Formas modulares y la curva $y^2 = x^3 - 35x - 98$

Dulcinea Raboso Paniagua

Trabajo de fin de Máster
Curso 2008–2009

Director: Fernando Chamizo Lorente

No es el conocimiento, sino el acto de aprendizaje,
y no la posesión, sino el acto de llegar allí,
lo que concede el mayor disfrute.

Carl Friedrich Gauss

Índice general

Introducción

Las integrales elípticas fueron estudiadas por importantes matemáticos y físicos del siglo XIX, trabajos que impulsaron el estudio de las curvas elípticas y de las formas modulares.

Una curva elíptica E es una curva cúbica no singular. En teoría de números son especialmente importantes las definidas sobre $\mathbb{Q}$, las cuales con cambios de variable adecuados siempre se pueden reducir a la forma canónica $y^2 = x^3 + Ax + B$ con A y B racionales (o incluso enteros).

Dados dos puntos racionales de la curva, el tercer punto de intersección de la recta que los une será de nuevo racional (si dos de las raíces de una cúbica racional son racionales, la otra también lo es), de este modo es posible dotar al conjunto de puntos racionales de la curva de una estructura de grupo abeliano, pero dar una prueba geométrica de la asociatividad sería difícil. Una manera de solventar este problema es la de construir una $\phi : \mathbb{C} \to E$ cuyas coordenadas son funciones meromorfas de periodos 1 y $\omega \notin \mathbb{R}$ de forma que la suma habitual de números complejos se transforma en la suma de puntos en la curva elíptica y puesto que la primera es asociativa, la segunda también debe serlo.

A pesar de su simplicidad, las curvas elípticas han mostrado tener una sorprendente riqueza aritmética que ha dado lugar a aplicaciones inesperadas por ejemplo en el campo de la criptografía.

Las formas modulares tienen su origen en trabajos clásicos del siglo XIX pero se puede decir que es en la actualidad cuando viven su edad de oro pues en los últimos años la investigación en este tema ha crecido espectacularmente, especialmente en relación con la teoría de números. Sin embargo, en principio, la definición de forma modular pertenece al análisis complejo. En su versión más sencilla una forma modular f de peso k es una función holomorfa en el semiplano superior que verifica

$$f(z) = f(z+1), \qquad f(z) = z^{-k} f(-1/z)$$

y que en cierta forma es también holomorfa en el infinito. Estas relaciones implican

$$f(z) = (cz+d)^{-k} f\left(\frac{az+d}{cz+d}\right) \qquad \text{para toda } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

donde $\mathrm{SL}_2(\mathbb{Z})$ son las matrices enteras con determinante uno. La definición se extiende cambiando el grupo $\mathrm{SL}_2(\mathbb{Z})$ por algunos subgrupos suyos, especialmente $\Gamma_0(N)$ que son las matrices en las que c es divisible por N.

Al ser funciones periódicas, tienen un desarrollo de Fourier $f(z) = \sum a_n e^{2\pi n z}$ y son estos coeficientes a_n los que a menudo aportan información aritmética.

En 1955, Y. Taniyama y G. Shimura enunciaron una importante conjetura relacionando las curvas elípticas definidas sobre $\mathbb{Q}$ y las formas modulares. Sin embargo, en el momento de su aparición, la conjetura no mereció mayor atención, por considerar que se basaba en algunos casos aislados y sólo llegó a ser ampliamente conocida tras su publicación en un artículo de André Weil en 1967.

Esencialmente la conocida como *conjetura de Shimura-Taniyama-Weil* establece que si N_p es el número de puntos de una curva elíptica sobre $\mathbb{Q}$ al considerarla módulo un primo p, entonces existe una forma modular de peso dos $f(z) = \sum a_n e^{2\pi n z}$ con ciertas características tal que sus coeficientes de Fourier a_p coinciden con N_p. Se dice entonces que la curva elíptica es modular.

Goro Shimura, Yutaka Taniyama y André Weil.

La importancia de la conjetura radica en que liga dos temas muy diferentes. Es algo totalmente inesperado que haya relaciones entre el número de soluciones de una ecuación cúbica para diferentes primos, pero resulta que estos números están ligados entre sí pues se pueden combinar para formar una función holomorfa con ciertas simetrías. Sin embargo la difusión de la conjetura entre el gran público matemático vino por un camino diferente a su profundidad.

La relación entre la conjetura de Shimura-Taniyama-Weil y el último teorema de Fermat aparecía en 1985, cuando G. Frey propuso asociar a la ecuación de Fermat $a^n + b^n = c^n$ la curva elíptica $y^2 = x(x + a^n)(x - b^n)$. Esta curva tiene propiedades demasiado bellas para ser verdaderas; por ejemplo, a partir de estos coeficientes, el discriminante

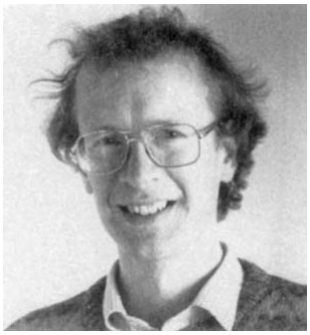
$$\Delta = \sqrt{(a^n - b^n)^2 + 4a^n b^n} = a^n + b^n = c^n$$

es una potencia n-ésima perfecta.

K. Ribet, con una sugerencia de B. Mazur, demostró en 1986 que la curva de Frey no puede ser parametrizada por funciones modulares. De este modo, la conjetura implicaba la no existencia de soluciones de Fermat. En el mismo año, A. Wiles se enteró de la

demostración de Ribet, y decidió concretar su sueño de juventud tratando de dar con una demostración de la conjetura.

En Junio de 1993, en la conferencia sobre Teoría de Números, en Cambridge, Wiles presentó sus resultados bajo el título de *Formas modulares, curvas elípticas y representaciones de Galois*, pero tres meses después y tras un análisis detallado del trabajo presentado por Wiles se encontró un fallo sustancial, una laguna en la demostración...



Andrew Wiles.

En 1995, Wiles con la ayuda de R. Taylor, demostró la conjetura para una clase de curvas elípticas llamadas semiestables, condición suficiente para probar el último teorema de Fermat. En 1999, la conjetura fue demostrada en su totalidad por C. Breuil, B. Conrad, F. Diamond y R. Taylor.

Teorema 1 (Breuil, Conrad, Diamond, Taylor, Wiles.)
Toda curva elíptica sobre $\mathbb{Q}$ *es modular.*

Nuestro objetivo en este trabajo será demostrar la conjetura para una sola curva elíptica especial, $E : y^2 = x^3 - 35x - 98$.

En el primer capítulo veremos el concepto de función elíptica, una función meromorfa doblemente periódica, asociada a un retículo Λ y un paralelogramo R, correspondientes a tales periodos.

De la relación existente entre las funciones elípticas y retículos, las primeras pueden identificarse como funciones meromorfas de un toro complejo $\mathbb{C}/\Lambda$, éste a su vez es isomorfo a una curva elíptica compleja, encontrando así la relación con las consabidas curvas. Antes de describir este isomorfismo se aportan varios resultados que ayudan a comprender cuándo dos curvas son isomorfas a partir de los toros correspondientes, que a su vez, se traduce en el estudio de los retículos y de cuándo dos de ellos son linealmente equivalentes [Di-Sh], [Kn].

Fijado un retículo, de entre todas las funciones elípticas hay dos de ellas que son básicas, $\wp(z)$ y $\wp'(z)$. Un estudio detallado mostrará cómo cualquier función elíptica

puede escribirse a partir de estas [Kn], lo que nos llevará a la relación $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$ donde g_1 y g_2 son constantes que dependen de Λ.

De este modo, llegamos al isomorfismo entre la superficie de Riemann $\mathbb{C}/\Lambda$ y la curva proyectiva $E : y^2 = 4x^3 - g_2x - g_3$, que vendrá dado por

$$\begin{array}{rccc} \Phi : & \mathbb{C}/\Lambda & \longrightarrow & E \\ & z & \mapsto & (\wp(z), \wp'(z)) \end{array}$$

Como $\mathbb{C}/\Lambda$ es una variedad abeliana vía el isomorfismo anterior podremos dotar a E de una ley de grupo $(E, +)$, que junto con varios ejemplos cierran el capítulo [Ch].

La relación existente entre dos retículos linealmente equivalentes es una transformación de Möbius asociada a los elementos del grupo modular $\mathrm{SL}_2(\mathbb{Z})$ actuando en $\mathbb{H}$.

En el capítulo 2 se darán las definiciones de funciones, formas modulares y formas cuspidales, todas ellas estrechamente vinculadas al grupo modular o como veremos también en el mismo capítulo, a subgrupos suyos [Di-Sh]. Definiremos los espacios correspondientes y la forma de calcular sus correspondientes dimensiones [Iw], [Di-Sh], [Se]. A lo largo de la exposición aparecerán varios ejemplos importantes, a saber, la serie de Eisenstein G_{2k} y su normalizada E_{2k}, la función discriminante Δ y la función de Klein j.

Estudiando con más detalle la estructura de los espacios aparecen los operadores de Hecke [Iw], [Se], con los que se afianza la conexión entre las formas modulares y la aritmética. En superficies de Riemann uniformizadas por ciertos subgrupos de $\mathrm{SL}_2(\mathbb{Z})$, se puede probar que los coeficientes de Fourier de las formas modulares de peso 2 de la base de Hecke correspondiente, son números algebraicos. Si además son enteros, la teoría de M. Eichler y G. Simura les asocia una curva elíptica sobre $\mathbb{Q}$ cuyo número de soluciones módulo p está relacionado con estos coeficientes.

Hablaremos sobre formas cuadráticas binarias en el marco de las formas modulares, estableciendo la relación existente entre formas cuadráticas y el grupo modular. Un estudio detallado del caso de discriminante 7, nos aportará más información sobre la curva tratada.

La última sección se centra en el estudio de una función theta en particular, la función θ de Jacobi [Di-Sh]. Daremos un resultado sobre la representación de un número como suma de cuadrados y la relación de la función con las formas cuadráticas [Iw].

La multiplicación compleja es una valiosa propiedad en las curvas elípticas [Si]. Si el retículo asociado a la curva posee esta propiedad, admite cierta noción de simetría. Veremos como en ciertos casos los coeficientes de estas curvas son todos ellos racionales. Todo ello estará incluido en el capítulo 3.

Introduciremos también el concepto de invariante j de una curva. Con respecto al grupo $\Gamma_0(N)$ encontraremos explícitamente los generadores del cuerpo de funciones meromorfas junto con una ecuación polinómica irreducible que los relaciona, la ecuación modular.

El estudio de la curva $E : y^2 = x^3 - 35x - 98$ tendrá lugar en el capítulo 4. A través de la ecuación modular y el invariante j calcularemos el retículo asociado y veremos cómo $j(\xi)$ cumple propiedades que ya anunciábamos en el capítulo anterior, puesto que E resultará ser una curva elíptica con multiplicación compleja.

Estudiaremos con detenimiento el endomorfismo de Frobenius basándonos en que sus puntos fijos cuando actúa sobre una curva algebraica, corresponden a soluciones módulo p. Distinguiremos dos casos, en los que Frob proviene de un endomorfismo sobre $\mathbb{C}$ y en los que este hecho no se puede asegurar [La]. En ambos, nuestro objetivo será hallar N_p, el número de puntos de E en $\mathbb{F}_p$.

Por último se demostrará que la curva es modular, concretamente encontraremos una forma modular de peso 2 tal que su p-ésimo coeficiente de Fourier es $p + 1 - N_p$.

De este modo, habremos probado el teorema de modularidad en un caso especial, lo que da por finalizado el trabajo.

Dulcinea Raboso Paniagua
Madrid, Septiembre de 2009

Capítulo 1

Funciones elípticas

1.1. Funciones elípticas

Definición: Una función meromorfa f es una *función elíptica* si es doblemente periódica, es decir, si existen $\omega_1, \omega_2 \in \mathbb{C}$ linealmente independientes sobre $\mathbb{R}$ tales que $f(z) = f(z+\omega_1) = f(z+\omega_2)$ para todo $z \in \mathbb{C}$.

La independencia lineal de ω_1 y ω_2 equivale a que sean no nulos y ω_1/ω_2 tenga parte imaginaria no nula. Podemos, si fuera necesario, intercambiar los generadores ω_1 y ω_2 de modo que $\Im(\omega_1/\omega_2) > 0$, es decir, podemos exigir que el punto $z = \omega_1/\omega_2$ viva en el semiplano superior

$$\mathbb{H} = \{z = x + iy \ : \ x \in \mathbb{R}, \ y > 0\}$$

Para f no constante, el conjunto $\{\lambda \ : \ f(z) = f(z+\lambda)\}$ es un retículo llamado *retículo de periodos*

$$\Lambda = \{m\omega_1 + n\omega_2 \ : \ m, n \in \mathbb{Z}\}$$

De ahora en adelante, siempre se dará por supuesto que ω_1 y ω_2 son generadores de Λ.

El paralelogramo con vértices 0, ω_1, ω_2, $\omega_1 + \omega_2$ es el llamado *paralelogramo fundamental* R. Para ser más precisos, R contiene al origen así como las dos partes adyacentes al mismo, pero no los otros dos lados y tres vértices. De este modo, el plano complejo se descompone en una unión disjunta de trasladados de R.

Proposición 1.1.1 (Teorema de Lioville) *No existe ninguna función elíptica no constante sin polos.*

Demostración: Una función de este tipo tendría que ser acotada en la clausura $\overline{R}$, por lo tanto, entera y acotada en $\mathbb{C}$. □

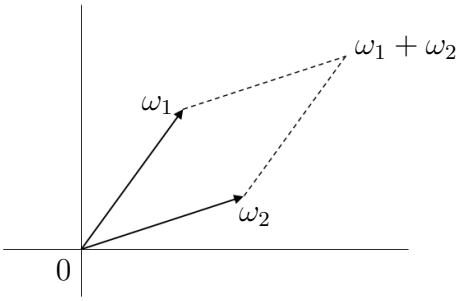


Figura 1.1: Paralelogramo fundamental

Corolario 1.1.2 *Si dos funciones elípticas tienen los mismos polos e idénticas partes principales, entonces difieren en una constante.*

Proposición 1.1.3 *Si $f(z)$ es una función elíptica sin polos en la frontera γ del paralelogramo fundamental R, entonces la suma de los residuos de $f(z)$ en R es cero.*

Corolario 1.1.4 *Si $f(z)$ es una función elíptica no constante, entonces f tiene más de un polo en R o bien, f tiene un polo de orden > 1.*

Corolario 1.1.5 *Supongamos que $f(z)$ es una función elíptica sin polos ni ceros en la frontera γ del paralelogramo R. Entonces f tiene el mismo número de ceros y de polos, contando multiplicidades.*

El *orden* de f es el número de ceros o de polos que tiene f en un paralelogramo fundamental de Λ (o en cualquiera de sus trasladados), contados siempre con su multiplicidad.

Corolario 1.1.6 *Supongamos que $f(z)$ es una función elíptica de orden n y R es su paralelogramo fundamental. Para cada $c \in \mathbb{C}$, f toma el valor c exactamente n veces, contando multiplicidades.*

1.2. Toros complejos

Una función elíptica puede considerarse como un elemento del cuerpo de funciones de la superficie de Riemann $\mathbb{C}/\Lambda$, es decir, de un toro complejo. Aquí el cociente se hace de la manera obvia: $z_1 \sim z_2 \Leftrightarrow z_1 - z_2 \in \Lambda$, denotando por $[z]$ la clase de z.

Todo toro complejo es isomorfo como grupo a una curva elíptica compleja. Este isomorfismo induce a su vez un isomorfismo entre el cuerpo de funciones racionales

de la curva elíptica y el cuerpo de funciones meromorfas del toro, las cuales pueden identificarse con las funciones meromorfas en $\mathbb{C}$ con periodos ω_1 y ω_2.

Dos números complejos ω_1 y ω_2 linealmente independientes sobre $\mathbb{R}$ determinan un paralelogramo en $\mathbb{C}$. Para trabajar más cómodamente en el toro que resulta de identificar los lados opuestos de dicho paralelogramo se trabaja con el retículo Λ generado por ω_1 y ω_2[1].

Definición: Un *homomorfismo analítico* $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ entre dos toros complejos es un homomorfismo de grupos que además es una aplicación holomorfa entre las dos superficies de Riemann.

Teorema 1.2.1 *Si $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ es una aplicación holomorfa entre dos toros complejos que cumple $\phi(0) = 0$, entonces ϕ es un homomorfismo analítico, inducido por la multiplicación por un cierto $\alpha \in \mathbb{C}$.*

Si $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ es un isomorfismo analítico entre dos toros complejos inducido por la multiplicación de un cierto $\alpha \in \mathbb{C}$ entonces $\alpha\Lambda = \Lambda'$. De forma análoga, si $\alpha \in \mathbb{C}$ es tal que $\alpha\Lambda = \Lambda'$ entonces induce un isomorfismo analítico entre los toros correspondientes.

Definición: Dos retículos complejos Λ y Λ' son linealmente equivalentes si existe $\alpha \in \mathbb{C}$ tal que $\alpha\Lambda = \Lambda'$.

Es decir, dos retículos complejos son linealmente equivalentes si se relacionan mediante una rotación y una homotecia. Usando los teoremas anteriores se tiene que dos toros $\mathbb{C}/\Lambda$ y $\mathbb{C}/\Lambda'$ son isomorfos si y sólo si los retículos Λ y Λ' son linealmente equivalentes.

Si Λ es el retículo generado por $\{\omega_1, \omega_2\}$, y Λ' es el generado por $\{\omega_1', \omega_2'\}$, entonces Λ y Λ' son equivalentes si y sólo si existe un $\alpha \in \mathbb{C}^*$ tal que $\mathbb{Z}\alpha\omega_1' + \mathbb{Z}\alpha\omega_2' = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Esto es equivalente a que existan enteros a, b, c, d tales que

$$\omega_1' = a\omega_1 + b\omega_2 \qquad \omega_2' = c\omega_1 + d\omega_2 \tag{1.1}$$

con $ad - bc = \pm 1$.

Llamando $z_\Lambda = \omega_1/\omega_2$ y $z_{\Lambda'} = \omega_1'/\omega_2'$ es equivalente a que existan números enteros a, b, c, d tales que

$$z_{\Lambda'} = \frac{az_\Lambda + b}{cz_\Lambda + d}$$

con $ad - bc = \pm 1$.

Suponiendo que los generadores de ambos retículos estén ordenados de modo que z_Λ y $z_{\Lambda'}$ estén ambos en $\mathbb{H}$, y tomando la parte imaginaria en la expresión anterior llegamos a que la única opción es $ad - bc = 1$.

[1]Dicho toro puede identificarse con el cociente $\mathbb{C}/\Lambda$, donde por comodidad se trabaja en todo el plano complejo en lugar de con el paralelogramo determinado por ω_1 y ω_2.

1.3. Función $\wp$ de Weierstrass

Vamos a definir una función elíptica no constante con períodos ω_1 y ω_2, demostrando la existencia de tales funciones. A continuación se desarrollan algunas propiedades de esta función.

Definición: Dado un retículo de periodos Λ se llama *función $\wp$ de Weierstrass* asociada a Λ a la función elíptica

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right). \tag{1.2}$$

Observación: Vamos a hacer uso reiterado del siguiente hecho en la teoría de variable compleja: si una serie de funciones analíticas en un conjunto abierto converge uniformemente, entonces el límite es analítico, y límites y derivadas pueden intercambiarse.

Lema 1.3.1 *Si s es un número real > 2, entonces*

$$\sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^s}$$

converge absolutamente.

Proposición 1.3.2 *Si F es un subconjunto finito de Λ y si los términos correspondientes a F se omiten en* (1.2)*, entonces la serie resultante converge absolutamente de forma uniforme en cualquier subconjunto compacto de $\mathbb{C} - (\Lambda - F)$. En consecuencia, $\wp(z)$ es meromorfa en $\mathbb{C}$, además sus únicos polos son de multiplicidad 2 en los puntos de Λ, y $\wp'(z)$ puede ser calculado término a término.*

Demostración: Podemos asumir que $\omega = 0 \in F$. La suma para $\Lambda - F$ es

$$\sum_{\omega\in\Lambda-F} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) = \sum_{\omega\in\Lambda-F} \frac{2z - \frac{z^2}{\omega}}{\omega(z-\omega)^2},$$

y se tiene que

$$\left| \frac{2z - \frac{z^2}{\omega}}{\omega(z-\omega)^2} \right| \leq \frac{C}{|\omega|^3}$$

en un conjunto compacto. Por el Lema 1.3.1, $\sum_{\omega\in\Lambda-F} \frac{C}{|\omega|^3} < \infty$, por lo que se tiene convergencia absoluta de forma uniforme. El resultado de la observación anterior muestra que el límite es meromorfo. Los polos son los que se indican a causa de la convergencia, y el mismo resultado muestra que podemos calcular $\wp'(z)$ término a término. □

Proposición 1.3.3 *La función $\wp(z)$ es una función elíptica con ω_1 y ω_2 periodos, par y de orden 2.*

Demostración: La función $\wp$ es meromorfa en $\mathbb{C}$, con polos dobles en los puntos de Λ. La serie que la define converge uniformemente en todo compacto que no contenga puntos de Λ, al igual que sucede con la serie que resulta de derivar término a término,

$$\wp'(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z+\omega)^3}.$$

Es evidente que $\wp'(z)$ es una función elíptica sobre Λ de orden 3.

La función $\wp(z)$ es par, pues

$$\wp(-z) = \frac{1}{(-z)^2} + \sum_{\omega\in\Lambda}\left(\frac{1}{(-z+\omega)^2} - \frac{1}{\omega^2}\right) =$$

$$= \frac{1}{(z)^2} + \sum_{\omega\in\Lambda}\left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right) = \wp(z)$$

donde se ha usado que $-\omega$ recorre Λ cuando ω lo hace.

Como $\wp'(z)$ es elíptica sobre Λ, la función $\wp(z+\omega) - \wp(z)$ con $\omega \in \Lambda$, es constante. Para $z = -\omega/2$ se tiene

$$\wp(z+\omega) - \wp(z) = \wp(\omega/2) - \wp(-\omega/2) = 0,$$

luego $\wp(z+\omega) - \wp(z)$ es la función nula. □

Observación: De la propia definición de serie infinita se sigue que $\wp'(z)$ es impar, es decir, que $\wp'(-z) = -\wp'(z)$.

Así, para cada retículo complejo Λ hemos encontrado dos funciones elípticas no constantes asociadas a Λ, las funciones $\wp(z)$ y $\wp'(z)$.

Teorema 1.3.4 *Cualquier función elíptica f puede escribirse como*

$$f(z) = G(\wp(z)) + \wp'(z)H(\wp(z)),$$

donde G y H son funciones racionales (cocientes de polinomios).

Por la identidad

$$f(z) = \frac{f(z)+f(-z)}{2} + \wp'(z)\frac{f(z)-f(-z)}{2\wp'(z)}$$

basta probar que toda función elíptica par g es una función racional de $\wp(z)$.

Para ello, veamos antes el siguiente resultado,

Lema 1.3.5 *Sea R el paralelogramo fundamental de Λ.*

1. *Para cualquier $u \in \mathbb{C}$, la función elíptica $\wp(z) - u$ tiene dentro de R o dos ceros simples o uno doble.*

2. *Los ceros de $\wp'(z)$ en R son $\omega_1/2$, $\omega_2/2$ y $(\omega_1 + \omega_2)/2$, todos ellos simples.*

3. *Los valores $u_1 = \wp(\omega_1/2)$, $u_2 = \wp(\omega_2/2)$ y $u_3 = \wp((\omega_1 + \omega_2)/2)$ son exactamente los u's en R donde $\wp(z) - u$ tiene un cero doble, y u_1, u_2, u_3 son distintos.*

Demostración:

1. Puesto que $\wp(z)$ tiene orden 2, basta aplicar el Corolario 1.1.6.

2. La función $\wp'(z)$ tiene orden 3, y por tanto como mucho 3 ceros. Usando que $\wp'(z)$ es impar y periódica, tomando $z = \omega_1/2$ se tiene

$$\wp'(\omega_1/2) = -\wp'(-\omega_1/2) = -\wp'(\omega_1 - \omega_1/2) = -\wp'(\omega_1).$$

   Por tanto $\omega_1/2$ es un cero y de forma similar, $\omega_2/2$ y $(\omega_1 + \omega_2)/2$ son también ceros.

3. Si $\wp(z) - u$ tiene un cero en z_0, dicho cero será doble si y sólo si $\wp'(z_0) = 0$. Por *2.*, $\wp(z) - u$ puede tener ceros dobles en $\omega_1/2$, $\omega_2/2$, $(\omega_1 + \omega_2)/2$, y en ese caso u debe ser u_1, u_2, u_3, respectivamente. Por otro lado, si $u = u_1$, entonces $\wp(z) - u_1$ es 0 en $z = \omega_1/2$, además $\wp'(\omega_1/2) = 0$, es por tanto un cero doble. Se obtiene un resultado análogo, aplicando el argumento en $\omega_2/2$ y en $(\omega_1 + \omega_2)/2$. Finalmente, si dos de ellos fueran iguales, digamos u_0, entonces $\wp(z) - u_0$ tendría dos ceros dobles, en contradicción con *1.*, lo que permite concluir que u_1, u_2, u_3 son todos distintos.

□

Demostración: (Teorema 1.3.4)
Sea $f(z)$ una función elíptica par. Sea $f(c) = 0$.

Supongamos $c \in R$ y $c \notin \{0, \omega_1/2, \omega_2/2, (\omega_1 + \omega_2)/2\}$. Sea c^* su punto simétrico, es decir, un punto en R congruente con $-c$. Si c tiene orden n, también lo tendrá c^*. De hecho

$$f(c^* - z) = f(-c - z) = f(c + z).$$

Si $f(c + z) = c_n z^n + (\text{orden superior})$, entonces

$$f(c^* + z) = f(c - z) = c_n z^n + (\text{orden superior})$$

Ahora supongamos que $c \in \{\omega_1/2, \omega_2/2, (\omega_1 + \omega_2)/2\}$, por ejemplo $c = \omega_1/2$. Entonces

$$f(\omega_1/2 - z) = f(-\omega_1/2 - z) = f(\omega_1/2).$$

f es par en $c = \omega_1/2$ y por tanto su orden es par.

Un argumento similar se aplica en los polos. Si f tiene un polo en $p \in R$ con $p \notin \{0, \omega_1/2, \omega_2/2, (\omega_1+\omega_2)/2\}$, entonces f tiene un polo en p^* del mismo orden. Para $\omega_1/2$, $\omega_2/2$, $(\omega_1+\omega_2)/2$ el orden del polo es par.

Tomamos ahora "la mitad" de la lista de ceros y polos de $f(z)$. Sea $\{c_i\}$ la lista de los ceros de $f(z)$ en R que no sean 0, $\omega_1/2$, $\omega_2/2$, $(\omega_1+\omega_2)/2$ tomado cada uno con su multiplicidad, pero tomado sólo uno para cada par c, c^*. Para los ceros entre $\omega_1/2$, $\omega_2/2$, $(\omega_1+\omega_2)/2$, la lista será el punto medio tomado tantas veces como indique su multiplicidad. De forma similar, sea $\{p_j\}$ la lista de "la mitad" de los polos en R excepto el 0.

Puesto que todos los c_i y p_j son distintos de cero, $\wp(c_i)$ y $\wp(pj)$ son finitos para todo i, j. Tiene sentido entonces definir

$$g(z) = \frac{\prod_i(\wp(z) - \wp(c_i))}{\prod_j(\wp(z) - \wp(p_j))}.$$

Es claro que g tiene los mismos ceros y polos que f, contando multiplicidades. Dado que los únicos polos del numerador y denominador se encuentran en $z = 0$, el resto de ceros y polos de $g(z)$ vienen dados por los ceros del numerador y del denominador.

Consideramos un cero z_0 del numerador, un punto que verifique $\wp(z_0) = \wp(c_i)$. Si c_i es uno de $\omega_1/2$, $\omega_2/2$, $(\omega_1+\omega_2)/2$, entonces usando el Lema 1.3.5, $\wp$ toma el valor $\wp(c_i)$ dos veces en ese momento y en ninguna otra parte. Por tanto $z_0 = c_i$ y $\wp(z)-\wp(c_i)$ tiene un cero de orden dos en z_0. Teniendo en cuenta la repetición de los factores para ese c_i, se tiene que f y g tienen un cero del mismo orden en z_0.

