Formas modulares y el Teorema de los Cuatro Cuadrados

Lorien Zamora Perpiñan

Trabajo de Fin de Grado de Matemáticas
Universidad de Zaragoza

Julio de 2025

Introducción

El siguiente trabajo estudia un problema clásico de las matemáticas, el Teorema de los Cuatro Cuadrados. Este teorema fue planteado y resuelto por Lagrange y afirma que cualquier número natural se puede escribir como suma de los cuadrados de cuatro enteros. Es decir para cualquier $n \in \mathbb{N}$ la ecuación:

$$n = a^2 + b^2 + c^2 + d^2$$

tiene solución para ciertos $a, b, c, d \in \mathbb{N} \cup \{0\}$.

Posteriormente Jacobi planteó la siguiente cuestión: ¿de cuántas formas diferentes se puede escribir un natural como suma de cuatro cuadrados? Esta va a ser la cuestión que vamos a resolver en este trabajo. Este problema puede ser estudiado desde diferentes ángulos, en este caso para demostrarlo vamos a introducir las formas modulares, funciones complejas del semiplano superior con ciertas propiedades de invariancia bajo el grupo modular:

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

También vamos a estudiar ciertos subgrupos de este grupo, los llamados subgrupos de congruencia, cuyo estudio (concretamente el de $\Gamma_0(N)$) será clave para probar el resultado. Las formas modulares son herramientas muy potentes del análisis complejo cuyas propiedades se van a estudiar a lo largo de este trabajo. Las formas modulares tienen un alcance mucho mayor al que veremos en este trabajo, de hecho, se utilizaron para probar el Último Teorema de Fermat, uno de los resultados más famosos de la historia de las matemáticas.

La relación entre ambos conceptos, aparentemente inexistente, nos permite apreciar la profunda relación que existe entre las diversas áreas de las matemáticas.

En el primer capítulo se presentan las primeras definiciones, necesarias para el resto de capítulos. Se introduce el concepto de forma modular, sus propiedades y algunos ejemplos sencillos. También se definen el grupo modular y los subgrupos de congruencia. Estos conceptos son clave pues sientan la base de las ideas sobre las que se trabaja en los siguientes capítulos.

En el segundo capítulo introducimos los conceptos de toro complejo y de curva elíptica (compleja). A lo largo del capítulo desarrollamos las herramientas necesarias para demostrar que en realidad son conceptos estrechamente relacionados y podemos trabajar como si fuesen equivalentes bajo ciertas condiciones. En la última sección introducimos las curvas modulares, eje del tercer capítulo, y su relación con las curvas elípticas.

El tercer capítulo trata principalmente sobre las propiedades topológicas de las curvas elípticas, centrándonos en el caso $\Gamma_0(4)$ pues es el que vamos a utilizar para probar el resultado que buscamos. El resultado más importante al que llegamos al final del capítulo es que una curva modular es una superficie de Riemann. También se ven otras propiedades de las curvas modulares, como sus puntos elípticos, sus cúspides y su género.

El capítulo cuarto es una breve conclusión, en la que, tras una pequeña introducción histórica del Teorema de los Cuatro Cuadrados, lo probamos finalmente haciendo uso de los resultados de los capítulos anteriores.

Summary

In this work we are going to study a classic mathematical problem, the Four Squares Theorem. This theorem was formulated and proved by Lagrange, and it states that any natural number can be written as the sum of the squares of four integers. That is to say, for any $n \in \mathbb{N}$ the equation

$$n = a^2 + b^2 + c^2 + d^2$$

has solutions with $a, b, c, d \in \mathbb{N} \cup \{0\}$. Afterwards, Jacobi formulated and proposed the following mathematical problem: in how many different ways can a natural number be written as a sum of four squares? This will be the problem we will solve in this essay. This problem could be studied in different angles. In our approach, we will use modular forms, which are complex functions defined in the upper half plane satisfying certain invariance properties under the modular group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

We will also study some subgroups of $\mathrm{SL}_2(\mathbb{Z})$, the so-called congruence subgroups. Particular attention will be deserved to $\Gamma_0(4)$, because of its important role in the proof of the main theorem.

Modular forms are a very important tool of complex analysis, and some of their properties will be studied over the course of this text. Modular forms have a much wider scope than what we will see here. Actually, modular forms are used to prove Fermat's Last Theorem, one of the most famous results in mathematics history. The connection between these two concepts, apparently nonexistent, unveils the deep relation between different areas of mathematics.

Índice general

Capítulo 1

Formas modulares

En este capítulo se introduce el grupo modular sus principales subgrupos de congruencia y las formas modulares. La principal referencia es [1, sec 1.1 y 1.2].

1.1. Acción del grupo modular en el semiplano complejo superior

Definición. El **grupo modular** $\mathrm{SL}_2(\mathbb{Z})$ es el grupo de matrices 2×2 con coeficientes enteros y determinante igual a 1:

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z},\ ad-bc=1 \right\}.$$

Efectivamente se trata de un grupo con la operación de la mutiplicación entre matrices, con la matriz identidad como elemento neutro ($Id \in \mathrm{SL}_2(\mathbb{Z})$). Dados $A,B \in \mathrm{SL}_2(\mathbb{Z})$ las entradas de AB siguen siendo enteras y $det(AB) = det(A)det(B) = 1$ por lo que $AB \in \mathrm{SL}_2(\mathbb{Z})$

Cada elemento del grupo modular define un automorfismo en $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, mediante la transformación de Möbius

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau+b}{c\tau+d}\, \tau \in \widehat{\mathbb{C}}$$

El **Semiplano Superior** del plano Complejo es

$$\mathbb{H} = \{\tau \in \mathbb{C} : Im(\tau) > 0\}$$

Observemos que dado $\gamma \in \mathrm{SL}_2$ *y* $\tau \in \mathbb{H}$ *entonces* $\gamma(\tau) \in \mathbb{H}$:

$$\mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{\mathrm{Im}\left((a\tau+b)\overline{(c\tau+d)}\right)}{|c\tau+d|^2} = \frac{(ad-bc)\mathrm{Im}(\tau)}{|c\tau+d|^2} = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2}.$$

Por tanto el grupo modular actúa en el semiplano superior.

Con estas definiciones podemos introducir el concepto de **forma modular**, cuyo estudio nos va a proporcionar las herramientas necesarias para poder resolver el problema de los cuatro cuadrados.

1.2. Formas Modulares para $\mathrm{SL}_2(\mathbb{Z})$

Definición (Forma modular de peso k)**.** Sea k un entero. Una función $f\colon \mathbb{H} \to \mathbb{C}$ se denomina **forma modular** de peso k si satisface:

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

2. f es **débilmente modular** de peso k, es decir, para toda matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ se cumple:

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau), \quad \forall \tau \in \mathbb{H};$$

3. f es **holomorfa en el infinito**.

El conjunto de formas modulares de peso k para $\mathrm{SL}_2(\mathbb{Z})$ se denota por $M_k(\mathrm{SL}_2(\mathbb{Z}))$.

Vamos a explicar qué quiere decir el tercer punto de la definición, que f sea holomorfa en el infinito. Por el segundo punto f es débilmente modular y por tanto $f(\tau+1) = f(\tau)$. Esto implica que f es $\mathbb{Z}$-periódicas. Ahora, sea $D = \{q \in \mathbb{C} : |q| < 1\}$ el disco unitario abierto complejo y $D' = D \setminus \{0\}$. Sabemos por análisis complejo que el mapa holomorfo $\mathbb{Z}$-periódico $\tau \mapsto e^{2\pi i \tau} = q$ lleva $\mathbb{H}$ a D'. Así, tomamos la función $g\colon D' \to \mathbb{C}$ donde $g(q) = f(\log(q)/(2\pi i))$ que está bien definida aunque el logaritmo esté determinado solo módulo $2\pi i\mathbb{Z}$, y $f(\tau) = g(e^{2\pi i\tau})$.

Si f es holomorfa en el semiplano superior entonces la composición g es holomorfa en el disco punteado ya que el logaritmo puede definirse holomórficamente alrededor de cada punto. Por tanto, g tiene un desarrollo de Laurent $g(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ para $q \in D'$. La relación $|q| = e^{-2\pi \mathrm{Im}(\tau)}$ muestra que $q \to 0$ cuando $\mathrm{Im}(\tau) \to \infty$. Entonces, tomamos ∞ como el límite en la dirección imaginaria de $\mathbb{H}$, decimos que f es holomorfa en ∞ si g tiene extensión holomorfa en el punto $q = 0$, es decir, si la serie de Laurent cumple que $a_n = 0$ cuando $n < 0$. Esto significa que f tiene un desarrollo de Fourier, es decir f se puede escribir como una suma infinita de exponenciales complejas de la siguiente manera:

$$f(t) = \sum_{n=0}^{\infty} c_n e^{in\omega_0 t}, \text{ donde } \omega_0 = 2\pi$$

Ejemplo 1. Veamos el caso de las formas modulares de peso 2, que tienen una importancia especial pues el análisis complejo depende de integrales de camino de diferenciales $f(\tau)d\tau$, y la integración de caminos $\mathrm{SL}_2(\mathbb{Z})$-invariantes en $\mathbb{H}$ requiere que tales diferenciales sean invariantes cuando τ es reemplazado por un $\gamma(\tau) \in \mathrm{SL}_2(\mathbb{Z})$. Como

$$d\gamma(\tau) = \frac{d}{d\tau}\left(\frac{a\tau+b}{c\tau+d}\right)d\tau = \frac{(a)(c\tau+d)-(a\tau+b)(c)}{(c\tau+d)^2}d\tau = \frac{ad-bc}{(c\tau+d)^2}d\tau = \frac{1}{(c\tau+d)^2}d\tau = (c\tau+d)^{-2}d\tau$$

La condición para que se cumpla la relación $f(\gamma(\tau))d(\gamma(\tau)) = f(\tau)d\tau$ es

$$f(\gamma(\tau)) = (c\tau+d)^2 f(\tau).$$

Proposición 1.1. *$M_k(\mathrm{SL}_2(\mathbb{Z}))$ forma un espacio vectorial sobre $\mathbb{C}$.*

Demostración. La holomorfía en la suma de dos funciones y en el producto de escalar por función se conserva por las propiedades de $\mathbb{C}$ así como las propiedades asociativas, conmutativas y distributivas. Veamos el resto de propiedades.

1. Cerrado bajo la suma: Dados f y $g \in M_k(\mathrm{SL}_2(\mathbb{Z}))$, entonces $f+g \in M_k(\mathrm{SL}_2(\mathbb{Z}))$.

$$(f+g)(\gamma\tau) = f(\gamma\tau)+g(\gamma\tau) = (c\tau+d)^k f(\tau)+(c\tau+d)^k g(\tau) = (c\tau+d)^k (f+g)(\tau)$$

2. Cerrado bajo el producto por escalar Dados $\lambda \in \mathbb{C}$ y $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$, entonces $\lambda f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$.

$$(\lambda f)(\gamma\tau) = \lambda f(\gamma\tau)\lambda(c\tau+d)^k f(\tau)(c\tau+d)^k (\lambda f)(\tau)$$

3. Elemento neutro y opuestos: $0 \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ y Si $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ entonces $-f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$

$$(-f)(\gamma\tau) = -f(\gamma\tau) = -(c\tau+d)^k f(\tau) = (c\tau+d)^k (-f)(\tau)$$

□

El hecho (que veremos más adelante) de que la dimensión de este espacio vectorial sea finita y el estudio de las dimensiones de ciertos subespacios concretos será importante, pues nos permitirá fijar una base a partir de la cual describir nuestro problema.

