

Pasemos ahora al caso de caracter χ_2. En este caso el espacio está generado por las formas $g\theta_{16}$ y $g\theta_4 - g\theta_{16}$; la primera tiene sólo coeficientes no nulos acompañando exponentes congruentes a 1 módulo 8, y la segunda acompañando exponentes congruentes a 5 módulo 8. Más aún este coeficiente coincide en ambos casos con el correspondiente coeficiente en la serie de Fourier de θ_4. Escribiendo la forma que da Waldspurger para cada elección de c_2 como combinación lineal $g\theta_{16}$ y $g\theta_4 - g\theta_{16}$ y razonando igual que en el caso de caracter trivial obtenemos que existen β_3, β_4 tales que:

$$b(n)^2 = \begin{cases} 0 = L(E^{2n}, 1) & \text{si } n \equiv 3, 7 \pmod 8, \\ \beta_3^{-2} 2(2\pi)^{-1} L(E^{2n}, 1) n^{1/2} & \text{si } n \equiv 1 \pmod 8, \\ \beta_4^{-2} 2(2\pi)^{-1} L(E^{2n}, 1) n^{1/2} & \text{si } n \equiv 5 \pmod 8. \end{cases}.$$

Nuevamente los casos $n = 1$ y $n = 5$ están calculados en [SDB65] y tenemos $L(E^2, 1)2^{1/2}/\beta = 1/2$ y $L(E^{10}, 1)10^{1/2}/\beta = 2$. Luego se tiene:

$$1 = b(1)^2 = \beta_3^{-2} 2(2\pi)^{-1} \frac{\beta}{2\sqrt{2}} \quad \Longrightarrow \quad \beta_3^{-2} = \frac{2\sqrt{2}\pi}{\beta},$$
$$4 = b(5)^2 = \beta_4^{-2} 2(2\pi)^{-1} \frac{2\beta}{\sqrt{2}} \quad \Longrightarrow \quad \beta_2^{-2} = \frac{2\sqrt{2}\pi}{\beta},$$

y reemplazando en las ecuaciones anteriores obtenemos:

$$L(E^{2n}, 1) = \frac{b(n)^2 \beta}{2\sqrt{2n}}$$

□

Finalmente esto nos permite obtener una caracterización parcial de los números congruentes como consecuencia del teorema de Coates-Wiles:

Corolario 4.5. *Si $n \in \mathbb{N}$ es un número impar y $a(n) \neq 0$, o si es un número par y $b(n/2) \neq 0$, entonces n no es un número congruente.*

Y la siguiente caracterización completa de los números asumiendo la conjetura de Birch y Swinnerton-Dyer:

Corolario 4.6. *Si la conjetura de Birch y Swinnerton-Dyer es cierta entonces un número impar n es congruente si y sólo si $a(n) = 0$ y un número par es congruente si y sólo si $b(n/2) = 0$.*

Apéndice

Cálculos Auxiliares

En el último capítulo tuvimos que ayudarnos de la computadora para poder calcular los coeficientes de las formas con las trabajamos. Para esto usamos el languaje de programación Sage, que nos permite trabajar con anillos de series formales en una variable. A continuación damos los códigos que utilizamos.

Primero usamos el siguiente código para calcular los coeficientes de la función g, definida en (4.0.1). De manera similar a como obtuvimos el Lema 4.2 se puede probar que la función g está también descripta por la siguiente serie:

$$g(z) = \sum_{(n,m)\in\mathbb{Z}} (-1)^{m+n} q^{(4m+1)^2+16n^2}.$$

Observemos que para que el exponente de q en el término que se corresponde al par (n, m) sea menor o igual que d se deben satisfacer las siguientes desigualdades:

$$\frac{-\sqrt{d}}{4} \leq m, n \leq \frac{\sqrt{d}}{4}.$$

Para calcular los coeficientes de g hasta un orden `dmax` que tomamos como entrada usamos entonces la siguiente función:

```
def g(dmax):
    nmax = int(sqrt(dmax)/4)+1
    mmax = int(sqrt(dmax)/4)+1
    ring= ZZ[['q']]
    q = ring.gen()
    res = 0
    for n in srange(-nmax,nmax+1):
        for m in srange(-mmax,mmax+1):
            d = (4*m+1)**2 + 16 * n**2
            res += (-1)**(m+n) * q**d
    return res + O(q**(dmax+1))
```

Lo que estamos haciendo es definir el anillo $\mathbb{Z}[[q]]$ e inicializar una variable `res` como cero en este anillo. Luego recorremos los pares de enteros (n, m) que satisfacen las desigualdades anteriores y en cada paso sumamos $(-1)^{m+n}q^{(4m+1)^2+16n^2}$ a la variable `res`. Habiendo recorrido estos pares obtenemos un elemento del anillo que coincide con g hasta orden `dmax` y esto es lo que devuelve la función como un elemento del anillo de series formales.