Supongamos ahora que $c_i \notin \{\omega_1/2, \omega_2/2, (\omega_1+\omega_2)/2\}$. Se tiene que $\wp(c_i^*) = \wp(c_i)$, de modo que $\wp(z) - \wp(c_i)$ tiene ceros distintos en c_i y en c_i^*. Por el lema, esos ceros son simples. Teniendo en cuenta la repetición de los factores para ese c_i, se tiene que f y g tienen un cero del mismo orden en z_0.

Por lo tanto, f y g tienen el mismo número de ceros (incluyendo los ordenes) y de forma similar, el mismo número de polos (incluyendo los ordenes) apartando el caso $z = 0$. Por el Corolario 1.1.5, tienen el mismo orden de cero o polo en $z = 0$. En consecuencia, f/g es entera y por tanto constante por la Proposición 1.1.1, lo que concluye la prueba. □

La función $(\wp')^2$ es elíptica y par, y por tanto se puede escribir en términos de $\wp$.

Teorema 1.3.6 *La función $\wp$ verifica*

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3,$$

donde g_2 y g_3 son constantes que dependen de Λ en el siguiente sentido:

$$G_m = G_m(\Lambda) = \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^m} \quad \text{para } m \geq 3 \tag{1.3}$$

$$\begin{aligned} g_2 &= g_2(\Lambda) = 60G_4, \\ g_3 &= g_3(\Lambda) = 140G_6. \end{aligned} \tag{1.4}$$

Demostración: Por un lado, usando

$$\frac{1}{(1-z)^2} = 1 + 2z + 3z^2 + \dots \qquad \text{si } |z| < 1,$$

se deduce

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}.$$

Por otro, puesto que $-\omega$ recorre Λ cuando ω lo hace, se tiene

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}.$$

La serie G_n definida por (1.3) es convergente para $n \geq 3$, además $G_n = 0$ si n es impar, se tiene entonces

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n} = \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + 7G_8z^6 + \dots$$

Derivando término a término,

$$\wp'(z) = -\frac{2}{z^3} + \sum_{n=1}^{\infty}(2n+1)2nG_{2n+2}z^{2n-1} = -\frac{2}{z^3} + 6G_4z + 20G_6z^3 + 42G_8z^5 + O(z^7)$$

Con unos cálculos más,

$$\begin{aligned} \wp'(z)^2 &= \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + (36G_4^2 - 168)z^2 + O(z^4) \\ \wp(z)^2 &= \frac{1}{z^4} + 6G_4 + 10G_6z^2 + O(z^4) \\ \wp(z)^3 &= \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + (21G_8 + 27G_4^2)z^2 + O(z^4) \\ \Longrightarrow \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 &= O(z^2) \end{aligned}$$

y puesto que no tiene polos ni término constante, usando la Proposición 1.1.1

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 = 0.$$

Por último, definiendo g_2 y g_3 por (1.4), se tiene el resultado. □

El cuerpo $\mathbb{C}(\wp, \wp')$ de las funciones elípticas sobre el retículo Λ es isomorfo al cuerpo de funciones racionales de la curva proyectiva E determinada por la ecuación $y^2 = 4x^3 - g_2x - g_3$. Como $\mathbb{C}(\wp, \wp')$ es también isomorfo al cuerpo de las funciones meromorfas del toro complejo $\mathbb{C}/\Lambda$ que tiene género 1, lo mismo le ha de suceder a E, luego E ha de ser una cúbica regular, es decir, una curva elíptica.

Teorema 1.3.7 *Si Λ es un retículo en $\mathbb{C}$ con base $\{\omega_1, \omega_2\}$, entonces*

$$4x^3 - g_2x - g_3 = 4\left(x - \wp(\omega_1/2)\right)\left(x - \wp(\omega_2/2)\right)\left(x - \wp((\omega_1+\omega_2)/2)\right).$$

En particular, la curva plana

$$E : y^2 = 4x^3 - g_2x - g_3$$

es regular.

Demostración: (véase [Kn]). □

Según hemos visto hasta aquí, a cada retículo complejo Λ le hemos asociado una función de Weierstrass $\wp$ y unos números complejos g_2 y g_3 que a su vez determinan una ecuación de Weierstrass que a su vez determina una curva elíptica plana. A continuación se demuestra que las funciones $\wp$ y $\wp'$ parametrizan la curva de forma natural.

Teorema 1.3.8 *La aplicación*

$$\begin{array}{rccc} \Phi: & \mathbb{C}/\Lambda & \longrightarrow & E \\ & z & \mapsto & (\wp(z), \wp'(z)) \end{array}$$

establece un isomorfismo holomorfo entre la superficie de Riemann $\mathbb{C}/\Lambda$ y la curva proyectiva $E : y^2 = 4x^3 - g_2x - g_3$, entendiendo que $\Phi([0])$ es el punto del infinito de E, de coordenadas proyectivas $(0:1:0)$.

Demostración: La inyectividad se sigue porque definiendo R como en la demostración del Teorema 1.3.4, $\wp(z) - \wp(z_1)$ sólo tiene como ceros z_1 y $-z_1$. La sobreyectividad se sigue porque ambas son superficies de Riemann compactas y Φ no es constante [Kn]. □

1.4. Ley de grupo

La superficie $\mathbb{C}/\Lambda$ es una *variedad abeliana* porque sus puntos conforman un grupo abeliano. Para sumar en el toro simplemente sumamos en $\mathbb{C}$ y tomamos módulo Λ. Entonces en E debe haber también una forma de sumar puntos.

Lema 1.4.1 *Si $u + v + w \in \Lambda$, es decir, si $[u], [v], [w]$ suman cero en $\mathbb{C}/\Lambda$, entonces los puntos $\Phi(u)$, $\Phi(v)$ y $\Phi(w)$ están alineados.*

El proceso se puede invertir asociando a cada curva no singular de la forma $E : y^2 = 4x^3 - \alpha x - \beta$ un toro $\mathbb{C}/\Lambda$ cuya imagen por Φ es E.

Consideramos $E : y^2 = x^3 + ax + b$ en lugar de $E : y^2 = 4x^3 - g_2x - g_3$, tales curvas sólo difieren en un cambio lineal que por tanto no destruye la alineación de los puntos. La no singularidad de E equivale a que $x^3 + ax + b$ no tenga raíces dobles, o equivalentemente, a que el determinante $4a^3 + 27b^2$ sea no nulo.

Proposición 1.4.2 *Sea $E : y^2 = x^3 + ax + b$ curva proyectiva sobre $\mathbb{C}$ no singular. Entonces se puede dotar a sus puntos de una ley de grupo $(E, +)$ de forma que el elemento neutro O es el punto del infinito, el elemento inverso de $P = (x, y)$ es $P = (x, -y)$ y si $P + Q = R$ entonces P, Q y $-R$ están alineados.*

Demostración: La ley de grupo viene heredada de la suma en $\mathbb{C}/\Lambda$, es decir,

$$P + Q = \Phi(\Phi^{-1}(P) + \Phi^{-1}(Q))$$

y comparte las propiedades de grupo abeliano con la suma usual.

Considerando $\Phi([0])$ y la paridad de $\wp$ podemos deducir los elementos neutro y opuesto. Si $P + Q - R = 0$, por definición $\Phi^{-1}(P) + \Phi^{-1}(Q) - \Phi^{-1}(R) = [0]$ y el lema anterior prueba que P, Q y $-R$ están alineados [Ch]. □

Definición: Una curva elíptica E sobre un cuerpo K admite varias definiciones todas ellas equivalentes,

- Una cúbica plana regular definida sobre K, junto con un punto $O \in E(K)$.
- Una curva en $\mathbb{P}^2$ regular definida por una *ecuación de Weierstrass*,

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

  con $a_i \in K$
- Una curva regular definida sobre K con género $g(E) = 1$, junto con un punto $O \in E(k)$

En cuerpos de característica distinta de 2 y 3, toda curva elíptica tras un cambio de variable se escribe como $y^2 = x^3 + ax + b$ con $4a^3 + 27b^2 \neq 0$, la existencia de tal cambio de coordenadas es una consecuencia del teorema de Riemann-Roch (véase [Si]). Cuando esto no es posible (por ejemplo en $\mathbb{F}_2$) harán falta más términos, pero es posible encontrar una expresión similar [Ca]. Por ello la ley de grupo se extiende a todas las curvas cúbicas no singulares.

La ley de grupo en una curva elíptica se define a través de la Proposición 1.4.2 como el simétrico del tercer punto de intersección de la recta secante.

Para una curva elíptica $E : y^2 = x^3 + ax^2 + b$, se tienen las fórmulas:

$$P = (x_1, y_1), \quad Q = (x_2, y_2), \quad P + Q = (x, y)$$

con

a) Si $x_1 \neq x_2$,

$$\begin{cases} x = \left(\frac{y_1-y_2}{x_1-x_2}\right)^2 - x_1 - x_2 \\ y = -\frac{y_1-y_2}{x_1-x_2}x - \frac{x_1y_2-x_2y_1}{x_1-x_2} \end{cases}$$

b) Si $x_1 = x_2$, pero $P \neq Q$, entonces $P + Q = O$.

c) Si $P = Q$,

$$\begin{cases} x = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1 \\ y = -\frac{3x_1^2+a}{2y_1}x - \frac{-x_1^3+ax_1+2b}{2y_1} \end{cases}$$

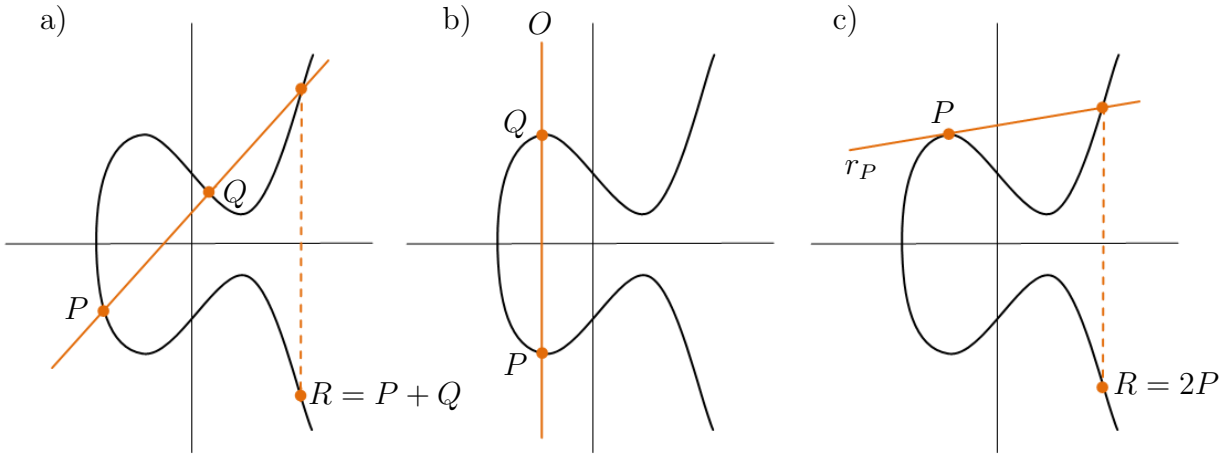


Figura 1.2: Sumas en la curva elíptica

Observación: Un punto $P \in E$ cumple $2P = O$ si la recta tangente a E en el punto P es vertical, lo que es equivalente a pedir que P sea de la forma $(a, 0)$.

⋆ *Ejemplo:* Considerando la curva elíptica $E : y^2 = x^3 + 1$ sobre $\mathbb{Q}$, el orden del punto $P = (2, 3)$ es 6.

$$P = (x_1, y_1) = (2, 3) \Rightarrow 2P = (x_2, y_2)$$

$$\begin{aligned} x_2 &= \left(\frac{3x_1^2}{2y_1}\right)^2 - 2x_1 = \left(\frac{3 \cdot 4}{2 \cdot 3}\right)^2 - 4 = 4 - 4 = 0, \\ y_2 &= -\frac{3x_1^2}{2y_1}x_2 - \frac{-x_1^3+2}{2y_1} = -\frac{-8+2}{2 \cdot 3} = 1, \end{aligned}$$

$$\Rightarrow 2P = (0, 1).$$

$$\begin{array}{c} P = (x_1, y_1) = (2, 3) \\ 2P = (x_2, y_2) = (0, 1) \end{array} \Rightarrow \ 3P = (x, y)$$

$$\begin{aligned} x &= \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2 = \left(\frac{3-1}{2}\right)^2 - 2 = 1 - 2 = -1, \\ y &= -\frac{y_1 - y_2}{x_1 - x_2}x - \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2} = \frac{3-1}{2} - 1 = 0, \end{aligned}$$

$$\Rightarrow 3P = (-1, 0).$$

Usando la observación anterior

$$2 \cdot 3P = O \Rightarrow 6P = O.$$

$\star$ *Ejemplo:* Considerando la curva E del ejemplo anterior sobre $\mathbb{F}_5$, el punto $Q = (2, 2)$ tiene orden 6.

$$Q = (x_1, y_1) = (2, 2) \Rightarrow 2Q = (x_2, y_2)$$

$$\begin{aligned} x_2 &= \left(\frac{3 \cdot 4}{2 \cdot 2}\right)^2 - 4 = 9 - 4 \equiv 0 \pmod 5, \\ y_2 &= -\frac{-8+2}{4} \equiv 4 \pmod 5, \end{aligned}$$

$$\Rightarrow 2Q = (0, 4).$$

$$\begin{array}{c} Q = (x_1, y_1) = (2, 2) \\ 2Q = (x_2, y_2) = (0, 4) \end{array} \Rightarrow \ 3Q = (x, y)$$

$$\begin{aligned} x &= \left(\frac{2-4}{2}\right)^2 - 2 \equiv 4 \pmod 5, \\ y &= -\frac{2-4}{2}4 - \frac{2 \cdot 4}{2} \equiv 0 \pmod 5, \end{aligned}$$

$$\Rightarrow 3Q = (4, 0).$$

Usando de nuevo la observación

$$2 \cdot 3Q = O \Rightarrow 6Q = O.$$

Capítulo 2

Formas modulares

Una función elíptica $f(z)$, además de ser una función meromorfa en $z \in \mathbb{C}$, es también una función asociada a un retículo, $f(z) = f(z, \omega_1, \omega_2)$, donde ω_1, ω_2 son los generadores. Esta dependencia de los retículos da la noción clásica de funciones modulares. En la sección anterior se vio como dos pares de números complejos, linealmente independientes sobre $\mathbb{R}$, determinan el mismo retículo si se relacionan por una transformación unimodular, es decir, una transformación de Möbius asociada a los elementos de $\mathrm{SL}_2(\mathbb{Z})$.

2.1. El grupo modular

La acción de transformaciones unimodulares en el retículo $\Lambda = \{n\omega_1 + m\omega_2 \ : \ n, m \in \mathbb{Z}\}$ se corresponde con la acción del grupo modular

$$\mathrm{SL}_2(\mathbb{Z}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \ : \ a, b, c, d \in \mathbb{Z}, ad - bc = 1\}$$

en $\mathbb{H}$ por las transformaciones lineales

$$\gamma z = \frac{az + b}{cz + d} \qquad \text{si} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

El grupo modular $\mathrm{SL}_2(\mathbb{Z})$ es el primer subgrupo discreto de $\mathrm{SL}_2(\mathbb{R})$ con interesantes propiedades aritméticas.

Los elementos de $\mathrm{SL}_2(\mathbb{Z})$ no envían un punto fijado a cualquier punto[1] de $\mathbb{H}$ porque no todos los retículos son iguales.

El grupo modular está generado por dos matrices,

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

[1]Se dice que dos puntos de $\mathbb{H}$ son *equivalentes* bajo un subgrupo Γ de $\mathrm{SL}_2(\mathbb{R})$ si uno puede transformarse en el otro mediante un elemento de Γ.

La primera corresponde a la traslación $z \mapsto z+1$ y la segunda a la inversión $z \mapsto -1/z$, [Kn].

El análogo al paralelogramo fundamental de un retículo es el concepto de dominio fundamental.

Definición: Un subconjunto cerrado $D \subset \mathbb{H}$ es un *dominio fundamental* para Γ si todo punto de $\mathbb{H}$ es equivalente a un punto de D y dos puntos de D no son equivalentes salvo quizá si ambos están en la frontera.

Ciertamente, los paralelogramos fundamentales de un retículo complejo Λ cumplen esta definición respecto al grupo de traslaciones asociadas a Λ.

Proposición 2.1.1 *El conjunto*

$$D = \{z \ : \ |\Re z| \leq \frac{1}{2}, |z| \geq 1\},$$

donde se identifica la parte izquierda de la frontera con la correspondiente parte derecha, es el dominio fundamental del grupo modular $\Gamma = SL_2(\mathbb{Z})$*, es decir, tiene las propiedades:*

- D *es dominio en* $\mathbb{H}$*.*
- *Toda órbita de* Γ *tiene un punto en* D*.*
- *Puntos distintos en el interior de* D *están en órbitas distintas de* Γ*.*

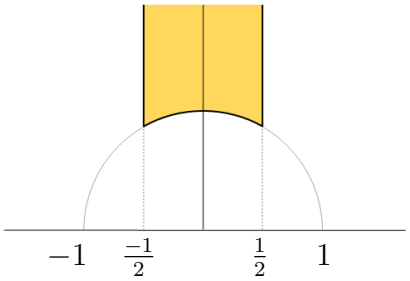


Figura 2.1: Dominio fundamental de $\mathrm{SL}_2(\mathbb{Z})$

Demostración: A base de trasladar podemos enviar cualquier $z \in \mathbb{H}$ a $|\Re z| \leq 1/2$ y con una inversión podemos sacar fuera lo que está dentro del círculo unidad $|z| \leq 1$. La traslación T y la inversión S, pasan la frontera izquierda a la derecha de ahí la ambigüedad de estos puntos y hay que suprimir una de ellas para preservar la unicidad [Ch]. □

2.2. Formas modulares

Definición: Una función meromorfa f en $\mathbb{H}$ se dice *función modular de peso k* si satisface:

$$f(z) = j_\gamma^{-k}(z) f(\gamma z) \qquad \forall\, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

donde $j_\gamma(z) = cz + d$. Además, existe un entero n_0 tal que la expansión de Fourier de f en la variable $e(z) = e^{2\pi i z}$ es de la forma

$$f(z) = \sum_{n=n_0}^{\infty} a_n \; e(nz).$$

Puesto que $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ generan cualquier $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, f será función modular de peso k si

$$f(z+1) = f(z) \quad \text{y} \quad f(-1/z) = z^{-k} f(z).$$

Una función modular de peso 0 es simplemente una función en $\mathbb{H}$ que es $\mathrm{SL}_2(\mathbb{Z})$-invariante. Las funciones modulares de peso 2 se corresponden con uno formas diferenciales, y las de peso superior a diferenciales invariantes de orden superior.

Observación: La $\mathrm{SL}_2(\mathbb{Z})$-invarianza en el semiplano superior requiere que las diferenciales $f(z)dz$ sean invariantes cuando z se reemplaza por γz, como

$$d(\gamma z) = d\left(\frac{az+b}{cz+d}\right) = \frac{ad-bc}{(cz+d)^2} dz = (cz+d)^{-2} dz,$$

junto con la relación $f(\gamma z) d(\gamma z) = f(z) dz$ se tiene que

$$f(z) = (cz+d)^{-2} f(\gamma z).$$

Observación: Tomando $\gamma = -I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, entonces $\gamma z = z$ para todo $z \in \mathbb{H}$. Por lo tanto, si f es una función modular de peso k, con k un entero impar, entonces

$$f(z) = (-1)^{-k} f(\gamma z) = -f(z)$$

y por tanto f es idénticamente cero. Así, una función modular no trivial en $\mathrm{SL}_2(\mathbb{Z})$ es necesariamente de peso par.
El caso de peso 2 es sin duda especial sobre el resto de pesos [2].

[2]Multiplicando dos funciones modulares de peso 2 se obtiene una función modular de peso 4 y así sucesivamente.

Otra idea para motivar la modularidad es que, si bien una función modular f no es plenamente $\mathrm{SL}_2(\mathbb{Z})$-invariante, al menos, $f(z)$ y $f(\gamma z)$ tienen siempre los mismos polos y ceros ya que el factor $cz+d$ en $\mathbb{H}$ no los tiene.

Definición: Una función f definida en $\mathbb{H}$ se dice *forma modular de peso k* si

1. f es holomorfa en $\mathbb{H}$.
2. f es función modular de peso k.
3. La expansión de Fourier de f es de la forma

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

Se dice entonces que f es *holomorfa en el infinito* y se define $f(i\infty) = a_0$.

El conjunto de formas modulares de peso k es denotado por $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ o simplemente por $\mathcal{M}_k$.

$\mathcal{M}_k$ es un espacio vectorial sobre $\mathbb{C}$ y el espacio de todas las formas modulares es la suma directa[3] de los $\mathcal{M}_k$,

$$\mathcal{M} = \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k.$$

Las formas modulares pueden verse como funciones homogéneas de cierto grado definidas en el espacio de retículos. Por ejemplo, si F es homogénea (de grado 0), la condición para que no dependa de los generadores elegidos es $F(\omega_1,\omega_2) = F(a\omega_1+b\omega_2, c\omega_1+d\omega_2)$, que equivale a que $F(z,1) = F(z) = F(\gamma z),\ \forall\gamma \in \mathrm{SL}_2(\mathbb{Z})$, con $z = \omega_1/\omega_2$.

La función cero en $\mathbb{H}$ es una forma modular para cada peso, y toda función constante en $\mathbb{H}$ es forma modular de peso 0. Un ejemplo de formas modulares no triviales son las llamadas series de Eisenstein,

Definición: Sea Λ un retículo y $k \geq 1$ entero, se define la *serie de Eisenstein de peso $2k$* como

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^{2k}}.$$

Para $z \in \mathbb{H}$, sea $\Lambda_z = \{mz+n \ : \ m,n \in \mathbb{Z}\}$ el retículo asociado, entonces

$$G_{2k}(z) = G_{2k}(\Lambda_z) = \sum_{\substack{n,m=-\infty \\ n^2+m^2\neq 0}}^{\infty} \frac{1}{(mz+n)^{2k}}.$$

[3]El producto de una forma modular de peso k con una forma modular de peso l es una forma modular de peso $k+l$, por lo que el espacio $\mathcal{M}$ puede ser considerado como un álgebra graduada con la estructura aditiva.

Se define la *serie de Eisenstein normalizada* como

$$E_{2k}(z) = \frac{G_{2k}(z)}{2\zeta(2k)}.$$

Proposición 2.2.1 *La serie de Eisenstein es una forma modular de peso $2k$ para $k \geq 2$.*

Demostración: Para $\alpha \in \mathbb{C}^*$ se tiene que

$$G_{2k}(\alpha\Lambda) = \alpha^{-2k} G_{2k}(\Lambda).$$

Por otro lado

$$\Lambda_{\gamma z} = \mathbb{Z}\frac{az+b}{cz+d} + \mathbb{Z} = \frac{1}{cz+d}(\mathbb{Z}(az+b) + \mathbb{Z}(cz+d)) = \frac{1}{cz+d}\Lambda_z.$$

Por lo tanto

$$G_{2k}(\gamma z) = G_{2k}(\Lambda_{\gamma z}) = G_{2k}((cz+d)^{-1}\Lambda_z) = (cz+d)^{2k} G_{2k}(\Lambda_z) = (cz+d)^{2k} G_{2k}(z),$$

se tiene entones que $G_{2k}(z)$ es función modular, queda ver que es holomorfa en $\mathbb{H}$ y en ∞. Una primera observación nos lleva a ver que si z pertenece al dominio fundamental D descrito en la Proposición 2.1.1, entonces

$$|mz+n|^2 = m^2|z|^2 + 2mn\Re z + n^2 \geq m^2 - mn + n^2 = |m\rho - n|^2.$$

Por lo tanto, la serie en valores absolutos obtenida de $G_{2k}(z)$ está dominada, término a término, por la serie en valores absolutos obtenida de $G_{2k}(\rho)$, se tiene entonces que G_{2k} es holomorfa en D. Pero $\mathbb{H}$ está cubierto por la acción de $\mathrm{SL}_2(\mathbb{Z})$ en D y $G_{2k}(\gamma z) = (cz+d)^{2k} G_{2k}(z)$, obteniéndose así la holomorfía en todo $\mathbb{H}$.

Por último, estudiamos el comportamiento de $G_{2k}(z) = G_{2k}(x+iy)$ cuando $y \to \infty$. Puesto que la serie G_{2k} converge absolutamente (para $k \geq 2$), podemos tomar el límite término a término. Los términos de la forma $(mz+n)^{-2k}$ con $m \neq 0$ tienden a cero, mientras que el resto dan n^{-2k}. Por lo tanto

$$\lim_{y\to\infty} G_{2k}(z) = \sum_{n=-\infty}^{\infty} \frac{1}{n^{2k}} = \zeta(2k).$$

Esto demuestra que G_{2k} es holomorfa en ∞, y por tanto es forma modular de peso $2k$. □

A partir del desarrollo de la cotangente

$$\pi i - 2\pi i \sum_{n=0}^{\infty} e(nz) = \pi \cot(\pi z) = \sum_{n=-\infty}^{\infty} \frac{1}{z+n}$$

se puede hallar el desarrollo de Fourier de las funciones E_k, obteniendo

$$E_{2k}(z) = 1 + \frac{(2\pi i)^{2k}}{\zeta(2k)(2k-1)!}\sum_{m=1}^{\infty}\sigma_{2k-1}(m)e(mz) \quad \text{donde } \sigma_{2k-1}(m) = \sum_{d|m} d^{2k-1}. \tag{2.1}$$

La serie de Eisenstein es forma modular para $k \geq 2$, el caso $k = 1$ es especial.

Caso $k = 1$.

La definición natural de la serie de Eisenstein de peso 2, $G_2(z) = \sum_m \sum_n (mz+n)^{-2}$ (con m y n no simultáneamente nulos), converge pero no absolutamente pues

$$\sum_{\substack{n,m=-\infty \\ n^2+m^2\neq 0}}^{\infty} \left|\frac{1}{(mz+n)^2}\right| = \sum_{\substack{n,m=-\infty \\ n^2+m^2\neq 0}}^{\infty} \frac{1}{|(mz+n)^2|} = \sum_{\substack{n,m=-\infty \\ n^2+m^2\neq 0}}^{\infty} \frac{1}{(mx+n)^2+(my)^2}.$$

Denotando la última suma por S y considerando para cada $m > 0$ los n tales que $m \leq n + mx \leq 2m$, se llega a que

$$S \geq \sum_{m=1}^{\infty} \sum_{m\leq n+mx\leq 2m} \frac{1}{(2m)^2+(my)^2} = \sum_{m=1}^{\infty} \frac{m}{(2m)^2+(my)^2} = \infty$$

La convergencia no absoluta impide invertir el orden de sumación. Sorprendentemente esto causa que la función definida por la serie deje de ser modular.

El desarrollo de Fourier de $E_{2k}(z)$ también es válido para $k = 1$,

$$\begin{aligned} G_2(z) &= 2\zeta(2)E_2(z) = \sum_{\substack{n,m=-\infty \\ n^2+m^2\neq 0}}^{\infty} \frac{1}{(mz+n)^2} = \sum_{m\neq 0}\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^2} + 2\sum_{n=1}^{\infty}\frac{1}{n^2} = \\ &= 2\zeta(2) + \sum_{m\neq 0}\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^2} = 2\zeta(2) + 2\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^2} = \\ &= 2\zeta(2) + 2\sum_{m=1}^{\infty}\frac{(-2\pi i)^2}{1!}\sum_{d=1}^{\infty} d\ e(dmz). \end{aligned}$$

Efectuando el cambio $dm \to m$,

$$G_2(z) = 2\zeta(2) - 2(2\pi)^2\sum_{m=1}^{\infty}\sum_{d|m} d\ e(mz) = 2\zeta(2) - 2(2\pi)^2\sum_{m=1}^{\infty}\sigma(m)e(mz).$$

$$\Longrightarrow E_2(z) = 1 - \frac{(2\pi)^2}{\zeta(2)}\sum_{m=1}^{\infty}\sigma(m)e(mz)$$

que corresponde a poner formalmente $k = 1$ en (2.1).