Directamente de la definición de forma modular introducimos la siguiente definición.

Veamos ahora uno de los ejemplos más sencillos de forma modular. Sea $k > 2$ un entero par y definamos la **serie de Eisenstein** de peso k como el análogo bidimensional de la evaluación de k de la función zeta de Riemann: $\zeta(k) = \sum_{d=1}^{\infty} \frac{1}{d^k}$,

$$G_k(\tau) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} \frac{1}{(c\tau+d)^k}, \quad \tau \in \mathbb{H}.$$

Teorema 1.1. *Para todo entero par $k > 2$, la serie de Eisenstein G_k es una forma modular de peso k para el grupo* $\mathrm{SL}_2(\mathbb{Z})$.

Demostración. Debemos verificar las tres condiciones de la definición de forma modular:

1. **Holomorfía en** $\mathbb{H}$. La serie $G_k(\tau)$ converge de manera absoluta y uniforme en subconjuntos compactos de $\mathbb{H}$. Para $k \geq 3$, se cumple que la suma:

   $$\sum_{(c,d)\neq(0,0)} \frac{1}{|c\tau+d|^k} \leq \sum_{(c,d)\neq(0,0)} \frac{1}{(c^2+d^2)^{k/2}}$$

   Como cada término $\frac{1}{(c\tau+d)^k}$ es holomorfo, G_k es holomorfa.

2. **Invariancia modular de peso** k. Dado $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, tenemos que:

   $$\begin{aligned} G_k\left(\frac{a\tau+b}{c\tau+d}\right) &= \sum_{(m,n)\neq(0,0)} \frac{1}{\left(m\left(\frac{a\tau+b}{c\tau+d}\right)+n\right)^k} = (c\tau+d)^k \sum_{(m,n)\neq(0,0)} \frac{1}{(m(a\tau+b)+n(c\tau+d))^k} \\ &= (c\tau+d)^k \sum_{(m,n)\neq(0,0)} \frac{1}{((ma+nc)\tau+(mb+nd))^k}. \end{aligned}$$

   Como γ es invertible, el par $(m',n') = (ma+nc, mb+nd)$ recorre todos los pares no nulos de enteros. Por tanto:

   $$G_k\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k G_k(\tau)$$

3. **Holomorfía en el infinito**. El desarrollo de G_k viene dado por (operando a partir de la definición):

   $$G_k(\tau) = 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

   donde $q = e^{2\pi i\tau}$, $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$, observamos que no aparecen términos con exponentes negativos lo que garantiza la holomorfía en ∞.

□

Normalizamos la expresión anterior, diviendo entre $2\zeta(k)$, y obtenemos la *Serie de Eisenstein normalizada*

$$E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)} = 1 + \frac{2(2\pi i)^k}{\zeta(k)(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

1.3. Subgrupos de congruencia

En esta sección vamos a estudiar subgrupos importantes de $\mathrm{SL}_2(\mathbb{Z})$.

Definición. Dado N entero positivo, el **Subgrupo principal de congruencia de nivel N** es

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

Definición. Un subgrupo Γ de $\mathrm{SL}_2(\mathbb{Z})$ se dice **subgrupo de congruencia de nivel N** si $\Gamma(N) \subseteq \Gamma$ para algún $N \in \mathbb{Z}^+$.

Los dos subgrupos de congruencia más relevantes son los siguientes:

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

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

Observemos que $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$.

En relación con el Teorema de los Cuatro Cuadrados, el subgrupo de congruencia más importante con el que vamos a trabajar es $\Gamma_0(4)$:

$$\Gamma_0(4) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{4} \right\}$$

Veamos ahora una proposición que nos da generadores para este grupo.

Proposición 1.2. *$\Gamma_0(4)$ está generado por* $\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *y* $\pm \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$.

Demostración. La primera parte de la demostración consiste en ver que efectivamente $\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ y $\pm \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \in \Gamma_0(4)$. Esto es trivial de la definición anterior y del hecho de que $4 \equiv 0 \pmod{4}$.

La segunda parte consiste en ver que cualquier matriz $M \in \Gamma_0(4)$ se puede escribir como producto de $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ y $S^k = \begin{pmatrix} 1 & 0 \\ 4k & 1 \end{pmatrix}$ para ciertos k y $n \in \mathbb{Z}$. Para verlo, sea $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ una matriz en $\Gamma_0(4)$, y notemos que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & an+b \\ c & nc+d \end{pmatrix}$$

Salvo si $c = 0$, existe un n y por tanto una matriz T^n que transforma la matriz de manera que tiene la fila inferior (c', d') con $|d'| < |c'|/2$. (La desigualdad es estricta porque $c' \equiv 0 \pmod{4}$ y d' es impar).

Multiplicando por S^n

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 4n & 1 \end{pmatrix} = \begin{pmatrix} a+4nb & b \\ c+4nd & d \end{pmatrix}$$

para mostrar que, como $d \neq 0$ (ningún elemento de $\Gamma_0(4)$ puede tener $d = 0$), obtenemos una matriz que tiene fila inferior (c', d') con $|c'| < 2|d'|$.

Cada iteración reduce $\min\{|c|, |2d|\}$ por lo que el proceso termina con $c = 0$ o $d = 0$, y $d = 0$ no es posible pues implicaría que $c = \pm 1$. Multiplicando por potencias de T y S hemos obtenido una matriz con $c = 0$ y $d = \pm 1$, tomando $n = -b/d$ tenemos que multiplicando esta matriz por T^n resulta la identidad. □

A continuación vamos a estudiar el índice de los subgrupos de congruencia y utilizarlo para el caso concreto $\Gamma_0(4)$.

Proposición 1.3. *1. El subgrupo principal de congruencia $\Gamma(N)$ es el kernel del homomorfismo de reducción módulo N $\mathrm{SL}_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ por lo que es un subgrupo normal.*

2. La aplicación anterior es suprayectiva, induciendo un isomorfismo $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

3. $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$, donde p recorre los divisores primos de N.

Demostración. 1. Es trivial por la definición de subgrupo de congruencia normal.

2. Observamos que cualquier matriz $\gamma = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ posee preimagen en $M_2(\mathbb{Z})$. Tomamos la matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ tal que:

$$a \equiv g_{11} \pmod{N}, b \equiv g_{12} \pmod{N}, c \equiv g_{21} \pmod{N}, d \equiv g_{22} \pmod{N}.$$

Podemos asegurar que $\gcd(c,d) = 1$ ya que como $det(\gamma) \equiv 1 \pmod{N}$ para cualquier p primo divisor de N tenemos que $det(\gamma) \equiv 1 \pmod{p}$ y por tanto g_{21} y g_{22} no pueden ser ambos divisibles por p. De esta manera podemos elegir representantes c y d que sean coprimos. Como $ad - bc \equiv 1 \pmod{N}$ tenemos que, $\exists m \in \mathbb{Z}$ tal que $ad - bc = 1 + mN$. Buscamos enteros k y l que resuelvan la ecuación $kd - lc = -m$ que existirán por el hecho de que $mcd(c,d) = 1$. Una vez encontrados k y l tomamos la matriz $\gamma' = \begin{pmatrix} a+kN & b+lN \\ c & d \end{pmatrix}$ y calculamos su determinante:

$$det(\gamma') = (a+kN)d - (b+lN)c = ad + kNd - bc - lNc =$$

$$= (ad - bc) + N(kd - lc) = (1 + mN) + N(-m) = 1 + mN - mN = 1$$

Por tanto $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ es preimagen de γ con lo que concluimos que la aplicación es suprayectiva.

3. Vamos a probar primero el caso $N = p$ con p primo. Tomamos el conjunto de matrices invertibles en $\mathbb{Z}/p\mathbb{Z}$, $GL_2(\mathbb{Z}/p\mathbb{Z})$, la única condición sobre las entradas es que $ad - bc \not\equiv 0 \pmod{p}$ por tanto el orden, $|GL_2(\mathbb{Z}/p\mathbb{Z})|$, corresponde al número de bases ordenadas que podemos tomar en $(\mathbb{Z}/p\mathbb{Z})^2$. El primer vector se puede elegir entre $(p^2 - 1)$ elementos y el segundo entre $(p^2 - p)$. Por tanto, $|GL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p) = p^4(1 - \frac{1}{p^2})(1 - \frac{1}{p})$.

El homomorfismo de grupos $det : GL_2(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^*$ es suprayectivo y tiene núcleo $SL_2(\mathbb{Z}/p\mathbb{Z})$. Por tanto,

$$|SL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|GL_2(\mathbb{Z}/p\mathbb{Z})|}{|(\mathbb{Z}/p\mathbb{Z})|} = \frac{p^4(1 - \frac{1}{p^2})(1 - \frac{1}{p})}{(p-1)} = p^3(1 - \frac{1}{p^2})$$

Estudiamos ahora el índice en el caso $N = p^m$ con $m \in \mathbb{N}$. Vamos a demostrar por inducción que $|SL_2(\mathbb{Z}/p^m\mathbb{Z})| = p^{3m}(1 - \frac{1}{p^2})$. El caso $m = 1$ ya esta probado, veamos ahora el caso $m+1$.

Tomamos la proyección natural $(\mathbb{Z}/p^{m+1}\mathbb{Z}) \to (\mathbb{Z}/p^m\mathbb{Z})$ que es suprayectiva con núcleo de orden p. Si conseguimos probar que el núcleo de la aplicación $\pi : SL(\mathbb{Z}/p^{m+1}\mathbb{Z}) \to SL(\mathbb{Z}/p^m\mathbb{Z})$ (que es claramente suprayectiva) tiene orden p^3 habremos terminado la demostración. Sea $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ una matriz que pertenece al núcleo y por tanto cumple que $ad - bc \equiv 1 \pmod{p^{m+1}}$ y $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p^m}$ entonces el problema se reduce a encontrar cuantas combinaciones diferentes de $n_1, n_2, n_3, n_4 \in 0, 1, ..., p-1$ cumplen la siguiente ecuación:

$$(1 + n_1 p^m)(1 + n_2 p^m) - (n_3 p^m)(n_4 p^m) \equiv 1 \pmod{p^{m+1}}$$

Como $p^{2m} \equiv 0 \pmod{p^{m+1}}$ la ecuación anterior se reduce a

$$p^m(n_1+n_2) \equiv 0 \pmod{p^{m+1}}$$

Fijando n_1 tenemos que la ecuación tiene solución única con $n_2 = p - n_1$ y podemos concluir tenemos p^3 soluciones diferentes y por tanto este es el orden del núcleo. Finalmente $|SL_2(\mathbb{Z}/p^{m+1}\mathbb{Z})| = |SL_2(\mathbb{Z}/p^m\mathbb{Z})||ker(\pi)| = p^{3m+1}(1-\frac{1}{p^2})$ y el resultado queda probado.

