Trabajo monográfico

Representaciones de enteros por formas cuadráticas

Matías Martres

20 de Diciembre, 2024

Orientador:

Dr. Gustavo Rama
Instituto de Matemática y Estadística Rafael Laguardia

Licenciatura en Matemática
Universidad de la República
Montevideo, Uruguay

Última revisión: 2 de febrero, 2025

0

Resumen

Un problema clásico en la Teoría de Números consiste en determinar cuáles enteros son representables como suma de dos cuadrados. Presentamos una solución que nos permite hallar $r_2(n)$ –la cantidad de formas en las que un entero n es representable como suma de dos cuadrados– reconociendo que estos están vinculados con los coeficientes de una cierta forma modular. Posteriormente trabajamos con intención de generalizar este resultado, probando entre otras cosas un teorema que afirma que *la función theta asociada a una forma cuadrática definida positiva en* $2n$ *variables es una forma modular*. Ese es el resultado central central de este trabajo monográfico. Luego presentamos algunas fórmulas para la cantidad de representaciones de un entero n como suma de k cuadrados. Concluimos esbozando una posible aplicación del trabajo realizado: el uso de funciones theta para el estudio de retículos.

Índice general

Introducción

> *The problem of the representation of an integer n as the sum of a given number k of integral squares is one of the most celebrated in the theory of numbers. Its history may be traced back to Diophantus, but begins effectively with Girard's (or Fermat's) theorem that a prime $4m+1$ is the sum of two squares. Almost every arithmetician of note since Fermat has contributed to the solution of the problem, and it has its puzzles for us still.*
>
> – G.H. Hardy, [Har99]

Dentro del problema que encierran las representaciones de un entero n como suma de k cuadrados, nos interesamos particularmente en:

Problema 1. *Determinar qué enteros n son representables como suma de 2 cuadrados.*

A. Girard da una solución a este problema en 1625: *todo cuadrado, primo de la forma $4m+1$, producto de los números anteriores, y el doble de alguno de los anteriores.* En otros términos, la respuesta al Problema 1 es:

Teorema 2. *Un entero positivo n es representable como suma de dos cuadrados si y solamente si todo primo de la forma $4n+3$ tiene exponente par en la factorización de n.*[1]

Fermat también pensó sobre este problema. De hecho, en la literatura puede encontrarse al Teorema 2 siendo llamado de *Teorema de Navidad de Fermat*, a raíz de que Fermat escribía en su correspondencia con Mersenne un 25 de diciembre de 1640[2]:

[1] Equivalentemente: si $n = n_o n_1^2$ con n_o libre de cuadrados, n es representable como suma de dos cuadrados si y solamente si n_o no es divisible por ningún primo de la forma $4n+3$.

[2] Extraído de [DF94, pág. 212-217]

1. *Todo número primo, que exceda en una unidad a un múltiplo de cuatro, es una sola vez la suma de dos cuadrados, y una sola vez la hipotenusa de un triángulo rectángulo.*

2. *El mismo número [primo] y su cuadrado son, cada uno, una vez la suma de dos cuadrados. Su cubo y su bi-cuadrado son, cada uno, dos veces la suma de dos cuadrados. Su cuadrado-cubo y su cubo-cubo son, cada uno, tres veces la suma de dos cuadrados. Y así, al infinito.*

Obsérvese que Fermat no solo habla sobre la representabilidad (o no) de un primo como suma de dos cuadrados, sino que también se refiere a la cantidad de formas en la que puede hacerse. En el primer ítem hace referencia a triángulos rectángulos pues, a la luz del afamado *Teorema de Pitágoras*, la cantidad de representaciones de p^2 como suma de dos cuadrados $a^2 + b^2$ con $a, b > 0$ (a menos de intercambiar a con b) se corresponde con la cantidad de triángulos rectángulos con hipotenusa de longitud p. De hecho, en el segundo ítem dice[3] de cuántas formas se pueden representar p, p^2, p^3, etc. como suma de dos cuadrados. Esto se relaciona con la versión *cuantitativa* del problema inicial:

Problema 3. *¿De cuántas formas puede representarse a n como suma de dos cuadrados?*

El problema cualitativo (Problema 1) está, en cierto sentido, "contenido" en el problema cuantitativo. Es decir, si notamos $r_2(n)$ a la cantidad de representaciones de n como suma de dos cuadrados, el problema cualitativo consiste en decidir si $r_2(n) = 0$ ó $r_2(n) > 0$. Así, de tener una fórmula para $r_2(n)$ podemos dar respuesta al problema que abre la introducción.

Diofanto también consideraba cuestiones relacionadas. Por ejemplo, en el Libro II de *Aritmética*[4] plantea el problema:

Problema 4. ***[Problema IX]*** *Escribir a un número que es suma de dos cuadrados, nuevamente, como suma de otros dos cuadrados.*

Este problema está emparentado con el problema cuantitativo: suponiendo que n es representable como suma de dos cuadrados, ¿puede representarse

[3] Aunque sin prueba, quizás el margen de la carta que escribía era demasiado estrecho para contenerla.

[4] Extraído de [JC22].

como suma de cuadrados de otra forma?[5] Fermat afirmaba que para un primo p (o su cuadrado) esto no es posible.[6]

La solución que damos al problema cuantitativo está relacionada con el trabajo de Jacobi, quien en 1828 publica algunas identidades –provenientes de la teoría de funciones elípticas– las cuales dan como corolario fórmulas para los números de representaciones de un entero n como suma de 2 (también 4, 6 y 8) cuadrados.[7]

En el Capítulo 2 definimos $r_2(n)$ y definimos la función

$$\theta_2(z) = \sum_n r_2(n) e^{2\pi i n z}, \quad z \in \mathbb{H}.$$

Esta *función theta* resulta ser una forma modular de peso 1 para cierto subgrupo de congruencia, que es un espacio vectorial de dimensión 1. Así, construyendo una función en este espacio, cuyos coeficientes podemos calcular, conseguimos obtener fórmulas para $r_2(n)$ dando una respuesta al Problema 3.

Una herramienta clave para la demostración de la modularidad de $\theta_2(z)$ es la *fórmula de sumación de Poisson*. Esta dice que si $f : \mathbb{R}^n \to \mathbb{C}$ es una función de Schwarz entonces:

$$\sum_{v \in \mathbb{Z}^n} f(x+v) = \sum_{v \in \mathbb{Z}^n} \hat{f}(v) e(x^t v),$$

donde $e(\alpha) = e^{2\pi i \alpha}$ y $\hat{f}$ denota la *transformada de Fourier* de f, es decir:

$$\hat{f}(v) = \int_{\mathbb{R}^n} f(y) e(-y^t v) dy.$$

[5] Diofanto tiene otro problema en mente, pues permite que la nueva representación de n como suma de dos cuadrados sea una que involucre cuadrados racionales, como puede verse en la solución que proporciona.

[6] Es importante explicar a qué nos referimos cuando hablamos de *unicidad*. A lo largo de este trabajo, cuando hablemos de *la cantidad de representaciones de un entero n como suma de dos cuadrados*, nos referimos a la cantidad de pares $(a, b) \in \mathbb{Z}^2$ que cumplen $a^2 + b^2 = n$. En ese sentido, como veremos oportunamente, si $p = a^2 + b^2$ entonces hay *ocho* representaciones: (a, b), (b, a), $(-a, b)$, $(a, -b)$, etc. Sin embargo, todas estas son, *esencialmente* la misma: consisten en permutar las coordenadas y cambiar los signos de las entradas de una solución (a, b).

[7] Todas las referencias históricas, salvo aquellos extractos debidamente señalados, se basan en [Dic20] y [Roy17]

De hecho, una vez probada la modularidad de $\theta_2(z)$, uno puede de forma análoga obtener fórmulas para $r_4(n)$, $r_6(n)$, etc. Presentamos sin prueba estas en el Capítulo 4.

En el Capítulo 3 generalizamos el razonamiento del segundo capítulo. Dada una forma cuadrática definida positiva $Q : \mathbb{Z}^n \to \mathbb{Z}$, podemos definir los coeficientes $r_Q(n)$ y a partir de estos la *función theta* asociada $\Theta_Q : \mathbb{H} \to \mathbb{C}$. De hecho, trabajamos con funciones theta *con peso*, y concluimos para estas que que si n es par, entonces el resultado del Capítulo 2 vale en general: *la función theta asociada a la forma cuadrática definida positiva es una forma modular para cierto subgrupo de congruencia.*

El Capítulo 5 da cierre a este trabajo exponiendo someramente cómo pueden usarse los resultados del capítulo central para estudiar retículos y extraer información de estos.

Capítulo 1

Preliminares

1.1. Enteros modulares y cuestiones relacionadas

Por ser $\mathbb{Z}$ un dominio de ideales principales, sus ideales son de la forma $n\mathbb{Z}$ para cierto $n \in \mathbb{Z}_{\geq 0}$. Llamamos de *enteros módulo* n al anillo $\mathbb{Z}/n\mathbb{Z}$. Para estos anillos tenemos:

Teorema 1.1 (**Teorema chino de los restos**). *Si* $(n, m) = 1$ *entonces:*

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

donde el isomorfismo está dado por $x \mapsto (x \text{ mód } n, x \text{ mód } m)$.

En particular, si escribimos a un entero positivo n como producto de primos $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ entonces tenemos:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}.$$

Dado un grupo $(G, \cdot, 1_G)$, decimos que un morfismo de grupos $\varphi : G \to \mathbb{C}^\times$ es un *carácter*. Un ejemplo es el *carácter trivial* definido por $\chi_o(g) = 1 \ \forall g \in G$. Denotamos $\widehat{G}$ al conjunto de los carácteres de G.