Observación: Para solventar el problema de la convergencia no absoluta se introduce el término "acelerador" $a(x,n) = 1/(x+n-1) - 1/(x+n)$. De este modo,

$$E_2(z) = 1 + \frac{1}{2\zeta(2)} \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \left(\frac{1}{(mz+n)^2} - a(mz,n) \right)$$

converge absolutamente.

Demostración: Primero nos aseguramos de que al introducir el término $a(x,n)$, la serie $E_2(z)$ permanece invariante,

$$\sum_{m\neq 0} \sum_{n=-\infty}^{\infty} a(mz,n) = \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \left(\frac{1}{mz+n-1} - \frac{1}{mz+n} \right).$$

Para m fijo, sea $a_n(mz) = \frac{1}{mz+n}$. De este modo se tiene que

$$\sum_{n=-\infty}^{\infty} \left(\frac{1}{mz+n-1} - \frac{1}{mz+n} \right) = \sum_{n=-\infty}^{\infty} (a_{n-1}(mz) - a_n(mz)) = 0$$

$$\Longrightarrow \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} a(mz,n) = 0.$$

Se tiene entonces que

$$\begin{aligned} E_2(z) &= 1 + \frac{1}{2\zeta(2)} \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^2} = \\ &= 1 + \frac{1}{2\zeta(2)} \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \left(\frac{1}{(mz+n)^2} - a(mz,n) \right). \end{aligned}$$

Y converge absolutamente pues

$$\frac{1}{(mz+n)^2} - \frac{1}{mz+n-1} + \frac{1}{mz+n} = \frac{1}{(mz+n)^2} - \frac{1}{(mz+n-1)(mz+n)} =$$

$$= -\frac{1}{(mz+n)^2(mz+n-1)}.$$

Escribiendo $z = x+iy$ con $y>0$, y sumando las normas se tiene

$$\sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \frac{1}{[(mx+n)^2+(my)^2]|mz+n-1|} \leqslant \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \frac{1}{[(mx+n)^2+(my)^2]|my|}$$

donde se ha usado que $|w| \geqslant |\Im w|$.

La suma en n es de la forma,

$$S = \sum_{n=-\infty}^{\infty} \frac{1}{(n+\alpha)^2+\beta^2}$$

donde $\alpha = mx$ y $\beta = my$. Con una traslación en n, podemos suponer que $0 \le \alpha < 1$ y $\beta > 0$, de modo que

$$S \le 2\sum_{n=0}^{\infty} \frac{1}{n^2+\beta^2} \le 2\sum_{n\le\beta}^{\infty} \frac{1}{n^2+\beta^2} + 2\sum_{n>\beta}^{\infty} \frac{1}{n^2+\beta^2}.$$

La primera suma es $< (\beta+1)/\beta^2$ y en la segunda dividimos en *intervalos diádicos*

$$\sum_{n>\beta}^{\infty} \frac{1}{n^2+\beta^2} \le \sum_{k=1}^{\infty} \sum_{2^k\beta<n\le 2^{k+1}\beta} \frac{1}{n^2+\beta^2} \le \sum_{k=1}^{\infty} \frac{2^k\beta+1}{2^{2k}\beta^2+\beta^2}.$$

Como $\sum 2^k/(2^{2k}+1)$ y $\sum 1/(2^{2k}+1)$ convergen, se tiene que $S \ll \beta^{-1}+\beta^{-2}$ y por tanto

$$\sum_{m\neq 0} \frac{1}{|my|} S \ll \sum_{m\neq 0} \frac{1}{|my|}\left(\frac{1}{my} + \frac{1}{(my)^2}\right) = 2\sum_{m=1}^{\infty} \frac{1}{(my)^3} < \infty.$$

□

Observación: E_2 no es modular pero satisface una relación parecida a la que satisfacen las formas de peso 2,

$$z^{-2}E_2(-1/z) = E_2(z) + 6/(\pi i z).$$

Demostración: Primero veamos que

$$E_2(z) + S(z)/(2\zeta(2)) = z^{-2}E_2(-1/z) \qquad \text{con} \qquad S(z) = \sum_{n=-\infty}^{\infty}\sum_{m\neq 0} a(mz,n).$$

$$\frac{1}{z^2}E_2\big(-\frac{1}{z}\big) - \frac{S(z)}{2\zeta(2)} = \frac{1}{z^2} + \frac{1}{2\zeta(2)}\sum_{m\neq 0}\sum_{n=-\infty}^{\infty} \frac{1}{z^2(n-\frac{m}{z})^2} - \frac{S(z)}{2\zeta(2)} =$$

$$= \frac{1}{z^2} + \frac{1}{2\zeta(2)}\sum_{m\neq 0}\sum_{n=-\infty}^{\infty} \frac{1}{(nz-m)^2} - \frac{S(z)}{2\zeta(2)} =$$

$$= \frac{1}{z^2} + \frac{1}{2\zeta(2)}\sum_{m\neq 0}\sum_{n\neq 0} \frac{1}{(nz-m)^2} + \frac{1}{\zeta(2)}\sum_{m=1}^{\infty}\frac{1}{m^2} - \frac{S(z)}{2\zeta(2)} =$$

$$= \frac{1}{z^2\zeta(2)} \sum_{n=1}^{\infty} \frac{1}{n^2} + \frac{1}{2\zeta(2)} \sum_{m\neq 0} \sum_{n\neq 0} \frac{1}{(nz-m)^2} + 1 - \frac{S(z)}{2\zeta(2)} =$$

$$= 1 + \frac{1}{2\zeta(2)} \sum_{m=-\infty}^{\infty} \sum_{n\neq 0} \frac{1}{(nz-m)^2} - \frac{S(z)}{2\zeta(2)} =$$

$$= 1 + \frac{1}{2\zeta(2)} \sum_{m=-\infty}^{\infty} \sum_{n\neq 0} \left(\frac{1}{(nz+m)^2} - a(nz,m) \right) = E_2(z).$$

Calculamos $S(z)$,

$$S(z) = \lim_{N\to\infty} \sum_{n=-N+1}^{N} \sum_{m\neq 0} a(mz,n) = \lim_{N\to\infty} \sum_{m\neq 0} \sum_{n=-N+1}^{N} a(mz,n)$$

$$\sum_{m\neq 0} \sum_{n=-N+1}^{N} a(mz,n) = \sum_{m\neq 0} \sum_{n=-N+1}^{N} \left(\frac{1}{mz+n-1} - \frac{1}{mz+n} \right).$$

De nuevo, para m fijo, sea $a_n(mz) = \frac{1}{mz+n}$,

$$\sum_{n=-N+1}^{N} \left(\frac{1}{mz+n-1} - \frac{1}{mz+n} \right) = \sum_{n=-N+1}^{N} \left(a_{(n-1)}(mz) - a_n(mz) \right) = a_{-N}(mz) - a_N(mz)$$

$$\Longrightarrow \sum_{m\neq 0} \sum_{n=-N+1}^{N} a(mz,n) = \sum_{m\neq 0} \left(\frac{1}{mz-N} - \frac{1}{mz+N} \right).$$

Usando el desarrollo de la cotangente $\pi \cot(\pi z) = \sum_{m=-\infty}^{\infty} \frac{1}{z+m}$,

$$\sum_{m\neq 0} \left(\frac{1}{mz-N} - \frac{1}{mz+N} \right) = \frac{1}{z} \sum_{m\neq 0} \left(\frac{1}{m-\frac{N}{z}} - \frac{1}{m+\frac{N}{z}} \right) =$$

$$= \frac{1}{z} \sum_{m=-\infty}^{\infty} \left(\frac{1}{m-\frac{N}{z}} - \frac{1}{m+\frac{N}{z}} \right) + \frac{2}{N} = \frac{2}{z} \sum_{m=-\infty}^{\infty} \frac{1}{m-\frac{N}{z}} + \frac{2}{N} =$$

$$= \frac{2\pi}{z} \cot\left(-\pi N/z\right) + \frac{2}{N}.$$

Se tiene entonces que

$$\begin{aligned} S(z) &= \lim_{N\to\infty} \sum_{n=-N+1}^{N} \sum_{m\neq 0} a(mz,n) = \lim_{N\to\infty} \sum_{m\neq 0} \sum_{n=-N+1}^{N} a(mz,n) = \\ &= \lim_{N\to\infty} \sum_{m\neq 0} \left(\frac{1}{mz-N} - \frac{1}{mz+N} \right) = \lim_{N\to\infty} \left(2\pi z^{-1} \cot(-\pi N/z) + 2/N \right). \end{aligned}$$

Además, como $\Im z > 0$,

$$\lim_{N\to\infty}\left(2\pi z^{-1}\cot(-\pi\frac{N}{z})+\frac{2}{N}\right)=\frac{-2\pi i}{z}.$$

Finalmente, usando que $\zeta(2)=\pi^2/6$, se obtiene la relación

$$z^{-2}E_2(-1/z)=E_2(z)+6/(\pi i z).$$

□

Definición: Una *forma cuspidal (o parabólica) de peso k* es una forma modular de peso k cuya expansión de Fourier tiene primer coeficiente $a_0 = 0$, es decir,

$$f(z)=\sum_{n=1}^{\infty}a_n e(nz).$$

El conjunto de formas cuspidales es denotado por $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, o simplemente por $\mathcal{S}_k$.

Observación: Una forma modular es forma cuspidal cuando $\lim_{y\to\infty} f(x+iy)=0$. Escribiremos entonces $f(i\infty)=0$.

$\mathcal{S}_k$ es un subespacio de $\mathcal{M}_k$ y el anillo graduado

$$\mathcal{S}=\bigoplus_{k\in\mathbb{Z}}\mathcal{S}_k.$$

un ideal en $\mathcal{M}$.

Observación: La holomorfía en el infinito hace que los espacios vectoriales $\mathcal{M}_k$ y $\mathcal{S}_k$ tengan dimensión finita. Además, como γ y $-\gamma$ dan lugar a la misma acción sobre $\mathbb{H}$, estos espacios sólo pueden ser no triviales cuando k es par.

Proposición 2.2.2 *Para $k \geq 0$ par*

$$\dim\mathcal{M}_k=\begin{cases}[k/12] & si\ 12\mid k-2\\ [k/12]+1 & si\ 12\nmid k-2\end{cases}\qquad \dim\mathcal{S}_k=\begin{cases}0 & si\ k<12\\ \dim\mathcal{M}_{k-12} & si\ k\geq 12\end{cases}$$

donde $[\cdot]$ indica la parte entera.

Demostración: (véase [Iw], [Se]). □

El primer ejemplo de forma cuspidal, que aparece para el peso $k = 12$, es la función Δ.

Definición: La *función discriminante* $\Delta : \mathbb{H} \to \mathbb{C}$, está dada por

$$\Delta(z) = g_2(z)^3 - 27g_3(z)^2 = 60^3 G_4(z)^3 - 27 \cdot 140^2 G_6(z)^2.$$

De la modularidad de las funciones $G_4(z)$ y $G_6(z)$, es claro que la función discriminante Δ es modular de peso 12 y holomorfa en $\mathbb{H}$. De hecho, puesto que $G_4(i\infty) = \zeta(4)$ y $G_6(i\infty) = \zeta(6)$, se tiene $\Delta(i\infty) = 0$, es decir, la función es además holomorfa en infinito y por tanto $\Delta(z) \in \mathcal{S}_{12}$.

La serie de Fourier de la serie de Eisenstein es a menudo reescrita utilizando la identidad

$$\sum_{n=1}^{\infty} \sigma_\alpha(n) e(nz) = \sum_{n=1}^{\infty} \frac{n^\alpha e(nz)}{1 - e(nz)}.$$

La función discriminante $\Delta(z)$ también posee una expansión en productos debida a Jacobi, [Si].

Teorema 2.2.3

$$\Delta(z) = (2\pi)^{12} e(z) \prod_{n=1}^{\infty} (1 - e(nz))^{24}. \tag{2.2}$$

En la demostración de la fórmula de Jacobi (2.2), nos valdremos de la función η de Dedekind definida en el semiplano $\mathbb{H}$ por

$$\eta(z) = e^{2\pi i z/24} \prod_{n=1}^{\infty} (1 - e^{2\pi n i z}).$$

Es claro que $\prod_{n=1}^{\infty}(1 - z^n)$ es absolutamente convergente para $|z| < 1$, luego $\eta(z)$ es una función holomorfa en $\mathbb{H}$ que no se anula en ningún punto.

La función η tiene derivada logarítmica

$$D(z) = \frac{\eta'(z)}{\eta(z)} = \frac{2\pi i}{24} + \sum_{n=1}^{\infty} \frac{-2\pi i n\, e(nz)}{1 - e(nz)} = 2\pi i \left(\frac{1}{24} - \sum_{n=1}^{\infty} \frac{n e(nz)}{1 - e(nz)} \right) =$$

$$= 2\pi i \left(\frac{1}{24} - \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} n e(nmz) \right).$$

Efectuando el cambio $nm \to n$, su derivada logarítmica queda

$$D(z) = \frac{\eta'(z)}{\eta(z)} = 2\pi i\left(\frac{1}{24} - \sum_{n=1}^{\infty}\sigma_1(n)e(nz)\right).$$

Por otro lado,

$$E_2(z) = 1 - \frac{4\pi^2}{\zeta(2)}\sum_{n=1}^{\infty}\sigma_1(n)e(nz) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)e(nz).$$

Se tiene entonces que $24D(z) = 2\pi i E_2(z)$.

La función f dada por

$$f(z) = \eta^{24}(z) = e(z)\prod_{n=1}^{\infty}(1-e(nz))^{24},$$

tiene derivada logarítmica

$$\frac{f'(z)}{f(z)} = 24D(z) = 2\pi i E_2(z)dz.$$

Usando la relación $z^{-2}E_2(-1/z) = E_2(z) + 6/(\pi i z)$,

$$\frac{f'(-1/z)}{f(-1/z)} = 2\pi i E_2(-1/z)\frac{dz}{z^2} = 2\pi i\left(z^2E_2(z) + \frac{6z}{\pi i}\right)\frac{dz}{z^2} = 2\pi i E_2(z)dz + 12\frac{dz}{z}.$$

La función $z^{12}f(z)$ tiene la misma derivada logarítmica,

$$\frac{\left(z^{12}f(z)\right)'}{z^{12}f(z)} = 2\pi i E_2(z)dz + 12\frac{dz}{z}.$$

Existirá por tanto una constante C tal que $f(-1/z) = Cz^{12}f(z) \quad \forall\ z \in \mathbb{H}$. Tomando, por ejemplo, $z = i$ se tiene que $z^{12} = 1,\ -1/z = z$ y $f(z) \neq 0$, y por tanto $C = 1$.

Por otro lado,

$$f(z+1) = e(z+1)\prod_{n=1}^{\infty}(1-e(n(z+1)))^{24} = e(z)\prod_{n=1}^{\infty}(1-e(nz))^{24} = f(z),$$

luego f es una forma modular de peso 12. Aún más, pues estudiando su comportamiento en infinito,

$$f(i\infty) = \eta(i\infty)^{24} = 0$$

se tiene que $f \in \mathcal{S}_{12}$.

Demostración: (Teorema 2.2.3)
Puesto que $\dim \mathcal{S}_{12} = 1$, la función Δ genera el espacio. Ahora bien, como $f(z) = \eta(z)^{24} \in \mathcal{S}_{12}$, entonces se debe tener $\Delta(z) = Cf(z)$, para C cierta constante. El coeficiente del primer término en el desarrollo de Fourier de $\Delta(z)$ es $(2\pi)^{12}$, mientras que el correspondiente a la función f es 1, se concluye entonces que $C = (2\pi)^{12}$, es decir,

$$\Delta(z) = (2\pi)^{12}\eta(z)^{24} = (2\pi)^{12}e(z)\prod_{n=1}^{\infty}(1-e(nz))^{24}.$$

□

Corolario 2.2.4 *La función $\Delta(z)$ tiene un desarrollo en serie de Fourier en $\mathbb{H}$ de la forma*

$$\Delta(z) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e(nz), \tag{2.3}$$

donde la función $\tau(n)$ toma valores enteros y $\tau(1) = 1$.

Definición: La función j, llamada *invariante de Klein* o *invariante modular* está dada por

$$j(z) = \frac{1728g_2^3}{g_2^3 - 27g_3^2} = \frac{1728g_2^3}{\Delta(z)}.$$

Teorema 2.2.5 *La función de Klein j tiene desarrollo de Fourier en $\mathbb{H}$ de la forma*

$$j(z) = e(-z) + \sum_{n=0}^{\infty}c(n)e(nz),$$

donde los coeficientes $c(n)$ son enteros.

Demostración: El desarrollo de Fourier de la serie de Eisenstein (2.1) y la expansión en productos (2.2) dan lugar a la expresión

$$j(z) = \frac{\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)e(nz)\right)^3}{e(z)\prod_{n=1}^{\infty}\left(1-e(nz)\right)^{24}}$$

donde $\sigma_3(n) = \sum_{d|n} d^3$.

Basta observar que

$$\frac{1}{1-e(nz)} = \sum_{m=0}^{\infty}e(mnz) \quad \Rightarrow \quad \prod_{n=1}^{\infty}\left(\frac{1}{1-e(nz)}\right)^{24} = \prod_{n=1}^{\infty}\left(\sum_{m=0}^{\infty}e(mnz)\right)^{24}$$

y por tanto

$$j(z) = e(-z)\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)e(nz)\right)^3 \prod_{n=1}^{\infty}\left(\sum_{m=0}^{\infty} e(mnz)\right)^{24}.$$

Ahora es claro que el desarrollo de Fourier es de la forma

$$j(z) = e(-z) + \sum_{n=0}^{\infty} c(n)e(nz)$$

donde todos sus coeficientes son enteros. □

2.3. Operadores de Hecke

Para profundizar en la estructura de los espacios de formas modulares es importante considerar endomorfismos especiales de $\mathcal{S}_k$, los *operadores de Hecke*.

Para definirlos se considera un conjunto Δ_n de representantes de los cogrupos a la derecha $\mathrm{SL}_2(\mathbb{Z})\backslash M_n$ con M_n las matrices de determinante n, o dicho de otra manera, se escoge Δ_n de manera que

$$M_n = \bigcup_{\alpha\in\Delta_n} \mathrm{SL}_2(\mathbb{Z})\alpha$$

sea una partición.

Proposición 2.3.1 *Sea M_n las matrices enteras de determinante n y Δ_n el subconjunto de M_n dado por las matrices triangulares $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ con $ad = n$, $0 \le b < d$, $a > 0$.*

1. *Para cada $\lambda \in M_n$ existe $\gamma \in SL_2(\mathbb{Z})$ tal que $\gamma\lambda \in \Delta_n$.*
2. *Para cada $\lambda \in M_n$ existe un único $\delta \in \Delta_n$ tal que $\lambda = \gamma\delta$ para algún $\gamma \in SL_2(\mathbb{Z})$.*
3. *Para cualquier $\gamma \in SL_2(\mathbb{Z})$ existen $\gamma_1, \gamma_2, \ldots, \gamma_s \in SL_2(\mathbb{Z})$, con s el cardinal de Δ_n, tales que $\{\delta_1\gamma, \delta_2\gamma, \ldots, \delta_s\gamma\} = \{\gamma_1\delta_1, \gamma_2\delta_2, \ldots, \gamma_s\delta_s\}$ donde δ_i son los elementos de Δ_n.*

Demostración:

1.
$$\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_n \qquad \gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

$$\gamma\lambda = \begin{pmatrix} aA + cB & bA + dB \\ aC + cD & bC + dD \end{pmatrix} \in \Delta_n \Longleftrightarrow \begin{cases} aC + cD = 0 \\ (aA + cB)(bC + dD) = n \\ 0 \leqslant bA + dB < bC + dD \end{cases}$$

Sea $m = (a, c)$, por el *teorema de Bezout* existen $k, l \in \mathbb{Z}$ tales que $m = ka + lc$

$$\Rightarrow 1 = k\,\frac{a}{m} + l\,\frac{c}{m}.$$

Tomando $A = k,\ B = l,\ C = -c/m,\ D = a/m$, se obtiene una matriz del tipo $\gamma\lambda = \left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)$ la cual, si fuera necesario, se multiplicaría por $-I$ para que los signos de x y z sean positivos.

Por otro lado, multiplicando γ por una traslación, es decir

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} x & y + zt \\ 0 & z \end{pmatrix}$$

siempre podemos elegir t de manera que $y + zt$ esté en $[0, z)$.

2. La existencia de tal matriz δ viene de *1.* ya que $\gamma\lambda \Rightarrow \lambda = \gamma^{-1}\delta$, por tanto sólo queda ver la unicidad, es decir, que si $\gamma_1\delta_1 = \gamma_2\delta_2$ entonces $\delta_1 = \delta_2$.

$$\delta_1 = \gamma_1^{-1}\gamma_2\delta_2$$

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix}$$

donde la primera y la última matriz están en Δ_n y la otra en $\mathrm{SL}_2(\mathbb{Z})$.

$$\begin{cases} x = AX \\ y = AY + BZ \\ 0 = CX \\ z = CY + DZ \end{cases}$$

$$X > 0 \Rightarrow C = 0 \ \Rightarrow \ \begin{cases} x = AX \\ y = AY + BZ \\ z = DZ \end{cases}$$

$$\left.\begin{array}{r} xz = n = XZ \\ xz = ADXZ \end{array}\right\} \Rightarrow \ AD = 1$$
$$\left.\begin{array}{r} x, X > 0 \\ x = AX \end{array}\right\} \Rightarrow \ A > 0$$
$$\Rightarrow A = D = 1 \ \Rightarrow \ \begin{cases} x = X \\ y = Y + BZ \\ z = Z \end{cases}$$

$$0 \le y < z \Rightarrow \ \left.\begin{array}{c} 0 \le Y + Bz < z \\ 0 \le Y < z \end{array}\right\} \Rightarrow B = 0 \ \Rightarrow \ \begin{cases} x = X \\ y = Y \\ z = Z \end{cases}$$

Por tanto, la única solución es $\delta_1 = \delta_2$.

3. Dado $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, cada $\delta_i\gamma$ con $i = 1, \ldots, s$ es un cierto $\lambda \in M_n$. Usando *2.*, existe un único $\delta \in \Delta_n$ tal que $\lambda = \widetilde{\gamma}\delta$ para algún $\widetilde{\gamma} \in \mathrm{SL}_2(\mathbb{Z})$, como Δ_n tiene cardinal finito, $\lambda = \widetilde{\gamma}\delta_i$ con $i = 1, \ldots, s$.
Para cada i, el $\widetilde{\gamma}$ correspondiente es el γ_i buscado.

□

Proposición 2.3.2 *Para $n \in \mathbb{N}$ el operador de Hecke definido como*

$$T_n f(z) = n^{k-1} \sum_{\delta \in \Delta_n} j_\delta^{-k}(z) f(\delta z),$$

aplica $\mathcal{M}_k$ en $\mathcal{M}_k$.

Demostración: Tomando f forma modular de peso k y usando la relación $j_\alpha(\beta z) j_\beta(z) = j_{\alpha\beta}(z)$,

$$T_n f(\gamma z) = n^{k-1} \sum_{\delta \in \Delta_n} j_\delta^{-k}(\gamma z) f(\delta\gamma z) = n^{k-1} \sum_{\delta \in \Delta_n} j_{\delta\gamma}^{-k}(z) j_\gamma^k(z) f(\delta\gamma z)$$

La modularidad de la función f no puede ser aplicada en este caso, pues $\delta\gamma \notin \mathrm{SL}_2(\mathbb{Z})$, usando el apartado *3.* de la Proposición 2.3.1, el problema queda resuelto.

$$T_n f(\gamma z) = n^{k-1} \sum_{i=1}^{s} j_{\gamma_i\delta_i}^{-k}(z) j_\gamma^k(z) f(\gamma_i\delta_i z) = j_\gamma^k(z) n^{k-1} \sum_{i=1}^{s} j_{\gamma_i\delta_i}^{-k}(z) j_{\gamma_i}^k(\delta_i z) f(\delta_i z) =$$

$$= j_\gamma^k(z) n^{k-1} \sum_{i=1}^{s} j_{\delta_i}^{-k}(z) f(\delta_i z) = j_\gamma^k(z) T_n f(z).$$

Por tanto T_n manda $\mathcal{M}_k$ en $\mathcal{M}_k$. □

Observación: La definición anterior se puede escribir como

$$T_n f(z) = n^{k-1} \sum_{ad=n} \sum_{b=0}^{d-1} d^{-k} f\Big(\frac{az+b}{d}\Big),$$

usando que $\Delta_n = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \ : \ ad = n,\ 0 \le b < d \right\}$ es un conjunto válido de representantes.

Corolario 2.3.3 *Si f es función modular y $P(X_1, \ldots, X_s)$ polinomio simétrico en las s variables, entonces*

$$G(z) = P(f(\delta_1 z), \ldots, f(\delta_s z)), \quad \delta_i \in \Delta_n$$

es modular, es decir, $\forall\ \gamma \in SL_2(\mathbb{Z})$

$$G(\gamma z) = P(f(\delta_1\gamma z), \ldots, f(\delta_s\gamma z)) = P(f(\delta_1 z), \ldots, f(\delta_s z)) = G(z).$$

Proposición 2.3.4 *Sea* $f(z)=\sum_{m=0}^{\infty} c_m(z)e(mz)\in\mathcal{M}_k$, *entonces*

$$T_nf(z)=\sum_{m=0}^{\infty} b_m e(mz), \qquad \textit{donde}\ \ b_m=\sum_{a|(n,m)} a^{k-1}c_{nm/a^2}.$$

En particular, aplica $\mathcal{S}_k$ *en* $\mathcal{S}_k$.

Demostración:

$$\begin{aligned} T_nf(z) &= n^{k-1}\sum_{\substack{ad=n\\ d>0}}\sum_{b=0}^{d-1} d^{-k}\sum_{m=0}^{\infty} c_m\, e\big(m\frac{az+b}{d}\big)= \\ &= n^{k-1}\sum_{m=0}^{\infty}\sum_{\substack{ad=n\\ d>0}} d^{-k}c_m\, e\big(\frac{am}{d}z\big)\sum_{b=0}^{d-1} e\big(\frac{mb}{d}\big). \end{aligned}$$

Observación: $\sum_{b=0}^{d-1} e\big(\frac{mb}{d}\big)=\begin{cases}0 & \text{si}\ \ d\nmid m\\ d & \text{si}\ \ d\mid m\end{cases}$

Efectuando el cambio $m\to ld$ obtenemos

$$\begin{aligned} T_nf(z) &= n^{k-1}\sum_{l=0}^{\infty}\sum_{\substack{ad=n\\ d>0}} d^{-k+1}c_{ld}\,e(alz)=\sum_{l=0}^{\infty}\sum_{\substack{ad=n\\ d>0}}\Big(\frac{n}{d}\Big)^{k-1}c_{ld}\,e(alz)= \\ &= \sum_{l=0}^{\infty}\sum_{\substack{a|n\\ a>0}} a^{k-1}c_{ln/a}\,e(alz). \end{aligned}$$

El coeficiente de $e(mz)$ viene dado por 3-uplas (l,a,d) con $al=m$ y $a\mid n$. El factor $c_{ln/a}$ es c_{mn/a^2} con $a\mid m$ y $a\mid n$, por lo tanto

$$b_m=\sum_{a|(n,m)} a^{k-1}c_{mn/a^2}.$$

Por otro lado, si $c_0=0$ entonces $b_0=0$ y por tanto T_n manda $\mathcal{S}_k$ en $\mathcal{S}_k$. □

Corolario 2.3.5 *Sea* $f(z)=\sum_{m=0}^{\infty} c_m(z)e(mz)\in\mathcal{M}_k$. *Si* $n=p$ *es primo, el coeficiente de Fourier* m*-ésimo de* $T_nf(z)$ *con* $p\nmid m$ *es* c_{mp}.

Proposición 2.3.6 *Los operadores de Hecke verifican*

$$T_mT_n=\sum_{a|(n,m)} a^{k-1}T_{mn/a^2}.$$

En particular los operadores de Hecke conmutan y si $(n,m)=1$ *se tiene* $T_mT_n=T_{mn}$.