Veamos el último caso, en el que N es un natural cualquiera. Desarrollamos N como producto de sus factores primos $N = \prod_{p|N} p^{m_p}$. El Teorema Chino del resto nos dice que

$$\mathbb{Z}/N\mathbb{Z} \cong \prod_{p|N} \mathbb{Z}/p^{m_p}\mathbb{Z}$$

y por tanto

$$|SL_2(\mathbb{Z}/N\mathbb{Z})| = |\prod_{p|N} SL_2(\mathbb{Z}/p^{m_p}\mathbb{Z})| \Rightarrow |SL_2(\mathbb{Z}/N\mathbb{Z})| = \prod_{p|N} |SL_2(\mathbb{Z}/p^{m_p}\mathbb{Z})|$$

A partir del caso anterior y el punto 2 de la proposición construimos la fórmula para el caso general.

$$|SL_2(\mathbb{Z}/N\mathbb{Z})| = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

□

El homomorfismo de grupos

$$\Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \mod N$$

es suprayectivo con núcleo $\Gamma(N)$. Por lo tanto, $\Gamma(N) \trianglelefteq \Gamma_1(N)$, y además

$$\Gamma_1(N)/\Gamma(N) \xrightarrow{\sim} \mathbb{Z}/N\mathbb{Z}, \quad [\Gamma_1(N) : \Gamma(N)] = N.$$

De manera similar, el homomorfismo de grupos

$$\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod N$$

es suprayectivo con núcleo $\Gamma_1(N)$, de modo que $\Gamma_1(N) \trianglelefteq \Gamma_0(N)$, y

$$\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^*, \quad [\Gamma_0(N) : \Gamma_1(N)] = \varphi(N).$$

donde $\varphi(N)$ es la función de Euler.

Con estas fórmulas y dado que $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z}))$ podemos determinar también el índice $[\Gamma_0(N) : \mathrm{SL}_2(\mathbb{Z})]$.

Ejemplo 2. Veamos el caso concreto $N = 4$,aplicando las fórmulas que acabamos de ver tenemos que,

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(4)] = 48, \quad [\Gamma_1(4) : \Gamma(4)] = 4, \quad [\Gamma_0(4) : \Gamma_1(4)] = 4$$

De lo que deducimos que

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4)] = 6$$

De esta manera como estamos trabajando con un índice pequeño podemos encontrar representantes para cada clase. Formalmente, existen γ_i tal que $\bigcup_{i=1}^{6} \gamma_i \Gamma_0(4) = \mathrm{SL}_2(\mathbb{Z})$. Observamos que la matriz $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ no pertenece a $\Gamma_0(4)$ por lo que tenemos los dos primeros representantes $\gamma_1 = Id$ y $\gamma_2 = S$. Para comprobar si una cierta matriz pertenece a una de las clases anteriores basta ver que $\gamma_j^{-} \gamma_i \notin \Gamma_0(4)\ \forall j < i$ Tomando $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ tenemos que, con una sencilla comprobación, podemos tomar $\gamma_3 = TS$, $\gamma_4 = T^2S$ y $\gamma_5 = T^3S$. Finalmente probando diferentes productos con S y T se encuentra el último representante $\gamma_6 = (TS)^2$.

1.4. Formas modulares para Γ

Análogamente a la idea de forma modular en $\mathrm{SL}_2(\mathbb{Z})$ podemos introducir el concepto de forma modular en un subgrupo de congruencia Γ. Los conceptos de holomorfía en $\mathbb{H}$ y ser débilmente modular de peso k se mantienen similares. El punto que tiene mayor interés es qué sucede con la holomorfía en los puntos límite. En $\mathrm{SL}_2(\mathbb{Z})$ todos los puntos de $\widehat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ son equivalentes pues existe un elemento τ en $\mathrm{SL}_2(\mathbb{Z})$ tal que para dos elementos a y b $\tau(a) = b$.

Definición. Sea Γ un subgrupo de congruencia de $\mathrm{SL}_2(\mathbb{Z})$ y sea k un entero. Una función $f\colon \mathbb{H} \to \mathbb{C}$ es una **forma modular de peso k con respecto a** Γ si:

1. f es holomorfa en $\mathbb{H}$,
2. f es **débilmente modular** de peso k, es decir, para toda matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$ se cumple:

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau), \quad \forall \tau \in \mathbb{H};$$

3. $f[\alpha]_k$ es holomorfa en ∞ para todo $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, donde $(f[\gamma]_k)(\tau) = (c\tau+d)^{-k} f(\gamma(\tau)), \quad \tau \in \mathbb{H}$.

El conjunto (espacio vectorial) de formas modulares de peso k para Γ se denota por $M_k(\Gamma)$.

Vamos a recuperar ahora la premisa inicial tomando el caso general, de cuántas formas podemos escribir un entero n como suma de $k \in \mathbb{N}$ cuadrados.

$$r(n,k) = \#\{v \in \mathbb{Z} \,:\, n = v_1^2 + \cdots + v_k^2\}$$

Consideremos la **función generadora de los números de representación**, es decir, la serie de potencias cuyo n-ésimo coeficiente es $r(n,k)$:

$$\theta(\tau,k) = \sum_{n=0}^{\infty} r(n,k) q^n, \quad \text{donde } q = e^{2\pi i \tau} \text{ y } \tau \in \mathbb{H}.$$

Para el caso $k = 4$, que es justamente el que nos interesa, la función va a pertenecer a $M_k(\Gamma)$ para un cierto subgrupo de congruencia Γ de $\mathrm{SL}_2(\mathbb{Z})$. Para probar esto vamos a ver como se transforma la función $\theta(\tau,4)$ bajo ciertos elementos del grupo modular. Es evidente que

$$\theta(\tau+1,k) = \theta(\tau,k) \text{ y por tanto también para k=4}$$

El otro elemento de $\mathrm{SL}_2(\mathbb{Z})$ que vamos a estudiar es $\gamma = \pm \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$

Denotamos $\theta(\tau,1)$ como $\theta(\tau)$

Utilizamos la igualdad $\theta\left(-1/(4\tau)\right) = \sqrt{-2i\tau} \cdot \theta(\tau)$ tenemos que:

$$\begin{aligned} \theta\left(\frac{\tau}{4\tau+1}\right) &= \theta\left(\frac{-1}{4(-1/(4\tau)-1)}\right) = \sqrt{2i\left(\frac{1}{4\tau+1}\right)}\,\theta\left(\frac{-1}{4\tau}-1\right) \\ &= \sqrt{2i\left(\frac{1}{4\tau+1}\right)}\,\theta\left(\frac{-1}{4\tau}\right) = \sqrt{2i\left(\frac{1}{4\tau}+1\right)}(-2i\tau)\theta(\tau) = \sqrt{4\tau+1}\cdot\theta(\tau). \end{aligned}$$

Veamos ahora la relación entre $\theta(\tau)$ y $\theta(\tau,4)$.

Observamos que

$$\theta(\tau) = \sum_{d\in\mathbb{Z}} e^{2\pi i d^2 \tau} \text{ y por tanto } \theta(\tau)^4 = \left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^4.$$

Desarrollamos en cuatro series:

$$\theta(\tau)^4 = \sum_{a\in\mathbb{Z}}\sum_{b\in\mathbb{Z}}\sum_{c\in\mathbb{Z}}\sum_{d\in\mathbb{Z}} q^{a^2+b^2+c^2+d^2}.$$

Como la suma de cuadrados es siempre un número no negativo podemos reescribir la serie agrupando por el valor del exponente, es decir tomamos la serie en función de $n = a^2+b^2+c^2+d^2$:

$$\theta(\tau)^4 = \sum_{n=0}^{\infty}\left(\sum_{\substack{(a,b,c,d)\in\mathbb{Z}^4\\ a^2+b^2+c^2+d^2=n}} 1\right) q^n.$$

Finalmente basta observar que:

$$\sum_{\substack{(a,b,c,d)\in\mathbb{Z}^4\\ a^2+b^2+c^2+d^2=n}} 1 = r(n,4).$$

Y por tanto tenemos que $\theta(\tau,4) = \theta(\tau)^4$ de lo cual obtenemos una segunda fórmula de transformación para la función generadora θ.

$$\theta\left(\frac{\tau}{4\tau+1},4\right) = (4\tau+1)^2\theta(\tau,4)$$

Una vez introducido el subgrupo $\Gamma_0(4)$, veamos qué funciones pertenecen a $M_2(\Gamma_0(4))$. Para ello veamos las *Series de Eisenstein* de peso 2 G_2.

$$G_2(\tau) = \sum_{(c,d)}{}' \frac{1}{(c\tau+d)^2}, \quad \tau\in\mathbb{H}$$

Donde el $(0,0)$ esta excluido del sumatorio. La serie G_2 no pertenece a $M_2(\Gamma_0(4))$ por problemas de invarianza y holomorfía. Esto motiva el siguiente resultado:

Proposición 1.4. *Sea $G_{2,N}(\tau) = G_2(\tau) - NG_2(N\tau)$. Entonces $G_{2,N}\in M_2(\Gamma_0(N))$.*

Demostración. La función $G_2(\tau)$ es holomorfa en $\mathbb{H}$ porque como $Img(\tau) > 0$ el denominador nunca se anula. Veamos que también es holomorfa en ∞. Utilizando el desarrollo de las Series de Eisenstein que hemos visto anteriormente para $k = 2$ tenemos que:

$$G_2(\tau) = \frac{3}{\pi^2}\left(1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n\right) \quad \text{donde } q = e^{2\pi i\tau} \text{ y } \sigma_1(n) = \sum_{d|n} d$$

Sustituyendo en $G_{2,N}(\tau)$ tenemos que:

$$G_{2,N}(\tau) = \frac{3}{\pi^2}\left(1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n\right) - N\frac{3}{\pi^2}\left(1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^{Nn}\right)$$

$$= \frac{3}{\pi^2}\left((1-N) - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n + 24N\sum_{n=1}^{\infty}\sigma_1(n)q^{Nn}\right)$$

Observamos que cuando $\tau\to i\infty$ $q^n, q^{Nn}\to 0$ y como la serie no tiene términos de exponente negativo, $G_{2,N}(\tau)$ tiende a $\frac{3}{\pi^2}(1-N)$ y por tanto es holomorfa en ∞.

Veamos que $G_{2,N}$ es débilmente modular de peso 2. Sea $\gamma = \begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma_0(N)$, tenemos que $ad-bc = 1$ y $c\equiv 0 \pmod N$, por tanto existe $c'\in\mathbb{Z}$ tal que $c = c'N$.