Proposición 1.2. *Sea* G *un grupo abeliano finito.*

1. $$\sum_{g \in G} \chi(g) = \begin{cases} |G| & si\ \chi = \chi_o \\ 0 & si\ \chi \neq \chi_o \end{cases},$$

2. $$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & si\ g = 1_G \\ 0 & si\ g \neq 1_G \end{cases},$$

3. *Los caracteres de G conforman un grupo con la multiplicación punto a punto y $G \cong \widehat{G}$. En particular $\#G = \#\widehat{G}$.*

Un carácter χ de $(\mathbb{Z}/n\mathbb{Z})^\times$ puede extenderse a una función $\tilde{\chi} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ como sigue:

$$\tilde{\chi}(a) = \begin{cases} \chi(a) & \text{si } a \in (\mathbb{Z}/n\mathbb{Z})^\times \\ 0 & \text{si } a \notin (\mathbb{Z}/n\mathbb{Z})^\times \end{cases}$$

y esta última a su vez puede extenderse a una función de $\mathbb{Z}$ en $\mathbb{C}$ dada por $k \mapsto \tilde{\chi}(k + n\mathbb{Z})$. La función resultante es un *carácter de Dirichlet módulo n*. Es decir, una función $\chi : \mathbb{Z} \to \mathbb{C}$ que cumple:

i. $\chi(ab) = \chi(a)\chi(b)$ (completamente multiplicativa),

ii. $\chi(a) = 0$ si y solo si $(a, n) > 1$,

iii. $\chi(a + n) = \chi(a)$ (n-periódica).

Un ejemplo notable de carácter de Dirichlet módulo p es el *símbolo de Legendre*. Dado $p \in \mathbb{Z}$ un primo impar, se define $\left(\frac{\cdot}{p}\right)$ como sigue:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } (a,p) = 1 \text{ y } a \text{ es un cuadrado módulo } p \\ -1 & \text{si } (a,p) = 1 \text{ y } a \text{ no es un cuadrado módulo } p \\ 0 & \text{si } (a,p) > 1 \end{cases}. \tag{1.3}$$

Además de ser un carácter módulo p, cumple:

Teorema 1.4 (**Reciprocidad cuadrática**). *Sean $p, q \in \mathbb{Z}$ primos. Vale:*

1. $$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{si } p \equiv 1 \pmod 4 \\ -1 & \textit{si } p \equiv 3 \pmod 4 \end{cases},$$

2. $$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{si } p \equiv \pm 1 \pmod 8 \\ -1 & \textit{si } p \equiv \pm 3 \pmod 8 \end{cases},$$

3. $$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

El símbolo de Legendre se extiende al *símbolo de Jacobi* del siguiente modo: si $n \in \mathbb{Z}_{>0}$ impar con $n = p_1^{\alpha_1}...p_k^{\alpha_k}$, entonces $\left(\frac{\cdot}{p}\right)$ está definido para cada $i = 1, \ldots, k$ (n es impar y es pues, producto de primos impares). Se define:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}. \tag{1.5}$$

El símbolo de Jacobi es ahora completamente multiplicativo, tanto como función de a como función de n. Nuevamente, $\left(\frac{\cdot}{n}\right) : \mathbb{Z} \to \mathbb{C}$ es un carácter de Dirichlet, ahora módulo n.

Observación 1.6. *En el símbolo de Jacobi perdemos la interpretación de ser (o no) residuo cuadrático. Más precisamente, si* $\left(\frac{a}{n}\right) = -1$ *sabemos que* a *no es un cuadrado módulo* n*; pero* $\left(\frac{a}{n}\right) = 1$ *no necesariamente implica que* a *sea un cuadrado módulo* n*. Por ejemplo* $\left(\frac{2}{9}\right) = 1$ *aunque* $x^2 \equiv 2$ (mód 9) *no tiene solución.*

Extendemos el símbolo de Jacobi para n un entero arbitrario poniendo:

$$\left(\frac{a}{-1}\right) = \begin{cases} \operatorname{sg}(a) & \text{si } a \neq 0 \\ 0 & \text{si } a = 0 \end{cases}, \tag{1.7}$$

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{si } a \equiv \pm 1 \text{ (mód 8)} \\ -1 & \text{si } a \equiv \pm 3 \text{ (mód 8)} \\ 0 & \text{si } a \equiv 0 \text{ (mód 2)} \end{cases}. \tag{1.8}$$

Dedicamos el resto de la sección a los *enteros p-ádicos*. Obsérvese primero que dado un primo $p > 0$ todo entero k puede escribirse de forma única como $k = p^n k_o$ donde $p \nmid k_o$. Se define entonces $\nu_p(k) := n$, la *valuación p-ádica de* k.

Denotando $A_n = \mathbb{Z}/p^n\mathbb{Z}$ y $\pi_n : \mathbb{Z} \to A_n$ a la proyección al cociente, se tienen morfismos $\phi_n : A_n \to A_{n-1}$ (inducidos por la propiedad universal del cociente aplicada los morfismos $\pi_{n-1} : \mathbb{Z} \to A_{n-1}$) que hacen de la secuencia $\{A_n\}_n$ un sistema proyectivo, definiéndose los *enteros p-ádicos*

$$\mathbb{Z}_p := \varprojlim(A_n, \phi_n).$$

Es decir, $x \in \mathbb{Z}_p$ es $x = (\ldots, x_2, x_1)$ donde $x_n \in A_n$ y $\phi_n(x_n) = x_{n-1}$ $\forall n \geq 2$.

Dotando a cada A_n con la topología discreta y a $\prod A_n$ de la topología

producto, $\mathbb{Z}_p$ hereda una topología que lo hace un espacio topológico compacto. La valuación p-ádica se extiende a $\mathbb{Z}_p$; más concretamente, se puede probar que $x \in \mathbb{Z}_p$ es invertible si y solamente si $p \nmid x$ de donde dado $x \in \mathbb{Z}_p$ existe un único n tal que $x = p^n u$ con $u \in (\mathbb{Z}_p)^\times$. Definimos pues $\nu_p(x) := n$.[1] La valuación cumple $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ y $\nu_p(x+y) \geq \text{máx}(\nu_p(x), \nu_p(y))$. A partir de la valuación de define la distancia ultramétrica $d_p : \mathbb{Z}_p \times \mathbb{Z}_p \to [0 + \infty),\ d_p(x, y) = p^{-\nu_p(x-y)}$, que induce en $\mathbb{Z}_p$ una topología de espacio métrico completo, que coincide con la heredada del producto de los A_n.

Denotamos $\mathbb{Q}_p$ al *cuerpo de los números p-ádicos*, cuerpo de fracciones de $\mathbb{Z}_p$. La distancia ultramétrica se extiende a un valor absoluto que notamos $|\cdot|_p : \mathbb{Q}_p \times \mathbb{Q}_p \to [0, +\infty)$ –pues la descomposición $k = p^n k_o$ tiene sentido también en $\mathbb{Q}$– con la cual $\mathbb{Q}_p$ es un espacio métrico completo.

1.2. Formas cuadráticas, retículos y espacios cuadráticos

1.2.1. Formas cuadráticas

Sea R un dominio. Decimos que $f \in R[x_1, ..., x_n]$ es una forma cuadrática en n variables si es un polinomio homogéneo de grado 2 dado por:

$$f(x_1, ..., x_n) = \sum_{i,j} f_{ij} x_i x_j \tag{1.9}$$

donde $F = (f_{ij})_{ij} \in M_n(R)$ es una matriz simétrica. Escribiendo $x = (x_1, ..., x_n)$, y notando x^t al vector x transpuesto, 1.9 se escribe:

$$f(x) = x^t F x. \tag{1.10}$$

Una noción relevante es la de R-equivalencia. Dos formas cuadráticas f y g son R-equivalentes si existe una matriz $T \in \text{GL}_n(R)$ tal que $f(Tx) = g(x)$. En términos de matrices, si $f(x) = x^t F x$ y $g(x) = x^t G x$, entonces f es R-equivalente a g cuando existe un matriz $T \in \text{GL}_n(R)$ de modo que $G = T^t F T$.

Llamamos *discriminante* de la forma cuadrática f al determinante de la

[1] Incluyendo a $\mathbb{Z}$ diagonalmente en $\mathbb{Z}_p$, esta definición coincide con la anterior, si $k = p^n k_o$ entonces $k_o \not\equiv 0$ (mód p^t) para ningún $t \geq 1$ por lo que $k_o \in (\mathbb{Z})_p^\times$.

matriz F y lo notamos $d\,f$. La clase de $d\,f$ en $R/(R^\times)^2$ es invariante por R-equivalencia. Además, dado $d \neq 0$, hay finitas clases de R-equivalencia de formas cuadráticas en n variables con discriminante d (ver por ejemplo [Cas08, 9.3]).

Llamamos a una matriz $T \in \mathrm{GL}_n(R)$ una autometría si da una equivalencia entre f y sí misma, es decir $f(Tx) = f(x)$. Una tal matriz necesariamente tiene $\det T = \pm 1$, lo que sigue de $d\,f = (\det T)^2 d\,f$. Denotamos $O_R(f)$ al conjunto de autometrías de f, y $O_R^+(f)$ al conjunto de autometrías propias, i.e.: las que tienen determinente 1.