Demostración: Suponiendo el resultado cierto, es claro que los operadores de Hecke conmutan pues $(n,m)=(m,n)$ y el producto de números enteros es conmutativo.

$$T_m f(z) = m^{k-1} \sum_{\substack{ad=m\\ d>0}} \sum_{b=0}^{d-1} d^{-k} f\big(\frac{az+b}{d}\big).$$

$$T_n f(z) = \sum_{s=0}^{\infty} b_s e(sz) = \sum_{s=0}^{\infty} \sum_{\substack{\tilde{a}|(n,s)\\ \tilde{a}>0}} \tilde{a}^{k-1} c_{sn/\tilde{a}^2} e(sz).$$

$$T_m T_n f(z) = m^{k-1} \sum_{\substack{ad=m\\ d>0}} \sum_{b=0}^{d-1} d^{-k} \sum_{s=0}^{\infty} \sum_{\substack{\tilde{a}|(n,s)\\ \tilde{a}>0}} \tilde{a}^{k-1} c_{sn/\tilde{a}^2}\ e\big(s\frac{az+b}{d}\big).$$

De nuevo, la suma $\sum_{b=0}^{d-1} e\big(\frac{mb}{d}\big)$ nos hace considerar únicamente el caso $d \mid m$. Efectuando el cambio $s \to ld$ obtenemos

$$\begin{aligned} T_m T_n f(z) &= m^{k-1} \sum_{l=0}^{\infty} \sum_{\substack{ad=m\\ d>0}} d^{-k+1} \sum_{\substack{\tilde{a}|(n,ld)\\ \tilde{a}>0}} \tilde{a}^{k-1} c_{ldn/\tilde{a}^2} e(laz) = \\ &= \sum_{l=0}^{\infty} \sum_{\substack{ad=m\\ d>0}} \big(\frac{m}{d}\big)^{k-1} \sum_{\substack{\tilde{a}|(n,ld)\\ \tilde{a}>0}} \tilde{a}^{k-1} c_{ldn/\tilde{a}^2} e(laz) = \\ &= \sum_{l=0}^{\infty} \sum_{\substack{a|m\\ a>0}} a^{k-1} \sum_{\tilde{a}|(n,\frac{lm}{a})} \tilde{a}^{k-1} c_{lmn/a\tilde{a}^2} e(laz) \end{aligned}$$

donde se ha usado que $m=ad$. Por último, efectuando el cambio $la \to s$,

$$\begin{aligned} T_m T_n f(z) &= \sum_{\substack{a|(m,n)\\ a>0}} a^{k-1} \sum_{s=0}^{\infty} \sum_{\tilde{a}|(\frac{nm}{a^2},s)} \tilde{a}^{k-1} c_{smn/a^2\tilde{a}^2} e(sz) = \\ &= \sum_{\substack{a|(n,m)\\ a>0}} a^{k-1} T_{mn/a^2}. \end{aligned}$$

□

Los operadores de Hecke son autoadjuntos con respecto al producto escalar de formas modulares dado por

$$\langle f, g\rangle = \int_D f(z)\overline{g(z)} y^{k-2}\, dxdy,$$

y por tanto se pueden diagonalizar. Por simple álgebra lineal si tenemos endomorfismos (aplicaciones lineales del espacio en sí mismo) diagonalizables y que conmutan, debe existir una base en la que todos ellos diagonalicen simultáneamente.

Proposición 2.3.7

1. *Dado un conjunto de matrices reales simétricas $n \times n$ que conmutan entre sí, existe una base en la que todas se diagonalizan simultáneamente.*

2. *Dado un espacio vectorial euclídeo sobre $\mathbb{R}$ de dimensión finita y un conjunto de endomorfismos autoadjuntos que conmutan entre sí, entonces existe una base cuyos elementos son autovectores de todos los endomorfismos.*

Demostración:

1. Las matrices reales simétricas son matrices que tienen todos los autovalores reales, y que se pueden diagonalizar ortogonalmente.
   Sean A y B dos matrices del conjunto, $AB = BA$. Es claro que si dos matrices conmutan en una base también conmutan en otra, pues $AB = BA \Leftrightarrow C^{-1}AC \cdot C^{-1}BC = C^{-1}BC \cdot C^{-1}AC$.
   Sean $\lambda_1, \lambda_2, \ldots, \lambda_n$ autovalores de A y sea Q la matriz formada por los autovectores asociados, se denota por A y B a las matrices en esta nueva base de modo que A es diagonal.
   Si $B = (b_{ij})$,
   $$AB = BA \Rightarrow \lambda_i b_{ij} = b_{ij}\lambda_j \Rightarrow (\lambda_i - \lambda_j)b_{ij} = 0,$$
   se tiene entonces que $b_{ij} = 0$ siempre que $\lambda_i \neq \lambda_j$.
   Si A tiene k autovalores distintos, las matrices serán de la forma
   $$A = \begin{pmatrix} \lambda_1 I & & & \\ & \lambda_2 I & & \\ & & \ddots & \\ & & & \lambda_k I \end{pmatrix}, \quad B = \begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_k \end{pmatrix}$$
   donde cada B_i es una matriz cuadrada de tamaño la multiplicidad del autovalor de A correspondiente.
   Como B es diagonalizable cada uno de los B_i será diagonalizable, sea P_i matriz invertible tal que $P_i^{-1}B_iP_i$ es diagonal.
   Se tiene entonces que $P^{-1}AP = P^{-1}\lambda IP = \lambda I$ y $P^{-1}BP$ son las dos diagonales donde P es
   $$P = \begin{pmatrix} P_1 & & & \\ & P_2 & & \\ & & \ddots & \\ & & & P_k \end{pmatrix}$$

2. Sea f un endomorfismo del espacio vectorial, como f es autoadjunto, es decir $f = f^*$, existe una base ortonormal B en la que la matriz de f es simétrica y por

lo tanto diagonalizable.
Que los endomorfismos del conjunto conmuten es equivalente a pedir que sus matrices asociadas conmuten.
Estamos en las condiciones del apartado anterior y por tanto, existe una base en la que todas las matrices se diagonalizan simultáneamente, es decir, existe una base cuyos elementos son autovectores de todos los endomorfismos.

□

Definición: Se dice que $\mathcal{B} = \{f_1, f_2, \ldots, f_r\}$ es una *base de Hecke* de $\mathcal{M}_k$ o de $\mathcal{S}_k$ si cada $f \in \mathcal{B}$ cumple $T_n f(z) = \lambda_n f(z)$ para todo $n \in \mathbb{N}$ y ciertos λ_n (dependiendo de f).

Proposición 2.3.8 *Sea $f(z) = \sum_{m=0}^{\infty} c_m e(mz)$ un elemento de una base de Hecke con $c_1 = 1$, entonces*

1. *$c_n = \lambda_n$, el autovalor de f en T_n.*
2. *$c_n c_m = \sum_{a|(n,m)} a^{k-1} c_{nm/a^2}$.*

Recordamos el desarrollo de Fourier de la función discriminante $\Delta(z)$ dado por

$$\Delta(z) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) e(nz)$$

La función $\tau(n)$ se conoce como *función tau de Ramanujan*. Esta función posee muchas propiedades aritméticas, muchas de las cuales fueron conjeturadas por Ramanujan.

Corolario 2.3.9 *La función τ es una función multiplicativa que satisface $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ para p primo.*

Demostración: Como $\dim \mathcal{S}_{12} = 1$, $\mathcal{B} = \{\Delta(z)\}$ es una base de Hecke. Puesto que $\tau(1) = 1$ se puede aplicar la proposición. Finalmente, aplicando *2.* se obtiene el resultado. □

2.4. Formas modulares respecto a Γ

Las necesidades aritméticas llevan a generalizar la definición de forma modular en dos sentidos. En primer lugar admitiendo una posible raíz de la unidad que multiplica a la relación modular básica, y por otro lado, considerando subgrupos Γ de $\mathrm{SL}_2(\mathbb{Z})$.

El subgrupo más importante de $\mathrm{SL}_2(\mathbb{Z})$ es

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \ (\mathrm{mod}\ N) \right\}, \qquad \text{con } N \in \mathbb{Z}^+.$$

En general, en las aplicaciones en teoría de números casi siempre aparecen *grupos de congruencias* que se definen como subgrupos de $\mathrm{SL}_2(\mathbb{Z})$ que contienen a

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

A $\Gamma(N)$ se le llama *subgrupo de congruencias principal de nivel* N.

Evidentemente $\Gamma(1) = \Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$.

Proposición 2.4.1 *$\Gamma_0(N)$ y $\Gamma(N)$ son subgrupos de $SL_2(\mathbb{Z})$, en particular $\Gamma(N)$ es subgrupo normal.*

Demostración:

$$\Gamma_0(N)$$

- $\Gamma_0(N)$ es no vacío.
- $\forall\ \gamma, \gamma' \in \Gamma_0(N), \quad \gamma\gamma' \in \Gamma_0(N)$.

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma(N) \quad \Rightarrow c, c' \equiv 0 \pmod{N}$$

$$\Rightarrow \gamma\gamma' = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \quad \Rightarrow \gamma\gamma' \in \Gamma_0(N).$$

- $\gamma^{-1} \in \Gamma_0(N)$ para cada $\gamma \in \Gamma_0(N)$.

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \quad \Rightarrow c \equiv 0 \pmod{N}$$

$$\Rightarrow \gamma^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \quad \Rightarrow \gamma^{-1} \in \Gamma_0(N).$$

$$\Gamma(N)$$

Para ver que es subgrupo normal de $\mathrm{SL}_2(\mathbb{Z})$, consideramos el homomorfismo de grupos

$$f : \ \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

que consiste en la reducción módulo N, entonces $\Gamma(N)$ es el núcleo de f y por tanto, subgrupo normal [Mi]. □

En general $\Gamma_0(N)$ no tiene generadores tan sencillos como los de $\mathrm{SL}_2(\mathbb{Z})$. El caso $N = 4$ es excepcional.

Proposición 2.4.2 *$\Gamma_0(4)$ está generado por $-I$, T y $\widetilde{S}$ donde*

$$-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad y \qquad \widetilde{S} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

Demostración: Es claro que $\langle -I, T, \widetilde{S}\rangle \subseteq \Gamma_0(4)$, para ver la inclusión contraria, basta demostrar que dada cualquier matriz de $\Gamma_0(4)$ se puede escribir como composición de elementos de $\langle -I, T, \widetilde{S}\rangle$.

Consideremos una matriz genérica $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(4)$.

a) Si $a^2 + b^2 = 1$ entonces $\gamma = \pm\widetilde{S}^k$ para algún $k \in \mathbb{Z}$.

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \Rightarrow c \equiv 0 \pmod 4 \Longrightarrow ad \equiv 1 \pmod 4.$$

$$a^2 + b^2 = 1 \Rightarrow \begin{cases} a = 0 \wedge b = \pm 1 & \Rightarrow ad \equiv 0 \pmod 4 \quad \rightarrow\leftarrow \\ a = \pm 1 \wedge b = 0 & \Rightarrow d = \pm 1 \end{cases}$$

$$\gamma = \pm \begin{pmatrix} 1 & 0 \\ 4k & 1 \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}^k = \pm\widetilde{S}^k.$$

b) Si $a^2 + b^2 > 1$ con $|a| < 2|b|$, al reemplazar γ o bien por γT o bien por γT^{-1} (por uno solo de los dos), $a^2 + b^2$ decrece.

$$\gamma T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b+a \\ c & d+c \end{pmatrix}.$$

$$\gamma T^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b-a \\ c & d-c \end{pmatrix}.$$

$a^2 + b^2 > 1$
$2|b| > |a| \Rightarrow |b| > |a||b| \Rightarrow b^2 > (|a||b|)^2$

$$a^2 + b^2 \overset{?}{>} \begin{cases} a^2 + (a+b)^2 \\ a^2 + (b-a)^2 \end{cases}$$

$$\text{si } a > 0, b < 0 \Rightarrow \quad b^2 > (|a| - |b|)^2 = (a+b)^2 \Rightarrow \quad \text{tomo } \gamma T.$$

$$\text{si } a > 0, b > 0 \Rightarrow b^2 > (|a| - |b|)^2 = (a-b)^2 = (b-a)^2 \Rightarrow \text{tomo } \gamma T^{-1}.$$

c) Si $a^2 + b^2 > 1$ con $|a| > 2|b|$, al reemplazar γ o bien por $\gamma\widetilde{S}$ o bien por $\gamma\widetilde{S}^{-1}$, $a^2 + b^2$ decrece.

$$\gamma\widetilde{S} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} a+4b & b \\ c+4d & d \end{pmatrix}.$$

$$\gamma\widetilde{S}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} = \begin{pmatrix} a-4b & b \\ c-4d & d \end{pmatrix}.$$

$a^2+b^2 > 1$
$2|b| < |a|$

$$a^2+b^2 \overset{?}{>} \begin{cases} (a+4b)^2+b^2 \\ (a-4b)^2+b^2 \end{cases}$$

$$\text{si } a>0, b<0 \;\Rightarrow |b| < \frac{a}{2} \Rightarrow (a+4b)^2 = (a-4|b|)^2 < (a-2a)^2 = a^2 \Rightarrow \text{tomo } \gamma\widetilde{S}.$$

$$\text{si } a>0, b>0 \Rightarrow \quad b < \frac{a}{2} \Rightarrow (a-4b)^2 < (a-2b)^2 = a^2 \Rightarrow \quad \text{tomo } \gamma\widetilde{S}^{-1}.$$

Por a), una matriz que cumple $a^2+b^2=1$, es una potencia de $\widetilde{S}$ salvo signo (lo que se corresponde con la multiplicación por $-I$), y por tanto, un elemento de $\langle -I, T, \widetilde{S}\rangle$. Usando b) y c), se puede llegar a la relación anterior multiplicando por los elementos T y $\widetilde{S}$ o por sus respectivas inversas.

Así, dada cualquier matriz $\gamma \in \Gamma_0(4)$, mediante las operaciones anteriores se llega a una matriz $\gamma\alpha = \widetilde{S}^k$, con $\alpha \in \langle -I, T, \widetilde{S}\rangle$. Basta entonces observar que $\gamma\alpha\alpha^{-1} = \gamma$, que vuelve a estar en $\langle -I, T, \widetilde{S}\rangle$. □

Si D es un dominio fundamental para $\mathrm{SL}_2(\mathbb{Z})$, entonces podemos considerar $i\infty$ como un punto límite de $\mathbb{H}$ que también es un punto límite de D. Cada conjunto $\sigma^{-1}D$, con $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, es también un dominio fundamental de $\mathrm{SL}_2(\mathbb{Z})$. Si $\sigma^{-1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, entonces $\sigma^{-1}(i\infty) = \frac{a}{c}$ es un punto límite de $\mathbb{H}$ y un punto límite de $\sigma^{-1}D$, decimos entonces que $\mathfrak{a} = \frac{a}{c}$ es una *cúspide* de σ^{-1}.

Para eliminar la dependencia de σ en la definición de cúspide, se acostumbra a definir las cúspides tomando $\mathbb{Q}\cup\{\infty\}$, identificando puntos equivalentes bajo la acción del grupo en cuestión.

Cuando $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ todos los números racionales son Γ-equivalentes a $i\infty$ y por tanto $\mathrm{SL}_2(\mathbb{Z})$ tiene una única cúspide, representada por $i\infty$ o simplemente ∞, pero cuando Γ es un subgrupo propio de $\mathrm{SL}_2(\mathbb{Z})$ el número de puntos Γ-equivalentes es menor, así Γ puede tener más cúspides, representadas por números racionales. Dado que cada $\mathfrak{a} \in \mathbb{Q}$ es de la forma $\mathfrak{a} = \sigma^{-1}(i\infty)$ para algún $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, el número de cúspides es a lo sumo el número de clases $\Gamma\sigma$ en $\mathrm{SL}_2(\mathbb{Z})$, un número finito ya que el índice $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ es finito, [Di-Sh].

Definición: Una función f definida en $\mathbb{H}$ se dice *forma modular de peso k respecto a* Γ si

1. f es holomorfa en $\mathbb{H}$.

2. f es función modular de peso k respecto a Γ, es decir

$$f(z) = j_\gamma^{-k}(z) f(\gamma z) \quad \forall\ \gamma \in \Gamma.$$

3. f es holomorfa en todas sus cúspides.

Si $\mathfrak{a}$ es una cúspide y f es una función modular para Γ, siempre se puede encontrar un $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\sigma\mathfrak{a} = i\infty$ y que $f(\sigma z)$ sea 1-periódica. Se dice que f es holomorfa en $\mathfrak{a}$ si $f(\sigma z)$ tiene un desarrollo del tipo $\sum_{n=0}^{\infty} a_n e(nz)$.

Definición: Una *forma cuspidal de peso k respecto a Γ*, es una forma modular respecto a Γ tal que en los desarrollos de Fourier de todas las cúspides se tiene $a_0 = 0$.

Se define $\mathcal{M}_k(\Gamma)$ como el espacio vectorial de formas modulares de peso k con respecto a un subgrupo de congruencias Γ. De forma análoga, el espacio de formas cuspidales respecto a Γ es denotado por $\mathcal{S}_k(\Gamma)$. Las fórmulas de las dimensiones correspondientes a estos espacios pueden verse en [Di-Sh].

Si $f \in \mathcal{M}_k = \mathcal{M}_k\big(\Gamma_0(1)\big)$, en general $f(Nz)$ no es una forma modular de $\mathcal{M}_k$. La importancia del caso $\Gamma = \Gamma_0(N)$ radica en parte en la siguiente propiedad,

Proposición 2.4.3 *Si $f \in \mathcal{M}_k = \mathcal{M}_k(\Gamma_0(1))$, entonces $f(Nz) \in \mathcal{M}_k(\Gamma_0(N))$.*

Demostración:
Sea $g(z) = f(Nz)$. Si $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, entonces $c = \tilde{c}N$, por lo tanto, si g es modular,

$$f(Nz) = g(z) = \frac{1}{(cz+d)^k}\, g\left(\frac{az+b}{cz+d}\right) = \frac{1}{(cz+d)^k}\, f\left(N\frac{az+b}{cz+d}\right) =$$

$$= \frac{1}{(\tilde{c}Nz+d)^k}\, f\left(\frac{aNz+\tilde{b}}{\tilde{c}Nz+d}\right)$$

que coincide con la definición de modularidad en f,

$$f(Nz) = \frac{1}{(cNz+d)^k}\, f\left(\frac{aNz+b}{cNz+d}\right).$$

□

Observación: La proposición anterior da una relación de inclusión entre $\mathcal{M}_k$, $\mathcal{M}_k\big(\Gamma_0(N)\big)$ y $\mathcal{M}_k\big(\Gamma_0(NM)\big)$, a saber,

$$\mathcal{M}_k \subset \mathcal{M}_k(\Gamma_0(N)) \subset \mathcal{M}_k(\Gamma_0(NM)).$$

Para ello, basta observar que

$$\Gamma_0(NM) \subset \Gamma_0(N) \subset \Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$$

y que por tanto, las restricciones para las funciones son más fuertes en $\mathcal{M}_k$ que en $\mathcal{M}_k(\Gamma_0(N)$, y claro está, que en $\mathcal{M}_k(\Gamma_0(NM))$.

Proposición 2.4.4 *$E_2(z)-2E_2(2z)$ y $E_2(2z)-2E_2(4z)$ forman una base de $\mathcal{M}_2\big(\Gamma_0(4)\big)$.*

Demostración: Usando que $\dim \mathcal{M}_2\big(\Gamma_0(4)\big) = 2$, [Di-Sh], hay que comprobar que $E_2(z) - 2E_2(2z)$ y $E_2(2z) - 2E_2(4z)$ están en $\mathcal{M}_2\big(\Gamma_0(4)\big)$ y son linealmente independientes.

$$E_2(z) = \frac{1}{z^2}E_2(-1/z) - \frac{6}{\pi i z},$$
$$2E_2(2z) = \frac{1}{2z^2}E_2(-1/2z) - \frac{6}{\pi i z},$$
$$\to f(z) = E_2(z) - 2E_2(2z) = \frac{1}{z^2}E_2(-1/z) - \frac{1}{2z^2}E_2(-1/2z).$$

$$E_2(2z) = \frac{1}{4z^2}E_2(-1/2z) - \frac{3}{\pi i z},$$
$$2E_2(4z) = \frac{1}{8z^2}E_2(-1/4z) - \frac{3}{\pi i z},$$
$$\to g(z) = E_2(2z) - 2E_2(4z) = \frac{1}{4z^2}E_2(-1/2z) - \frac{1}{8z^2}E_2(-1/4z).$$

Para ver que $f, g \in \mathcal{M}_2(\Gamma_0(4))$ basta comprobar que son modulares para los generadores,

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad Tz = z + 1$$
$$\widetilde{S} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \quad \widetilde{S}z = \frac{z}{4z+1}$$

- $f(Tz) = f(z)$,
$$E_2(z) = E_2(z+1) \Rightarrow f(z) = f(z+1).$$
- $f(\widetilde{S}z) = (4z+1)^2 f(z)$,

$$\begin{aligned} E_2(z) &\longleftrightarrow E_2(-1/z) \\ E_2\left(\frac{z}{4z+1}\right) &\longleftrightarrow E_2\left(\frac{-1}{\frac{z}{4z+1}}\right) = E_2\left(\frac{-4z-1}{z}\right) = E_2\left(-4-\frac{1}{z}\right) = E_2(-1/z) \\ E_2\left(2\frac{z}{4z+1}\right) &\longleftrightarrow E_2\left(\frac{-1}{\frac{2z}{4z+1}}\right) = E_2\left(\frac{-4z-1}{2z}\right) = E_2\left(-2-\frac{1}{2z}\right) = E_2(-1/2z) \end{aligned}$$

$$f\left(\frac{z}{4z+1}\right) = E_2\left(\frac{z}{4z+1}\right) - 2E_2\left(2\frac{z}{4z+1}\right) =$$

$$= \left(\frac{4z+1}{z}\right)^2 E_2(-1/z) - \frac{1}{2}\left(\frac{4z+1}{z}\right)^2 E_2(-1/2z) =$$

$$= (4z+1)^2\left[\frac{1}{z^2}E_2(-1/z) - \frac{1}{2z^2}E_2(-1/2z)\right] = (4z+1)^2 f(z).$$

- $g(Tz) = g(z)$,

$$E_2(z) = E_2(z+1) \Rightarrow f(z) = f(z+1).$$

- $g(\widetilde{S}z) = (4z+1)^2 g(z)$,

$$\begin{array}{rcl} E_2(z) & \longleftrightarrow & E_2(-1/z) \\ E_2\left(2\frac{z}{4z+1}\right) & \longleftrightarrow & E_2\left(\frac{-1}{\frac{2z}{4z+1}}\right) = E_2\left(\frac{-4z-1}{2z}\right) = E_2\left(-2-\frac{1}{2z}\right) = E_2(-1/2z) \\ E_2\left(4\frac{z}{4z+1}\right) & \longleftrightarrow & E_2\left(\frac{-1}{\frac{4z}{4z+1}}\right) = E_2\left(\frac{-4z-1}{4z}\right) = E_2\left(-1-\frac{1}{4z}\right) = E_2(-1/4z) \end{array}$$

$$g\left(\frac{z}{4z+1}\right) = E_2\left(\frac{2z}{4z+1}\right) - 2E_2\left(\frac{4z}{4z+1}\right) =$$

$$= \left(\frac{4z+1}{4z}\right)^2 E_2(-1/2z) - \frac{1}{8}\left(\frac{4z+1}{z}\right)^2 E_2(-1/4z) =$$

$$= (4z+1)^2\left[\frac{1}{4z^2}E_2(-1/2z) - \frac{1}{8z^2}E_2(-1/4z)\right] = (4z+1)^2 g(z).$$

Por otro lado,

$$f(z) = E_2(z) - 2E_2(2z) = 1 - 24\sum_{m=1}^{\infty}\sigma(m)e(mz) - 2 + 48\sum_{m=1}^{\infty}\sigma(m)e(2mz) =$$

$$= -1 - 24\left[\sum_{m=1}^{\infty}\sigma(m)e(mz) - 2\sum_{m=1}^{\infty}\sigma(m)e(2mz)\right] =$$

$$= -1 - 24\left[\sum_{m=1}^{\infty}\sigma(m)e(mz) - 2\sum_{m=1}^{\infty}\sigma\left(\frac{m}{2}\right)e(mz)\right] =$$

$$= -1 - 24 \sum_{m=1}^{\infty} \left(\sigma(m) - 2\sigma\left(\frac{m}{2}\right) \right) e(mz),$$

donde $\sigma(n) = 0$ si $n \notin \mathbb{Z}$.

$$\Rightarrow f(z) = -1 - 24 \left(e(z) + (1 + 2 - 2)e(2z) + (1 + 3)e(3z) + \cdots \right) =$$

$$= -1 - 24 \left(e(z) + e(2z) + 4e(3z) + \cdots \right)$$

$$g(z) = E_2(2z) - 2E_2(4z) = 1 - 24 \sum_{m=1}^{\infty} \sigma(m)e(2mz) - 2 + 48 \sum_{m=1}^{\infty} \sigma(m)e(4mz) =$$

$$= -1 - 24 \left[\sum_{m=1}^{\infty} \sigma(m)e(2mz) - 2 \sum_{m=1}^{\infty} \sigma(m)e(4mz) \right] =$$

$$= -1 - 24 \left[\sum_{m=1}^{\infty} \sigma\left(\frac{m}{2}\right) e(mz) - 2 \sum_{m=1}^{\infty} \sigma\left(\frac{m}{4}\right) e(mz) \right] =$$

$$= -1 - 24 \sum_{m=1}^{\infty} \left(\sigma\left(\frac{m}{2}\right) - 2\sigma\left(\frac{m}{4}\right) \right) e(mz)$$

donde $\sigma(n) = 0$ si $n \notin \mathbb{Z}$.

$$\Rightarrow g(z) = -1 - 24 \left((1 + 2)e(2z) + (1 + 2 + 4 - 2)e(4z) + (1 + 3)e(6z) + \cdots \right) =$$

$$= -1 - 24 \left(3e(2z) + 5e(4z) + 4e(6z) + \cdots \right)$$

f y g son linealmente independientes, pues no son múltiplo una de la otra. □

2.5. Formas cuadráticas binarias

Las *formas cuadráticas binarias* de discriminante d son los elementos de

$$\mathcal{Q}_d = \{ax^2 + bxy + cy^2 \ : \ a \in \mathbb{Z}^+, \ b, c, \in \mathbb{Z}, \quad b^2 - 4ac = d\}.$$

Diremos que una forma $Q \in \mathcal{Q}_d$ representa un entero n si existen enteros $(x, y) \neq (0, 0)$ tales que $ax^2 + bxy + cy^2 = n$.

Gauss creó una teoría aritmética de formas cuadráticas en su obra maestra *Disquisitiones Arithmeticae*. Aquí sólo consideraremos el caso $d < 0$, definido positivo.

Definición: Se dice que $Q_1, Q_2 \in \mathcal{Q}_d$ son *equivalentes*, y escribiremos $Q_1 \sim Q_2$ si Q_1 se transforma en Q_2 después de hacer un cambio de variable $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto A\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ con $A \in \mathrm{SL}_2(\mathbb{Z})$.

Como indica la notación, $\sim$ define una relación de equivalencia en $\mathcal{Q}_d$. Además es bastante evidente que si $Q_1 \sim Q_2$ entonces ambas formas cuadráticas representan los mismos enteros cuando $(x, y) \in \mathbb{Z}^2$.

Fijado $d < 0$, a cada $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}_d$ se le asigna la raíz de $ax^2 + bx + c = 0$ en $\mathbb{H}$, es decir, $z_Q = (-b + i\sqrt{-d})/(2a)$.