Cuando aplicamos $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ a G_2 tenemos que:

$$G_2(\gamma\tau) = (c\tau+d)^2 G_2(\tau) - 2\pi i c(c\tau+d).$$

Definimos $\gamma' = \begin{pmatrix} a & bN \\ c' & d \end{pmatrix}$. Como $ad-bc=1$ y $c=c'N$, tenemos que el determinante de γ_N es:

$$\det(\gamma_N) = ad - (bN)c' = ad - bc = 1,$$

y por tanto γ' pertenece a $\mathrm{SL}_2(\mathbb{Z})$. Observamos también que:

$$\gamma'(N\tau) = \frac{a(N\tau)+bN}{c'(N\tau)+d} = N\frac{a\tau+b}{c'N\tau+d} = N\frac{a\tau+b}{c\tau+d} = N\gamma\tau,$$

Aplicamos la transformación anterior de G_2 para γ':

$$G_2(\gamma'(N\tau)) = (c'\cdot(N\tau)+d)^2 G_2(N\tau) - 2\pi i c'(c'\cdot(N\tau)+d).$$

Aplicando que $c'(N\tau)+d = c\tau+d$ y $c' = c/N$ obtenemos la siguiente igualdad:

$$G_2(N\gamma\tau) = (c\tau+d)^2 G_2(N\tau) - 2\pi i \frac{c}{N}(c\tau+d).$$

Una vez obtenida esta expresión desarrollamos $G_{2,N}(\gamma\tau)$:

$$G_{2,N}(\gamma\tau) = G_2(\gamma\tau) - NG_2(N\gamma\tau) = \left[(c\tau+d)^2 G_2(\tau) - 2\pi i c(c\tau+d)\right]$$

$$-N\left[(c\tau+d)^2 G_2(N\tau) - 2\pi i \frac{c}{N}(c\tau+d)\right]$$

Operando tenemos que:

$$= (c\tau+d)^2 G_2(\tau) - 2\pi i c(c\tau+d) - N(c\tau+d)^2 G_2(N\tau) + 2\pi i c(c\tau+d)$$

$$= (c\tau+d)^2 \left[G_2(\tau) - NG_2(N\tau)\right] = (c\tau+d)^2 G_{2,N}(\tau).$$

Concluimos que $G_{2,N}$ es efectivamente invariante de peso 2 bajo la acción de $\Gamma_0(N)$. □

Utilizando esta proposición para $G_{2,2}$ y $G_{2,4}$ y teniendo en cuenta que $M_2(\Gamma_0(2)) \subset M_2(\Gamma_0(4))$ (El subgrupo más pequeño, $\Gamma_0(4) \subset \Gamma_0(2)$, permite un mayor número de funciones por ser "menos exigente") obtenemos dos formas modulares linealmente independientes que pertenecen a $M_2(\Gamma_0(4))$.
Si conseguimos probar que $dim(M_2(\Gamma_0(4))) = 2$ tendremos una base. En el momento en que este fijada, como $\theta(\tau,4) = \sum_{n=0}^{\infty} r(n,4)q^n \in M_2(\Gamma_0(4))$, será combinación lineal de los elementos de la base y por tanto tendremos una fórmula explícita, lo que nos proporcionará la solución del Teorema de los Cuatro Cuadrados. A partir de ahora vamos a desarrollar las herramientas necesarias para probar esta igualdad.

Capítulo 2

Curvas elípticas y espacios modulares

En este capítulo vamos a estudiar el cociente $\Gamma \setminus \mathbb{H}$ para diferentes subgrupos de congruencia y daremos una interpretación como espacio modular en términos de curvas elípticas complejas con cierta estructura adicional. Para poder estudiar sus propiedades vamos a ver que posee una la estrecha relación con las curvas elípticas complejas. Estas vienen determinadas, salvo isomorfía, por un retículo en $\mathbb{C}$. Es decir, vamos a probar que existe una biyección entre toros complejos (salvo homotecia) y curvas elípticas complejas (salvo isomorfismo). La principal referencia será [1, sec 1.3,1.4 y 1.5] y en menor medida [2, capítulo 7].

2.1. Toros Complejos

Comenzamos el capítulo introduciendo algunas nociones básicas sobre toros complejos, cuya utilidad se verá más adelante.

Definición. Un **retículo** en $\mathbb{C}$ es un subconjunto de la forma $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$, donde $\{\omega_1, \omega_2\}$ es una base de $\mathbb{C}$ sobre $\mathbb{R}$.

Dado un retículo como en la definición, normalizamos tomando $\omega_1/\omega_2 \in \mathbb{H}$.

Lema 2.1. *Consideremos dos retículos $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ y $\Lambda' = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$, con $\omega_1/\omega_2 \in \mathbb{H}$ y $\omega_1'/\omega_2' \in \mathbb{H}$. Entonces $\Lambda' = \Lambda$ si y solo si*

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \text{ para alguna matriz } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

Demostración. Veamos la implicación a derecha, dado $\Lambda' = \Lambda$, los generadores de Λ' están en Λ:

$$\begin{cases} \omega_1' = a\omega_1 + b\omega_2, \\ \omega_2' = c\omega_1 + d\omega_2, \end{cases} \qquad \text{con } a,b,c,d \in \mathbb{Z}.$$

Esto define una matriz $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$.

Análogamente, como los generadores de Λ están en Λ' tenemos que:

$$\begin{cases} \omega_1 = a'\omega_1' + b'\omega_2', \\ \omega_2 = c'\omega_1' + d'\omega_2', \end{cases} \qquad \text{con } a',b',c',d' \in \mathbb{Z}.$$

con lo que obtenemos una segunda matriz $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ de manera que $\gamma\gamma' = Id$, y por tanto $det(\gamma) = \pm 1$. Finalmente, como ω_1/ω_2 y $\omega_1'/\omega_2' \in \mathbb{H}$ se conserva la orientación por lo que $det(\gamma) = 1$ y por tanto $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

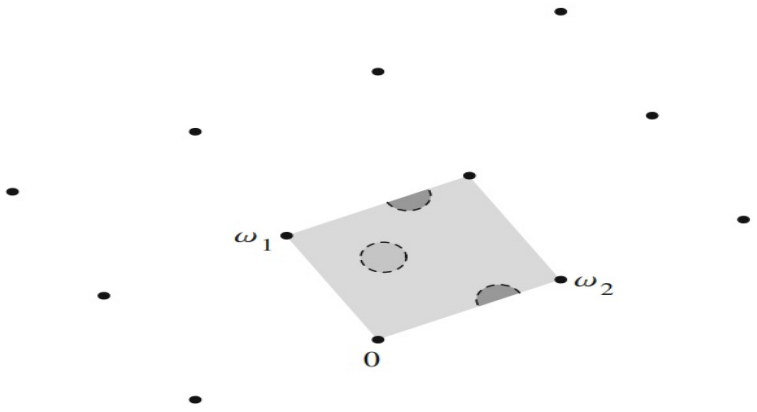

Figura 2.1: Toro Complejo

Probamos la implicación a izquierda. Veamos que $\Lambda' \subset \Lambda$. Tomamos $z' \in \Lambda'$ que es de la forma $z' = n\omega_1' + m\omega_2'$ como

$$\begin{cases} \omega_1' = a\omega_1 + b\omega_2, \\ \omega_2' = c\omega_1 + d\omega_2, \end{cases} \qquad \text{con } a,b,c,d \in \mathbb{Z}.$$

sustituyendo tenemos que $z' = n(a\omega_1 + b\omega_2) + m(c\omega_1 + d\omega_2) \in \Lambda$. Como γ tiene inversa en $\mathrm{SL}_2(\mathbb{Z})$ por el mismo razonamiento $\Lambda \subset \Lambda'$. □

Con este lema introducimos la siguiente definición.

Definición. Un **toro complejo** es un cociente del plano complejo por un retículo:

$$\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}$$

Si observamos un toro complejo desde el punto de vista algebraico, es un grupo abeliano con la suma heredada de $\mathbb{C}$.

Dado un toro complejo tiene sentido hablar de función holomorfa pues es una *Superficie de Riemann*, lo que quiere decir que localmente difeomorfo a $\mathbb{C}$.

Proposición 2.1. *Supongamos que*

$$\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$$

es una aplicación holomorfa entre toros complejos. Entonces existen números complejos m, b con $m\Lambda \subset \Lambda'$ tales que

$$\varphi(z + \Lambda) = mz + b + \Lambda'.$$

La aplicación es invertible si y solo si $m\Lambda = \Lambda'$.

Nos interesan concretamente las aplicaciones holomorfas entre toros complejos en las que $b = 0$, dado que en este caso φ es un homomorfismo de grupos respecto a la suma entre $\mathbb{C}/\Lambda$ y $\mathbb{C}/\Lambda'$ que es un isomorfimo en el caso de que $m\Lambda = \Lambda'$.
Lo interesante de este punto es que podemos reemplazar el retículo por otro homotético (reescalado por un factor m). Es decir que dos toros complejos son isomorfos si y solo si los retículos que los definen son homotéticos.

Veamos un isomorfismo de particular interés, partamos de un retículo arbitrario

$$\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} \quad \text{con} \quad \omega_1/\omega_2 \in \mathbb{H}.$$

Sea $\tau = \omega_1/\omega_2$ y sea $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$. Entonces, como $(1/\omega_2)\Lambda = \Lambda_\tau$, tenemos que la aplicación

$$\varphi_\tau : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda_\tau, \quad \varphi(z + \Lambda) = z/\omega_2 + \Lambda_\tau$$

es un isomorfismo. Por tanto todo toro complejo es isomorfo a otro cuyo retículo está generado por un número complejo $\tau \in \mathbb{H}$ y por 1.

Vamos a introducir dos casos concretos de homomorfismos que aparecerán más adelante. La aplicación **Multiplicar por entero** se define como sigue: dado $N \in \mathbb{N}^+$ y Λ un retículo,

$$[N] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda, \quad z+\Lambda \to Nz+\Lambda$$

Observamos que este homomorfismo es suprayectivo y su núcleo es un subgrupo de $\mathbb{C}/\Lambda$ isomorfo a $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, se denomina como los **N-Puntos de torsión de** $\mathbb{C}/\Lambda$ y se denota como $E[N]$ (Esta notación tendrá más sentido cuando introduzcamos las curvas elípticas).
Veamos un ejemplo, tomamos $\tau \in \mathbb{H}$ y el retículo Λ_τ. Por la definición tenemos que $E_\tau[N] = \ker([N]) = \{z \in \mathbb{C}/\Lambda_\tau \mid Nz \in \Lambda_\tau\}$ o equivalentemente $E_\tau[N] = \left\{\frac{a}{N} + \frac{b}{N}\tau + \Lambda_\tau \mid a,b \in \mathbb{Z}/N\mathbb{Z}\right\}$. Por tanto $E_\tau[N]$ es el subgrupo en el cociente generado por las clases $1/N+\Lambda$ y $\tau/N+\Lambda$, que tiene orden N^2.

Sea Λ_τ un retículo y C un subgrupo cíclico de $E[N]$ isomorfo a $\mathbb{Z}/N\mathbb{Z}$, los elementos de C son de la forma $\{c' + \Lambda_\tau\}$. Sea c el punto que genera C como subgrupo de $E[N]$. Entonces, la aplicación **cociente ciclo** se define como:

$$\pi : \mathbb{C}/\Lambda_\tau \longrightarrow \mathbb{C}/\Lambda_C, \quad z+\Lambda_\tau \mapsto z+\Lambda_C$$

Donde $\Lambda_c = \bigcup_{k=0}^{N-1} \left(\frac{kc}{N} + \Lambda\right) = \Lambda' = \mathbb{Z}\cdot\frac{c}{N} + \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\tau$. Observamos que $\Lambda_\tau \subsetneq N\Lambda_C$ cuando $N > 1$. Esta aplicación no es un isomorfismo y tiene núcleo C.

En el caso en el que $c = 1$, Λ_C será el retículo $\tau\mathbb{Z} \oplus \frac{1}{N}\mathbb{Z}$.

2.2. Curvas elípticas

En este trabajo no vamos a desarrollar en profundidad los conceptos relacionados con las curvas elípticas. Para una idea más amplia de este campo se puede consultar la siguiente referencia [3].

Definición. Dados $p, q \in \mathbb{C}$ llamamos **Curva elíptica compleja**, o Curva elíptica cuando no haya ambigüedad, al conjunto de soluciones en los complejos de la ecuación:

$$y^2 = x^3 - px - q$$

Decimos que dos curvas elípticas son isomorfas si dadas $E_1 = y^2 = x^3 - px - q$ y $E_2 = y^2 = x^3 - Px - Q$ existe $z \in \mathbb{C}$ tal que $p = z^4P$ y $q = z^6Q$.