Observación 1.11. *Las autometrías $O_R(f)$ son un subgrupo multiplicativo de $\mathrm{GL}_n(R)$. Además, $O_R^+(f)$ es subgrupo multiplicativo de $O_R(f)$ (y por tanto, también de $\mathrm{GL}_n(R)$).*

1.2.2. Espacios cuadráticos

Dado un espacio vectorial $(V, \Bbbk)$, decimos que $b : V \times V \to \Bbbk$ es una *forma bilineal simétrica* si:

a. $b(v, w) = b(w, v)$ para $v, w \in V$;

b. $b(a_1 v_1 + a_2 v_2, w) = a_1 b(v_1, w) + a_2 b(v_2, w)$ para $a_i \in \Bbbk$, $v_i, w \in M$.

Si V es de dimensión n y $\mathcal{B} = \{v_i\}_{i=1}^n$ es una base, la matriz definida por $A_{ij} = b(v_i, v_j)$ cumple que, escritos $v, w \in V$ en coordenadas de esta base, digamos $x, y \in \Bbbk^n$ respectivamente, cumple:

$$b(v, w) = x^t A y.$$

Observación 1.12. *De la simetría de $b(v, w)$ sigue que A es una matriz simétrica.*

Si $\mathcal{B}' = \{u_i\}_{i=1}^n$ es otra base, podemos construir una matriz A' de forma análoga. Notando $S = (s_{ij})_{ij} \in \mathrm{GL}_n(\Bbbk)$ a la matriz cambio de base –que cumple $u_i = \sum_{j=1}^n s_{ji} v_j$ para $i = 1, \ldots, n$– tenemos que:

$$\begin{aligned} A'_{ij} &= b(u_i, u_j) \\ &= b(\sum_k s_{ki} v_k, \sum_l s_{lj} v_l) \\ &= \sum_k \sum_l s_{ki} s_{lj} b(v_k, v_l) \\ &= (S^t A S)_{ij}, \end{aligned}$$

de donde concluimos que $A' = S^t AS$.

Definición 1.13. *Diremos que $(V, ||\cdot||, \Bbbk)$ es un espacio cuadrático si es un espacio vectorial equipado con un mapa $||\cdot|| : V \to \Bbbk$ que satisface:*

a. $||av|| = a^2||v||$ *para* $a \in \Bbbk$, $v \in V$;

b. $b : V \times V \to \Bbbk$ *definida por* $b(v, w) := ||v + w|| - ||v|| - ||w||$ *es una forma bilineal simétrica.*

Diremos que el espacio cuadrático es regular si la forma bilineal es no-degenerada, es decir, si $b(v, w) = 0 \quad \forall w \in V$ *implica* $v = 0$. *En lo que sigue diremos "espacio cuadrático" para referirnos a un espacio cuadrático regular.*

Observación 1.14. *Para la forma bilineal de (b) vale:*

$$b(v, v) = 2||v||.$$

Dado un espacio cuadrático $(V, ||\cdot||, \Bbbk)$ de dimensión n; al tomar una base $\mathcal{B}$ el mapa $||\cdot||$ induce una forma cuadrática $q_{\mathcal{B}} : \Bbbk^n \to \Bbbk$. Más específicamente, sea b la forma bilineal de la definición 1.13, A la matriz $(b(v_i, v_j))_{ij}$ (que es simétrica). El mapa $q_{\mathcal{B}}$ queda definido por:

$$q_{\mathcal{B}}(x) = \frac{1}{2} x^t A x,$$

y $q_{\mathcal{B}}(x) = ||v||$ donde v es el vector cuyas coordenadas en la base $\mathcal{B}$ son x.

Distintas elecciones de base dan a luz a distintas formas cuadráticas, pero todas ellas $\Bbbk$-equivalentes entre sí. Las distintas bases de V se corresponden con los distintos elementos de una clase de $\Bbbk$-equivalencia de formas cuadráticas en n variables.

Decimos que una transformación lineal $\varphi : (V, ||\cdot||_V) \to (W, ||\cdot||_W)$ es una isometría si respeta la estructura de espacio cuadrático, es decir:

$$||\varphi(v)||_W = ||v||_V \quad \forall v \in V.$$

Decimos que $\sigma : V \to V$ es una autometría si es una isometría de V en sí mismo. Fijada una base $\mathcal{B}$, esto se traduce en que $[\sigma]_{\mathcal{B}}$ –la matriz asociada a σ en dicha base– cumple:

$$q_{\mathcal{B}}([\sigma]_{\mathcal{B}} x) = q_{\mathcal{B}}(x),$$

por lo que $[\sigma]_{\mathcal{B}} \in O_{\Bbbk}(q_{\mathcal{B}})$.

1.2.3. Retículos

En la presente sección supondremos que R es un DIP contenido en $\Bbbk$, que típicamente será el cuerpo de fracciones de R (pero podría ser mayor). En las aplicaciones que nos son de interés, R será o bien $\mathbb{Z}$ o bien $\mathbb{Z}_p$.

Sea $(V, ||\cdot||, \Bbbk)$ un espacio cuadrático de dimensión n. Dada una base $\mathcal{B} = \{v_i\}_{i=1}^n$ de V decimos que $L \subseteq V$ definido por

$$L = Rv_1 \oplus \cdots \oplus Rv_n$$

es un *retículo*. Equivalentemente, L es un R-submódulo (necesariamente libre) de rango n de V tal que $L \otimes \Bbbk = V$.

Notaremos $\Lambda(v_1, \cdots, v_n)$ al retículo generado por los vectores $v_1, \ldots, v_n$. Dos retículos $\Lambda(v_1, \ldots, v_n)$ y $\Lambda(v_1', \ldots, v_n')$ son el mismo si y solamente si la matriz cambio de base está en $\mathrm{GL}_n(R)$. Luego, diferentes elecciones de bases que generan un mismo retículo L dan luz a elementos en una misma clase de R-equivalencia dentro de la clase de $\Bbbk$-equivalencia asociada a la estructura de V como espacio cuadrático. Sin embargo, diferentes retículos podrían dar luz a formas cuadráticas R-equivalentes. Diremos que dos retículos L y L' son R-equivalentes si este es el caso. Se puede probar que dos retículos son R-equivalentes precisamente cuando existe una isometría $\sigma : V \to V$ tal que $L' = \sigma L$. Así, las clases de equivalencia de retículos se corresponden con las clases de R-equivalencia en las que se subdivide la clase de $\Bbbk$-equivalencia que se corresponde con $(V, ||\cdot||)$.

Proposición 1.15. *Sea $L = \Lambda(e_1, \ldots, e_n)$ y $v \in L$. Si $v = \sum_i a_i e_i$ con $(a_1, \ldots, a_n) = 1$, entonces existe una base $\{v, v_2, \ldots, v_n\}$ de modo que*

$$L = \Lambda(v, \ldots, v_n).$$

1.2.4. Formas cuadráticas enteras

Dada una matriz $A \in M_n(\mathbb{R})$ simétrica, le asociamos la forma cuadrática:

$$Q : \mathbb{R}^n \to \mathbb{R},\ Q(x) = \frac{1}{2} x^t A x.$$

Diremos que A es la *matriz asociada a la forma cuadrática* Q. Asociamos a A también la forma bilineal simétrica:

$$B : \mathbb{R}^n \to \mathbb{R},\ B(x, y) = x^t \widetilde{A} y$$

donde $\widetilde{A} = \frac{1}{2}A$. Nuevamente, diremos que A es la *matriz asociada a la forma bilineal simétrica* B.

Obsérvese que si Q y B son asociadas a A, entonces vale:

$$B(x, x) = Q(x).$$

Una forma cuadrática Q se dice *definida positiva* si $Q(x) > 0$ para todo $x \in \mathbb{R}^n \backslash \{0\}$, *definida negativa* si $Q(x) < 0$ para todo $x \in \mathbb{R}^n \backslash \{0\}$ e *indefinida* si representa valores tanto negativos como positivos.

El siguiente teorema también nos será de suma utilidad:

Teorema 1.16 (**Teorema espectral**)**.** *Sea $A \in M_n(\mathbb{R})$ simétrica. Entonces existe una matriz ortogonal $U \in M_n(\mathbb{R})$, i.e.: $UU^t = Id$, de modo que $U^tAU = D$ con D diagonal.*

Observación 1.17. *Sea $A \in M_n(\mathbb{R})$ una matriz simétrica, cuya forma cuadrática asociada Q es definida positiva. El Teorema espectral nos dice que existen matrices U y D tales que $U^tAU = D$. Como Q es definida positiva, las entradas de la diagonal de D son positivas. En efecto, si se define $\widetilde{Q}(x) := Q(Ux)$ se tiene que Q es definida positiva si y solamente si lo es $\widetilde{Q}$; y vale $\widetilde{Q}(e_i) = d_{ii}$. Por lo tanto, podemos definir:*

$$R := \begin{pmatrix} \sqrt{d_{11}} & & \\ & \ddots & \\ & & \sqrt{d_{rr}} \end{pmatrix} U.$$

Observamos que $R^TR = A$. Luego, si $y = Rx$ entonces:

$$\begin{aligned} Q(x) &= \frac{1}{2}x^tAx \\ &= \frac{1}{2}(R^{-1}y)^tAR^{-1}y \\ &= \frac{1}{2}y^t(R^{-1})^tAR^{-1}y \\ &= \frac{1}{2}y^t(R^t)^{-1}AR^ty \\ &= \frac{1}{2}y^ty. \end{aligned}$$

Del mismo modo, si escribimos $v = Ru$ tenemos que:

$$B(x, u) = \frac{1}{2}y^tv.$$

Son para nosotros de particular interés las formas cuadráticas *enteras*; aquellas que son polinomios con coeficientes enteros. Estas son aquellas que tienen por matriz asociada una matriz $A \in M_n(\mathbb{Z})$ simétrica con diagonal par.