Proposición 2.5.1 *$Q_1 \sim Q_2 \Leftrightarrow z_{Q_1} = \gamma z_{Q_2}$ con $\gamma \in SL_2(\mathbb{Z})$.*

Demostración:

$$Q_1(x, y) = a_1x^2 + b_1xy + c_1y^2 \quad \leftrightarrow \quad z_{Q_1} = (-b_1 + i\sqrt{-d})/(2a_1)$$

$$Q_2(x, y) = a_2x^2 + b_2xy + c_2y^2 \quad \leftrightarrow \quad z_{Q_2} = (-b_2 + i\sqrt{-d})/(2a_2)$$

$\Rightarrow$) $Q_1 \sim Q_2$, entonces Q_1 se transforma en Q_2 después de hacer un cambio de variable $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto \gamma\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ con $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

$$\begin{aligned} \Rightarrow Q_2(x, y) &= Q_1(Ax + By, Cx + Dy) \\ a_2x^2 + b_2xy + c_2y^2 &= a_1(Ax + By)^2 + b_1(Ax + By)(Cx + Dy) + c_1(Cx + Dy)^2. \end{aligned}$$

Como z_{Q_2} es raíz de $a_2x^2 + b_2x + c_2$ se tiene que

$$\begin{aligned} Q_2(z_{Q_2}, 1) &= 0 = Q_1(Az_{Q_2} + B, Cz_{Q_2} + D) \\ a_2z_{Q_2}^2 + b_2z_{Q_2} + c_2 &= 0 = a_1(Az_{Q_2} + B)^2 + b_1(A_{Q_2} + B)(Cz_{Q_2} + D) + c_1(Cz_{Q_2} + D)^2. \end{aligned}$$

$\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $Cz_{Q_2} + D \neq 0$, entonces

$$a_1\left(\frac{Az_2 + B}{Cz_2 + D}\right)^2 + b_1\frac{Az_2 + B}{Cz_2 + D} + c_1 = 0.$$

Teniendo en cuenta que las únicas raíces del polinomio $a_1x^2 + b_1x + c_1$ son z_{Q_1} y $\overline{z}_{Q_1}$, se tendría que o bien $\gamma z_{Q_2} = z_{Q_1}$ o bien $\gamma z_{Q_2} = \overline{z}_{Q_1}$.

Por otro lado, como γ tiene determinante $+1$, conserva la orientación, y puesto que la conjugación la invierte, la única opción es que $\gamma z_{Q_2} = z_{Q_1}$.

$\Leftarrow$) $z_{Q_1} = \gamma z_{Q_2}$ con $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Como z_{Q_1} es raíz de $a_1x^2 + b_1x + c_1$, la factorización del polinomio queda $a_1(x - z_{Q_1})(x - \overline{z}_{Q_1})$, y por tanto la factorización de la forma Q_1 será

$$Q_1(x, y) = a_1(x - z_{Q_1}y)(x - \overline{z}_{Q_1}y).$$

Por otro lado, puesto que $z_{Q_1} = \gamma z_{Q_2}$ se tiene que

$$Q_1(x,y) = a_1(x - \gamma z_{Q_2} y)(x - \gamma \overline{z}_{Q_2} y).$$

Si ahora hacemos el cambio de variable $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto \gamma\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ se tiene

$$Q_1(Ax+By, Cx+Dy) = a_1\big(Ax+By-\gamma z_{Q_2}(Cx+Dy)\big)\big(Ax+By-\gamma z_{Q_2}(Cx+Dy)\big)$$

tomando $y = 1$ obtenemos

$$a_1(C_x + D)(\gamma x - \gamma z_{Q_2})(\gamma x - \gamma \overline{z_{Q_2}}),$$

y es evidente entonces que $x = z_{Q_2}$ es raíz. Entonces $Q_1(Ax+By, Cx+Dy) = Q_2(x,y)$ y por tanto $Q_1 \sim Q_2$. □

Definición: Al número de clases de equivalencia para el discriminante d se le llama *número de clases* y se denota con $h(d)$.

La acción de $\mathrm{SL}_2(\mathbb{Z})$ sobre las formas cuadráticas es equivalente a la acción de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathbb{H}$. Definiendo $\mathcal{H}(d) \subset \mathcal{Q}_d$, con $h(d) = \#\mathcal{H}(d)$, la condición de que la raíz asociada a una forma esté en el dominio fundamental es equivalente a que pedir que la forma esté en $\mathcal{H}(d)$. Utilizando este hecho se puede describir de manera más precisa el conjunto,

Proposición 2.5.2

$$\mathcal{H}(d) = \{(a,b,c) \in \mathbb{Z}^3 \ : \ b^2 - 4ac = d \ \ con \ \ -a < b \leq a < c \ \ \acute{o} \ \ 0 \leq b \leq a = c\}$$

donde (a,b,c) *se corresponde con la forma cuadrática* $Q = ax^2 + bx + c \in \mathcal{Q}_d$.

Demostración: Sea $z_Q = (-b + i\sqrt{-d})(2a) \in \mathbb{H}$ la raíz asociada a la forma cuadrática $Q \in \mathcal{Q}_d$ tal que z_Q pertenece al dominio fundamental

$$D = \{z \ : \ |\Re z| \leq 1/2, \ |z| \geq 1\}.$$

Observación: Dado $z \in \mathbb{H}$ existe $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\gamma z \in D$, y usando la equivalencia en las formas cuadráticas asociadas, queda garantizada la existencia de tal z_Q.

Entonces,

$$|z| \geq 1 \Rightarrow |z|^2 = \left|\frac{-b + i\sqrt{-d}}{2a}\right|^2 = \frac{b^2 - d}{4a^2} = \frac{b^2 - b^2 + 4ac}{4a^2} = \frac{c}{a} \geq 1 \Rightarrow c \geq a$$

$$|\Re z| \leq \frac{1}{2} \Rightarrow \left|\frac{-b}{2a}\right| \leq \frac{1}{2} \Rightarrow -a \leq b \leq a.$$

Además, puesto que en D se identifica la parte derecha de la frontera con la parte izquierda,

$$|z| > 1 \;\Rightarrow\; \Re z \in \left[\frac{-1}{2}, \frac{1}{2}\right) \quad (c > a \Rightarrow -a < b \leq a)$$
$$|z| = 1 \;\Rightarrow\; \Re z \in \left[\frac{-1}{2}, 0\right] \quad (c = a \Rightarrow b \geq 0).$$

□

En general, dada una forma cuadrática Q definida positiva con coeficientes enteros y m variables se define la función theta correspondiente como

$$\theta_Q(z) = \sum_{\vec{n}\in\mathbb{Z}^m} e(Q(\vec{n})z) = \sum_{n=0}^{\infty} r_Q(n)\, e(nz), \tag{2.4}$$

donde $r_Q(n)$ es el número de soluciones de $Q(\vec{n}) = n$ con $\vec{n} \in \mathbb{Z}^m$.

2.5.1. Formas cuadráticas de $\mathcal{Q}_{-7}$

El caso que más nos interesa debido al contenido del capítulo 4 es el de $d = -7$. Lo estudiamos a continuación con más detalle.

De la proposición anterior se deducirá que todas las formas cuadráticas de $\mathcal{Q}_{-7}$ son equivalentes a $x^2 + xy + 2y^2$. Para ello debemos hallar el número de clases en $\mathcal{Q}_{-7}$,

- Si $0 \leq b \leq a = c$,

$$\Rightarrow b^2 - 4a^2 = (b + 2a)(b - 2a) = -7$$

  Pero las posibles soluciones tales que $0 \leq b \leq a$ no son enteras.

- Si $-a < b \leq a < c$,

$$\Rightarrow -7 = b^2 - 4ac < b^2 - 4a_2 \leq a^2 - 4a^2 = -3a^2 \Rightarrow a = 1$$
$$\Rightarrow \begin{cases} -1 < b \leq 1 < c \\ -7 = b^2 - 4c \end{cases} \Rightarrow \begin{cases} b = 1 \\ c = 2 \end{cases}$$

Se tiene entonces que $h(-7) = \#\{(1, 1, 2)\} = 1$ y por tanto, todas las formas cuadráticas de $\mathcal{Q}_{-7}$ son equivalentes a $x^2 + xy + 2y^2$.

Proposición 2.5.3 *Para p primo, tal que $\left(\frac{-7}{p}\right) = 1$, existen b y c con $px^2 + bxy + cy^2 \in \mathcal{Q}_{-7}$, que evidentemente representa a p tomando $x = 1$, $y = 0$.*

Demostración:

$x^2 + 7 \equiv 0$ tiene solución módulo p (ley de reciprocidad cuadrática) y módulo 4 (elemental). El *teorema chino del resto* asegura que existen $b, c \in \mathbb{Z}$ tales que $b^2+7 = 4pc$. Entonces $px^2+bxy+cy^2 \in \mathcal{Q}_{-7}$ es equivalente a $x^2+xy+2y^2$ y como la primera representa a p, la segunda también. □

Teorema 2.5.4

$$4p = x^2 + 7y^2 \text{ tiene solución } x, y \in \mathbb{Z} \;\Leftrightarrow\; p = 7 \;\; ó \;\; p \equiv 1, 2, 4 \; (mod\ 7).$$

Demostración:

$\Rightarrow$) Tomando congruencias módulo p,

$$x^2 + 7y^2 \equiv 0 \pmod{p} \;\Rightarrow\; x^2 \equiv -7y^2 \pmod{p}$$

que tiene solución si y sólo si $-7 \equiv 0 \pmod{p} \Rightarrow p = 7$, o bien, -7 es residuo cuadrático módulo p, es decir, si $\left(\frac{-7}{p}\right) = 1$ y esta situación ocurre si y sólo si $p \equiv 1, 2, 4 \pmod{7}$.

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = (-1)^{(p-1)/2}(-1)^{3(p-1)/2}\left(\frac{p}{7}\right) = \left(\frac{p}{7}\right),$$

donde en el segundo paso se ha empleado la ley de la reciprocidad cuadrática y la ley suplementaria. Teniendo en cuenta que $\{\text{cuadrados mod } 7\} = \{0, 1, 2, 4\}$, entonces

$$\left(\frac{-7}{p}\right) = 1 \Leftrightarrow \left(\frac{p}{7}\right) = 1 \Leftrightarrow p \equiv 1, 2, 4 \pmod{7}. \tag{2.5}$$

$\Leftarrow$) Si $p = 7$, la solución sería $x = 0$, $y = 2$. Para $p \neq 7$, multiplicando por 4 la expresión $x^2 + xy + 2y^2$ y completando cuadrados se obtiene la identidad

$$4(x^2 + xy + 2y^2) = (2x + y)^2 + 7y^2.$$

Basta observar entonces que la forma $x^2 + xy + 2y^2$ representa a p para ciertos $x, y \in \mathbb{Z}$, escribiendo $z = 2x + y$ se llega al resultado. □

Observación: Si p es un primo > 2, entonces $4p$ se puede sustituir por p en el primer miembro. Esto es así debido a que x e y son pares. Si fueran impares $x^2 \equiv y^2 \equiv 1 \pmod{8}$ implica $8 \mid x^2 + 7y^2 = 4p$ que es una contradicción para $p > 2$.

En número de clases nos aporta información sobre la factorización única en los anillos de enteros de un cuerpo cuadrático, así cuando es uno se tiene factorización única y a medida que crece estamos más alejados de ella.

Observación: En el Capítulo 4 consideraremos $\mathbb{Z}[\xi]$ con $\xi = (1 + i\sqrt{7})/2$. Será entonces de gran importancia saber si se tiene o no factorización única en este caso.

Utilizando argumentos realizados con las formas de Q_7 es posible dar una solución a esta cuestión:

Todo ideal es de la forma $I = \{\alpha x + \beta y \quad : \quad x, y \in \mathbb{Z}\}$ y la factorización única está asegurada si todos los ideales son principales, es decir, si $I = \delta\mathbb{Z}[\xi]$. Se puede probar que esto equivale a que exista un cambio lineal entero invertible $(x, y) \mapsto (x', y')$ tal que $N(x' + \xi y') \mid N(\alpha x + \beta y)$. Tomando $\lambda \in \mathbb{Z}^+$ la norma del ideal, $\lambda^{-1}N(\alpha x + \beta y) \in \mathcal{Q}_{-7}$, usando que $h(-7) = 1$, todas las formas son equivalentes a $x^2 + xy + 2y^2 = N(x + \xi y)$, de donde se tiene factorización única.

2.6. La función θ de Jacobi

Las formas modulares más antiguas son las funciones theta.

Las funciones theta clásicas fueron introducidas de dos maneras diferentes en la teoría de números, por un lado su modularidad permitió a Riemann demostrar la ecuación funcional de su célebre función zeta (véase [Ed]), por otro lado se utilizaron para contar el número exacto de formas de representar un entero como la suma de n cuadrados.

Definición: La función θ de Jacobi está definida por

$$\theta(z) = \sum_{n=-\infty}^{\infty} e(n^2 z) \qquad \text{para} \quad z \in \mathbb{H}.$$

Proposición 2.6.1 *La función θ verifica*

$$\theta(\frac{-1}{4z}) = \sqrt{\frac{2z}{i}}\, \theta(z).$$

Demostración: La fórmula de sumación de Poisson afirma

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \widehat{f}(n) \qquad \text{con} \quad \widehat{f}(\xi) = \int_{-\infty}^{\infty} f(x)e(-x\xi)dx.$$

Sea $f(x) = e^{2\pi i x^2 z}$, su transformada de Fourier será

$$\widehat{f}(\xi) = \int_{-\infty}^{\infty} e^{2\pi i x^2 z} e^{-2\pi i x\xi}\, dx.$$

Derivando bajo el signo de la integral obtenemos

$$\widehat{f}'(\xi) = \int_{-\infty}^{\infty} -2\pi i x\, e^{2\pi i x^2 z} e^{-2\pi i x\xi}\, dx =$$

$$\begin{cases} u = -e^{-2\pi i x\xi} \\ dv = 2\pi i x\, e^{2\pi i x^2 z}\, dx \end{cases} \Rightarrow \begin{cases} du = 2\pi i\xi\, e^{-2\pi i x\xi}\, dx \\ v = \frac{1}{2z}\, e^{2\pi i x^2 z} \end{cases}$$

$$= -\frac{1}{2z}\, e^{2\pi i x^2 z} e^{-2\pi i x\xi}\Big]_{-\infty}^{\infty} - \frac{\pi i\xi}{z}\int_{-\infty}^{\infty} e^{2\pi i x^2 z} e^{-2\pi i x\xi}\, dx$$

$$\begin{cases} z \in \mathbb{H},\ z = a + bi,\ b > 0 \\ e^{2\pi i x^2 z} = e^{2\pi i x^2 (a+bi)} = e^{-2\pi x^2 b} e^{2\pi i x^2 a} \end{cases} \quad \Longrightarrow\ -\tfrac{1}{2z} e^{2\pi i x^2 z} e^{-2\pi i x\xi}\big]_{-\infty}^{\infty} = 0$$

Se tiene entonces que $\widehat{f}'(\xi) = \frac{-\pi i\xi}{z}\widehat{f}(\xi)$, de donde se puede calcular explícitamente $\widehat{f}(\xi)$,

$$\frac{\widehat{f}'(\xi)}{\widehat{f}(\xi)} = \frac{-\pi i\xi}{z} \Rightarrow \ln \widehat{f}(\xi) = \frac{-\pi i\xi^2}{2z} + C \Rightarrow \widehat{f}(\xi) = \widetilde{C} e^{-\pi i\xi^2/2z}.$$

$$\begin{cases} \int_{-\infty}^{\infty} e^{-x^2}\, dx = \sqrt{\pi} \\ 2\pi i x^2 z = -y^2 \ \Rightarrow\ y = \sqrt{-2\pi i z}\, x \ \Rightarrow\ x = \frac{1}{\sqrt{-2\pi i z}} y \ \Rightarrow\ dx = \frac{1}{\sqrt{-2\pi i z}}\, dy \end{cases}$$

Usando ahora que la función $I(\xi) = \int_{-\infty}^{\infty} e^{-x^2} e^{-ix\xi}\, dx$ verifica $I(0) = \sqrt{\pi}$,

$$\widehat{f}(0) = \int_{-\infty}^{\infty} e^{2\pi i x^2 z}\, dx = \frac{1}{\sqrt{-2\pi i z}} \int_{\infty}^{\infty} e^{-y^2}\, dy = \frac{\sqrt{\pi}}{\sqrt{-2\pi i z}} = \sqrt{\frac{i}{2z}}$$

$$\Longrightarrow \widehat{f}(\xi) = \sqrt{\frac{i}{2z}}\, e^{-\pi i\xi^2/2z}.$$

Por último, usando la fórmula de sumación de Poisson, se obtiene

$$\theta(z) = \sum_{n=-\infty}^{\infty} e(n^2 z) = \sum_{n=-\infty}^{\infty} \sqrt{\frac{i}{2z}}\, e\left(\frac{-n^2}{4z}\right) = \sqrt{\frac{i}{2z}}\, \theta\left(\frac{-1}{4z}\right).$$

□

Proposición 2.6.2 *La función θ verifica*

$$\theta(z) = w_\gamma j_\gamma^{-1/2}(z)\theta(\gamma z) \qquad \textit{para } \gamma \in \Gamma_0(4)$$

donde w_γ es cierta raíz cuarta de la unidad, esto es, $w_\gamma \in \{\pm 1, \pm i\}$.

Demostración: Basta comprobarlo para los generadores de $\Gamma_0(4)$.

- $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\quad Tz = z + 1$.

$$\theta(Tz) = \theta(z+1) = \sum_{n=-\infty}^{\infty} e(n^2(z+1)) = \sum_{n=-\infty}^{\infty} e(n^2 z) = \theta(z).$$

- $\widetilde{S} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \quad \widetilde{S}z = \frac{z}{4z+1}$.

  Observación:

$$\theta\left(\frac{-1}{4z}\right) = \sqrt{\frac{2z}{i}}\,\theta(z) = (-2zi)^{1/2}\theta(z).$$

  Nos gustaría poder utilizar la matriz $\alpha = \left(\begin{smallmatrix} 0 & -1 \\ 4 & 0 \end{smallmatrix}\right)$, pues $\alpha z = \frac{-1}{4z}$, pero nos encontramos con el problema de que $\alpha \notin \mathrm{SL}_2(\mathbb{Z})$, sin embargo esto lo ponemos solucionar usando los generadores de $\Gamma_0(4)$,

$$\alpha^{-1}T^{-1}\alpha = \underbrace{\begin{pmatrix} 0 & 1/4 \\ -1 & 0 \end{pmatrix}}_{-1/4z}\underbrace{\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}}_{z-1}\underbrace{\begin{pmatrix} 0 & -1 \\ 4 & 0 \end{pmatrix}}_{-1/4z} = \underbrace{\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}}_{z/(4z+1)} = \widetilde{S}.$$

  De este modo,

$$\theta\left(\frac{z}{4z+1}\right) = \theta\left(-\frac{1}{4\left(\frac{-1}{4z}-1\right)}\right) = \left(-2\left(\frac{-1}{4z}-1\right)i\right)^{1/2}\theta\left(\frac{-1}{4z}-1\right) =$$

$$= \left(\left(\frac{1}{2z}+2\right)i\right)^{1/2}\theta\left(\frac{-1}{4z}\right) = \left(\left(\frac{1}{2z}+2\right)i\right)^{1/2}(-2zi)^{1/2}\theta(z) =$$

$$= w_{\widetilde{S}}\left(\left(\frac{1}{2z}+2\right)2z\right)^{1/2}\theta(z) = w_{\widetilde{S}}(1+4z)^{1/2}\theta(z) = w_{\widetilde{S}}j_{\widetilde{S}}^{1/2}(z)\theta(z).$$

Se concluye entonces

$$\theta(z) = w_\gamma j_\gamma^{-1/2}(z)\theta(\gamma z) \qquad \text{para } \gamma \in \Gamma_0(4).$$

□

Observación: La dependencia de w_γ en γ viene dada por la fórmula

$$w_\gamma = \begin{cases} \left(\frac{c}{d}\right) & \text{si } \ d \equiv 1 \pmod 4 \\ i\left(\frac{c}{d}\right) & \text{si } \ d \equiv 3 \pmod 4 \end{cases} \qquad \text{para } \ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4),$$

donde $\left(\frac{*}{*}\right)$ es el símbolo de Legendre.

θ es por tanto una forma modular de peso $1/2$ respecto a $\Gamma_0(4)$ salvo porque la relación modular está afectada por un "multiplicador" w_γ, pero este problema lo podemos solventar elevando a una potencia adecuada. Por ejemplo, si estamos interesados en $r_4(n)$, el número de representaciones de n como suma de cuatro cuadrados,

$$\theta^4(z) = \sum_{n=0}^{\infty} r_4(n)\, e(nz),$$

se tiene

$$\theta^4(z) = j_\gamma^{-2}(z)\theta^4(\gamma z) \quad \forall\ \gamma \in \Gamma_0(4).$$

Es decir, $\theta^4 \in \mathcal{M}_2(\Gamma_0(4))$. En términos generales,

Proposición 2.6.3

$$\theta^{4k}(z) = j_\gamma^{-2k}(z)\theta^{4k}(\gamma z) \in \mathcal{M}_{2k}(\Gamma_0(4)).$$

Una bella consecuencia de la modularidad es el siguiente resultado de Jacobi,

Proposición 2.6.4 *El número de representaciones de $n \in \mathbb{Z}^+$ como suma de cuatro cuadrados es $8\big(\sigma_1(n) - \sigma_1(n/4)\big)$ donde $\sigma_1(n/4)$ se define como 0 si $n/4$ no es entero.*

Demostración: Por un lado, usando los primeros valores de $r_4(n)$,

$$\theta^4(z) = \sum_{n=0}^{\infty} r_4(n)e(nz) = 1 + 8e(z) + 24e(2z) + \dots$$

Por otro lado, ya vimos en la Proposición 2.4.4 cómo $f = E_2(z) - 2E_2(2z)$ y $g = E_2(2z) - 2E_2(4z)$ forman una base de $\mathcal{M}_2(\Gamma_0(4))$. Recordando que estas funciones venían dadas por

$$f(z) = -1 - 24\sum_{m=1}^{\infty}\left(\sigma(m) - 2\sigma\left(\frac{m}{2}\right)\right)e(mz) = -1 - 24e(z) - 24e(2z) - \dots$$

$$g(z) = -1 - 24\sum_{m=1}^{\infty}\left(\sigma\left(\frac{m}{2}\right) - 2\sigma\left(\frac{m}{4}\right)\right)e(mz) = -1 - 24e(2z) - 24e(4z) - \dots$$

se tiene que

$$3\theta^4(z) = -f(z) - 2g(z) \Longrightarrow \theta^4(z) = -\frac{1}{3}f(z) - \frac{2}{3}g(z).$$

$$\theta^4(z) = \frac{1}{3} + 8\sum_{n=1}^{\infty}\left(\sigma(n) - 2\sigma\left(\frac{n}{2}\right)\right)e(nz) + \frac{2}{3} + 16\sum_{n=1}^{\infty}\sigma\left(\frac{n}{2}\right) - \sigma\left(\frac{n}{4}\right)e(nz) =$$

$$= 1 + 8\sum_{n=1}^{\infty}\left(\sigma(n) - \sigma\left(\frac{n}{4}\right)\right)e(nz).$$

El número de representaciones de $n \in \mathbb{Z}^+$ como suma de cuatro cuadrados será

$$r_4(n) = 8\left(\sigma(n) - \sigma\left(\frac{n}{4}\right)\right),$$

donde $\sigma(n) = 0$ si n no es entero. $\square$

Observación: La multiplicación compleja en el retículo induce una función en la curva elíptica que relaciona unos puntos con otros. De una forma que no es fácil de describir, dicha relación lleva a que contar el número de puntos módulo p tenga que ver con las representaciones de p por cierta forma cuadrática.

Recordando la definición dada por (2.4), el número de representaciones por una forma cuadrática son los coeficientes de una forma modular θ_Q.

Capítulo 3

Multiplicación compleja y la ecuación modular

En el Capítulo 1, vimos como a través de las funciones elípticas cada retículo Λ tenía asociada una curva elíptica sobre $\mathbb{C}$. Tal retículo puede tener cierta noción de simetría y aplicarse en sí mismo al multiplicar por un número α complejo (no real).

Esta propiedad se llama *multiplicación compleja* y fue estudiada clásicamente a partir de la idea de generar números algebraicos, a través de valores especiales de funciones meromorfas, en el caso de las extensiones abelianas de los cuerpos cuadráticos imaginarios, ideas estudiadas por Kronecker, Weber y otros que evidenciaron su gran importancia en teoría algebraica de números.

Este tipo de curvas elípticas se dice que son curvas de multiplicación compleja. Además, si tal número α está en un dominio de factorización única, entonces las curvas de este tipo poseen una importante propiedad, la de que sus coeficientes, que en principio son complejos, realmente todos ellos están en $\mathbb{Q}$.

3.1. Multiplicación compleja

Definición: Sea $\Lambda = \{m\omega_1 + n\omega_2\}$ con $\Im(\omega_2/\omega_1) > 0$. Se dice que Λ tiene *multiplicación compleja* si existe un número complejo $\alpha \notin \mathbb{R}$ tal que $\alpha\Lambda \subset \Lambda$. (Cuando tal número existe, no es único).

Observación: Sin perdida de generalidad se puede suponer que $\omega_1 = 1$ y $\omega_2 \in \mathbb{H}$, pues Λ es linealmente equivalente a un retículo complejo de la forma $\{m + n\omega\}$ con $\omega = \omega_2/\omega_1 \in \mathbb{H}$.

Proposición 3.1.1 *Λ tiene multiplicación compleja si y sólo si ω_2/ω_1 está en una extensión cuadrática (imaginaria) de $\mathbb{Q}$, es decir, si y sólo si es raíz de una ecuación de segundo grado con coeficientes enteros. En particular α también está en dicha extensión.*

Demostración:
Sea $\Lambda = \{m + n\omega\}$.
$\Rightarrow$) Si Λ tiene multiplicación compleja, $\alpha\Lambda \subset \Lambda$ con $\alpha \notin \mathbb{R}$, entonces $\exists\, a, b, c, d \in \mathbb{Z}$ tales que

$$\alpha\omega = a\omega + b, \qquad \alpha = c\omega + d$$

$\alpha \notin \mathbb{R} \Rightarrow c \neq 0$, entonces

$$(c\omega + d)\omega = a\omega + b \quad \Rightarrow \quad c\omega^2 + (d - a)\omega - b = 0.$$

ω es raíz de una ecuación de segundo grado con coeficientes enteros, por lo tanto ω está en una extensión cuadrática imaginaria de $\mathbb{Q}$.
En particular, como $\alpha = c\omega + d$ con $c, d \in \mathbb{Z}$, α también está en la extensión.
$\Leftarrow$) Sea $\omega \in \mathbb{Q}(\sqrt{h})$ cuerpo cuadrático ($h < 0$ entero libre de cuadrados), entonces $\exists\, a, b, c \in \mathbb{Z}$ con $a \neq 0$ tales que

$$a\omega^2 + b\omega + c = 0.$$

Tomando $\alpha = a\omega$ se tiene que

$$\alpha = a\omega \in \Lambda, \qquad \alpha\omega = a\omega^2 = -c - b\omega \in \Lambda.$$

Por tanto, $\alpha\Lambda \subset \Lambda$ con $\alpha \notin \mathbb{R}$, es decir, Λ tiene multiplicación compleja. □

Proposición 3.1.2 *Sea Λ (con multiplicación compleja) y α como en la proposición anterior, entonces α es un entero algebraico.*

Demostración: $\alpha\Lambda \subset \Lambda$ con $\alpha \notin \mathbb{R}$, entonces $\exists\, a, b, c, d \in \mathbb{Z}$ tales que

$$\alpha\omega = a\omega + b, \qquad \alpha = c\omega + d.$$

$$(\alpha - a)\omega - b = 0, \qquad -c\omega + \alpha - d = 0.$$

$$\Rightarrow \begin{vmatrix} \alpha - a & -b \\ -c & \alpha - d \end{vmatrix} = (\alpha - a)(\alpha - d) - bc = \alpha^2 - (a + d)\alpha - bc = 0$$

$\Rightarrow \alpha$ es un entero algebraico en $\mathbb{Q}(\sqrt{h})$. □

Proposición 3.1.3 *Si $\alpha\Lambda \subset \Lambda$ y $\wp$ es la función de Weierstrass de Λ, entonces $\wp(\alpha z) = P\big(\wp(z)\big)/Q\big(\wp(z)\big)$ para ciertos polinomios P y Q con $gr\, P = gr\, Q + 1$.*

Demostración: $\wp(\alpha z)$ es función elíptica pues, para $\beta \in \Lambda$

$$\wp(\alpha(z + \beta)) = \wp(\alpha z + \underbrace{\alpha\beta}_{\in \Lambda}) = \wp(\alpha z)$$

y es par, pues

$$\wp(-\alpha z) = \frac{1}{(-\alpha z)^2} + \sum_{\omega \in \Lambda} \left(\frac{1}{(-\alpha z + \omega)^2} - \frac{1}{\omega^2} \right) =$$

$$= \frac{1}{(\alpha z)^2} + \sum_{\omega \in \Lambda} \left(\frac{1}{(\alpha z + \omega)^2} - \frac{1}{\omega^2} \right) = \wp(\alpha z).$$

Es por tanto una función racional de $\wp(z)$ (Teorema 1.3.4), es decir

$$\wp(\alpha z) = \frac{P\left(\wp(z)\right)}{Q\left(\wp(z)\right)},$$

para ciertos polinomios P y Q.
Se tiene entonces que

$$\wp(\alpha z) Q\left(\wp(z)\right) = P\left(\wp(z)\right).$$

El primer término en el desarrollo de ambas funciones es $1/z^2 \left(1/z^2\right)^n$ y $\left(1/z^2\right)^m$, donde m y n son los grados de los polinomios P y Q respectivamente.
Puesto que el orden debe coincidir en ambas funciones $1 + n = m$, es decir, gr $P =$ gr $Q + 1$. □

Si $E_1/\mathbb{C}$ y $E_2/\mathbb{C}$ son dos curvas complejas, podemos representarlas mediante dos toros complejos $E_i \simeq \mathbb{C}/\Lambda_i$, es claro entonces que se tiene un isomorfismo $\mathrm{Hom}(E_1, E_2) \simeq \mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$, donde es segundo grupo es el de los homomorfismos analíticos entre los toros. Identificando cada homomorfismo analítico entre $\mathbb{C}/\Lambda_1$ y $\mathbb{C}/\Lambda_2$ con el número complejo α que lo determina podemos ver a $\mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$ como un subgrupo de $\mathbb{C}$. (La suma de números complejos se corresponde con la suma de homomorfismos definida puntualmente).