Ahora vamos a ver que un toro complejo $\mathbb{C}/\Lambda$ puede ser visto como una curva elíptica compleja.

Dado un retículo Λ una función meromorfa $f : \mathbb{C}/\Lambda \to \hat{\mathbb{C}}$ se puede ver como una función $f : \mathbb{C} \to \hat{\mathbb{C}}$ Λ-periódica. El ejemplo más importante es la Función $\wp$ de Weierstrass, dado un retículo Λ definimos:

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right), \quad z \in \mathbb{C},\ z \notin \Lambda$$

y su derivada

$$\wp'_\Lambda(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}, \quad z \in \mathbb{C},\ z \notin \Lambda$$

Extendemos la aplicación a los puntos del retículo Λ haciéndolos corresponder al infinito.

Veamos que efectivamente la función $\wp_\Lambda$ (la denotamos como $\wp$ cuando no haya confusión del retículo al que se refiere) es Λ-periódica y por tanto está bien definida como función del toro complejo. Observemos que $\wp$ es par. Como ω recorre todo el retículo se puede sustituir por $-\omega$, por tanto

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

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

Además su derivada $\wp'$ es Λ-periódica. Sea $\omega' \in \Lambda$, como ω recorre todo el retículo también lo hará $\omega + \omega'$

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

Finalmente, dado $\omega' \in \Lambda$ tomamos $\wp(z+\omega') - \wp(z)$ que es constante por tener derivada nula. Evaluando en $-\omega'/2$ tenemos que

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

Podemos escribir las serie de Eisenstein de peso k en función de Λ_τ como $G_k(\Lambda) = \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^k}$

Proposición 2.2. *Dado un retículo $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ y sea $\omega_3 = \omega_1 + \omega_2$ se cumple lo siguiente:*

1. *La función $\wp$ y su derivada $\wp'$ cumplen esta ecuación*

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

   donde $g_2(\Lambda) = 60\,G_4(\Lambda)$ y $g_3(\Lambda) = 140\,G_6(\Lambda)$.

2. *La ecuación del punto 1. $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ es igual a*

$$y^2 = 4(x-e_1)(x-e_2)(x-e_3), \quad \text{donde } e_i = \wp\Big(\frac{\omega_i}{2}\Big) \text{ para } i = 1,2,3.$$

   Esta ecuación es no singular, lo que quiere decir que el lado derecho de la misma no tiene raíces iguales.

Demostración. 1.La serie de Laurent de $\wp$ es $\frac{1}{z^2} + \sum_{\substack{n=2\\ n \text{ par}}}^{\infty}(n+1)G_{n+2}(\Lambda)z^n$ para $|z| < |\omega|$. La demostración de esta afirmación se puede encontrar en [1, pág 33] . Entonces

$$\wp(z) = \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + O(z^6) \text{ y } \wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + O(z^7)$$

Utilizando esto podemos operar para ver que ambos lados de la ecuación son iguales a

$$\frac{4}{z^6} - \frac{24G_4(\Lambda)}{z^2} - 80G_6(\Lambda) + O(z^2)$$

Tenemos que la diferencia entre ambas partes de la ecuación es holomorfa y Λ-periódica por lo que es acotada y por tanto constante. Como $O(z^2) \to 0$ cuando $z \to 0$ tenemos que ambas partes son iguales. □

La proposición anterior muestra que la aplicación

$$z \mapsto \big(\wp_\Lambda(z), \wp'_\Lambda(z)\big)$$

lleva los puntos que no pertenecen al retículo Λ a puntos $(x,y) \in \mathbb{C}^2$ que satisfacen la ecuación cúbica $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$. La aplicación es biyectiva, ya que en general un valor $x \in \mathbb{C}$ es tomado dos veces por $\wp_\Lambda$ en $\mathbb{C}/\Lambda$, es decir,

$$x = \wp_\Lambda(\pm z + \Lambda),$$

y los dos valores y que satisfacen la ecuación cúbica son

$$\wp'(\pm z + \Lambda) = \pm\wp'(z+\Lambda).$$

De este modo hemos encontrado una aplicación, que viene determinada por la función de Weierstrass $\wp$ y su derivada $\wp'$, que asocia los puntos del retículo Λ con las soluciones de la curva elíptica E.

$$(\wp, \wp') : \text{toro complejo} \longrightarrow \text{curva elíptica}.$$

De hecho esta aplicación es una biyección, como queda claro tras ver la siguiente proposición, cuya demostración puede encontrarse en [1, pág 35]:

Proposición 2.3. *Dada una curva elíptica $y^2 = 4x^3 - a_2x - a_3$, $\quad a_2^3 - 27a_3^2 \neq 0$, existe un retículo Λ tal que $a_2 = g_2(\Lambda) \quad y \quad a_3 = g_3(\Lambda)$.*

Hemos conseguido establecer una relación entre toros complejos y curvas elípticas complejas. Más concretamente, hemos visto que curvas elípticas isomorfas equivalen a toros complejos homotéticos.

2.3. Curvas y Espacios Modulares

En esta sección vamos a estudiar el espacio cociente resultante de relacionar dos puntos de $\mathbb{H}$ de la siguiente forma: $\tau \sim \tau'$ si $\exists\, \gamma \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\gamma(\tau) = \tau'$. Esta relación se puede extender a los subgrupos de congruencia de $\mathrm{SL}_2(\mathbb{Z})$ como vamos a ver a continuación.

Vamos a estudiar el subgrupo $\Gamma_0(N)$. Sea N un entero positivo, llamamos **curva elíptica enriquecida para** $\Gamma_0(N)$ a un par ordenado (E,C), donde:

- E es una curva elíptica compleja, y
- $C \subset E$ es un subgrupo cíclico de orden N.

Dos pares (E,C) y (E',C') son equivalentes, $(E,C) \sim (E',C')$, si existe un isomorfismo $E \xrightarrow{\sim} E'$que lleva C a C'.

El conjunto de clases de equivalencia se denota

$$S_0(N) = \{\text{curvas elípticas enriquecidas para } \Gamma_0(N)\}/\sim .$$

$S_0(N)$ es un **espacio modular** de clases de isomorfía de curvas elípticas complejas y subgrupos cíclicos de la curva de orden N. Un elemento de $S_0(N)$ se denota $[E,C]$, donde los corchetes indican clase de equivalencia.

Para un subgrupo de congruencia Γ de $\mathrm{SL}_2(\mathbb{Z})$, actuando en $\mathbb{H}$ por la izquierda, definimos la **curva modular** $Y(\Gamma)$ (Llamamos a este cociente curva porque puede probarse que es una curva algebraica, en el sentido de que viene definida por una ecuación, sin embargo en este trabajo no llegamos a probar este hecho, simplemente la estudiaremos como superficie de Riemann) como el espacio cociente de órbitas bajo Γ:

$$Y(\Gamma) = \Gamma\backslash\mathbb{H} = \{\Gamma\tau : \tau \in \mathbb{H}\}.$$

La curva modular correspondiente a $\Gamma_0(N)$, se denota como :

$$Y_0(N) = \Gamma_0(N)\backslash\mathbb{H},$$

Dadas estas definiciones veamos el siguiente teorema que establece la relación entre ambos conceptos.

Teorema 2.2. *Sea N entero positivo, El espacio modular para* $\Gamma_0(N)$ *es*

$$S_0(N) = \left\{[E_\tau, \tfrac{1}{N} + \Lambda_\tau] : \tau \in \mathbb{H}\right\}.$$

Dos puntos $[E_\tau, \frac{1}{N} + \Lambda_\tau]$ *y* $[E_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}]$ *son iguales si y solo si* $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$.

Por lo tanto, existe una biyección $\psi_0 : S_0(N) \xrightarrow{\sim} Y_0(N), \quad [\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau] \mapsto \Gamma_0(N)\tau.$

Un esbozo de la demostración de este teorema se encuentra en [1, pág 414].

Capítulo 3

Curvas modulares como Superficies de Riemann

En este capítulo vamos a estudiar las curvas modulares, $Y(\Gamma)$, ver que son Superficies de Riemann y que pueden ser compactificadas. En este capítulo se sigue principalmente el capítulo 2 de [1] y también se utilizan algunos resultados aislados del capítulo 3.

3.1. Topología de una Curva Modular

El semiplano superior $\mathbb{H}$ hereda la topología euclídea como subespacio de $\mathbb{R}^2$. La proyección natural

$$\pi\colon \mathbb{H} \to Y(\Gamma), \quad \pi(\tau) = \Gamma\tau$$

dota a $Y(\Gamma)$ de la topología cociente, lo que significa que un subconjunto de $Y(\Gamma)$ es abierto si su imagen inversa bajo π en $\mathbb{H}$ es abierta.

Dado que $\mathbb{H}$ es conexo y π es continua, el cociente $Y(\Gamma)$ también es conexo. $\mathbb{H}$ es Hausdorff por ser un subconjunto de $\mathbb{R}^2$, aunque esto no implica que $Y(\Gamma)$ lo sea. Para probar esto, necesitamos más herramientas.

Lema 3.1. *Dado π como la proyección natural y U_1 y U_2 conjuntos cualesquiera de $\mathbb{H}$ tenemos que,*

$$\pi(U_1) \cap \pi(U_2) = \emptyset \text{ en } Y(\Gamma) \quad \Longleftrightarrow \quad \Gamma(U_1) \cap U_2 = \emptyset \text{ en } \mathbb{H}$$

La idea clave de esta sección es ver que para dos puntos distintos de $\mathbb{H}$ existen entornos suficientemente pequeños tales que la acción de $\mathrm{SL}_2(\mathbb{Z})$ que lleva un punto "lejos"del otro también lleve su entorno fuera del entorno del otro. Esta idea se formaliza con la siguiente proposición.

Proposición 3.1. *Dados $\tau_1, \tau_2 \in \mathbb{H}$, existen entornos U_1 de τ_1 y U_2 de τ_2 en $\mathbb{H}$ tal que:*

$$\text{Para todo } \gamma \in \mathrm{SL}_2(\mathbb{Z}), \text{ si } \gamma(U_1) \cap U_2 \neq \emptyset \text{ entonces } \gamma(\tau_1) = \tau_2.$$

Demostración. Tomamos U_1^* y U_2^* entornos con clausuras compactas de τ_1 y τ_2 respectivamente. Vamos a estudiar la intersección de $\gamma(U_1^*)$ con U_2^* con $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Para todo par de enteros (c,d) con $mcd(c,d) = 1$ salvo para un número finito se satisface la siguiente condición:

$$\sup\{Im(\gamma(\tau)) : \gamma \in \mathrm{SL}_2(\mathbb{Z}) \text{ con fila inferior } (c,d), \tau \in U_1^*\} < \text{ínf}\{\mathrm{Im}(\tau) : \tau \in U_2^*\}$$

(Se prueba del hecho de que $Im(\gamma(\tau)) = Im(\tau)/|c\tau + d|^2$). Y por tanto $\gamma(U_1^*) \cap U_2^*$ es vacío salvo para un número finito de γ. Además, para todo par de enteros (c,d) tal que $mcd(c,d) = 1$, las matrices $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ cuya fila inferior sea (c,d) se pueden escribir de la siguiente forma:

$$\left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} : k \in \mathbb{Z} \right\}$$

donde (a,b) es cualquier par que satisfaga que $ad-bc=1$. (Por el hecho de que $\det = (a+kc)(d) - (b+kd)(c) = ad-bc+k(cd-cd) = 1$).