1.3. Formas modulares

1.3.1. El grupo modular y subgrupos de congruencia

Dada una matriz γ en $\mathrm{GL}_2^+(\mathbb{R})$ –conjunto de las matrices 2×2 con coeficientes reales y determinante positivo– se define para z en el semiplano superior $\mathbb{H} = \{z = x + iy : y > 0\}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

Vale la siguiente identidad:

$$\mathrm{im}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z\right) = \det(\gamma)\frac{im(z)}{|cz+d|^2}. \tag{1.18}$$

A la luz de esta identidad vemos que para $z \in \mathbb{H}$ tenemos $\gamma \cdot z \in \mathbb{H}$ para toda $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$. Así, se puede verificar que definimos una acción de $\mathrm{GL}_2^+(\mathbb{R})$ en el semiplano superior, a la que llamamos *acción por transformaciones de Möbius*.

Se define el *grupo modular* como el subgrupo de matrices con coordenadas enteras y determinante 1,

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

Proposición 1.19. $\mathrm{SL}_2(\mathbb{Z})$ *es generado por:*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{1.20}$$

Demostración. Denotemos $G = \langle T, S \rangle$, subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ que pretendemos probar que es todo el grupo modular.

Sea $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Afirmamos que existe una matriz $\gamma \in G$ tal que $\gamma\alpha$ tiene entrada inferior izquierda 0.

Si $c = 0$ no hay nada que probar. En caso contrario, observemos que por un lado:

$$T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

donde $a' = a + cn$, por lo que salvo cuando $c = 0$ podemos elegir n de modo que $0 \leq a' < |c|$.

Por otro lado:

$$S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}.$$

Así que, en caso de que $c \neq 0$ procedemos del siguiente modo:

a. Si la entrada superior izquierda es 0, aplicamos S y obtenemos una matriz cuya entrada inferior izquierda es 0.

b. En otro caso, podemos suponer que la entrada inferior izquierda es menor o igual en módulo a la entrada superior izquierda (de no ser así, multiplicamos por S). Si aplicamos T^n (con n elegido como indicamos arriba) seguido por S, entonces obtenemos una matriz con una entrada superior izquierda estrictamente menor en módulo que la anterior. Aplicamos entonces esta transformación repetidas veces hasta arribar a una matriz cuya entrada superior izquierda es 0. Aplicamos S y obtenemos una matriz cuya entrada inferior izquierda es 0.

Así, denotando $\gamma \in G$ a la matriz que se corresponde con el proceso descrito arriba, tenemos que:

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

Como la matriz del miembro derecho debe tener determinante 1 concluimos que $\hat{a} = \hat{d} = \pm 1$, por lo que de hecho:

$$\gamma\alpha = \pm \begin{pmatrix} 1 & \hat{b} \\ 0 & 1 \end{pmatrix}.$$

Según el signo en la igualdad anterior definimos $\gamma' \in G$:

$$\gamma' = \begin{cases} T^{-\hat{b}} & \text{si el signo en la igualdad es } + \,, \\ S^2 T^{-\hat{b}} = -T^{-\hat{b}} & \text{si el signo en la igualdad es } - \,. \end{cases}$$

Multiplicando por γ' obtenemos $\gamma'\gamma\alpha = \mathrm{Id}$ y concluimos que $\alpha \in G$. □

Siendo un subgrupo de $\mathrm{GL}_2^+(\mathbb{R})$, $\mathrm{SL}_2(\mathbb{Z})$ actúa por transformaciones de Möbius en $\mathbb{H}$.

Proposición 1.21. *El conjunto*

$$D = \left\{ z = x + iy : |x| < \frac{1}{2},\ y > 0,\ |z| > 1 \right\}$$

es un dominio fundamental para el grupo modular, es decir que:

- $D \subseteq \mathbb{H}$ *es un dominio.*
- *Cada órbita* $SL_2(\mathbb{Z})\backslash\mathbb{H}$ *intersecta a* D *o a* ∂D*.*
- *Distintos puntos de* D *no pertenecen a la misma órbita.*

Demostración. Ver por ejemplo [Iwa97, Teorema 1.2]. □

Definimos, para N un entero positivo el *subgrupo principal de congruencia de nivel* N:

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

núcleo del morfismo de reducción módulo N de $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. De hecho se puede probar que el morfismo en cuestión es sobreyectivo, por lo que $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Diremos que Γ es un *subgrupo de congruencia de nivel* N si es un subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ que contiene a $\Gamma(N)$. Nótese que esta definición es relevante cuando $N > 1$, pues $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. Otros subgrupos de congruencia relevantes son los siguientes:

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

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

Valen las inclusiones $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$.

Observación 1.22. *Sea* $N > 1$*. Como las matrices de* $\Gamma_0(N)$ *tienen determinante* 1*, las entradas de la diagonal deben ser coprimas con* N*. Considérese entonces el morfismo:*

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

Este es sobreyectivo y tiene núcleo $\Gamma_1(N)$*. En efecto, para lo primero, dado un* d (mód N) *en el codominio, como* $(d, N) = 1$ *tenemos por Bezout que existen* $a, b \in \mathbb{Z}$ *tales que* $ad + Nb = 1$*. Tenemos pues:*

$$\begin{pmatrix} a & -b \\ N & d \end{pmatrix} \mapsto d \text{ (mód } N).$$

Para la segunda afirmación, es claro que $\Gamma_1(N)$ *está contenido en el núcleo. Para la otra inclusión, obsérvese que si* $d \equiv 1$ (mód N)*, reduciendo la igualdad* $ad - bc = 1$ *módulo* N *obtenemos* $a \equiv 1$ (mód N)*.*

Luego vale $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ *lo cual implica* $[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N)$ *donde* φ *denota la función phi de Euler.*[2]

1.3.2. Formas modulares

Los números complejos $\mathbb{C}$ son un $\mathbb{R}$-espacio vectorial de dimensión 2. Además, para dos números complejos ω_1 y ω_2 vale:

$$\{\omega_1, \omega_2\} \text{ es LI} \iff \omega_1/\omega_2 \notin \mathbb{R}.$$

A su vez, la identidad

$$z^{-1} = \frac{\overline{z}}{|z|^2}$$

nos dice que dado $\{\omega_1, \omega_2\} \subseteq \mathbb{C}$ linealmente independiente sobre $\mathbb{R}$ podemos suponer que $\text{im}(\omega_1/\omega_2) > 0$.

Sea $\mathcal{R}$ el conjunto de todos los retículos de $\mathbb{C}$ como $\mathbb{R}$-espacio vectorial y sea

$$M = \{(\omega_1, \omega_2) \in (\mathbb{C}^\times)^2 : \text{im}(\omega_1/\omega_2) > 0\}.$$

Tenemos el mapa $\Lambda : M \to \mathcal{R}$ dado por $\Lambda(\omega_1, \omega_2) = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ que es sobreyectivo. Además, dos elementos $(\omega_1, \omega_2), (\omega_1', \omega_2') \in M$ definen el mismo retículo si y solo si existe una matriz $\gamma \in \text{GL}_2(\mathbb{Z})$ que lleva (ω_1, ω_2) en (ω_1', ω_2'); pero como $\omega_1/\omega_2, \omega_1'/\omega_2'$ tienen parte imaginaria positiva, por 1.18 vemos que $\det(\gamma) = 1$.

[2]Para un entero positivo n vale

$$\varphi(n) = \#\{x \in \{1, \ldots, n\} : (x, n) = 1\}.$$

Podemos pues identificar $\mathcal{R}$ con M módulo la acción de $\mathrm{SL}_2(\mathbb{Z})$.

Por otro lado, $\mathbb{C}^\times$ actúa por homotecias en M, $\lambda \cdot (\omega_1, \omega_2) = (\lambda\omega_1, \lambda\omega_2)$. El cociente $M/\mathbb{C}^\times$ se identifica con $\mathbb{H}$ vía $(\omega_1, \omega_2) \mapsto \omega_1/\omega_2$. Y a través de esta identificación, la acción de $\mathrm{SL}_2(\mathbb{Z})$ en M se transforma en la de $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\mathrm{Id}, -\mathrm{Id}\}$ en $\mathbb{H}$.

Definición 1.23. *Sea $k \in \mathbb{Z}$. Una función de retículos $F : \mathcal{R} \to \mathbb{C}$ se dice homogénea de peso k si:*

$$F(\lambda\Lambda) = \lambda^{-k} F(\Lambda) \; \forall \lambda \in \mathbb{C}^\times, \; \Lambda \in \mathcal{R}.$$

Observación 1.24. *Si $k \equiv 1$ (mód 2) una función de peso k es necesariamente nula, pues $-\Lambda = \Lambda$.*

Para $(\omega_1, \omega_2) \in M$, notamos $F(\omega_1, \omega_2)$ a F evaluada en $\Lambda(\omega_1, \omega_2)$. Por un lado, F es invariante por la acción de $\mathrm{SL}_2(\mathbb{Z})$ sobre M y por otro: $F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-k} F(\omega_1, \omega_2)$. Si se observa esto último con mayor cuidado, se ve que F solo depende de $z = \omega_1/\omega_2$:

$$F(\omega_1, \omega_2) = \omega_2^{-k} F(z, 1).$$

Es decir, existe una función $f : \mathbb{H} \to \mathbb{C}$ de modo que:

$$F(\omega_1, \omega_2) = \omega_2^{-k} f(\omega_1/\omega_2). \tag{1.25}$$

La invarianza de F bajo la acción de $\mathrm{SL}_2(\mathbb{Z})$ se traduce en la siguiente propiedad para f:

$$f(\gamma \cdot z) = (cz + d)^k f(z) \;\; \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}). \tag{1.26}$$

Es claro que recíprocamente, una función $f : \mathbb{H} \to \mathbb{C}$ que cumpla 1.26 –a una tal función la llamamos *función modular de peso k*– define una función de retículos $F : \mathcal{R} \to \mathbb{C}$ homogénea de peso k vía 1.25.