Si los dos toros son el mismo $\mathbb{C}/\Lambda$, entonces la composición de endomorfismos de $\mathbb{C}/\Lambda$ se corresponde con el producto de números complejos, por lo que $\mathrm{End}(\mathbb{C}/\Lambda)$ resulta ser un subanillo de $\mathbb{C}$.

En particular, $\mathrm{End}(\mathbb{C}/\Lambda)$ es un anillo conmutativo.

Definición: Las curvas elípticas sobre $\mathbb{C}$ que corresponden a un retículo con multiplicación compleja se dice que son *curvas elípticas de multiplicación compleja* o *curvas elípticas CM.*

Multiplicar por un entero n en el retículo se traduce en multiplicar por n en la curva elíptica. Por ejemplo, si $n = 2$, utilizando la parametrización $z \mapsto (\wp(z), \wp'(z))$ y la fórmula de duplicación para $\wp(2z)$ que relaciona esta función con $\wp(z)$ se puede deducir la fórmula para calcular $2P$ en la curva elíptica sin ninguna referencia a la interpretación geométrica con tangentes e intersecciones. De forma similar, la multiplicación compleja en un retículo por un número α corresponde a cierto endomorfismo de la curva elíptica.

Usando la Proposición 3.1.3, tal endomorfismo admite una fórmula como función racional de las coordenadas.

Una curva elíptica de multiplicación compleja tiene simetrías ocultas que pasan puntos a puntos, distintas[1] de multiplicar por cualquier $n \in \mathbb{Z}$.

En el caso de multiplicación compleja $\mathrm{End}(E)$ es (isomorfo a) $\mathbb{Z}[\alpha]$.

$\star$ *Ejemplo:* Uno de los ejemplos más sencillos de multiplicación compleja es la curva elíptica $E:\ y^2 = 4x^3 - x$ que corresponde a un retículo de la forma $\Lambda = \{\omega_1(n + im)\}$ con cierto ω_1 que no tiene una expresión explícita sencilla (es una integral elíptica).

Para este retículo se verifica $\wp(iz) = -\wp(z)$.

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda}\left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right)$$

$$\wp(iz) = \frac{1}{(iz)^2} + \sum_{\omega\in\Lambda}\left(\frac{1}{(iz+\omega)^2} - \frac{1}{\omega^2}\right) = \frac{-1}{z^2} + \sum_{\omega\in\Lambda}\left(\frac{-1}{(-z+i\omega)^2} - \frac{1}{\omega^2}\right) =$$

$$= \frac{-1}{z^2} + \sum_{\omega\in\Lambda}\left(\frac{-1}{(z-i\omega)^2} - \frac{1}{(i\omega)^2}\right).$$

Como $\omega \in \Lambda, \quad \omega = \omega_1(n + im)$, entonces $i\omega = \omega_1(in - m) \in \Lambda$, de donde

$$\wp(iz) = \frac{-1}{z^2} + \sum_{\omega\in\Lambda}\left(\frac{-1}{(z+\omega)^2} - \frac{1}{\omega^2}\right) = -\left(\frac{1}{z^2} + \sum_{\omega\in\Lambda}\left(\frac{1}{(z+\omega)^2} + \frac{1}{\omega^2}\right)\right) = -\wp(z).$$

Por otro lado

$$\wp(iz) = -\wp(z) \Rightarrow i\wp'(iz) = -\wp'(z) \Rightarrow \wp'(iz) = i\wp'(z).$$

Usando que la aplicación

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & E \\ z & \longmapsto & (\wp(z), \wp'(z)) \\ iz & \longmapsto & (-\wp(z), i\wp'(z)) \end{array}$$

establece un isomorfismo holomorfo entre la superficie de Riemann $\mathbb{C}/\Lambda$ y la curva proyectiva $E:\ y^2 = 4x^3 - x$, el endomorfismo correspondiente a la multiplicación por i está dado por

$$\begin{array}{rccc} \phi: & E & \longrightarrow & E \\ & (x, y) & \longmapsto & (-x, iy) \end{array}$$

[1] En términos algebraicos esta definición pasa a ser $\mathrm{End}(E) \ncong \mathbb{Z}$. En cambio, las curvas "normales" cumplen $\mathrm{End}(E) \cong \mathbb{Z}$.

Por tanto el isomorfismo $\mathrm{End}(E) \cong \mathbb{Z}[i]$ vendrá dado por $a+bi \mapsto aP + b\phi(P)$ donde la multiplicación por a y b se hace en la curva elíptica (sumar un punto consigo mismo).

La existencia de multiplicaciones complejas se conserva por isomorfismos. Ponemos hablar entonces de invariantes con multiplicación compleja.

Un retículo $\Lambda = \{m\omega_1 + n\omega_2\}$, $\Im(\omega_2/\omega_1) > 0$, da lugar a una curva elíptica sobre $\mathbb{C}$, $E:\ y^2 = 4x^3 - g_2x - g_3$, que puede ser reescrita tras un cambio de variable en la forma $E:\ y^2 = x^3 + Ax + B$.

Recordando la Definición 1.2, dos retículos son linealmente equivalentes si existe $\alpha \in \mathbb{C}$ tal que $\alpha\Lambda = \Lambda'$. Tal α puede verse como una aplicación lineal en $\mathbb{C}$, que induce un isomorfismo entre curvas elípticas.

Todo retículo es linealmente equivalente a uno de la forma $\{m + n\omega\}$ (en este caso la aplicación lineal vendría dada por $f(z) = z/\omega_1$), que coincide con $\{m + n\omega'\}$ si y sólo si $\gamma(\omega) = \omega'$ con $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

La función de Klein j, es una función modular de peso cero inyectiva en el dominio fundamental [Kn], por tanto las curvas elípticas correspondientes a los retículos $\Lambda = \{m\omega_1 + n\omega_2\}$ y $\Lambda' = \{m\omega_1' + n\omega_2'\}$ son isomorfas (sobre $\mathbb{C}$) si y sólo si $j(\omega_2/\omega_1) = j(\omega_2'/\omega_1')$.

Los coeficientes de la curva elíptica dependen del retículo y j se puede relacionar con ellos. Las fórmulas son:

$$E:\ y^2 = 4x^3 - g_2x - g_3 \quad \longrightarrow \quad j = \frac{1728g_2^3}{g_2^3 - 27g_3^2},$$

$$E:\ y^2 = x^3 + Ax + B \quad \longrightarrow \quad j = \frac{6912A^3}{4A^3 + 27B^2}.$$

Por una variante del principio del máximo, las únicas funciones modulares de peso cero acotadas son las constantes. En particular,

Proposición 3.1.4 *Toda función modular de peso cero con un desarrollo de Fourier $\sum_{n=-N}^{\infty} a_n e(nz)$ es un polinomio de grado N en $j(z)$.*

Demostración: Sea f función modular de peso cero con un desarrollo de Fourier $\sum_{n=-N}^{\infty} a_n e(nz)$. Por inducción sobre N,

- $N = 0$,
  $f(z)$ es función modular de peso cero, cuyo desarrollo de Fourier es de la forma $\sum_{n=0}^{\infty} a_n e(nz)$, en particular es acotada, aplicando el teorema de Lioville 1.1.1, f es constante y por tanto la podemos ver como un polinomio en $j(z)$ de grado 0.

- Suponemos cierto hasta $N = m$, es decir, si f tiene desarrollo de Fourier $\sum_{n=-N}^{\infty} a_n e(nz)$ entonces
  $$f(z) = P_N(j(z)),$$
  donde P_N es un polinomio de grado N en $j(z)$, para todo $N \leqslant m$.

- $N = m + 1$,

$$f(z) = \sum_{n=-(m+1)}^{\infty} a_n e(nz) = a_{-(m+1)} e(-(m+1)z) + \sum_{n=-m}^{\infty} a_n e(nz).$$

Sea $g(z) = f(z) - a_{-(m+1)}(j(z))^{m+1}$.
g es función modular de peso cero, cuyo desarrollo de Fourier es de la forma $\sum_{n=-m}^{\infty} b_n e(nz)$, aplicando la hipótesis de inducción en la función g se tiene que

$$g(z) = P_m(j(z)),$$

donde P_m es un polinomio de grado m en $j(z)$.

Por tanto

$$f(z) = a_{-(m+1)}(j(z))^{m+1} + g(z) = P_{m+1}(j(z)),$$

donde P_{m+1} es un polinomio de grado $m + 1$ en $j(z)$.

□

Identificando los lados opuestos de un paralelogramo fundamental asociado a un retículo Λ, obtenemos una superficie de Riemann $\mathbb{C}/\Lambda$ de género 1, de modo que las funciones elípticas sobre Λ pueden verse como funciones holomorfas sobre $\mathbb{C}/\Lambda$.

Podemos repetir el mismo argumento, esta vez con la función j. Identificando los puntos del domino fundamental D, obtenemos una superficie de Riemann S, que topológicamente se corresponde con una esfera menos un punto. De este modo, j puede verse como una función holomorfa sobre S. Si añadimos un punto infinito para compactificar la superficie S, tenemos que j se extiende a una función holomorfa $j : S^* \to \mathbb{C}^\infty$. Los coeficientes de j (respecto a una carta adecuada) alrededor del punto infinito son sus coeficientes de Fourier, y puesto que el coeficiente de $e(-z)$ es no nulo se tiene que j tiene un polo en el infinito. Como j es inyectiva en S, es por tanto una transformación conforme entre dos esferas, podemos asegurar entonces que toma todos los valores complejos.

3.2. Funciones modulares

Las funciones modulares están muy relacionadas con ciertas superficies compactas llamadas superficies modulares. La superficie modular más simple es la que se obtiene al identificar los puntos de $\mathbb{H}$ equivalentes respecto al grupo modular. Las superficies modulares en general se obtienen del mismo modo a partir de grupos de transformaciones adecuados, por ejemplo, el espacio cociente $X_0(N) = \mathbb{C}/\Gamma_0(N)$, añadiéndole un número finito de puntos para compactificarlo, es una *curva modular*.

El cuerpo de las funciones meromorfas sobre una superficie de Riemann es un cuerpo de funciones algebraicas, pero en general no es fácil determinar una ecuación que lo determine. Sin embargo, para el cuerpo de las funciones modulares respecto al grupo $\Gamma_0(N)$ podemos encontrar explícitamente unos generadores de su cuerpo de funciones meromorfas junto con una ecuación polinómica irreducible que los relaciona.

Proposición 3.2.1 *Para cada entero positivo n existe un polinomio en dos variables $\Psi_n \in \mathbb{C}[X,Y]$ tal que*

$$\Psi_n(X, j(z)) = \prod_{\substack{ad=n \\ a,d>0}} \prod_{b=0}^{d-1} \Big(X - j\big(\frac{az+b}{d}\big) \Big).$$

Demostración:

Observación: Sea $P(X, X_1, \ldots, X_s) = \prod_{i=1}^{s}(X - X_i) \in \mathbb{C}[X, X_1, \ldots, X_s]$. Es claro que P visto como polinomio en X, es de la forma $X^s + \sigma_{s-1}X^{s-1} + \cdots + \sigma_0$, donde $\sigma_{s-k}(X_1, \ldots, X_s)$ es un polinomio simétrico en $X_1, \ldots, X_s$ igual a la suma de todos los posibles productos de k de estas variables[2].

Denotando por s a la dimensión de Δ_n, sea

$$\Psi_n(X, j(z)) = P(X, j(\delta_1 z), \ldots, j(\delta_s z)).$$

Ψ_n es un polinomio mónico de grado s.

Cada coeficiente es un polinomio, σ_{s-k}, simétrico en $j(\delta_i z)$ con $i = 1, \ldots, s$. Usando la Proposición 2.3.1 junto con el Corolario 2.3.3, cada σ_{s-k} será una función modular de peso 0 (por serlo j), y por la Proposición 3.1.4, un polinomio en $j(z)$, es decir, en $\mathbb{C}[j(z)]$. Podemos por tanto ver a Ψ como polinomio en $\mathbb{C}[X,Y]$ para cada $n \in \mathbb{Z}_+$. □

Proposición 3.2.2 *Si $\lambda \in \mathcal{M}_{2\times 2}(\mathbb{Z})$ con $\det \lambda = n$, entones $\Psi_n\big(j(\lambda z), j(z)\big) = 0$.*

Demostración: Para comprobarlo, bastará ver que algún factor de Ψ_n es cero.

Fijado X, sea $G(z) = P(X, j(\delta_1 z), \ldots, j(\delta_s z))$. $G(z)$ es un polinomio simétrico en $j(\delta_i)$, $i = 1, \ldots, s$. Usando de nuevo la Proposición 2.3.1 junto con Corolario 2.3.3, como j es modular de peso 0, G también lo será.

Teniendo en cuenta que el producto por el que se define la función Ψ_n recorre todos los elementos de Δ_n, usando la Proposición 2.3.1, uno de ellos cumplirá $\lambda = \delta\gamma$ para algún $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Tomando precisamente dicho γ se tiene que $j(\lambda z) = j(\delta_i \gamma z)$, y por tanto, para $X = j(\lambda z)$, $G(\gamma z) = P(j(\lambda z), j(\delta_1\gamma z), \ldots, j(\delta_s \gamma z)) = 0$, usando ahora que $G(z)$ es modular de peso cero, se tiene el resultado. □

[2]A $\sigma_{s-k}(X_1, \ldots, X_s)$ se le suele llamar *polinomio simétrico elemental* de grado k y s variables.

Proposición 3.2.3 $\Psi_n \in \mathbb{Z}[X,Y]$.

Demostración: La función j tiene desarrollo de Fourier $e(-z)+\sum_{k=0}^{\infty} a_k\, e(kz)$, entonces para $\delta \in \Delta_n$

$$\begin{aligned} j(\delta z) &= j\left(\frac{az+b}{d}\right) = e\left(-\frac{az+b}{d}\right) + \sum_{k=0}^{\infty} a_k\, e\left(k\frac{az+b}{d}\right) = \\ &= e\left(\frac{-az}{d}\right)\, e\left(\frac{-b}{d}\right) + \sum_{k=0}^{\infty} a_k\, e\left(\frac{kaz}{d}\right)\, e\left(\frac{kb}{d}\right) = \\ &= e\left(\frac{-az}{d}\right)\zeta_d^{-b} + \sum_{k=0}^{\infty} a_k\, e\left(\frac{kaz}{d}\right)\zeta_d^{kb} = \\ &= \sum_{k=-1}^{\infty} \widetilde{a_k}\, e\left(\frac{kaz}{d}\right), \end{aligned}$$

donde $\zeta_d = e(1/d)$ y $\widetilde{a_k} \in \mathbb{Z}[\zeta_d]$. Los coeficientes de $\Psi_n(X, j(z))$ son todos ellos polinomios, σ_{s-k}, simétricos en $j(\delta_i z)$, $i = 1, \ldots, s$, cada σ_{s-k} tendrá entonces un desarrollo de Fourier de la forma

$$\sum_{k=-N}^{\infty} b_k\, e\left(\frac{kz}{n}\right), \quad \text{donde } \; b_k \in \mathbb{Z}[\zeta_n]$$

para cierto N entero (donde se ha usado que $ad = n$ al sacar factor común en los denominadores de los exponentes). Aplicando la conjugación de Galois $\zeta_n \mapsto \zeta_n^r$ con $r \in (\mathbb{Z}/n\mathbb{Z})^*$, estos automorfismos permutan las series $j(\delta_i z)$ y por tanto fijan la serie σ_{s-k}, por lo que los coeficientes b_k realmente están en $\mathbb{Z}$.

Por otro lado, cada σ_{s-k} es modular, en particular cada σ_{s-k} debe cumplir

$$\sum_{k=-N}^{\infty} b_k\, e\left(\frac{k(z+1)}{n}\right) = \sum_{k=-N}^{\infty} b_k \zeta_n^k\, e\left(\frac{kz}{n}\right) = \sum_{k=-N}^{\infty} b_k\, e\left(\frac{kz}{n}\right)$$

de la igualdad se tiene que sólo sobreviven los coeficientes b_k tales que $\zeta_n^k = 1$, es decir, si $n \mid k$, y por tanto cada σ_{s-k} tendrá un desarrollo de la forma

$$\sum_{k=-N}^{\infty} b_k\, e(kz), \quad \text{donde } \; b_k \in \mathbb{Z}$$

Finalmente, como los coeficientes de $\Psi_n(X, j(z))$ son (usando la Proposición 3.1.4) polinomios en $j(z)$ todos ellos con coeficientes enteros, se concluye que $\Psi_n(X,Y) \in \mathbb{Z}[X,Y]$. □

3.2.1. La ecuación modular

Φ_n es el llamado *polinomio modular*, definido como Ψ_n pero exigiendo ahora que en el producto $\text{mcd}(a, b, d) = 1$.

Si $n = p_1 \dots p_k$, con p_i primos todos distintos, es claro que $\Phi_n = \Psi_n$, pues en este caso como $ad = n$ se tiene que $(a, d) = 1$, y el añadir b no aporta nada, se sigue teniendo $(a, b, d) = 1$.

Para ver que $\Psi_n \in \mathbb{Z}[X, Y]$ no se hizo ninguna distinción en función del valor de n, por tanto si $\Psi_n(X, Y) \in \mathbb{Z}[X, Y]$ para todo n entero positivo, también lo será para aquellos n's en cuya descomposición no aparecen potencias, es decir, $\Phi_n \in \mathbb{Z}[X, Y]$.

Proposición 3.2.4 *Si $z \in \mathbb{H}$ está en una extensión cuadrática de $\mathbb{Q}$, entonces $j(z)$ es un entero algebraico.*

Demostración: Si $z \in \mathbb{H}$ está en una extensión cuadrática imaginaria, entonces $\Lambda = \{m + nz\}$ tiene multiplicación compleja, es decir, $\exists\ \alpha \in \mathbb{C}/\mathbb{R}$ tal que $\alpha\Lambda \subset \Lambda$, entonces

$$\alpha z = az + b, \qquad \alpha = cz + d$$

con $a, b, c, d \in \mathbb{Z}$ tales que $(a, b, c, d) = 1$ (si $(a, b, c, d) = m$, se puede reducir a este caso tomando α/m).

Sea $\lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con $ad - bc = n$ para cierto n, entonces

$$\lambda \in M_n \quad \text{y} \quad \lambda z = \frac{az + b}{cz + d} = \frac{\alpha z}{\alpha} = z.$$

Se tiene que $j(\lambda z) = j(z)$ y por tanto

$$\Phi_n(j(\lambda z), j(z)) = \Phi_n(j(z), j(z)).$$

Por otra parte, por la Proposición 3.2.2, los ceros de $\Phi_n(X, j(z))$ son precisamente $j(\lambda z)$ con $\lambda \in M_n$ por tanto

$$\Phi_n(j(\lambda z), j(z)) = 0.$$

Es decir, $j(z)$ es un cero de $\Phi_n(x, x)$. El objetivo por tanto, es demostrar que o bien el polinomio $\Phi_n(x, x)$, o bien $-\Phi_n(x, x)$ es mónico.

El coeficiente del término de menor potencia en el desarrollo de cada factor es ± 1 o una raíz de la unidad, en cualquier caso, al evaluar en todas las combinaciones posibles de a, b, d y teniendo en cuenta que los coeficientes son enteros, el término de menor potencia en el desarrollo final será siempre ± 1 y por tanto dará lugar a un polinomio mónico. $\square$

De este modo, se ha probado que j manda irracionales cuadráticos en enteros algebraicos, lo que aporta más información sobre las curvas que poseen multiplicación compleja, concretamente, todas ellas (salvo isomorfismos sobre $\mathbb{C}$) están definidas sobre cuerpos de números.

Pasada la primera mitad del siglo XX se probó que sólo hay nueve cuerpos cuadráticos imaginarios con anillos de enteros de factorización única[3], resolviendo así una conjetura que provenía de los trabajos de Gauss. Entonces, salvo isomorfismos sobre $\mathbb{C}$, sólo hay nueve curvas elípticas sobre $\mathbb{Q}$ de multiplicación compleja (o más bien nueve familias de ellas por los subanillos que no estamos considerando y por isomorfismos).

[3] $\mathbb{Q}(\sqrt{d})$, donde $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

Capítulo 4

La curva elíptica $y^2 = x^3 - 35x - 98$

En lo sucesivo p será un primo $p > 7$ y E denotará la curva elíptica

$$E: \ y^2 = x^3 - 35x - 98.$$

También se considerará $\mathbb{Z}[\xi]$ con $\xi = (1+\sqrt{-7})/2$ que es el anillo de enteros de $\mathbb{Q}(\sqrt{-7})$ y es un dominio de factorización única.

4.1. La ecuación modular y el invariante j

En esta sección se probará que $j(\xi)$ es un entero sin apelar a la relación mencionada en el capítulo anterior con la factorización única. Esencialmente lo que haremos es resolver la ecuación modular para $n = 2$. Consideramos

$$P(x) = -\Psi_2(x, x) = -\Phi_2(x, x).$$

Proposición 4.1.1 *P es un polinomio mónico de grado 4 en $\mathbb{Z}[x]$ y $j(i)$ es una de sus raíces. Además, $j(i) = 1728$.*

Demostración:

$$P(j(z)) = -\Phi_2(j(z), j(z)) = -\left(j(z) - j(2z)\right)\left(j(z) - j(z/2)\right)\left(j(z) - j((z+1)/2)\right)$$

$$j(z) - j(2z) = e(-z) + \sum_{k=0}^{\infty} a_k e(kz) - e(-2z) - \sum_{k=0}^{\infty} a_k e(2k)$$

$$j(z) - j(z/2) = e(-z) + \sum_{k=0}^{\infty} a_k e(kz) - e(-z/2) - \sum_{k=0}^{\infty} a_k \, e\big(kz/2\big)$$

$$j(z) - j((z+1)/2) = e(-z) + \sum_{k=0}^{\infty} a_k e(kz) - \ e\big(-(z+1)/2\big) - \sum_{k=0}^{\infty} a_k \ e\big(k(z+1)/2\big).$$

En la Proposición 3.1.4, se vio cómo la menor potencia en el desarrollo se corresponde con el grado del polinomio en $j(z)$, dicho término será el producto de los correspondientes términos de menor grado en cada uno de los factores, en este caso $e(-2z)e(-z)e(-z) = e(-4z)$, entonces es claro que $P(x) = -\Phi_2(x,x)$ será un polinomio de grado 4 y mónico.

Para ver que $j(i)$ es una raíz de $P(x) = -\Phi_2(x,x)$ repetimos los pasos dados en la demostración de la Proposición 3.2.4.
Si se considera $z = i$, $\Lambda = \{m + ni\}$ tiene multiplicación compleja, tomando $\alpha = i + 1$

$$\alpha i = -1 + i = ai + b, \qquad \alpha = i + 1 = ci + d$$

$$\Rightarrow a = 1,\ b = -1,\ c = 1,\ d = 1$$

Sea $\lambda = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in M_2$, entonces

$$\lambda i = \frac{i-1}{i+1} = \frac{\alpha i}{i} = i \quad \Rightarrow \quad j(\lambda i) = j(i)$$

$$\Rightarrow -\Phi_2(j(\lambda i), j(i)) = -\Phi_2(j(i), j(i)) = P(j(i)).$$

Aplicando la Proposición 3.2.2, (los ceros de $\Phi_n(X, j(z))$ son $j(\lambda z)$ con $\lambda \in M_n$)

$$\Rightarrow P(j(i)) = -\Phi_2(j(\lambda i), j(i)) = 0.$$

Es decir, $j(i)$ es un cero de $P(x) = -\Phi_2(x,x)$.

Por otro lado,

$$j(z) = \frac{1728 E_4^3(z)}{E_4^3(z) - E_6^2(z)} \qquad \text{donde} \quad E_{2k}(z) = \frac{1}{2} \sum_{\substack{n,m=-\infty \\ (n,m)=1}}^{\infty} \frac{1}{(mz+n)^{2k}}.$$

Sea $\Lambda = \{mi + n \ : \ m, n \in \mathbb{Z}, (n,m) = 1\}$, entonces se tiene que $i\Lambda = \Lambda$ y por tanto

$$E_6(i) = \frac{1}{2} \sum_{\substack{n,m=-\infty \\ (n,m)=1}}^{\infty} \frac{1}{(mi+n)^6} = \frac{1}{2} \sum_{\substack{n,m=-\infty \\ (n,m)=1}}^{\infty} \frac{1}{(i(mi+n))^6} =$$

$$= -\frac{1}{2} \sum_{\substack{n,m=-\infty \\ (n,m)=1}}^{\infty} \frac{1}{(mi+n)^6} = -E_6(i) \quad \Rightarrow E_6(i) = 0$$

$$\Longrightarrow j(i) = \frac{1728 E_4^3(i)}{E_4^3(i)} = 1728.$$

□

Las soluciones de $\Psi_2\big(x, j(z)\big) = 0$ son $x = j(\gamma z)$ con $\gamma \in \mathcal{M}_{2\times 2}(\mathbb{Z})$ y $\det \gamma = 2$. De aquí $\Phi_2\big(j((2\gamma^{-1})z), j(z)\big) = 0$ y cambiando la variable $z \mapsto \gamma z$ se tiene $\Phi_2\big(j(z), j(\gamma z)\big) = 0$. Entonces $\Phi_2\big(x, j(z)\big) = 0$ y $\Phi_2\big(j(z), x\big) = 0$ tienen las mismas raíces. De ello se deduce fácilmente la simetría $\Phi_2(X, Y) = \Phi_2(Y, X)$ que, con prácticamente la misma prueba, es en realidad una propiedad general de Φ_n para $n > 1$.

Proposición 4.1.2 *$j(\xi)$ es raíz doble de $P(x)$.*

Demostración:

$$P(j(\xi)) = -\Phi_2(j(\xi), j(\xi)) = -\left(j(\xi) - j(\delta_1\xi)\right)\left(j(\xi) - j(\delta_2\xi)\right)\left(j(\xi) - j(\delta_3\xi)\right)$$

donde $\delta_1 = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right),\ \delta_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right),\ \delta_3 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 2 \end{smallmatrix}\right) \in \Delta_2$.

Un par de observaciones, sobre el factor $j(\xi) - j(\delta_2\xi)$,

- $\delta_2 = \gamma\lambda$ con $\gamma = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ y $\lambda = \left(\begin{smallmatrix} 1 & -2 \\ 1 & 0 \end{smallmatrix}\right)$ tal que $\lambda\xi = \xi$.

$$\Rightarrow j(\delta_2\xi) = j(\gamma\lambda\xi) = j(\gamma\xi).$$

- Usando que $j(z)$ es modular, $j(\gamma\xi) = j(\xi)$.