Con estas dos condiciones tenemos que $\gamma(U_1^*)\cap U_2^* = \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}(U_1^*)+k\right)\cap U_2^*$ es vacío para todos excepto un número finito de γ.

Sea $F = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma(U_1^*)\cap U_2^* \neq \emptyset, \gamma(\tau_1) \neq \tau_2\}$, sabemos que es un conjunto finito. Para cada $\gamma \in F$ existen entornos disjuntos $U_{1,\gamma}$ de $\gamma(\tau_1)$ y $U_{2,\gamma}$ de τ_2 en $\mathbb{H}$. Definidos como:

$$U_1 = U_1^* \cap \left(\bigcap_{\gamma\in F} \gamma^{-1}(U_{1,\gamma})\right), \text{ entorno de } \tau_1$$

$$U_2 = U_2^* \cap \left(\bigcap_{\gamma\in F} U_{2,\gamma}\right), \text{ entorno de } \tau_2$$

Tomamos un $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\gamma(U_1)\cap U_2 \neq \emptyset$. Basta con ver que $\gamma(\tau_1) = \tau_2$ y por tanto $\gamma \notin F$. Pero si $\gamma \in F$, entonces $\gamma^{-1}(U_{1,\gamma}) \supset U_1$ y $U_{2,\gamma} \supset U_2$, así que

$$U_{1,\gamma}\cap U_{2,\gamma} \supset \gamma(U_1)\cap U_2 \neq \emptyset,$$

una contradicción ya que $U_{1,\gamma}$ y $U_{2,\gamma}$ son disjuntos y por tanto queda probada la proposición. □

Proposición 3.2. *Para cualquier subgrupo de congruencia* Γ *de* $\mathrm{SL}_2(\mathbb{Z})$*, la curva modular* $Y(\Gamma)$ *es Hausdorff.*

Demostración. Sean $\pi(\tau_1)$ y $\pi(\tau_2)$ puntos distintos en $Y(\Gamma)$. Tomamos entornos U_1 de τ_1 y U_2 de τ_2 como en la proposición anterior. Como $\gamma(\tau_1) \neq \tau_2$ para todo $\gamma \in \Gamma$, la proposición implica que $\Gamma(U_1)\cap U_2 = \emptyset$ en $\mathbb{H}$, y por el Lema 3.1 sumado a que π es abierta tenemos que $\pi(U_1)$ y $\pi(U_2)$ son entornos disjuntos de $\pi(\tau_1)$ y $\pi(\tau_2)$ en $Y(\Gamma)$. □

3.2. Cartas

Ahora vamos a buscar cartas apropiadas para cada punto de $Y(\Gamma)$, vamos a ver que para la mayoría de los puntos no va a haber ningún problema pero van a existir unos ciertos puntos, característicos de cada curva, en los que tendremos que afinar un poco más. Formalmente buscamos para cada $\pi(\tau) \in Y(\Gamma)$ un entorno $\tilde{U}$ y un homeomorfismo $\phi : \tilde{U} \to V \subset \mathbb{C}$ de tal forma que dados $\phi_1,\ \phi_2$ si $U_i \cap U_j \neq \emptyset$, entonces:

$$\phi_j \circ \phi_i^{-1} :\ \phi_i(U_i\cap U_j) \to \phi_j(U_i\cap U_j) \quad \text{es holomorfa}$$

Para aquellos puntos $\pi(\tau)$ tales que τ solo es fijado por la identidad, es decir, no existe elemento de $\gamma \in \Gamma$ no trivial ($\gamma \neq \pm Id$) tal que $\gamma(\tau) = \tau$ la Proposición 3.1 nos asegura que podemos encontrar un entorno suficientemente pequeño que no contenga ningún punto Γ-equivalente a τ.

El problema se da en aquellos puntos tales que existe $\gamma \in \Gamma$ no trivial tal que $\gamma(\tau) = \tau$. Esto motiva la siguiente definición.

Definición. Sea Γ un subgrupo de congruencia de $\mathrm{SL}_2(\mathbb{Z})$. Para cada punto $\tau \in \mathbb{H}$, sea Γ_τ el *subgrupo de isotropía de* τ, es decir, el subgrupo que fija τ en Γ:

$$\Gamma_\tau = \{\gamma \in \Gamma : \gamma(\tau) = \tau\}.$$

Un punto $\tau \in \mathbb{H}$ es un **punto elíptico** de Γ si Γ_τ es no trivial como grupo de transformaciones, es decir, si $\{\pm I\} \subsetneq \{\pm I\}\Gamma_\tau$

Proposición 3.3. *Sea* Γ *un subgrupo de congruencia de* $\mathrm{SL}_2(\mathbb{Z})$*. Para cada punto elíptico* τ *de* Γ*, el subgrupo de isotropía* Γ_τ *es finito y cíclico.*

Para probar esta proposición se necesitan varios resultados previos que pese a no tener una dificultad mayor que otros que se ven a lo largo del trabajo por la limitación de espacio no se añaden. Se pueden encontrar dichos resultados junto a la demostración de la proposición en [1, sec 2.3].

A cada punto $\tau \in \mathbb{H}$ le asociamos un entero positivo h que llamamos **periodo**,

$$h_\tau = |\{\pm I\}\Gamma_\tau/\{\pm I\}| = \begin{cases} |\Gamma_\tau|/2 & \text{si } -I \in \Gamma_\tau, \\ |\Gamma_\tau| & \text{si } -I \notin \Gamma_\tau. \end{cases}$$

El motivo de no tomar $h_\tau = |\Gamma_\tau|$ es el hecho de que $-Id$ actúa de manera trivial sobre $\mathbb{H}$.

Para tomar coordenadas en un punto elíptico de $Y(\Gamma)$ empezamos definiendo

$$\delta_\tau = \begin{pmatrix} 1 & -\tau \\ 1 & -\bar{\tau} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}) \quad \text{porque } \tau \in \mathbb{H}$$

El subgrupo de isotropía de 0 en el grupo $\left(\delta_\tau\{\pm I\}\Gamma\delta_\tau^{-1}\right)_0/\{\pm I\}$ es el subgrupo de isotropía de τ en $\{\pm I\}\Gamma/\{\pm I\}$ y por tanto es cíclico de orden h_τ. Dado el hecho de que este grupo de transformaciones lineares fraccionales fija el 0 y el infinito (porque en Γ se fijan τ y $\bar{\tau}$) tenemos que es de la forma $z \to az$ y como el grupo es cíclico deben ser rotaciones de $2\pi/h_\tau$ entorno al 0.

Como consecuencia de la Proposición 3.1 tenemos el siguiente corolario,

Corolario 3.1. Sea Γ un subgrupo de congruencia de $\mathrm{SL}_2(\mathbb{Z})$. Cada punto $\tau \in \mathbb{H}$ tiene un entorno U en $\mathbb{H}$ tal que para todo $\gamma \in \Gamma$, si $\gamma(U) \cap U \neq \emptyset$ entonces $\gamma \in \Gamma_\tau$. U no contiene puntos elípticos salvo τ en caso de que lo sea.

Dado cualquier punto $\pi(\tau) \in Y(\Gamma_0(4))$, tomamos un entorno U como en el corolario. Definimos $\psi : U \to \mathbb{C}$ como $\psi = \rho \circ \delta$ donde $\delta = \delta_\tau$ y ρ es la función potencia $\rho(z) = z^h$ con $h = h_\tau$. De esta manera ψ actúa como en la Figura 3.1. $V = \psi(U)$ es abierto por el Teorema de la función abierta de Análisis Complejo.

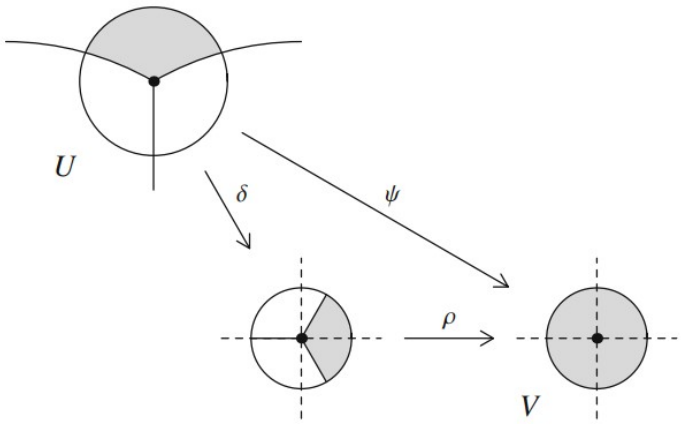

Figura 3.1: Acción de ψ

Dado que la proyección π y la aplicación ψ identifican los mismos puntos de U, debería existir una equivalencia entre las imágenes de U bajo las dos aplicaciones. Se puede probar que existe una biyección φ entre $\pi(U)$ y V, además φ es un homeomorfismo.

$$\pi(U) \xrightarrow{\varphi} V$$

Finalmente tenemos que verificar que las aplicaciones de transición entre cartas coordenadas son holomorfas. Es decir, dados $\pi(U_1)$ y $\pi(U_2)$ con intersección no nula, necesitamos verificar que $\phi_{2,1}$, la restricción de $\phi_2 \circ \phi_1^{-1}$ a $\phi_1(\pi(U_1) \cap \pi(U_2))$ sea holomorfa. Esto se puede probar a partir de como hemos definido la aplicación ψ. La demostración completa se encuentra en [1, pág 50 y 51].

Tenemos el siguiente lema técnico de gran utilidad a la hora de estudiar puntos elípticos.

Lema 3.2. *Para cada punto elíptico τ de Γ, el subgrupo de isotropía Γ_τ es cíclico finito.*

Demostración. Como $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{j=1}^{d} \Gamma\gamma_j$, los puntos elípticos de $Y(\Gamma)$ son un subconjunto de $E_\Gamma = \{\Gamma\gamma_j(i),\ \Gamma\gamma_j(\mu_3) : 1 \leq j \leq d\}$. La segunda afirmación proviene de que Γ_τ es un subgrupo de $\mathrm{SL}_2(\mathbb{Z})_\tau$ para todo $\tau \in \mathbb{H}$. □

La idea detrás del siguiente resultado es que el estudio de los puntos elípticos de $\Gamma_0(4)$ puede reducirse a estudiar ciertas ecuaciones cuadráticas o más generalmente los anillos de enteros cuadráticos correspondientes. Más concretamente, las propiedades de los puntos elípticos se traducen en propiedades aritméticas de $\mathbb{Z}[i]$ y $\mathbb{Z}[\mu_6]$. La demostración del teorema escapa en complejidad del alcance de este trabajo pero puede encontrarse en [1, pág. 92 y sig.]

Teorema 3.3. *Los puntos elípticos de periodo 2 de $\Gamma_0(N)$ están en biyección con los ideales J de $\mathbb{Z}[i]$ tales que $\mathbb{Z}[i]/J \cong \mathbb{Z}/N\mathbb{Z}$.*

Los puntos elípticos de periodo 3 de $\Gamma_0(N)$ están en biyección los ideales J de $\mathbb{Z}[\mu_6]$ (donde $\mu_6 = e^{2\pi i/6}$) tales que $Z[\mu_6]/J \cong \mathbb{Z}/N\mathbb{Z}$.