Definición 1.27. *Sea $k \in \mathbb{Z}$. Una función $f : \mathbb{H} \to \mathbb{C}$ se dice una forma modular de peso k si:*

1. *f es holomorfa en $\mathbb{H}$,*
2. *f es modular de peso k,*
3. *f es holomorfa en ∞.*

A continuación explicamos lo que significa la última condición en la definición anterior. Como $T \in \mathrm{SL}_2(\mathbb{Z})$, una función que satisface (2) en particular cumple $f(z+1) = f(z)$. El mapa holomorfo $z \to e^{2\pi iz}$ mapea $\mathbb{H}$ en $\mathbb{D}^* = \mathbb{D}\backslash\{0\}$. Si escribimos $g(q) = f(log(q)/2\pi i)$, como f es $\mathbb{Z}$-periódica, define una función $g : \mathbb{D}^* \to \mathbb{C}$. Si f cumple (1) de la definición, entonces g es holomorfa en $\mathbb{D}^*$ y por lo tanto g tiene un desarrollo en serie de Laurent:

$$g(q) = \sum_{n\in\mathbb{Z}} a_n q^n \ \ \forall q \in \mathbb{D}^*.$$

Si para $z \in \mathbb{H}$ tomamos $q = e^{2\pi iz}$ entonces vale $|q| = e^{-2\pi\,\mathrm{im}(z)}$, por lo que $z \to \infty$ equivale a $q \to 0$. Decimos que f es holomorfa en infinito si g se puede extender de manera holomorfa al 0, es decir si la suma anterior es sobre $n \geq 0$. Por lo tanto, una forma modular tiene una expansión de Fourier:

$$f(z) = \sum_{n=0}^{\infty} a_n q^n \ , \ \ q = e^{2\pi iz}.$$

Definimos:

$$\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) = \{f : \mathbb{H} \to \mathbb{C} : f \text{ es una forma modular de peso } k\}.$$

El conjunto $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ es un $\mathbb{C}$-espacio vectorial. Más aún, con el producto usual tenemos

$$\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))\mathcal{M}_l(\mathrm{SL}_2(\mathbb{Z})) \subseteq \mathcal{M}_{k+l}(\mathrm{SL}_2(\mathbb{Z})).$$

Ejemplo 1.28 (**Serie de Eisenstein**). *Para $k > 2$, sea:*

$$F_k(\Lambda) = \sum_{\omega\in\Lambda'} \omega^{-k},$$

donde $\Lambda' = \Lambda\backslash\{0\}$, y la convergencia absoluta de la serie está dada por el lema 2.20. Queda así definida una función homogénea de retículos de peso k, la cual da a luz a la función modular $G_k(z)$:

$$G_k(z) = \sum_{(m,n)\neq(0,0)} (mz+n)^{-k},$$

que resulta ser una forma modular de peso k a la que llamamos ***Serie de***

Eisenstein. *Obsérvese que:*

$$\begin{aligned} G_k(z) &= \sum_{(m,n)}{}' (mz+n)^{-k} \\ &= \sum_{d\geq 1} \sum_{\substack{(m,n)=d \\ (m,n)}}{}' (mz+n)^{-k} \\ &= \zeta(k) \sum_{\substack{(m,n)=1 \\ (m,n)}}{}' (mz+n)^{-k}, \end{aligned}$$

donde el apóstrofe en la suma indica que la suma se hace sobre $(n,m) \neq (0,0)$ *y* ζ *denota la función zeta de Riemann:*

$$\zeta(s) = \sum_{n\geq 1} n^{-s}.$$

Cuando k *es par, se puede probar que*

$$\zeta(k) = -\frac{(2\pi i)^k}{2k!} B_k,$$

donde B_k *es el* k*-ésimo número de Bernoulli, definidos como los coeficientes de la serie de potencia:*

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

En cualquier caso, definimos la ***Serie de Eisenstein normalizada*** *de modo que* $a_0 = 1$*, como* $E_k(z) = G_k(z)/2\zeta(k)$*:*

$$E_k(z) = \frac{1}{2} \sum_{(n,m)=1} (mz+n)^{-k},$$

que tiene expansión de Fourier[3]*:*

$$E_k(z) = 1 + \frac{(2\pi i)^k}{\zeta(k)(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \tag{1.29}$$

[3]La función σ_α está definida por:

$$\sigma_\alpha(n) := \sum_{d|n} d^\alpha.$$

Observación 1.30. *Para* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *se define* $j(\gamma, z) := cz + d$. *Así se puede definir el operador de peso* k, *al que notamos* $[\gamma]_k$, *para las funciones* $f : \mathbb{H} \to \mathbb{C}$ *por:*

$$(f[\gamma]_k)(z) := j(\gamma, z)^{-k} f(\gamma \cdot z).$$

Observamos que la modularidad de peso k *definida en 1.26 es, en estos términos:*

$$f[\gamma]_k = f \ \ \forall \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Definición 1.31. *Una forma cuspidal de peso* k *es una forma modular* f *de peso* k *cuya expansión de Fourier tiene* $a_0 = 0$.

Denotamos $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ al conjunto de formas cuspidales de peso k, que es un subespacio de $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$.

La observación 1.24 en este contexto nos dice que $f \equiv 0$ es el único elemento de $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ cuando k es impar, pues $-I \in \mathrm{SL}_2(\mathbb{Z})$. Esto muestra que la condición (2) de la definición 1.27 es quizás muy restrictiva; la siguiente definición aligera dicha condición.

Definición 1.32. *Sea* $k \in \mathbb{Z}$ *y* $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ *un subgrupo de congruencia. Una función* $f : \mathbb{H} \to \mathbb{C}$ *se dice una forma modular de peso* k *para* Γ *si:*

1. f *es holomorfa en* $\mathbb{H}$,
2. f *cumple:*
$$f[\gamma]_k = f \ \ \forall \gamma \in \Gamma, \tag{1.33}$$
3. $f[\alpha]_k$ *es holomorfa en* ∞ *para toda* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

   ó equivalentemente[4]

3'. f *es holomorfa en* ∞ *y en la expansión de Fourier de* f *los coeficientes para* $n > 0$ *están acotados:* $|a_n| \leq Cn^r$ *para ciertas constantes positivas* C, r.

Si además $a_0 = 0$ *para toda* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ *entonces decimos que la forma es cuspidal de peso* k *para* Γ.

[4]Para una función como en la definición que cumpla (1) y (2), es equivalente satisfacer (3) que satisfacer (3') [DS05, ver sección 1.2].

Es importante puntualizar que la expansión de Fourier que tienen estas funciones es:

$$f(z) = \sum_{n \geq 0} a_n e^{\frac{2\pi i n z}{N}},$$

donde N es el nivel del subgrupo de congruencia Γ.

Como antes, notamos $\mathcal{M}_k(\Gamma)$ y $\mathcal{S}_k(\Gamma)$ a los espacios de formas modulares de peso k y formas cuspidales de peso k para Γ respectivamente. Dado un subgrupo de congruencia Γ, el espacio de formas modulares de peso k para Γ se descompone en las *Series de Eisenstein* y las *formas cuspidales*:

$$\mathcal{M}_k(\Gamma) = \mathcal{E}_k(\Gamma) \oplus \mathcal{S}_k(\Gamma),$$

subespacios ortogonales para el producto interno de Petersson. En particular, toda forma modular se escribe $f = E_f + S_f$ para $E_f \in \mathcal{E}_k(\Gamma)$ y $S \in \mathcal{S}_k(\Gamma)$.

Si se considera un carácter χ módulo N, se puede definir:

$$\mathcal{M}_k(N, \chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) : f(\gamma \cdot z) = \chi(d_\gamma) f(z) \forall \gamma \in \Gamma_0(N)\}.$$

Estos subespacios[5] descomponen a $\mathcal{M}_k(\Gamma_1(N))$ en suma directa:

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathcal{M}_k(N, \chi).$$

Los subespacios $\mathcal{E}_k(N, \chi)$ y $\mathcal{S}_k(N, \chi)$ se definen análogamente, descomponen a los espacios de series de Eisenstein y formas cuspidales en suma directa y a su vez vale:

$$\mathcal{M}_k(N, \chi) = \mathcal{E}_k(N, \chi) \oplus \mathcal{S}_k(N, \chi).$$

El espacio de formas modulares de peso k para cierto subgrupo de congruencia es un espacio vectorial de dimensión finita.

[5] Recuérdese que $\Gamma_1(N) \triangleleft \Gamma_0(N)$ y que de hecho, es el núcleo del morfismo $\gamma \mapsto d_\gamma$; por lo que lo anterior está bien definido y "separa" a las formas modulares de $\Gamma_1(N)$ según su comportamiento por la acción de $\Gamma_0(N)$.