Se tiene entonces que $j(\xi) - j(\delta_2\xi) = 0$ y por tanto $j(\xi)$ es raíz de $P(x)$.

Con un argumento similar para el factor $j(\xi) - j(\delta_3\xi)$,

- $\delta_3 = \gamma'\lambda'$ con $\gamma' = \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ y $\lambda' = \left(\begin{smallmatrix} 0 & -2 \\ 1 & -1 \end{smallmatrix}\right)$ tal que $\lambda'\xi = \xi$.

$$\Rightarrow j(\delta_3\xi) = j(\gamma'\lambda'\xi) = j(\gamma'\xi).$$

- Usando que $j(z)$ es modular, $j(\gamma'\xi) = j(\xi)$.

Se tiene entonces que $j(\xi) - j(\delta_3\xi) = 0$.

$$\begin{aligned}
\Phi_2(X, j(\xi)) &= \left(X - j(\delta_1\xi)\right)\left(X - j(\delta_2\xi)\right)\left(X - j(\delta_3\xi)\right). \\
\frac{\partial\Phi_2}{\partial X}\left(X, j(\xi)\right) &= -j(\delta_1\xi)\left(X - j(\delta_2\xi)\right)\left(X - j(\delta_3\xi)\right) + \\
&\quad + \left(X - j(\delta_1\xi)\right)\left(-j(\delta_2\xi)\left(X - j(\delta_3\xi)\right) - j(\delta_3\xi)\left(X - j(\delta_2\xi)\right)\right).
\end{aligned}$$

Aplicando las observaciones anteriores,

$$\frac{\partial\Phi_2}{\partial X}\big(j(\xi), j(\xi)\big) = 0.$$

Como $\Phi(X,Y) = \Phi(Y,X)$,

$$\frac{\partial \Phi_2}{\partial Y}\big(X,Y\big) = \frac{\partial \Phi_2}{\partial Y}\big(Y,X\big) = \frac{\partial \Phi_2}{\partial X}\big(X,Y\big)$$

$$\Rightarrow P'\big(j(\xi)\big) = \left(\frac{\partial \Phi_2}{\partial X} + \frac{\partial \Phi_2}{\partial Y}\right)\big(j(\xi), j(\xi)\big) = 0$$

de donde se concluye que $j(\xi)$ es raíz doble de $P(x)$.

□

Llegamos así al objetivo de la sección,

Proposición 4.1.3 *$j(\xi)$ es un entero.*

Demostración: Por la Proposición 3.2.3 sabemos que $P(x) \in \mathbb{Z}[x]$, que es mónico lo vimos en la demostración de la Proposición 3.2.4.

Usando ahora el *Lema de Gauss* se tiene que $\mathrm{mcd}(P, P') \in \mathbb{Z}[x]$ y es mónico. Puesto que P tiene una raíz doble, $j(\xi)$, entonces $\mathrm{mcd}(P, P') = x - j(\xi)$ llegando así al resultado.
□

Con la ayuda de una calculadora, unos pocos términos del numerador y denominador de la fórmula $j(z) = \big(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)e(nz)\big)^3/\Delta(z)$ dan una aproximación de $j(\xi)$ y el resultado anterior permite llegar a nuestro objetivo.
$\xi = \frac{1+i\sqrt{7}}{2}$, llamando $q = e^{-\pi\sqrt{7}}$,

$$e(n\xi) = e^{2\pi i\xi} = e^{n\pi i}e^{-\pi n\sqrt{7}} = (-1)^n q^n.$$

$$1 + 240\sum_{n=1}^{\infty}\sigma_3(n)e(nz) = 1 + 240(-q + 9q^2 - 28q^3 + 53q^4 - \dots) \simeq 0{,}941189901$$

$$\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)e(nz)\right)^3 \simeq 0{,}833742185$$

$$\prod_{n=1}^{\infty}(1 - e(n\xi))^{24} = (1+q)^{24}(1-q^2)^{24}(1+q^3)^{24}\cdot\ldots \simeq 1{,}005909227$$

$$e(\xi)\prod_{n=1}^{\infty}(1 - e(n\xi))^{24} \simeq -0{,}000247034$$

$$\Rightarrow j(\xi) \simeq -3375{,}009857$$

Usando que $j(\xi)$ es entero, podemos entonces asegurar que

$$j(\xi) = -3375.$$

Proposición 4.1.4 *El invariante j de E es -3375, en particular E es $\mathbb{C}/\Lambda$ con $\Lambda = \{\omega_1(m+n\xi)\}$.*

Demostración:

$$E:\ y^2 = x^3 - 35x - 98.$$

$$j = \frac{6912(-35)^3}{4(-35)^3 + 27(-98)^2} = \frac{-29635200}{-171500 + 259308} = -3375.$$

Por otro lado, $\Lambda = \{\omega_1(m+n\xi)\} = \{m\omega_1 + n\omega_1\xi\} = \{m+n\xi\}$, y acabamos de ver que el invariante de la curva elíptica asociada a este retículo es $j(\xi) = j(\frac{1+\sqrt{-7}}{2}) = -3375$.

Puesto que dos curvas elípticas son isomorfas si y sólo si tienen el mismo invariante, $E \simeq \mathbb{C}/\Lambda$. □

4.2. Endomorfismo de Frobenius

La aplicación $x \mapsto x^p$ pertenece a $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ y cuando se considera E sobre $\overline{\mathbb{F}}_p$ induce un endomorfismo de E dado por $\mathrm{Frob}(x,y) = (x^p, y^p)$, $\mathrm{Frob}(O) = O$ llamado *endomorfismo de Frobenius*. El interés de Frob es que sus puntos fijos cuando actúa sobre una curva algebraica corresponden a soluciones módulo p.

$\wp(\xi z)$ se puede escribir como una función racional de $\wp(z)$ y eso se traduce en un endomorfismo $\phi : E \longrightarrow E$, una simetría oculta se corresponde con la multiplicación por ξ en $\mathbb{C}/\Lambda$. El procedimiento para hallar dicha función racional, y por tanto ϕ, es constructivo. La fórmula resultante para el endomorfismo es

$$\phi(x,y) = \left(\overline{\xi}^{-2}\big(x - \frac{7\xi^4}{x+3+\xi}\big), \overline{\xi}^{-3} y\big(1 + \frac{7\xi^4}{(x+3+\xi)^2}\big)\right)$$

donde $\overline{\xi}$ es el conjugado de ξ.

En particular E es una curva CM con anillo de multiplicación compleja $\mathbb{Z}[\xi]$ y todos los endomorfismos de E sobre $\mathbb{C}$ son de la forma $f(P) = [n]P + [m]\phi(P)$ con $n, m \in \mathbb{Z}$ donde $[n]$ significa el endomorfismo multiplicación por n (en la curva elíptica). Continuando con esta notación denotaremos en lo sucesivo a f con $[n + m\xi]$.

Si $\left(\frac{-7}{p}\right) = 1$ (-7 es residuo cuadrático módulo p), llamando $\alpha \in \mathbb{F}_p$ a la solución de la congruencia $x^2 \equiv -7 \pmod{p}$, se tiene

$$\xi = \frac{1+\sqrt{-7}}{2} \equiv 2^{-1}(1+\alpha) \pmod{p},$$

entonces el endomorfismo de E sobre $\mathbb{C}$ dado por $[n+m\xi]$ induce también un endomorfismo de E sobre $\mathbb{F}_p$, que para no complicar la notación seguiremos llamando $[n+m\xi]$.

Observación: Esta situación ya vimos en (2.5) que ocurre si y sólo si $p \equiv 1, 2, 4 \pmod{7}$.

Deuring demostró que si en una curva elíptica de multiplicación compleja todos los endomorfismos sobre $\mathbb{C}$ inducen endomorfismos sobre $\mathbb{F}_p$ entonces todos los endomorfismos sobre $\mathbb{F}_p$ (y sobre $\overline{\mathbb{F}}_p$) se obtienen de esta forma. Esto sugiere distinguir para E dos casos: $\left(\frac{-7}{p}\right) = 1$ en el que Frob $= [n_0 + m_0\xi]$ para ciertos $n_0, m_0 \in \mathbb{Z}$ y $\left(\frac{-7}{p}\right) = -1$ en el que no se asegura que Frob provenga de un endomorfismo de E sobre $\mathbb{C}$.

Nuestro objetivo en ambos casos es hallar N_p, el número de puntos de E en $\mathbb{F}_p$ incluyendo O, es decir,

$$N_p = 1 + \#\{(x, y) \ : \ 0 \leq x, y < p, \ y^2 \equiv x^3 - 35x - 98 \pmod{p}\}. \tag{4.1}$$

Para ello emplearemos el endomorfismo definido por $H(P) = P - \text{Frob}(P)$ que verifica $N_p = \#H^{-1}(\{O\}) = \#\text{Ker } H$.

En geometría algebraica, un morfismo de curvas algebraicas definidas sobre un cuerpo K, $f : C_1 \to C_2$, induce un monomorfismo $K(C_2) \to K(C_1)$ que nos permite considerar a $K(C_1)$ como una extensión algebraica de $K(C_2)$. Usando que la extensión es finita[1], se define el *grado* de f como $\deg f = |K(C_1) : K(C_2)|$. Si $\deg f = n$, entonces cada punto de C_2 tiene a lo sumo n preimágenes en C_2.

Cuando K es algebraicamente cerrado, $K = \overline{K}$, el grado de f coincide con el número de preimágenes de un punto contando multiplicidades (índices de ramificación). Se dice que f es no ramificada si lo es en todo punto.

Los endomorfismos de curvas elípticas sobre $\mathbb{C}$ son no ramificados, y por tanto todo punto de E tiene exactamente $\deg f$ preimágenes. Frob es inyectivo pero tiene grado p, entonces el mismo resultado no se aplica en general sobre $\overline{\mathbb{F}}_p$, esto se debe esencialmente a que $x^p = \alpha$ tiene p raíces iguales en $\overline{\mathbb{F}}_p$. Sin embargo se puede probar que las únicas excepciones son Frob y en general $f \circ \text{Frob}$. Estos endomorfismos son *inseparables*, y el resto *separables*.

Observación: Para $p > 7$ primo, no tenemos problemas pues el grado de un endomorfismo de E definido sobre $\mathbb{C}$ es igual al grado cuando lo consideramos definido sobre $\overline{\mathbb{F}}_p$. Esto se debe a que los únicos primos que darían problemas son $p = 7$, pues en este caso denominador y numerador no conservarían el grado al tomar módulos y $p = 2$, donde tendríamos problemas para definir ξ.

[1] $K(C_1)$ es finitamente generado sobre K.

4.2.1. Caso $\left(\frac{-7}{p}\right) = 1$

(o equivalentemente $p \equiv 1, 2, 4$ módulo 7).

Comenzamos recordando que para $\alpha \in \mathbb{Q}(\sqrt{-7})$, la *norma* de α se define como

$$N_{\mathbb{Q}(\sqrt{-7})}(\alpha) = N_{\mathbb{Q}(\sqrt{-7})/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha}$$

donde $\overline{\alpha}$ es el conjugado de α.

Proposición 4.2.1 *Si* $\alpha \in \mathbb{Z}[\xi] \Rightarrow N_{\mathbb{Q}(\sqrt{-7})}(\alpha) \in \mathbb{Z}$.

Por otro lado, dado $\mathfrak{a} \subset \mathbb{Z}[\xi]$ ideal, la *norma* de $\mathfrak{a}$ viene dada por

$$N_{\mathbb{Q}(\sqrt{-7})}(\mathfrak{a}) = \#\mathbb{Z}[\xi]/\mathfrak{a}.$$

Además, si $\alpha \in \mathbb{Z}[\xi]$ es tal que $\langle\alpha\rangle = \mathfrak{a}$ entonces,

$$N_{\mathbb{Q}(\sqrt{-7})}(\mathfrak{a}) = N_{\mathbb{Q}(\sqrt{-7})}(\langle\alpha\rangle) = N_{\mathbb{Q}(\sqrt{-7})}(\alpha).$$

El grado de la función $[n+m\xi]$ coincide con el número de preimágenes de $z \mapsto (n+m\xi)z$ actuando en $\mathbb{C}/\mathbb{Z}[\xi]$. Este número coincide con el número de veces que $\mathbb{Z}[\xi]$ contiene a $(n+m\xi)\mathbb{Z}[\xi]$, es decir, el número de elementos del anillo cociente $\mathbb{Z}[\xi]/(n+m\xi)\mathbb{Z}[\xi]$, y por tanto

$$\deg[n+m\xi] = N_{\mathbb{Q}(\sqrt{-7})}(\langle n+m\xi\rangle) = (n+m\xi)\overline{(n+m\xi)} = |n+m\xi|^2 =$$

$$= \left(n+\frac{m}{2}\right)^2 + \left(\frac{m\sqrt{7}}{2}\right)^2 = n^2 + nm + \frac{m^2}{4} + \frac{7m^2}{4} = n^2 + mn + 2m^2.$$

Recordando que en este caso Frob $= [n_0 + m_0\xi]$ para ciertos $n_0, m_0 \in \mathbb{Z}$, y que el endomorfismo de Frobenius tiene grado p primo se tiene

$$N_{\mathbb{Q}(\sqrt{-7})}(n_0 + m_0\xi) = p.$$

Observación: Si $\mathfrak{a}, \mathfrak{b} \in \mathbb{Z}[\xi]$ ideales, entonces $N_{\mathbb{Q}(\sqrt{-7})}(\mathfrak{ab}) = N_{\mathbb{Q}(\sqrt{-7})}(\mathfrak{a})N_{\mathbb{Q}(\sqrt{-7})}(\mathfrak{b})$, de donde $\mathfrak{a} \subset \mathfrak{b} \Leftrightarrow N_{\mathbb{Q}(\sqrt{-7})}(\mathfrak{b}) \mid N_{\mathbb{Q}(\sqrt{-7})}(\mathfrak{a})$

Si $\mathfrak{a}, \mathfrak{b}$ son ideales de $\mathbb{Z}[\xi]$ de normas r y s respectivamente, tales que $\mathfrak{ab} \subset n_0 + m_0\xi$, entonces $p \mid rs$, usando ahora la primalidad de p se tiene que $\mathfrak{a} \subset n_0 + m_0\xi$ o bien $\mathfrak{b} \subset n_0 + m_0\xi$ y por tanto llegamos a que $n_0 + m_0\xi$ es un primo (de norma p) de $\mathbb{Z}[\xi]$.

$$H(P) = P - \text{Frob}(P) = [1]P - [n_0 + m_0\xi]P = [1 - n_0 - m_0\xi]P.$$

Como $N_p = \#H^{-1}(\{O\}) = \#\text{Ker } H$, podemos buscar el número de preimágenes del elemento $O \in E$, puesto que H es separable, dicho número coincide con $\deg H = \deg[1-$

$n_0 - m_0\xi]$, que como ya se vio antes, se corresponde con la norma del ideal $1 - n_0 - m_0\xi$, es decir,

$$N_p = \deg[1 - n_0 - m_0\xi] = |1 - n_0 - m_0\xi|^2 = (1 - n_0)^2 + (1 - n_0)(-m_0) + 2m_0^2.$$

Frob $= [n_0 + m_0\xi]$ es de grado p y por tanto $n_0^2 + n_0m_0 + 2m_0^2 = p$, entonces

$$N_p = 1 + n_0^2 - 2n_0 - m_0 + n_0m_0 + 2m_0^2 = 1 + p - (2n_0 + m_0).$$

Supongamos ahora que n y m satisfacen $n^2 + nm + 2m^2 = p = n_0^2 + n_0m_0 + 2m_0^2$ entonces es claro que $(n+m\xi)\overline{(n + m\xi)} = (n_0+m_0\xi)\overline{(n_0 + m_0\xi)}$. Usando la factorización única de $\mathbb{Z}[\xi]$ junto con que las unidades de $\mathbb{Z}[\xi]$ son ± 1, llegamos a que o bien $n_0+m_0\xi = \pm(n + m\xi)$ o bien $n_0 + m_0\xi = \pm\overline{(n + m\xi)}$,

$$\text{Si } n_0 + m_0\xi = n + m\xi \;\Rightarrow\; \begin{cases} n_0 = n \\ m_0 = m \end{cases}$$

$$\text{Si } n_0 + m_0\xi = \overline{(n + m\xi)} \;\Rightarrow\; \begin{cases} n_0 + m_0/2 = n + m/2 \\ m_0/2 = -m/2 \end{cases} \Rightarrow \begin{cases} n_0 = n + m \\ m_0 = -m \end{cases}$$

En ambos casos el resultado es $2n_0 + m_0 = 2n + m$.

$$\text{Si } n_0 + m_0\xi = -(n + m\xi) \;\Rightarrow\; \begin{cases} n_0 = -n \\ m_0 = -m \end{cases}$$

$$\text{Si } n_0 + m_0\xi = -\overline{(n + m\xi)} \;\Rightarrow\; \begin{cases} n_0 + m_0/2 = -n - m/2 \\ m_0/2 = m/2 \end{cases} \Rightarrow \begin{cases} n_0 = -n - m \\ m_0 = m \end{cases}$$

En ambos casos el resultado es $2n_0 + m_0 = -(2n + m)$.

Finalmente, como $N_p = |1 - n_0 - m_0\xi|^2 = p + 1 - (2n_0 + m_0)$, entonces

$$N_p - p - 1 = \pm(2n + m).$$

El último cálculo determina $N_p - p - 1$ salvo un signo.

La determinación del signo pasa por el cálculo explícito de $E[\sqrt{-7}]$, que es el grupo de puntos sobre $\mathbb{C}$ (incluyendo O) que cumplen $[\sqrt{-7}]P = O$, es decir, $[-1 + 2\xi]P = O$.

$[\sqrt{-7}]P = O$ equivale a $[\xi]P = [\overline{\xi}]P$ y esto a $\phi(P) = \overline{\phi}(P)$ donde $\overline{\phi}(P)$ tiene la misma fórmula que ϕ pero cambiando ξ por $\overline{\xi}$. La primera coordenada de la ecuación $\phi(x, y) = \overline{\phi}(x, y)$ lleva a que x satisface la ecuación cúbica

$$\overline{\xi}^{-2}\big(x - 7\xi^4/(x + 3 + \xi)\big) = \xi^{-2}\big(x - 7\overline{\xi}^4/(x + 3 + \overline{\xi})\big),$$

cuyas raíces son $x = a_k - 1$ con $a_k = 8\cos(2\pi k/7)$ y $k = 1, 2, 4$. Despejando y se obtiene $E[\sqrt{-7}] = \{O, P, 2P, 3P, 4P, 5P, 6P\}$ donde

$$\begin{aligned} &P = (a_1 - 1, \sqrt{-7}a_1), && 2P = (a_4 - 1, \sqrt{-7}a_4), && 3P = (a_2 - 1, -\sqrt{-7}a_2), \\ &4P = (a_2 - 1, \sqrt{-7}a_2), && 5P = (a_4 - 1, -\sqrt{-7}a_4), && 6P = (a_1 - 1, -\sqrt{-7}a_1). \end{aligned}$$

Estos puntos se pueden "reducir" a $\overline{\mathbb{F}}_p$ asignando a $e^{2\pi i/7}$ una raíz ($\neq 1$) de $x^7 = 1$ que seguiremos denotando con $e^{2\pi i/7}$ y a_k será $4\big((e^{2\pi i/7})^k + (e^{2\pi i/7})^{-k}\big)$, en particular Frob actuará sobre ellos.

El endomorfismo de E sobre $\overline{\mathbb{F}}_p$ es el dado por $\mathrm{Frob}(x, y) = (x^p, y^p)$, $\mathrm{Frob}(O) = O$. Si $P = (a_1 - 1, \sqrt{-7}a_1)$ en $\overline{\mathbb{F}}_p$, entonces

$$\mathrm{Frob}(P) = \mathrm{Frob}(a_1 - 1, \sqrt{-7}a_1) = ((a_1 - 1)^p, (\sqrt{-7}a_1)^p).$$

Estudiando primera y segunda coordenada por separado,

- Usando el binomio de Newton,

$$(a_1 - 1)^p = \binom{p}{0}a_1^p + \binom{p}{1}a_1^{p-1}(-1) + \cdots + \binom{p}{p-1}a_1(-1)^{p-1} + \binom{p}{p}(-1)^p$$

  y que el número combinatorio se define por

$$\binom{p}{n} = \frac{p(p-1)\cdots(p-n+1)}{n!},$$

  excepto el primero y el último, todos estos términos desaparecen en $\mathbb{F}_p$. Por tanto

$$(a_1 - 1)^p = a_1^p - 1.$$

- -7 es residuo cuadrático módulo p, sea α la solución de la congruencia $x^2 \equiv -7 \pmod{p}$, entonces la segunda coordenada quedará

$$(\sqrt{-7}a_1)^p = (\sqrt{-7})^p a_1^p = \alpha^p a_1^p = \alpha a_1^p = \sqrt{-7}a_1^p,$$

  donde se ha utilizado el *pequeño teorema de Fermat* para ver que $\alpha^p \equiv \alpha \pmod{p}$.

  Por último, como $a_1 = 4\big(e^{2\pi i/7} + (e^{2\pi i/7})^{-1}\big)$ entonces $a_1^p = 4^p\big(e^{2\pi i/7} + (e^{2\pi i/7})^{-1}\big)^p$, y de nuevo usando el desarrollo del binomio de Newton y el *pequeño teorema de Fermat* llegamos a que

$$a_1^p = a_p.$$

Se tiene entonces que

$$\text{Frob}(P) = (a_p - 1, \sqrt{-7}a_p).$$

Definición: Para cada $Q \in E[\sqrt{-7}]$ se define $s(Q)$ como el signo que acompaña a $\sqrt{-7}a_k$ en la segunda coordenada.

Observación: Si $7 \nmid k$,

$$s(kP) = \left(\frac{k}{7}\right) = \begin{cases} 1 & \text{si } \ k = 1, 2, 4 \\ -1 & \text{si } \ k = 3, 5, 6 \end{cases}$$

Como

$$[n_0 + \frac{m_0}{2}]P = [n_0 + \frac{m_0}{2}]P + O = [n_0 + \frac{m_0}{2}]P + [\frac{m_0}{2}\sqrt{-7}]P =$$

$$= [n_0 + m_0\xi]P = \text{Frob}(P) = (a_p - 1, \sqrt{-7}a_p)$$

es claro que en este caso se debe cumplir

$$s\big([n_0 + \frac{m_0}{2}]P\big) = 1$$

y esta condición es equivalente a

$$\left(\frac{n_0 + \frac{m_0}{2}}{7}\right) = \left(\frac{\frac{2n_0+m_0}{2}}{7}\right) = 1.$$

Por último, observando que

$$\left(\frac{2n_0 + m_0}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{\frac{2n_0+m_0}{2}}{7}\right)$$

y que 2 es residuo cuadrático módulo 7, es decir $\left(\frac{2}{7}\right) = 1$, se tiene

$$\left(\frac{2n_0 + m_0}{7}\right) = 1 \Leftrightarrow \left(\frac{\frac{2n_0+m_0}{2}}{7}\right) = 1.$$

Conclusión:

Si $p \equiv 1, 2, 4 \ (mod\ 7)$ entonces p se puede escribir como $n^2 + mn + 2m^2$ y se tiene

$$N_p = p + 1 - \left(\frac{2n + m}{7}\right)(2n + m).$$

4.2.2. Caso $\left(\frac{-7}{p}\right) = -1$

(o equivalentemente $p \equiv 3, 5, 6$ módulo 7).

Procederemos en dos fases: la primera es que $E[p]$, el grupo de puntos en $\overline{\mathbb{F}}_p$ que cumplen $[p]P = O$, es trivial, mientras que en la segunda obtendremos que si $E[p] = \{O\}$ entonces $N_p = p+1$. Esto último no requiere la multiplicación compleja y es un resultado general de curvas elípticas.

En el razonamiento aparecerá el *endomorfismo dual*. Dado un endomorfismo f se define su dual $\widehat{f}$ como el endomorfismo que asigna a cada punto la suma de las coordenadas de sus preimágenes. Como en el caso del grado esta definición es literalmente válida para $\mathbb{C}$ y para endomorfismos separables definidos sobre $\overline{\mathbb{F}}_p$. Para Frob de nuevo el problema de que $x^p = \alpha$ tenga p raíces iguales en $\overline{\mathbb{F}}_p$ lleva a que la definición correcta sea $\widehat{\mathrm{Frob}}(x, y) = [p](x^{1/p}, y^{1/p})$ que se extiende de manera natural a cualquier endomorfismo inseparable (con $\widehat{f \circ \mathrm{Frob}} = \widehat{\mathrm{Frob}} \circ \widehat{f}$). Está claro que $\widehat{f} \circ f = [\deg f]$ y $\widehat{f \circ g} = \widehat{g} \circ \widehat{f}$. Una propiedad más complicada, pero creíble, es $\widehat{f+g} = \widehat{f} + \widehat{g}$ cuya prueba requiere un poco de geometría algebraica.

Si consideramos $E[p]$ sobre $\mathbb{C}$ sería $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pero al "reducir" a $\overline{\mathbb{F}}_p$ algunos puntos se podrían pegar, por tanto $E[p]$ sobre $\overline{\mathbb{F}}_p$ es isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, a $\mathbb{Z}/p\mathbb{Z}$ o a $\{O\}$. Veamos que los dos primeros casos son imposibles.

$$\widehat{\mathrm{Frob}} \circ \mathrm{Frob} = [\deg \mathrm{Frob}] = [p]$$
$$\Rightarrow \deg\left(\widehat{\mathrm{Frob}} \circ \mathrm{Frob}\right) = \deg \widehat{\mathrm{Frob}} \deg \mathrm{Frob} = p^2 \Rightarrow \deg \widehat{\mathrm{Frob}} = p.$$

Por otro lado,

$$E[p] = [p]^{-1}(O) = \left(\widehat{\mathrm{Frob}} \circ \mathrm{Frob}\right)^{-1}(O) = \left(\mathrm{Frob}^{-1} \circ \widehat{\mathrm{Frob}}^{-1}\right)(O).$$

De la inseparabilidad de Frob se tiene que $\mathrm{Frob}^{-1}(O) = \{O\}$. Además, el número de preimágenes del elemento O por $\widehat{\mathrm{Frob}}$, será siempre menor o igual que el grado de $\widehat{\mathrm{Frob}}$, por lo tanto

$$\#E[p] \leq \#\left(\widehat{\mathrm{Frob}}\right)^{-1}(O) \leq \deg \widehat{\mathrm{Frob}} = p < p^2$$

lo que nos permite asegurar que

$$E[p] \ncong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

El endomorfismo ϕ induce un endomorfismo en E sobre $\overline{\mathbb{F}}_p$ y cumple $\phi \circ \phi + [2] = \phi$

$$\xi^2 = \left(\frac{1+\sqrt{-7}}{2}\right)^2 = \frac{1+2\sqrt{-7}-7}{4} = -2 + \frac{1+\sqrt{-7}}{2} = -2 + \xi$$

como $[\xi] = \phi$, es claro que

$$\phi \circ \phi = [\xi^2] = [-2+\xi] = -[2] + [\xi] = -[2] + \phi$$

y por tanto

$$\phi \circ \phi + [2] = \phi.$$

Sea $n \in \mathrm{End}(\mathbb{Z}/p\mathbb{Z})$ el endomorfismo multiplicar por n, (los posibles endomorfismos son todos de esta forma), si $n \neq 0$ fuera tal que $n^2 + 2 \equiv n \pmod p$ se tendría que $n^2 - n + 2 = kp$ en $\mathbb{Z}$ pero $\sqrt{b^2 - 4ac} = \sqrt{-7 + 4kp} \notin \mathbb{Z}$ pues -7 no es residuo cuadrático módulo p.

Por tanto,

$$E[p] \ncong \mathbb{Z}/p\mathbb{Z}.$$

Dadas dos curvas elípticas $E : y^2 = x^3 + ax + b$, $E' : y^2 = x^3 + z'x + b'$, no podemos hacer cambios de grado mayor o igual que uno para pasar de una a otra porque no serían invertibles, y entre los cambios lineales sólo aquellos de la forma $y \mapsto \lambda^3 y$, $x \mapsto \lambda^2 x$ preservan la forma de la ecuación cúbica. Así pues la única posibilidad para que sean isomorfas es que $a' = \lambda^{-4}a$ y $b' = \lambda^{-6}b$.