Este teorema nos permite dar una fórmula exacta para el número de puntos elípticos de periodo 2 y 3. Definiendo $\left(\frac{-1}{p}\right)$ como ± 1 si $p \equiv \pm 1 \pmod 4$ y como 0 si $p = 2$, se tiene:

$$\varepsilon_2(\Gamma_0(N)) = \begin{cases} \sum_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{si } 4 \nmid N, \\ 0 & \text{si } 4 \mid N, \end{cases}$$

De manera similar, si $\left(\frac{-3}{p}\right)$ es ± 1 si $p \equiv \pm 1 \pmod 3$ y 0 si $p = 3$, entonces

$$\varepsilon_3(\Gamma_0(N)) = \begin{cases} \sum_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{si } 9 \nmid N, \\ 0 & \text{si } 9 \mid N, \end{cases}$$

En el caso concreto de $N = 4$ tenemos que $\varepsilon_2 = 0$ y $\varepsilon_3 = 0$.

3.3. Puntos límite

En esta sección vamos a estudiar como se comporta la acción de $\mathrm{SL}_2(\mathbb{Z})$ cuando tendemos a los límites de $\mathbb{H}$. Dado $\tau \in \mathbb{H}$ y un $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con $mcd(a,c) = 1$ tenemos que cuando τ tiende a infinito en $\mathbb{H}$ ($Im(\tau) \to \infty$) $\gamma(\tau) \to a/c$. Por la Identidad de Bezout podemos escoger a y c coprimos como queramos. Por tanto la idea que subyace es que el conjunto $\mathbb{Q} \cup \{\infty\}$ forma una órbita para la acción de $\mathrm{SL}_2(\mathbb{Z})$. En el caso de trabajar con un subgrupo de congruencia Γ todos puntos de $\mathbb{Q} \cup \{\infty\}$ no tienen porque ser equivalentes entre si y por tanto se requiere un estudio en mayor profundidad.

Definición. Sea $Y(\Gamma)$ curva modular, llamamos **Dominio fundamental** a un subconjunto $D \subseteq \mathbb{H}$ que satisface las siguientes propiedades:

1. Cobertura
$$Y(\Gamma) = \bigcup_{\gamma \in \Gamma} \gamma \cdot D,$$
es decir, cada punto de $Y(\Gamma)$ es equivalente bajo la acción de Γ a algún punto de D.

2. Traslaciones casi disjuntas
$$\gamma \cdot Int(D) \cap Int(D) = \emptyset \quad \text{para todo} \quad \gamma \in \Gamma \setminus \{\mathrm{id}\},$$
es decir, los puntos del interior de D no se superponen bajo la acción de Γ

Ejemplo 3. Veamos el caso más simple, $Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. $Y(1)$ puede identificarse esencialmente con el conjunto

$$D = \{\tau \in \mathbb{H} : |\mathrm{Re}(\tau)| \leq 1/2, |\tau| \geq 1\}.$$

La demostración de esta afirmación se encuentra en [1, pág 52 y 53].

Dada una curva modular Γ vamos a ver qué puntos debemos añadir para transformarla en una superficie de Riemann Compacta que denotaremos $X(\Gamma)$. Recordamos el concepto de cúspide introducido en el capítulo uno, Γ-clases de equivalencia de $\mathbb{Q}\cup\{\infty\}$.

Observamos que el subgrupo de isotropía de ∞ en $\mathrm{SL}_2(\mathbb{Z})$ esta formado por las traslaciones de la forma,

$$\mathrm{SL}_2(\mathbb{Z})_\infty = \left\{ \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} : m \in \mathbb{Z} \right\}.$$

En general, sea Γ un subgrupo de congruencia de $\mathrm{SL}_2(\mathbb{Z})$. Para compactificar la curva modular $Y(\Gamma) = \Gamma\backslash\mathbb{H}$, definimos $\mathbb{H}^* = \mathbb{H}\cup\mathbb{Q}\cup\{\infty\}$ y tomamos el cociente extendido.

$$X(\Gamma) = \Gamma\backslash\mathbb{H}^* = Y(\Gamma)\cup\Gamma\backslash(\mathbb{Q}\cup\{\infty\}).$$

Los puntos Γs en $\Gamma\backslash(\mathbb{Q}\cup\infty)$ también se llaman las *cúspides* de $X(\Gamma)$. En el caso de $\mathrm{SL}_2(\mathbb{Z})$ solo tiene una cúspide, pues para todo $a,b \in \mathbb{Q}\cup\infty\ \exists\ \gamma \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\gamma(a) = b$. Una vez visto esto es claro que dado un subgrupo Γ, $X(\Gamma)$ va a tener un número finito de cúspides (por el hecho de que $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ es finito para cualquier Γ).

Vamos a dotar ahora a $\mathbb{H}^*$ de una topología adecuada para obtener buenas propiedades en $X(\Gamma)$. Definimos, para cualquier número real $M > 0$, el entorno de ∞

$$N_M = \{\tau \in \mathbb{H} : \mathrm{Im}(\tau) > M\}.$$

Tomando como base la topología de $\mathbb{H}$, añadimos los siguientes conjuntos en $\mathbb{H}^*$ para servir como base de entornos de las cúspides:

$$\alpha(N_M \cup \{\infty\}) \quad M > 0, \alpha \in \mathrm{SL}_2(\mathbb{Z}),$$

y se toma la topología resultante en $\mathbb{H}^*$.

Con esta topología, dotamos a $X(\Gamma)$ de la topología cociente y se extiende la proyección natural a $\pi : \mathbb{H}^* \longrightarrow X(\Gamma)$.

Proposición 3.4. *La curva modular $X(\Gamma)$ es Hausdorff, conexa y compacta.*

Demostración. Para probar que $X(\Gamma)$ es Hausdorff tenemos que ver que para dos puntos distintos $x_1, x_2 \in X(\Gamma)$ existen entornos disjuntos. El caso $x_1 = \Gamma\tau_1, x_2 = \Gamma\tau_2$ con $\tau_1, \tau_2 \in \mathbb{H}$ coincide con el Corolario 3.1.

Supongamos $x_1 = \Gamma s_1, x_2 = \Gamma\tau_2$ con $s_1 \in \mathbb{Q}\cup\{\infty\}$ y $\tau_2 \in \mathbb{H}$. Entonces $\exists\alpha \in \mathrm{SL}_2(\mathbb{Z})$ tal que $s_1 = \alpha(\infty)$. Sea U_2 un entorno cualquiera de τ_2 con clausura compacta K. Gracias a la siguiente fórmula (que se deduce del hecho ya probado de que $Im(\gamma(\tau)) = Im(\tau)/(c\tau + d)^2$)

$$Im(\gamma(\tau)) \leq \mathrm{máx}\{Im(\tau), 1/Im(\tau)\} \quad \text{para } \tau \in \mathbb{H} \text{ y } \gamma \in \mathrm{SL}_2(\mathbb{Z})$$

se obtiene que dado un M suficientemente grande tenemos un conjunto $N_M = \{\tau \in \mathbb{H} | Im(\tau) > M\}$ que satisface que $\mathrm{SL}_2(\mathbb{Z})K \cap N_M = \emptyset$. Sea $U_1 = \alpha(N_M \cup \{\infty\})$ queremos ver que $\pi(U_1)$ y $\pi(U_2)$ son disjuntos. Definimos $m_K = \mín_{\sigma\in K} Im(\sigma)$, $\quad M_K = \mathrm{máx}_{\sigma\in K} Im(\sigma)$. Como K es compacto tenemos que $M > \mathrm{máx}\{M_k, 1/m_k\}$. Dado $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ estudiamos $\gamma(N_m \cup \{\infty\}) \cap K$. Para $\tau \in \mathbb{H}$ tenemos dos casos. Si $c = 0$ tenemos que $\gamma(\tau) = \tau + k$ y por tanto $Im(\gamma(\tau)) = Im(\tau) > M > M_k \geq Im(\sigma)$ para cualquier $\sigma \in K$. Si $c \neq 0$ tenemos que $Im(\gamma(\tau)) \leq 1/Im(\tau) < 1/M < m_k \leq Im(\sigma)$ para cualquier $\sigma \in K$. En el caso $\tau \in \mathbb{Q}\cup\{\infty\}$ $\gamma(\infty) = a/c \in \mathbb{Q}\cup\{\infty\}$ y como $K \subset H$ compacto $a/c \notin K$. Dado $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ tenemos que $\gamma(U_1) = \gamma'\alpha(N_M \cup \{\infty\}) = \gamma(N_M \cup \{\infty\})$ para algún $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Como $\gamma(U_1) \cap U_2 = \emptyset$ para todo γ por la Proposición 3.1 tenemos que $\pi(U_1) \cup \pi(U_2) = \emptyset$.

Estudiamos ahora el último caso, donde $x_1 = \Gamma s_1, x_2 = \Gamma s_2$ con $s_1, s_2 \in \mathbb{Q}\cup\{\infty\}$. Entonces $s_1 = \alpha_1(\infty)$ y $s_2 = \alpha_2(\infty)$ para unos $\alpha_1, \alpha_2 \in \mathrm{SL}_2(\mathbb{Z})$. Tomamos $U_1 = \alpha_1(N_2 \cup \{\infty\})$ y $U_2 = \alpha_2(N_2 \cup \{\infty\})$ y queremos

ver que $\pi(U_1)$ y $\pi(U_2)$ son disjuntos. Supongamos que no lo son, entonces existe algún $\gamma \in \Gamma$ y elementos $\tau_1, \tau_2 \in N_2$ tal que $\gamma\alpha_1(\tau_1) = \alpha_2(\tau_2)$. Tenemos que $\alpha_2^{-1}\gamma\alpha_1$ lleva τ_1 a τ_2 y (como N_2 no contiene puntos elípticos) por tanto debe ser $\pm \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ para algún $m \in \mathbb{Z}$. Concluimos que $\alpha_2^{-1}\gamma\alpha_1$ fija ∞ y por tanto $\gamma(s_1) = s_2$ lo que contradice la hipótesis inicial de que x_1 y x_2 son distintos. Queda probado que $X(\Gamma)$ es Hausdorff.

Para ver que $\mathbb{H}^*$ es conexa supongamos que no lo es y llegamos a una contradicción. Supongamos que $\mathbb{H}^* = O_1 \cup O_2$ con O_1, O_2 abiertos no vacíos disjuntos, como $\mathbb{H}$ es conexo tenemos que $O_1 \supset \mathscr{H}$ y por tanto $O_2 \subset \mathbb{Q} \cup \{\infty\}$. Entonces la única forma de que O_2 sea es que sea vacío lo que contradice la hipótesis incial. como $\mathbb{H}^*$ es conexo también lo es $X(\Gamma)$ por ser su imagen continua.

Para probar la compacidad el punto clave es ver que D^* es compacto en $\mathbb{H}^*$ (donde D^* es la compactificación del dominio fundamental de $\mathrm{SL}_2(\mathbb{Z})$).$D^*$ es compacto si dado un subrecrubimiento cualquiera que lo cubre admite un subrecubrimiento finito que lo sigue recubriendo. Como $\infty \in D^*$ existirá un abierto del recubrimiento que lo contenga y por la definición de la topología de $\mathbb{H}^*$ este será de la forma $\{\tau \in \mathbb{H} | Im(\tau) > r\}$ para algún $r > 0$. Dado ese abierto al que llamamos A_r tenemos que $D^* \cup A_r$ es claramente compacto por ser cerrado y acotado.
Una vez visto esto como $\mathbb{H}^* = \mathrm{SL}_2(\mathbb{Z})D^*$ y además $\bigcup_{i=1}^{n} \gamma_i\Gamma = \mathrm{SL}_2(\mathbb{Z})$ para un n finito, obtenemos la siguiente igualdad, $X(\Gamma) = \bigcup_j \pi(\gamma_j(D^*))$. Como tanto γ_j (para todo j) como π son continuas queda probado que $X(\Gamma)$ es compacta. □

Una vez visto esto solo queda encontrar cartas apropiadas para ver que $X(\Gamma)$ es Riemann. Cuando $U \in \mathbb{H}$ tomamos la aplicación ϕ como en la sección anterior.