Capítulo 2

Suma de dos cuadrados

En este capítulo resolvemos el Problema 3 teniendo como referencia principal [DS05]. Con ese objetivo comenzamos definiendo los coeficientes $r_k(n)$ y las funciones $\theta_k(z)$. Vemos cómo estas se relacionan entre ellas para luego probar que θ_2 es una forma modular de peso 1 para $\mathcal{M}_1(\Gamma_1(4))$. Finalmente construimos dicho espacio para dar una solución al problema.

2.1. Sumas de cuadrados

Sea $Q_k : \mathbb{Z}^k \to \mathbb{Z}_{\geq 0}$ la forma cuadrática asociada a la suma de k cuadrados, i.e: para $v = (v_1, \ldots, v_k) \in \mathbb{Z}^k$ se tiene:

$$Q_k(v) = v_1^2 + \cdots + v_k^2.$$

Definición 2.1. *Sea $k \in \mathbb{Z}_{>0}$, definimos el conjunto de representaciones de n como suma de k cuadrados:*

$$R_k(n) := \{v \in \mathbb{Z}^k : Q_k(v) = n\} \tag{2.2}$$

así como el número de representaciones de n como suma de k cuadrados:

$$r_k(n) := \#R_k(n). \tag{2.3}$$

Como Q_k es definida positiva, $r_k(n) = 0$ si $n < 0$. Además, existe una biyección entre $R_{k+l}(n)$ y $\bigsqcup_{a+b=n} R_k(a) \times R_l(b)$, dada por

$$(v_1, \ldots, v_{k+l}) \mapsto ((v_1, \ldots, v_k), (v_{k+1}, \ldots, v_{k+l})).$$

Tenemos entonces que vale la siguiente identidad:

$$r_{k+l}(n) = \sum_{a+b=n} r_k(a) r_l(b). \tag{2.4}$$

Definición 2.5. *Para $k > 0$, definimos la función theta asociada al problema de los k cuadrados $\theta_k : \mathbb{H} \to \mathbb{C}$ dada por:*

$$\theta_k(z) = \sum_n r_k(n) e^{2\pi i n z}. \tag{2.6}$$

Sea $\mathbb{H}_\sigma = \{z \in \mathbb{H} : \mathrm{im}(z) \geq \sigma\}$ para $\sigma > 0$, luego para $z \in \mathbb{H}_\sigma$ vale:

$$\begin{aligned} |\theta_k(z)| &\leq \sum_n |r_k(n) e^{-2\pi i n z}| \\ &\leq 1 + \sum_{n \geq 1} r_k(n) e^{-2\pi n \cdot \mathrm{im}(z)} \\ &\leq 1 + 2^k \sum_{n \geq 1} n^k e^{-2\pi \sigma n} \end{aligned}$$

donde usamos que si $|v_i| \geq \sqrt{n}$ para cada $i = 1, \ldots, k$ y $n > 0$ entonces $Q_k(v) > n$, lo que nos da la cota $r_k(n) \leq (2\sqrt{n}+1)^k$ de donde $r_k(n) \leq (2n)^k$ si $k \geq 2$ (pero de hecho, para $k = 1$ también vale la misma cota trivialmente pues $r_1(n) \leq 2$). Luego θ_k converge absolutamente y uniformemente en $\mathbb{H}_\sigma$ para todo $\sigma > 0$ por el criterio M de Weierstrass, y define en $\mathbb{H}_\sigma$ una función holomorfa. Como $\mathbb{H} = \cup_{\sigma > 0} \mathbb{H}_\sigma$ concluimos que θ_k define una función holomorfa en $\mathbb{H}$.

Además, la fórmula 2.4 se traduce en la siguiente identidad para las funciones theta:

$$\theta_k(z)\theta_l(z) = \theta_{k+l}(z). \tag{2.7}$$

En particular, vale:

$$\theta_k(z) = \theta_1(z)^k \tag{2.8}$$

2.2. Modularidad de θ_2

En la presente sección probaremos que $\theta_2(z)$ es una forma modular para $\mathcal{M}_1(\Gamma_1(4))$. Ya verificamos que es una función holomorfa en el semiplano superior, y la cota $r_2(n) < 4n^2$ que utilizamos a esos efectos nos dice que se satisface la condición $(3')$ de la definición 1.32. Por lo tanto, nos resta probar la modularidad respecto a $\Gamma_1(4)$.

Lema 2.9. *El subgrupo $\Gamma_1(4)$ es generado por $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ y $\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$.*

Demostración. La demostración es análoga a la de 1.19. Sea Γ el subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ generado por las dos matrices en cuestión. Es claro que $\Gamma \subseteq \Gamma_1(4)$.

Para una matriz $\alpha \in \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(4)$, por un lado:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

donde $d' = nc + d$, por lo que salvo cuando $c = 0$ podemos elegir n de modo que $|d'| < \frac{|c|}{2}$; siendo la desigualdad estricta por ser d impar y $c/2$ es par.

Por otro lado:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 4n & 1 \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

donde $c' = c + 4nd$, por lo que eligiendo n adecuadamente ($d \neq 0$, ¡es impar!) podemos obtener $|c'| < 2|d|$; nuevamente la desigualdad es estricta, pues $c' \equiv 0$ (mód 4) y $2d' \equiv 2$ (mód 4).

Ahora bien, para α, o bien su entrada inferior izquierda es 0 (tómese $\gamma = \mathrm{Id}$), o bien aplicando estas dos transformaciones alternadamente, como en cada paso decrece estrictamente la cantidad mín$\{|c|, 2|d|\}$, concluimos que existe $\gamma \in \Gamma$ de modo que:

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

Como $\det(\alpha\gamma) = 1$ y tanto $\hat{a}$ como $\hat{d}$ son 1 módulo 4, tenemos $\hat{a} = \hat{d} = 1$. Ahora bien:

$$\begin{pmatrix} 1 & \hat{b} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \hat{b} + n \\ 0 & 1 \end{pmatrix}$$

por lo que eligiendo $n = -b$, tenemos una matriz γ' de modo que que:

$$\alpha\gamma\gamma' = \mathrm{Id},$$

por lo que $\alpha \in \Gamma$ como queríamos probar. □

A la luz del lema anterior, para verificar que $\theta_2(z)$ es modular para $\Gamma_1(4)$ nos basta con verificar que se cumple:

$$\theta_2(z+1) = \theta_2(z)\,, \qquad \theta_2\left(\frac{z}{4z+1}\right) = (4z+1)\theta_2(z); \tag{2.10}$$

La primera igualdad de 2.10 es clara por la periodicidad de la exponencial. Para la segunda, por 2.8 es suficiente probar:

$$\theta_1\left(\frac{z}{4z+1}\right) = (4z+1)^{1/2}\theta_1(z). \tag{2.11}$$

Los coeficientes que definen a θ_1 son:

$$r_1(n) = \begin{cases} 1 & \text{si } n = 0 \\ 2 & \text{si } n \text{ es cuadrado} \\ 0 & \text{si } n \text{ no es cuadrado} \end{cases},$$

por lo que

$$\begin{aligned} \theta_1(z) &= 1 + 2q + 2q^4 + 2q^9 + \dots \\ &= \sum_{n\in\mathbb{Z}} q^{n^2}. \end{aligned}$$

Si escribimos:

$$\vartheta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z},$$

vemos que $\vartheta(z)$ que se vincula con $\theta_1(z)$ por:

$$\theta_1(z) = \sum_{n\in\mathbb{Z}} e^{2\pi i n^2 z} = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 (2z)} = \vartheta(2z). \tag{2.12}$$

Por lo que $\vartheta : \mathbb{H} \to \mathbb{C}$ define una función holomorfa en el semiplano superior. Además vale la siguiente identidad para la acción por S:

Proposición 2.13. *Para $z \in \mathbb{H}$, tenemos:*

$$\vartheta(-1/z) = (-iz)^{-1/2}\vartheta(z). \tag{2.14}$$

Demostración. Sea $f(x) = e^{-\pi x^2}$. Obsérvese que si $\tau = it$ con $t > 0$, entonces

$$\vartheta(\tau) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t} = \sum_{n\in\mathbb{Z}} f(nt^{1/2}).$$

Escribamos $h_{\sqrt{t}}(n) = f(nt^{1/2})$ y obsérvese que por Sumación de Poisson:

$$\vartheta(\tau) = \sum_{n\in\mathbb{Z}} h_{\sqrt{t}}(n) = \sum_{n\in\mathbb{Z}} \widehat{h_{\sqrt{t}}}(n).$$

Para $h_r(x)$ vale que $\widehat{h_r}(x) = r^{-1}\widehat{f}(r^{-1}x)$ y f es su propia transformada de Fourier, de donde sigue que:

$$\begin{aligned}\vartheta(it) &= t^{-1/2}\sum_{n\in\mathbb{Z}} f(nt^{-1/2}) \\ &= t^{-1/2}\sum_{n\in\mathbb{Z}} e^{-\pi n^2 t^{-1/2}} \\ &= t^{-1/2}\sum_{n\in\mathbb{Z}} e^{-\pi n^2 t^{-1}} \\ &= t^{-1/2}\sum_{n\in\mathbb{Z}} e^{\pi i n^2\left(\frac{i}{t}\right)} \\ &= t^{-1/2}\vartheta(i/t).\end{aligned}$$

Probamos, recordando que $\tau = it$, que vale:

$$\vartheta(-1/\tau) = (-i\tau)^{1/2}\vartheta(\tau) \quad t > 0,$$

que por el principio de identidad para funciones holomorfas se extiende a $z \in \mathbb{H}$ dando 2.14. □

Antes de continuar probamos las propiedades sobre la transformada de Fourier que omitimos en la prueba anterior. Para eso primero calculamos una integral.