Para cualquier curva elíptica que no sea de la forma $y^2 = x^3 + Ax$ o $y^2 = X^3 + B$, $[1]$ y $[-1]$ son los únicos endomorfismos invertibles[2], esto es, automorfismos.

Suponemos que $E[p]$ es trivial (sobre $\overline{\mathbb{F}}_p$), tal y como aseguran los cálculos anteriores.

Puesto que $E[p] = \{0\}$, entonces $\widehat{\mathrm{Frob}}$ es inseparable y por tanto, debe ser igual a algún $f \circ \mathrm{Frob}$. Tomando grados se tiene que $\deg f = 1$, es decir, f es un automorfismo.

Por otro lado, como E es de la forma $y^2 = x^3 - 35x - 98$ los únicos automorfismos son $[1]$ y $[-1]$, de modo que o bien $\widehat{\mathrm{Frob}} = \mathrm{Frob}$ o bien $\widehat{\mathrm{Frob}} = [-1]\mathrm{Frob}$.

Desarrollando $[\deg H] = \widehat{H} \circ H$ con la fórmula para H,

$$H = [1] - \mathrm{Frob}, \quad \widehat{H} = \widehat{[1] - \mathrm{Frob}} = [1] - \widehat{\mathrm{Frob}}$$

$$[\deg H] = \widehat{H} \circ H = \big([1] - \widehat{\mathrm{Frob}}\big) \circ \big([1] - \mathrm{Frob}\big) =$$

$$= [1] - \widehat{\mathrm{Frob}} - \mathrm{Frob} + \widehat{\mathrm{Frob}} \circ \mathrm{Frob} = [1] + [p] - \widehat{\mathrm{Frob}} - \mathrm{Frob}.$$

[2]Si $a, b \neq 0$ los λ posibles son $\lambda = \pm 1$.

Usando que $N_p = \deg H$ se tiene que

$$\widehat{\text{Frob}} + \text{Frob} = [1 + p - N_p].$$

Si $\widehat{\text{Frob}} = \text{Frob}$, entonces

$$\widehat{\text{Frob}} + \text{Frob} = [2]\text{Frob} = [1 + p - N_p].$$

Por un lado,

$$\deg[2]\text{Frob} = \deg[2] \deg \text{Frob} = 4p.$$

Por otro,

$$\deg[1 + p - N_p] = (1 + p - N_p)^2$$

donde se ha utilizado que $1 + p - N_p$ es entero y por tanto la norma coincide con el cuadrado del elemento.

Comparando normas llegamos a una contradicción pues $4p$ no es un cuadrado perfecto. Por tanto $\widehat{\text{Frob}} = [-1]\text{Frob}$, de donde

$$\widehat{\text{Frob}} + \text{Frob} = [0] = [1 + p - N_p] \quad \Rightarrow \; N_p = p + 1.$$

Conclusión:

Si $p \equiv 3, 5, 6 \ (mod\ 7)$ *entonces* $N_p = p + 1$.

4.3. Forma modular asociada a la curva

Dada la curva elíptica $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$, N_p es su número de puntos sobre $\mathbb{F}_p$ (es decir, las soluciones módulo p) contando el punto del infinito O. Se define

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

El teorema de modularidad, en una forma débil, afirma que los a_p son los coeficientes p-ésimos de una forma modular de peso 2 con respecto a algún grupo $\Gamma_0(N)$.

Para nuestra curva procederemos en dos fases: primero veremos que los a_p son los coeficientes de cierta serie de Fourier (Prop. 4.3.1) y finalmente probaremos que dicha serie define una forma modular (Prop. 4.3.4).

Proposición 4.3.1 *Para la curva* $E: y^2 = x^3 - 35x - 98$, a_p *coincide con el coeficiente de Fourier p-ésimo de*

$$\Xi(z) = \frac{1}{2} \sum_{n,m \in \mathbb{Z}} n \left(\frac{n}{7}\right) e\big((n^2 + 7m^2)z\big).$$

Demostración: El coeficiente p-ésimo de Ξ es $n\left(\frac{n}{7}\right)$, donde n ha de cumplir que $n^2 + 7m^2 = p$.

Por el Teorema 2.5.4, $n^2 + 7m^2 = p$ tiene solución si y sólo si $p = 7$ o bien $p \equiv 1, 2, 4 \pmod 7$.

- Si $p = 2, 3, 5$ entonces $n^2 + 7m^2 = p$ no tiene soluciones enteras, por tanto el p-ésimo coeficiente de Ξ es 0.

  Recordando que la curva E viene dada por $y^2 = x^3 - 35x - 98$ y la definición de N_p por (4.1), calculamos su valor en estos casos,

  $p = 2$

  $$y^2 \equiv x^3 + x \pmod 2$$
  $$\Rightarrow N_2 = 1 + \#\{(0,0),(1,0)\} = 3 \quad \Rightarrow a_2 = 2 + 1 - N_2 = 0.$$

  $p = 3$

  $$y^2 \equiv x^3 + x + 1 \pmod 3$$
  $$\Rightarrow N_3 = 1 + \#\{(0,1),(0,2),(1,0)\} = 4 \quad \Rightarrow a_3 = 3 + 1 - N_3 = 0.$$

  $p = 5$

  $$y^2 \equiv x^3 + 2 \pmod 5$$
  $$\Rightarrow N_5 = 1 + \#\{(2,0),(3,2),(3,3),(4,2),(4,3)\} = 6 \quad \Rightarrow a_5 = 5 + 1 - N_5 = 0.$$

- Si $p = 7$, las soluciones de $n^2 + 7m^2 = 7$ son $n = 0$, $m = \pm 1$ por tanto el coeficiente 7-ésimo de Ξ es 0. En este caso

  $p = 7$

  $$y^2 \equiv x^3 \pmod 7$$
  $$\Rightarrow N_7 = 1 + \#\{(0,0),(1,1),(1,6),(2,1),(2,6),(4,1),(4,6)\} = 8$$
  $$\Rightarrow a_7 = 7 + 1 - N_7 = 0.$$

- Si $p > 7$ y $p \equiv 3, 5, 6 \pmod 7$ entonces $n^2 + 7m^2 = p$ no tiene soluciones enteras y por tanto el p-ésimo coeficiente de Ξ es 0. Pero en este caso habíamos visto que $N_p = p + 1$ por lo que

  $$a_p = p + 1 - N_p = 0.$$

- Si $p > 7$ y $p \equiv 1, 2, 4 \pmod 7$. En el Teorema 2.5.4 vimos

$$4(x^2 + xy + 2y^2) = (2x + y)^2 + 7y^2 = 4p$$

para ciertos $x, y \in \mathbb{Z}$, además como $p > 7$ entonces $4p$ se puede sustituir por p obteniendo $(2a+b)^2 + 7b^2 = p$ para ciertos enteros $a, b \in \mathbb{Z}$, entonces el coeficiente p-ésimo de Fourier de Ξ será

$$\frac{1}{2}(2a + b)\left(\frac{2a+b}{7}\right).$$

Por otro lado, en este caso se tiene que $N_p = p + 1 - (2n + m)\left(\frac{2n+m}{7}\right)$. Llamando $a = 2n$, $b = 2m$ y teniendo en cuenta que 2 es residuo cuadrático módulo 7, se tiene

$$\begin{aligned} N_p &= p + 1 - \frac{2a+b}{2}\left(\frac{\frac{2a+b}{2}}{7}\right) = p + 1 - \frac{1}{2}(2a + b)\left(\frac{2}{7}\right)\left(\frac{\frac{2a+b}{2}}{7}\right) = \\ &= p + 1 - \frac{1}{2}(2a + b)\left(\frac{2a+b}{7}\right). \end{aligned}$$

por lo que

$$a_p = p + 1 - N_p = \frac{1}{2}(2a + b)\left(\frac{2a+b}{7}\right).$$

□

En lo que sigue suponemos que $\gamma z = (az + b)/(cz + d)$ cumple $\gamma \in \Gamma_0(196)$.

Proposición 4.3.2

$$\Xi(\gamma z) = \frac{1}{2}\sum_{k=1}^{6}\left(\frac{k}{7}\right)\sum_{u,v=1}^{d} e\left(\frac{u^2 + 7v^2}{d}b\right) S(r, v) \quad con \quad S(r, v) = \sum_{\substack{n \equiv r \ (7d) \\ m \equiv v \ (d)}} n\, e\left(\frac{n^2 + 7m^2}{d(cz + d)}z\right)$$

donde $r = r(u, d, k)$ es cualquier número congruente con u módulo d y con k módulo 7.

Aquí y en lo sucesivo se emplea (N) como abreviatura de (mod N).
Demostración:

$$\Xi(z) = \frac{1}{2}\sum_{n,m\in\mathbb{Z}} n\left(\frac{n}{7}\right)\, e\left((n^2 + 7m^2)z\right).$$

Usando la identidad $\gamma z = \frac{b}{d} + \frac{z}{d(cz+d)}$,

$$\Xi(\gamma z) = \frac{1}{2}\sum_{n,m\in\mathbb{Z}} n\left(\frac{n}{7}\right)\, e\left((n^2 + 7m^2)\gamma z\right) =$$

$$= \frac{1}{2} \sum_{n,m \in \mathbb{Z}} n \left(\frac{n}{7}\right) \; e\left((n^2+7m^2)\left(\frac{b}{d} + \frac{z}{d(cz+d)}\right)\right) =$$

$$= \frac{1}{2} \sum_{n,m \in \mathbb{Z}} n \left(\frac{n}{7}\right) \; e\left(\frac{n^2+7m^2}{d}\, b\right) \; e\left(\frac{n^2+7m^2}{d(cz+d)}\, z\right) =$$

$$= \frac{1}{2} \sum_{k=1}^{6} \left(\frac{k}{7}\right) \sum_{m \in \mathbb{Z}} \sum_{n \equiv k \; (7)} n \; e\left(\frac{n^2+7m^2}{d}\, b\right) \; e\left(\frac{n^2+7m^2}{d(cz+d)}\, z\right) =$$

$$= \frac{1}{2} \sum_{k=1}^{6} \left(\frac{k}{7}\right) \sum_{m \in \mathbb{Z}} e\left(\frac{7m^2}{d}\, b\right) \sum_{n \equiv k \; (7)} n \; e\left(\frac{n^2}{d}\, b\right) \; e\left(\frac{n^2+7m^2}{d(cz+d)}\, z\right) =$$

tomando $v = 1, \ldots, d$, si $m \equiv v (\mathrm{mod}\; d)$ entonces $e\,(m^2/d) = e\,(v^2/d)$, podemos por tanto separar la suma en función de los valores de v,

$$= \frac{1}{2} \sum_{k=1}^{6} \left(\frac{k}{7}\right) \sum_{v=1}^{d} e\left(\frac{7v^2}{d}\, b\right) \sum_{n \equiv k \; (7)} n \; e\left(\frac{n^2}{d}\, b\right) \sum_{m \equiv v \; (d)} e\left(\frac{n^2+7m^2}{d(cz+d)}\, z\right) =$$

aplicando ahora el mismo argumento en n se tiene

$$= \frac{1}{2} \sum_{k=1}^{6} \left(\frac{k}{7}\right) \sum_{u,v=1}^{d} e\left(\frac{u^2+7v^2}{d}\, b\right) \sum_{\substack{n \equiv k \; (7) \\ n \equiv u \; (d)}} \sum_{m \equiv v \; (d)} n \; e\left(\frac{n^2+7m^2}{d(cz+d)}\, z\right) =$$

Finalmente, usando el *teorema chino del resto*,

$$= \frac{1}{2} \sum_{k=1}^{6} \left(\frac{k}{7}\right) \sum_{u,v=1}^{d} e\left(\frac{u^2+7v^2}{d} b\right) \sum_{\substack{n \equiv r \; (7d) \\ m \equiv v \; (d)}} n \; e\left(\frac{n^2+7m^2}{d(cz+d)} z\right)$$

donde $r = r(u, d, k)$ es cualquier número congruente con u módulo d y con k módulo 7. □

A partir de la fórmula de sumación de Poisson clásica, se puede deducir la fórmula de sumación de Poisson en progresiones aritméticas:

$$\sum_{\substack{n \equiv \alpha \; (q_1) \\ m \equiv \beta \; (q_2)}} f(n,m) = \frac{1}{q_1 q_2} \sum_{n,m \in \mathbb{Z}} e\big(\frac{n\alpha}{q_1} + \frac{m\beta}{q_2}\big) \widehat{f}\big(\frac{n}{q_1}, \frac{m}{q_2}\big)$$

donde $\widehat{f}(\vec{\xi})$ es la transformada de Fourier $\iint_{\mathbb{R}^2} f(\vec{x}) e(-\vec{x} \cdot \vec{\xi})\, d\vec{\xi}$.

Para $f(x,y) = x\, e\big((x+7y^2)z\big)$ se tiene $\widehat{f}(\xi,\eta) = \frac{i\sqrt{7}}{28z^2}\xi\, e\big(-\frac{7\xi^2+\eta^2}{28z}\big)$, que junto con la fórmula de sumación anterior

$$S(r,v) = \frac{i\sqrt{7}}{1372dz^2}(cz+d)^2 \sum_{n,m\in\mathbb{Z}} n\, e\big(\frac{nr}{7d}+\frac{mv}{d}\big)\, e\bigg(-\frac{n^2+7m^2}{196dz}(cz+d)\bigg).$$

Entonces

$$\Xi(\gamma z) = \frac{i\sqrt{7}}{2744dz^2}(cz+d)^2 \sum_{n,m\in\mathbb{Z}} nA(n,m)\, e\big(-\frac{n^2+7m^2}{196z}\big)$$

donde

$$A(n,m) = \sum_{k=1}^{6}\left(\frac{k}{7}\right)\sum_{u,v=1}^{d} e\bigg(\frac{u^2+7v^2}{d}b+\frac{nr}{7d}+\frac{mv}{d}-\frac{(n^2+7m^2)c}{196d}\bigg).$$

Los resultados y cálculos descritos a continuación conllevan la simplificación de $A(n,m)$, necesaria antes de aplicar Poisson por segunda vez.

Proposición 4.3.3 $\sum_{k=1}^{6}\left(\frac{k}{7}\right)\, e\big(\frac{nk}{7}\big) = i\sqrt{7}\left(\frac{n}{7}\right)$.

Demostración:

Si $7 \mid n$ es fácil, pues por definición de símbolo de Legendre, la parte derecha es cero, y puesto que hay tantos residuos cuadráticos como no residuos, la parte de la izquierda también.

Si $7 \nmid n$,

$$S = \sum_{k=1}^{6}\left(\frac{k}{7}\right)\, e\big(\frac{k}{7}\big) = e\big(\frac{1}{7}\big)+e\big(\frac{2}{7}\big)+e\big(\frac{4}{7}\big)-e\big(\frac{3}{7}\big)-e\big(\frac{5}{7}\big)-e\big(\frac{6}{7}\big) =$$

$$= 1+2\left(e\big(\frac{1}{7}\big)+e\big(\frac{2}{7}\big)+e\big(\frac{4}{7}\big)\right)$$

elevando al cuadrado,

$$S^2 = 1+8\left(e\big(\frac{1}{7}\big)+e\big(\frac{2}{7}\big)+e\big(\frac{3}{7}\big)+e\big(\frac{4}{7}\big)+e\big(\frac{5}{7}\big)+e\big(\frac{6}{7}\big)\right) =$$

$$= 1+8(-1) = -7$$

$$\Rightarrow S = \pm i\sqrt{7}.$$

Por otro lado

$$S = \sum_{k=1}^{6}\left(\frac{k}{7}\right)\, e\big(\frac{k}{7}\big) = \sum_{k=1}^{6}\left(\frac{k}{7}\right)\left(\cos\big(\frac{2k\pi}{7}\big)+i\sin\big(\frac{2k\pi}{7}\big)\right) =$$

$$= 2i\left(\sin\left(\frac{2\pi}{7}\right) + \sin\left(\frac{4\pi}{7}\right) + \sin\left(\frac{8\pi}{7}\right)\right)$$

teniendo en cuenta que $\left(\sin(\frac{2\pi}{7}) + \sin(\frac{4\pi}{7}) + \sin(\frac{8\pi}{7})\right) > 0$, es signo queda determinado y por tanto

$$\Rightarrow S = i\sqrt{7}.$$

Por último, efectuando un cambio de variable $k \mapsto nk$ (multiplicar por la clase de n es un isomorfismo en $\mathbb{Z}_7$), se tiene

$$\sum_{k=1}^{6}\left(\frac{k}{7}\right)\ e(\frac{k}{7}) = \sum_{k=1}^{6}\left(\frac{nk}{7}\right)\ e(\frac{nk}{7}) = \left(\frac{n}{7}\right)\sum_{k=1}^{6}\left(\frac{k}{7}\right)\ e(\frac{nk}{7})$$

por lo que

$$\sum_{k=1}^{6}\left(\frac{k}{7}\right)\ e(\frac{nk}{7}) = i\sqrt{7}\left(\frac{n}{7}\right).$$

□

El número $r = r(u, d, k)$ que aparece en la Proposición 4.3.2, es cualquier número congruente con u módulo d y con k módulo 7, es decir, es la solución del sistema de congruencias,

$$\begin{cases} x \equiv u \pmod{d} \\ x \equiv k \pmod{7} \end{cases}$$

aplicando ahora el *teorema chino del resto*, se llega a que

$$x \equiv 7^* \cdot 7u + d^* \cdot dk \pmod{7d}$$

donde 7^* y d^* son los inversos de 7 y d módulo d y 7 respectivamente. Entonces

$$A(n,m) = \sum_{k=1}^{6}\left(\frac{k}{7}\right)\sum_{u,v=1}^{d} e\left(\frac{u^2+7v^2}{d}b + \frac{nr}{7d} + \frac{mv}{d} - \frac{(n^2+7m^2)c}{196d}\right) =$$

$$= \sum_{k=1}^{6}\left(\frac{k}{7}\right)\sum_{u,v=1}^{d} e\left(\frac{u^2+7v^2}{d}b + \frac{n(7^*\cdot 7u + d^*\cdot dk)}{7d} + \frac{mv}{d} - \frac{(n^2+7m^2)c}{196d}\right) =$$

$$= \sum_{k=1}^{6}\left(\frac{k}{7}\right)\ e\left(\frac{nd^*k}{7}\right)\sum_{u,v=1}^{d} e\left(\frac{b(u^2+7v^2) + 7^*nu + mv - (n^2+7m^2)c/196}{d}\right).$$

Aplicando ahora la Proposición 4.3.3, y notando que $\left(\frac{d^*}{7}\right) = \left(\frac{d}{7}\right)$, pues el conjunto de los inversos de $\{1,2,4\}$ y de $\{3,5,6\}$ módulo 7, coincide en ambos casos con el propio conjunto, se tiene que

$$A(n,m) = i\sqrt{7}\left(\frac{nd}{7}\right)\sum_{u,v=1}^{d} e\left(\frac{b(u^2+7v^2) + 7^*nu + mv - (n^2+7m^2)c/196}{d}\right).$$

Esta suma es invariante por cualquier traslación entera de u y v (porque estas variables recorren todas las clases módulo d).

Efectuando el cambio

$$u \mapsto u + \frac{cn}{14} \qquad v \mapsto v + \frac{cm}{14}$$

se obtiene

$$b\left(u^2 + \frac{nuc}{7} + \frac{n^2c^2}{196} + 7v^2 + mvc + \frac{m^2c^2}{28}\right) + 7^*nu + \frac{7^*n^2c}{14} + mv + \frac{m^2c}{14} - \frac{(n^2+7m^2)c}{196} =$$

$$= b(u^2+7v^2) + (7^*nu + mv)(bc+1) + \frac{bc^2(n^2+7m^2) + 2c(n^2+7m^2) - c(n^2+7m^2)}{196} =$$

$$= b(u^2+7v^2) + (7^*un + vm)(bc+1) + (n^2+7m^2)(bc+1)\frac{c}{196}$$

teniendo en cuenta que $\gamma \in \Gamma_0(196) \subset \mathrm{SL}_2(\mathbb{Z})$, $196 \mid c$ y $d \mid bc+1$,

$$d \mid (7^*un + vm)(bc+1) + (n^2+7m^2)(bc+1)\frac{c}{196} = B$$

ahora es claro que $e(B) = 1$ y por tanto

$$A(n,m) = i\sqrt{7}\left(\frac{nd}{7}\right)\sum_{u,v=1}^{d} e\left(\frac{b(u^2+7v^2) + 7^*nu + mv - (n^2+7m^2)c/196}{d}\right) =$$

$$= i\sqrt{7}\left(\frac{nd}{7}\right)\sum_{u,v=1}^{d} e\left(\frac{b(u^2+7v^2)}{d}\right).$$

Observación: d es impar pues $d \mid bc+1$, y

$$\gamma \in \Gamma_0(196) \Rightarrow 196 \mid c \Rightarrow c \text{ es par } \Rightarrow bc+1 \text{ es impar}$$

d y b son coprimos pues $d \mid bc+1$, de hecho también será coprimo con $7b$ porque $7 \mid c$.

Utilizando un resultado de Gauss que afirma que para b y d coprimos con d impar, se cumple $\sum_{n=1}^{d} e(bn^2/d) = \frac{1}{2}(1+i)(1-i^d)\left(\frac{b}{d}\right)\sqrt{d}$, se tiene

$$A(n,m) = i\sqrt{7}\left(\frac{nd}{7}\right)\sum_{u,v=1}^{d} e\left(\frac{b(u^2+7v^2)}{d}\right) = i\sqrt{7}\left(\frac{nd}{7}\right)\sum_{u,v=1}^{d} e\left(\frac{bu^2}{d}\right) e\left(\frac{7bv^2}{d}\right) =$$

$$= i\sqrt{7}\left(\frac{nd}{7}\right)\frac{1}{4}(1+i)^2(1-i^d)^2\left(\frac{b}{d}\right)\left(\frac{7b}{d}\right)d = -i\sqrt{7}\left(\frac{n}{7}\right)d\left(\frac{d}{7}\right)\left(\frac{7}{d}\right)\left(\frac{b^2}{d}\right)i^{d+3}$$

donde se ha utilizado que $(1+i)^2 = 2i$ y que $(1-i^d)^2 = 1+(-1)^d - 2i^d = -2i^d$ usando que d es impar.

Por último, observando que

$$\left(\frac{7}{d}\right) = (-1)^{\frac{6(d-1)}{4}} \left(\frac{d}{7}\right) = i^{3(d-1)} \left(\frac{d}{7}\right)$$

concluimos

$$A(n,m) = -i\sqrt{7}\left(\frac{n}{7}\right) d \left(\frac{d^2}{7}\right) i^{3(d-1)} i^{d+3} = i\sqrt{7}\left(\frac{n}{7}\right) d.$$

Terminamos probando tras los resultados anteriores que Ξ es una forma modular.

Proposición 4.3.4

$$\Xi \in \mathcal{M}_2\big(\Gamma_0(196)\big).$$

Demostración:

$$\Xi(\gamma z) = \frac{i\sqrt{7}}{2744dz^2}(cz+d)^2 \sum_{n,m\in\,\mathbb{Z}} nA(n,m)\; e\left(-\frac{n^2+7m^2}{196z}\right) =$$

$$= \frac{i\sqrt{7}}{2744dz^2}(cz+d)^2 \sum_{n,m\in\,\mathbb{Z}} n\; i\sqrt{7}\left(\frac{n}{7}\right) d\; e\left(-\frac{n^2+7m^2}{196z}\right) =$$

$$= \frac{-1}{392z^2}(cz+d)^2 \sum_{n,m\in\,\mathbb{Z}} n\left(\frac{n}{7}\right)\; e\left((n^2+7m^2)\left(\frac{-1}{196z}\right)\right).$$

Teniendo en cuenta que para $f(x,y) = x\; e\left((x^2+7y^2)\left(\frac{-1}{196z}\right)\right)$ se tiene $\widehat{f}(\xi,\eta) = \frac{i\sqrt{7}}{28} 196^2 z^2 \xi\; e\left(\frac{7\xi^2+\eta^2}{28} 196z\right)$, usando la fórmula de sumación de Poisson, para cada $k \in \mathbb{Z}$,

$$\sum_{\substack{n\equiv k\ (7)\\ m\in\,\mathbb{Z}}} f(n,m) = \frac{1}{7} \sum_{n,m\in\,\mathbb{Z}} e\big(\frac{nk}{7}+m\big)\widehat{f}\big(\frac{n}{7},m\big) =$$

$$= \frac{1}{7} \sum_{n,m\in\,\mathbb{Z}} e\big(\frac{nk}{7}\big)\frac{i\sqrt{7}}{28} 196^2 z^2 \frac{n}{7}\; e\left(\frac{\frac{n^2}{7}+m^2}{28} 196z\right) =$$

$$= 28i\sqrt{7}z^2 \sum_{n,m\in\,\mathbb{Z}} e\big(\frac{nk}{7}\big) n\; e\left((n^2+7m^2)z\right).$$

Entonces

$$\Xi(\gamma z) = \frac{-(cz+d)^2}{392z^2} \sum_{k=1}^{6} \left(\frac{k}{7}\right) \sum_{\substack{n\equiv k\ (7)\\ m\in\,\mathbb{Z}}} f(n,m) =$$

$$= \frac{-(cz+d)^2}{14} i\sqrt{7} \sum_{n,m\in Z} \left(\sum_{k=1}^{6} \left(\frac{k}{7}\right)\ e\left(\frac{nk}{7}\right) \right) n\, e\big((n^2+7m^2)z\big) =$$

$$= \frac{-(cz+d)^2}{14} i\sqrt{7} i\sqrt{7} \sum_{n,m\in Z} n \left(\frac{n}{7}\right)\ e\big((n^2+7m^2)z\big) =$$

$$= (cz+d)^2 \frac{1}{2} \sum_{n,m\in Z} n \left(\frac{n}{7}\right)\ e\big((n^2+7m^2)z\big) = (cz+d)^2 \Xi(z)$$

donde se ha usado la relación $\sum_{k=1}^{6} \left(\frac{k}{7}\right)\ e\big(\frac{nk}{7}\big) = i\sqrt{7}\left(\frac{n}{7}\right)$. Se concluye entonces que

$$\Xi \in \mathcal{M}_2\big(\Gamma_0(196)\big).$$

□

Con un poco más de trabajo se puede probar que de hecho $\Xi \in \mathcal{M}_2\big(\Gamma_0(49)\big)$ y este 49 no se puede reducir más.

Este nivel mínimo de la forma modular asociada es el llamado *conductor* de la curva elíptica.

Bibliografía

[Ba-Gu-Tr] P. Bayer, J. Guàrdia, A. Travesa. *El sueño de juventud de Kronecker*, Notes del Seminari de Teoria de Nombres (UB-UAB-UPC), Barcelona-La Rábida, 2005.

[Ca] J.W.S. Cassels. *Lectures on elliptic curves*, London Mathematical Society Student Texts 24, Cambridge University Press, 1991.

[Ch] F. Chamizo. *Seminario Avanzado. Teoría de números*, Capítulo 5, 2006.

[Da] H. Davenport. *Multiplicative number theory*, volume 74 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2000.

[Di-Sh] F. Diamond, J. Shurman. *A first course in modular forms*, volume 228 of Graduate Texts in Mathematics. Springer, New York, 2005.

[Ed] H.M. Edwards *Riemann's Zeta Function*. Academic Press, New York, 1974.

[Ga] C. F. Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag, New York, 1986.

[Iw] H. Iwaniec. *Topics in classical automorphic forms*. Graduate Studies in Mathematics, 17. American Mathematical Society, Providence, RI, 1997.

[Kn] A.W. Knapp. *Elliptic curves*, volume 40 of Mathematical Notes. Princeton University Press, Princeton, NJ, 1992.

[La] S. Lang. *Elliptic functions*, Springer-Verlag, 1987.

[Mi] J. S. Milne. *Modular functions and modular forms*, notes for Math 678, University of Michigan, 1990.

[Mi2] J. S. Milne. *Elliptic curves*, notes for Math 679, University of Michigan, 1996.

[Se] J-P. Serre. *A course in arithmetic*. Graduate Texts in Mathematics, 7. Springer-Verlag, New York-Heidelberg, 1973.

[Si] J. Silverman. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106. Springer-Verlag, 1986.