Para cada cúspide $s \in \mathbb{Q} \cup \{\infty\}$, existe $\delta = \delta_s \in \mathrm{SL}_2(\mathbb{Z})$ que lleva s a ∞. Se define la **anchura** de s como

$$h_s = h_{s,\Gamma} = \left|\mathrm{SL}_2(\mathbb{Z})_\infty / (\delta\{\pm I\}\Gamma\delta^{-1})_\infty\right|.$$

La idea detrás de la anchura es que en una cúspide convergen infinitos "sectores"(conjuntos que se solapan bajo la acción de $\mathrm{SL}_2(\mathbb{Z})$), el objetivo ver cuántos de ellos no son equivalentes bajo la acción de Γ.

El subgrupo $\mathrm{SL}_2(\mathbb{Z})_\infty = \{\pm I\}\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ es cíclico infinito, por tanto la anchura se caracteriza por las condiciones $\{\pm I\}(\delta\Gamma\delta^{-1})_\infty = \{\pm I\}\left\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle$, $h > 0$. La anchura es finita e independiente del δ elegido pues de hecho

$$h_s = \left|\mathrm{SL}_2(\mathbb{Z})_s / \{\pm I\}\Gamma_s\right|.$$

Definimos $U = U_s = \delta^{-1}(N_2 \cup \{\infty\})$ y como antes tomamos ψ como la composición $\psi = \rho \circ \delta$ donde ρ es la aplicación h-periódica $\rho(z) = e^{2\pi i z/h}$. Sea $V = \mathrm{im}(\psi)$, un subconjunto abierto de $\mathbb{C}$, ψ se define como,

$$\psi \colon U \longrightarrow V, \quad \psi(\tau) = e^{2\pi i\delta(\tau)/h}.$$

Al igual que en el caso anterior existe una biyección φ entre $\pi(U)$ y V, además φ es un homeomorfismo.

$$\pi(U) \xrightarrow{\varphi} V$$

Finalmente tenemos que verificar que las aplicaciones de transición entre cartas coordenadas son holomorfas, el caso nuevo que debemos estudiar es cuando $\pi(U_i)$ es entorno de una cúspide. Necesitamos verificar que $\phi_{2,1}$, la restricción de $\phi_2 \circ \phi_1^{-1}$ a $\phi_1(\pi(U_1) \cap \pi(U_2))$ es holomorfa. La demostración de estás dos últimas afirmaciones se puede encontrar en [1, pág 60 y 61].

Hemos conseguido ver lo que buscábamos al principio del capítulo, para cualquier subgrupo de congruencia Γ de $\mathrm{SL}_2(\mathbb{Z})$, tenemos que el cociente extendido $X(\Gamma)$ es una Superficie de Riemann compacta.

Para terminar la sección introducimos un resultado muy potente que nos permite determinar el número de cúspides de $\Gamma_0(N)$.

$$\varepsilon_\infty(\Gamma_0(N)) = \sum_{d|N} \varphi\big(\gcd(d, N/d)\big)$$

Las herramientas necesarias para poder probar este resultado no se ven en este trabajo debido a su complejidad pero pueden encontrase en [1, sec 3.8]. Para el caso $N = 4$ tenemos que $\varepsilon_\infty(\Gamma_0(4)) = 3$.

3.4. Dimensión de $M_2(\Gamma_0(4))$

Volviendo a la idea que se planteó al final del Capítulo 1, si conseguimos determinar la dimensión del espacio vectorial $M_2(\Gamma_0(4))$ y encontrar una base, como $\theta(\tau,4) = \sum_{n=0}^{\infty} r(n,4)q^n \in M_2(\Gamma_0(4))$ podremos escribir $\theta(\tau,4)$ como combinación lineal de los elementos de la base y por tanto podremos escribir esta función con una fórmula explícita. Para probar esta afirmación vamos a utilizar las herramientas y conceptos introducidos a lo largo de los capítulos anteriores e introduciremos dos nuevos teoremas que quedarán sin demostrar debido a que profundizar en las herramientas necesarias para probarlos escapa a los límites de este trabajo.

Introducimos la idea de género, dicho de manera poco rigurosa, para una superficie de Riemann $X(\Gamma)$ el género, g, es el número de agujeros que posee. El género de la esfera es 0 y el del toro 1 por dar ejemplos de los casos más sencillos.

El género de $X(\Gamma)$ está relacionado con la dimensión del espacio de 1-formas diferenciables en $X(\Gamma)$, que a su vez se corresponden con las formas modulares de peso 2 para Γ como vimos en el Ejemplo 1. Esta es la idea de la relación que existe entre el género y la dimensión de $M_2(\Gamma_0(4))$.

Introducimos el primer teorema que nos permite conocer el género de una curva modular $X(\Gamma)$ a partir de otros de sus invariantes introducidos anteriormente. La demostración de esta indicada como ejercicio en [1, sec 3.1].

Teorema 3.4. *Sea Γ un subgrupo de congruencia de $\mathrm{SL}_2(\mathbb{Z})$. Sea $f\colon X(\Gamma) \longrightarrow X(1)$ la proyección natural, y sea d su grado. Sean ε_2 y ε_3 el número de puntos elípticos de período 2 y 3 en $X(\Gamma)$, y ε_∞ el número de cúspides de $X(\Gamma)$. Entonces el género de $X(\Gamma)$ es*

$$g = 1 + \frac{d}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}.$$

A continuación enunciamos el siguiente teorema que nos da una fórmula explicita para la dimensión del espacio $M_k(\Gamma)$. Se puede encontrar la demostración completa de este teorema en [1, sec 3.5].

Teorema 3.5. *Sea k un entero par mayor o igual que 2. Sea Γ un subgrupo de congruencia de $\mathrm{SL}_2(\mathbb{Z})$, g el género de $X(\Gamma)$,ε_2 el número de puntos elípticos de período 2, ε_3 el número de puntos elípticos de período 3, y ε_∞ el número de cúspides. Entonces*

$$dim(M_k(\Gamma)) = (k-1)(g-1) + \frac{k}{4}\varepsilon_2 + \frac{k}{3}\varepsilon_3 + \frac{k}{2}\varepsilon_\infty$$

Combinando ambos teoremas obtenemos la siguiente fórmula para la dimensión que no depende del género.

$$dim(M_k(\Gamma)) = \frac{(k-1)d}{12} + \frac{\varepsilon_2}{4} + \frac{\varepsilon_3}{3} + \frac{\varepsilon_\infty}{2}$$

Para el caso $M_2(\Gamma_0(4))$ tenemos, $k = 2,\ d = 6,\ \varepsilon_2 = 0,\ \varepsilon_3 = 0, \varepsilon_\infty = 3$. Sustituyendo en la fórmula anterior tenemos que

$$dim(M_2(\Gamma_0(4))) = 2.$$

Capítulo 4

El Teorema de los Cuatro Cuadrados

El teorema de los cuatro cudadrados de Lagrange, también conocido como la conjetura de Bachet, afirma que todo número natural se puede representar como una suma de cuatro cuadrados enteros no negativos. La primera demostración de este teorema data de 1772 cuando fue probado por el propio Joseph-Louis Lagrange, pero ya había sido enunciado como conjetura por Claude-Gaspard Bachet de Méziriac en el año 1612. En 1658, Fermat escribió en una carta dirigida a Pierre de Carcavi en la que aseguraba haber encontrado la demostración de este teorema, sin embargo dicha demostración nunca llegó a ser encontrada. [5, pág 3]

Teorema 4.1 (Lagrange)**.** *Todo número natural se puede representar como una suma de cuatro cuadrados enteros no negativos.*

$$n = a^2 + b^2 + c^2 + d^2$$

para ciertos $a,b,c,d \in \mathbb{N} \cup \{0\}$

En 1834 Carl Gustav Jacob Jacobi encontró el número exacto de formas en las que se puede expresar un número entero positivo n como suma de cuatro cuadrados.

Teorema 4.2 (Jacobi)**.** *El número de representaciones de un número natural n como la suma de cuatro cuadrados viene dado por la siguiente fórmula:*

$$r_4(n) = 8 \sum_{\substack{0<d|n \\ 4\nmid d}} d, \quad n \geq 1.$$

Demostración. Recordamos las series de Eisenstein $G_{2,2}$ y $G_{2,4} \in M_2(\Gamma_0(4))$ que son linealmente independientes.

$$G_{2,2}(\tau) = -\frac{\pi^2}{3}\left(1 + 24\sum_{n=1}^{\infty}\left(\sum_{\substack{0<d|n \\ d \text{ odd}}} d\right)q^n\right)$$

y

$$G_{2,4}(\tau) = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\left(\sum_{\substack{0<d|n \\ 4\nmid d}} d\right)q^n\right) \quad q = e^{2\pi i\tau}.$$

Como hemos visto que $M_2(\Gamma_0(4))$ tiene dimensión 2, se sigue que $G_{2,2}$ y $G_{2,4}$ forman una base de este espacio. En particular, existen algunos $a,b \in \mathbb{C}$ tal que $\theta = aG_{2,2} + bG_{2,4}$. Desarrollamos las expansiones de la serie para los dos primeros términos teniendo en cuenta que $r(1,4) = 8$.

$$\theta(\tau,4) = 1 + 8q + \cdots,$$

$$-\frac{3}{\pi^2}G_{2,2}(\tau) = 1 + 24q + \cdots,$$

$$-\frac{1}{\pi^2}G_{2,4}(\tau) = 1 + 8q + \cdots,$$

Despejando el sistema obtenemos que $a = 0,\ b = -\frac{1}{\pi^2}$ y por tanto que $\theta(\tau,4) = -\frac{1}{\pi^2}G_{2,4}(\tau)$. Igualando los coeficientes de Fourier se obtiene el número de representaciones de n como suma de cuatro cuadrados.

$$r(n,4) = 8 \sum_{\substack{0<d|n \\ 4\nmid d}} d, \quad n \geq 1.$$

Por tanto, queda probado que todo número $n \in \mathbb{N}$ se puede escribir como suma de cuatro cuadrados y hemos obtenido una fórmula explícita para saber exactamente de cuántas formas diferentes. □

Bibliografía

[1] FRED DIAMOND Y JERRY SHURMAN, *A First Course in Modular Forms.* Springer, 2005.

[2] JEAN-PIERRE SERRE, *A Course in Arithmetic.* Springer, 1973.

[3] JOSEPH H. SILVERMAN, *The Arithmetic of Eliptic Curves.* Springer, 2009.

[4] NEAL KOBLITZ, *Introduction to Eliptic Curves and Modular Forms.* Springer 1993.

[5] JENNY BOUCARD, Lagrange and the four-square theorem. *Lett Mat Int* (2014) 59—66, `https://doi.org/10.1007/s40329-014-0052-2`.