De manera análoga definimos una función que toma como entrada un natural `dmax` y un caracter `chi` $= \chi$ y devuelve la serie h_χ hasta orden `dmax`:

```
def theta(chi,dmax):
    nmax = int(sqrt(dmax))
    ring = ZZ['q']
    q = ring.gen()
    res = 0
    for n in srange(-nmax,nmax+1):
        res += chi(n) * n * q**(n * n)
    return res + O(q**(dmax+1))
```

y una función que toma como entrada dos naturales `t` y `dmax` y devuelve la serie $\theta_{\mathtt{t}}$ hasta orden `dmax`:

```
def thetat(t,dmax):
    ring = ZZ['q']
    q = ring.gen()
    res = 1
    nmax = int(sqrt(dmax))+1
    for n in srange(1,nmax+1):
        res += 2 * q**(t * n * n)
    return res + O(q**(dmax+1)).
```

Como todos los elementos que estamos obteniendo están definidos como elementos del anillo de funciones formales podemos multiplicarlos y sumarlos para obtener las series que necesitamos hasta el orden necesario.

Por otro lado también necesitamos definir funciones que nos permitan obtener los coeficientes luego de aplicar los operadores de Hecke a formas de peso medio entero. En este definimos una función que toma como entrada un natural `p`, que asumimos que es primo, un elemento `f` de $\mathbb{Z}[[q]]$, que asumimos que es una forma modular de caracter trivial y peso $3/2$, y un natural `dmax` y devuelve $T_p($`f`$)$ hasta orden `dmax`:

```
def heckeptriv(f,p,dmax):
    ring = ZZ['q']
    q = ring.gen()
    res = 0
    l = 0
    for n in srange(0,dmax):
        if mod(n,p**2) == 0:
            l = n // (p**2)
```

```
            res += (f[p**2 * n] +p * f[l]) * q**n
        else:
            res += (f[p**2 * n] + \
            kronecker(-n,p) * f[n]) * q**n
    return res + O(q**(dmax+1))
```

y definimos también una segunda función que tiene las mismas entradas pero asume que `f` es una forma de caracter χ_2:

```
def heckepnotriv(f,p,dmax):
    ring = ZZ['q']
    q = ring.gen()
    res = 0
    l = 0
    for n in srange(0,dmax):
        if mod(n,p**2) == 0:
            l = n // (p**2)
            res += (f[p**2 * n] + p*f[l]) * q**n
        else:
            res += (f[p**2 * n] + \
            kronecker(p,2) * kronecker(-n,p) * f[n]) * q**n
    return res + O(q**(dmax+1)).
```

En ambos casos estamos simplemente recorriendo los naturales menores o iguales que `dmax` y aplicando el Teorema 3.3.1 para calcular el coeficiente correspondiente. Observemos que en ambos casos estamos asumiendo que los coeficientes de `f` están definidos hasta orden por lo menos $\texttt{p}^2\texttt{dmax}$.

Bibliografía

[CO77] Henri Cohen and Joseph Oesterlé. Dimensions des espaces de formes modulaires. In *Modular functions of one variable VI*, pages 69–78. Springer, 1977.

[Kob93] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Mathematics. Springer New York, 1993.

[Ono04] K. Ono. *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and Q-series*. Number no. 102 in Regional conference series in mathematics. American Mathematical Society, 2004.

[Rie59] Bernhard Riemann. Ueber die anzahl der primzahlen unter einer gegebenen grosse. *Ges. Math. Werke und Wissenschaftlicher Nachlaß*, 2:145–155, 1859.

[SDB65] H.P.F. Swinnerton-Dyer and B.J. Birch. Notes on elliptic curves. ii. *Journal für die reine und angewandte Mathematik*, 218:79–108, 1965.

[Shi73] Goro Shimura. On modular forms of half integral weight. *Annals of Mathematics*, 97(3):440–481, 1973.

[ST94] J.H. Silverman and J.T. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer New York, 1994.

[The19] The LMFDB Collaboration. The l-functions and modular forms database. http://www.lmfdb.org, 2019.

[Tun83] J.B. Tunnell. A classical diophantine problem and modular forms of weight 3/2. *Inventiones mathematicae*, 72:323–334, 1983.

[Wal81] J-L Waldspurger. Sur les coefficients de fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl.*, 60:375–484, 1981.

[Wil95] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 141(3):443–551, 1995.