Lema 2.15. *Para $y \in \mathbb{R}$:*

$$\int_{\mathbb{R}} e^{-\pi(x+iy)^2} dx = 1.$$

Demostración. Concluiremos viendo que la integral a calcular es igual a la del caso $y = 0$, la conocida *integral Gaussiana*.

Sea $\varphi : \mathbb{C} \to \mathbb{C}$ la función $\varphi(z) = e^{-\pi z^2}$, holomorfa en todo el plano complejo. Por el Teorema de Cauchy vale:

$$\oint_{\mathcal{R}} \varphi(z)dz = 0.$$

donde $\mathcal{R}$ es el rectángulo (orientado) de vértices $-N$, N, $N+iy$ y $-N+iy$ que puede verse en la figura.

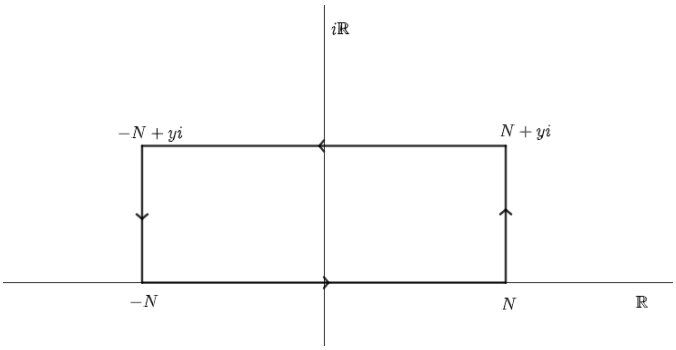

Figura 2.1: Contorno rectangular.

Descomponiendo la integral de interés en la suma de integrales tenemos:

$$\oint_{\mathcal{R}} \varphi(z)dz = I_1 + I_2 + I_3 + I_4.$$

Las integrales a lo largo de los lados verticales, digamos I_2 e I_4, tienden a 0 conforme $N \to \infty$. En efecto:

$$\begin{aligned} I_2 &= \int_0^y e^{-\pi(N+it)^2} dt \\ |I_2| &\leq \ell([N, N+iy]) \cdot \sup_{z \in [N+iy, N]} |\varphi(z)| \\ &= y e^{-\pi N^2}. \end{aligned}$$

Así $I_2 \to 0$ conforme $N \to \infty$. Del mismo modo $I_4 \to 0$ cuando $N \to \infty$. Concluimos tomando límite en N que:

$$\int_{\mathbb{R}} e^{-\pi(t+iy)^2} dt = \int_{\mathbb{R}} e^{-\pi t^2} dt = 1.$$

□

Probado el lema, probamos aquello que había quedado pendiente:

Proposición 2.16. *Sea $f : \mathbb{R} \to \mathbb{R}$ y para $r \in \mathbb{R}_{>0}$ sea $h_r(x) = f(rx)$.*

i. $\widehat{h_r}(x) = r^{-1}\widehat{f}(r^{-1}x)$,

ii. *Si $f(x) = e^{-\pi x^2}$, entonces $\widehat{f} = f$.*

Demostración. La afirmación (i) sigue del cambio de variable $rt = u$.

Para (ii):

$$\begin{aligned}\hat{f}(x) &= \int_{\mathbb{R}} e^{-\pi y^2} e^{-2\pi i x y} dy \\ &= \int_{\mathbb{R}} e^{-\pi(y^2+2ixy)} dy \\ &= \int_{\mathbb{R}} e^{-\pi(y+ix)^2} e^{-\pi x^2} dy \\ &= e^{-\pi x^2} \int_{\mathbb{R}} e^{-\pi(y+ix)^2} dy.\end{aligned}$$

Por el Lema 2.15 la integral que multiplica a $e^{-\pi x^2}$ vale 1, de donde concluimos que $\widehat{f}(x) = e^{-\pi x^2}$. □

Expresando 2.14 en términos de θ_1 por medio de 2.12 obtenemos:

$$\theta_1\left(\frac{-1}{4z}\right) = (-2iz)^{1/2}\theta_1(z). \tag{2.17}$$

Ahora bien, la matriz que lleva z en $-1/4z$ es $\begin{pmatrix} 0 & -1 \\ 4 & 0 \end{pmatrix}$. Obsérvese que:

$$\begin{pmatrix} 0 & 1/4 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 4 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

Por lo tanto, usamos 2.17 junto con la 1-periodicidad de θ_1 para dar una fórmula para la transformación asociada a actuar por dicha matriz, que lleva

z en $\frac{z}{4z+1}$.

$$\begin{aligned}
\theta_1\left(\frac{z}{4z+1}\right) &= \theta_1\left(\frac{-1}{4\left(-\frac{4z+1}{4z}\right)}\right) \\
&= \left(\frac{i}{2z}(4z+1)\right)^{1/2}\theta_1\left(-\frac{4z+1}{4z}\right) \\
&= \left(\frac{i}{2z}(4z+1)\right)^{1/2}\theta_1\left(-1-\frac{1}{4z}\right) \\
&= \left(\frac{i}{2z}(4z+1)\right)^{1/2}\theta_1\left(-\frac{1}{4z}\right) \\
&= \left(\frac{i}{2z}(4z+1)\right)^{1/2}\theta_1\left(-\frac{1}{4z}\right) \\
&= \left(\frac{i}{2z}(4z+1)\right)^{1/2}(-2iz)^{1/2}\theta_1(z).
\end{aligned}$$

Afirmamos que vale

$$\left(\frac{i}{2z}(4z+1)\right)^{1/2}(-2iz)^{1/2} = (4z+1)^{1/2} \quad \forall z \in \mathbb{H}, \tag{2.18}$$

que es un caso particular de 3.49. Por lo tanto probamos 2.11, completando la prueba de las identidades 2.10: concluimos que $\theta_2(z)$ es una forma modular para $\mathcal{M}_1(\Gamma_1(4))$.

2.3. El espacio $\mathcal{M}_1(\Gamma_1(4))$

Un teorema de Weierstrass permite la construcción de una función entera con un cierto conjunto de ceros.

Teorema 2.19 (**Prescripción de ceros**). *Sea $\{a_n\}_n$ una sucesión de números complejos no nulos con $|a_n| \to \infty$ conforme $n \to \infty$ y sea $\{p_n\}$ una sucesión de enteros positivos de modo que:*

$$\sum_n \left(\frac{r}{|a_n|}\right)^{p_n+1} < \infty$$

para todo $r > 0$.

Entonces la función:

$$P(z) := \prod_{n=1}^{\infty} E_{p_n}(z/a_n),$$

donde los factores E_k están definidos por:

$$E_k(z) = \begin{cases} 1-z & si\ k=0 \\ (1-z)e^{z+z^2/2+\cdots+z^k/k} & si\ k \geq 1 \end{cases}$$

define una función holomorfa en todo el plano complejo que tiene $\{a_n\}$ por conjunto de ceros.

Dado un retículo $\Lambda = \Lambda(\omega_1, \omega_2) \subseteq \mathbb{C}$ nos interesa construir una función cuyo conjunto de ceros sea precisamente Λ. Con eso en mente, establecemos el siguiente lema.

Lema 2.20. *Sea $\Lambda = \Lambda(\omega_1, \omega_2) \subseteq \mathbb{C}$ un retículo. Si $\alpha > 2$:*

$$\sum_{\omega \in \Lambda'} |\omega|^{-\alpha} < \infty.$$

Demostración. Sea ω_o el vector de Λ' con menor módulo, digamos r_o. Luego dado $\omega \in \Lambda'$, $B(\omega, r_o) \cap \Lambda' = \{\omega\}$. Por lo tanto, si definimos

$$\Lambda_n = \{\omega \in \Lambda' : n \leq |\omega| < n+1\}$$

y llamamos λ_n al cardinal de este conjunto, tenemos que

$$\lambda_n \cdot vol(B(\omega, r_o)) \leq vol(B(0, n+1+r_o) \backslash B(0,n)).$$

De lo anterior concluimos que $\lambda_n = O(n)$. Luego, sumando sobre los Λ_n:

$$\begin{aligned} \sum_{\omega \in \Lambda'} \left(\frac{1}{|\omega|}\right)^{\alpha} &= \sum_{n \geq 0} \sum_{\omega \in \Lambda_n} |\omega|^{-\alpha} \\ &\leq C \sum_{n} n^{-\alpha+1} \\ &< \infty \end{aligned}$$

□

Dado un retículo $\Lambda \subseteq \mathbb{C}$, por el lema anterior vemos que la sucesión constante $p_n = 3$ satisface la hipótesis del teorema, por lo que definimos $\sigma_\Lambda : \mathbb{C} \to \mathbb{C}$ cuyos ceros simples son los puntos de Λ.

$$\sigma_\Lambda(z) := z \prod_{\omega \in \Lambda'} \left(1 - \frac{z}{\omega}\right) e^{z/\omega + \frac{1}{2}(z/\omega)^2}.$$

La función σ de Weierstrass es la función que toma un par $(z, \Lambda) \in \mathbb{C} \times \mathcal{R}$ y le asigna $\sigma_\Lambda(z)$. Es una función homogénea de grado 1, es decir que para $\lambda \in \mathbb{C}$:

$$\sigma(\lambda z, \lambda\Lambda) = \lambda\sigma(z, \Lambda).$$

La función Z de Weierstrass es la derivada logarítmica de σ:

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

Esta última es una función meromorfa con polos simples en los puntos de Λ y además es homogénea de grado -1, i.e.: $Z(\lambda z, \lambda\Lambda) = \lambda^{-1} Z(z, \Lambda)$ para $\lambda \in \mathbb{C}$. Dado que la suma converge absolutamente y uniformemente en compactos en $\mathbb{C}\backslash\Lambda$, calculamos su derivada derivando término a término obteniendo $Z'(z, \Lambda) = -\wp(z, \Lambda)$, donde $\wp$ es la conocida función $\wp$ de Weierstrass. Esta última función es periódica respecto de Λ, i.e.:

$$\wp(z + \omega, \Lambda) = \wp(z, \Lambda) \ \ \forall \omega \in \Lambda.$$

A la luz de esto, si $\Lambda = \Lambda(\omega_1, \omega_2)$, las siguientes cantidades son constantes:

$$\eta_1(\Lambda) = Z(z + \omega_1, \Lambda) - Z(z, \Lambda) \ \ ; \ \ \eta_2(\Lambda) = Z(z + \omega_2, \Lambda) - Z(z, \Lambda)$$

Un $\omega \in \Lambda$ es combinación lineal entera de ω_1 y ω_2, por lo que escribimos $\omega = n_1\omega_1 + n_2\omega_2$ y de lo anterior sigue:

$$Z(z + \omega, \Lambda) = Z(z, \Lambda) + n_1\eta_1(\Lambda) + n_2\eta_2(\Lambda). \tag{2.21}$$

Una aplicación del teorema de los residuos da la siguiente relación entre η_1 y η_2:

Lema 2.22 (**Relación de Legendre**). *En lo que respecta a la expansión de Fourier de las funciones σ y Z, supongamos $\Lambda = \Lambda(\omega_1, \omega_2)$ con $\omega_1/\omega_2 \in \mathbb{H}$. Entonces vale*

$$\eta_1(\Lambda)\omega_1 + \eta_2(\Lambda)\omega_2 = 2\pi i$$

Escribiendo $\Lambda_\tau = \Lambda(\tau, 1)$, se puede probar que :

$$\sigma(z, \Lambda_\tau) = (2\pi i)^{-1} e^{\frac{1}{2}\eta_2 z^2}(e^{\pi i z} - e^{-\pi i z}) \prod_{n\geq 1} \frac{(1 - e^{2\pi i(n\tau+z)})(1 - e^{2\pi i(n\tau-z)})}{(1 - e^{2\pi i n\tau})^2},$$

Que se traduce en que:

$$Z(z, \Lambda_\tau) = \eta_2 z - \pi i \frac{1 + e^{2\pi i z}}{1 - e^{2\pi i z}} - 2\pi i \sum_{n\geq 1} \left(\frac{e^{2\pi i(n\tau+z)}}{1 - e^{2\pi i(n\tau+z)}} - \frac{e^{2\pi i(n\tau-z)}}{1 - e^{2\pi i(n\tau-z)}} \right).$$

Además, $\eta_2(\Lambda_\tau) = G_2(\tau)$ [DS05, Capítulo 1], función holomorfa en el semiplano superior, de donde la relación de Legendre da $\eta_1(\Lambda_\tau) = 2\pi i - \tau G_2(\tau)$.

Nuestro objetivo en la presente sección es el de construir el espacio $\mathcal{M}_1(\Gamma_1(4))$. Por las fórmulas de dimensión [DS05, Capítulo 3] que siguen de estudiar la curva modular $X(\Gamma)$, contando puntos y cúspides para aplicar el Teorema de Riemann-Roch, sabemos que este espacio es de dimensión 1. Más precisamente, el género para $\Gamma_1(4)$ es 0, por lo que se satisface $\varepsilon_\infty^{reg} > 2g - 2$ de donde el Teorema 3.6.1 [DS05] dice que $\dim(\mathcal{M}_1(\Gamma_1(4))) = \varepsilon_\infty^{reg}/2$ y que $\dim(\mathcal{S}_1(\Gamma_1(4))) = 0$. Como para $\Gamma_1(4)$ la cantidad de cúspides ε_∞ es 3, y solamente hay una cúspide irregular $s = 1/2$ tenemos que $\varepsilon_\infty^{reg} = \varepsilon_\infty - \varepsilon_\infty^{irreg} = 2$.

En lo que sigue construimos una serie de Eisenstein E_1^χ, de donde

$$\mathcal{M}_1(\Gamma_1(4)) = \{\lambda E_1^\chi : \lambda \in \mathbb{C}\}.$$

Sea $v \in \mathbb{Z}^2$ y notemos $\hat{v}$ a la proyección de v módulo 4. Supongamos que $\hat{v} = (c_v, d_v) \in (\mathbb{Z}/4\mathbb{Z})^2$ es de orden 4. Definimos la siguiente función:

$$F_1^{\hat{v}}(\mathbb{C}/\Lambda_\tau, (\tau/4 + \Lambda_\tau, 1/4 + \Lambda_\tau)) = Z\left(\frac{c_v\tau + d_v}{4}, \Lambda_\tau\right) - \frac{c_v\eta_1(\Lambda_\tau) + d_v\eta_2(\Lambda_\tau)}{4}.$$

Si se toma $w \in \mathbb{Z}^2$ de modo que $\hat{w} = \hat{v}$, por 2.21 vemos que $F_1^{\hat{v}} = F_1^{\hat{w}}$. En lo que sigue asumimos entonces que $0 \leq c_v < N$. Además, $F_1^{\hat{v}}$ es homogénea de grado -1:

$$\begin{aligned}
&F_1^{\hat{v}}(\mathbb{C}/\lambda\Lambda, (\lambda\tau/4 + \lambda\Lambda_\lambda\tau, \lambda/4 + \lambda\Lambda_\tau)) \\
&\qquad = Z\left(\frac{c_v\lambda\tau + d_v\lambda}{4}, \lambda\Lambda_\tau\right) - \frac{c_v\eta_1(\lambda\Lambda_\tau) + d_v\eta_2(\lambda\Lambda_\tau)}{4} \\
&\qquad = \lambda^{-1}\left(Z\left(\frac{c_v\tau + d_v}{4}, \Lambda_\tau\right) - \frac{c_v\eta_1(\Lambda_\tau) + d_v\eta_2(\Lambda_\tau)}{4}\right) \\
&\qquad = \lambda^{-1} F_1^{\hat{v}}(\mathbb{C}/\Lambda_\tau, (\tau/4 + \Lambda_\tau, 1/4 + \Lambda_\tau)).
\end{aligned}$$

Esto se traduce en que la función

$$g_1^{\hat{v}} : \mathbb{H} \to \mathbb{C}, \;\; g_1^{\hat{v}}(\tau) = \frac{1}{4} F_1^{\hat{v}}(\mathbb{C}/\Lambda_\tau, (\tau/4 + \Lambda_\tau, 1/4 + \Lambda_\tau))$$

es modular de peso 1 con respecto a $\Gamma(4)$; para $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(4)$, escribiendo $m = (c\tau + d)^{-1}$:

$$\begin{aligned}
g_1^{\hat{v}}(\gamma \cdot \tau) &= \frac{1}{4} F_1^{\hat{v}}(\mathbb{C}/\Lambda_{\gamma\cdot\tau}, ((\gamma \cdot \tau)/4 + \Lambda_{\gamma\cdot\tau}, (\gamma \cdot 1)/4 + \Lambda_{\gamma\cdot\tau})) \\
&= \frac{1}{4} F_1^{\hat{v}}(\mathbb{C}/m\Lambda_\tau, (m(a\tau + b)/4 + m\Lambda_\tau, m(c\tau + d)/4 + m\Lambda_\tau)) \\
&= m^{-1} \frac{1}{4} F_1^{\hat{v}}(\mathbb{C}/\Lambda_\tau, ((a\tau + b)/4 + \Lambda_\tau, (c\tau + d)/4 + \Lambda_\tau)) \\
&\overset{*}{=} m^{-1} \frac{1}{4} F_1^{\hat{v}}(\mathbb{C}/\Lambda_\tau, (\tau/4 + \Lambda_\tau, 1/4 + \Lambda_\tau)) \\
&= m^{-1} g_1^{\hat{v}}(\tau) \\
&= (c\tau + d) g_1^{\hat{v}}(\tau),
\end{aligned}$$

donde en * usamos que $a, d \equiv 1$ (mód 4) y $b, c \equiv 0$ (mód 4) junto con que $\Lambda_\tau = \Lambda(\tau, 1)$.

Se puede probar que:

$$g_1^{\hat{v}}(\tau) = G_1^{\hat{v}}(\tau) - \frac{C_1}{4}\left(\frac{c_v}{4} - \frac{1}{2}\right), \tag{2.23}$$

donde

$$G_1^{\hat{v}}(\tau) = \delta(c_v)\zeta^{d_v}(1) + \frac{C_1}{4} \sum_{n \geq 1} \sigma_0^{\hat{v}}(n) e^{\frac{2\pi i n \tau}{N}}. \tag{2.24}$$

Precisemos un poco sobre las definiciones 2.23 y 2.24. La constante y las funciones involucradas son:

$$\begin{aligned}
C_1 &= -2\pi i, \\
\delta(c_v) &= \begin{cases} 1 & \text{si } c_v \equiv 0 \text{ (mód 4)} \\ 0 & \text{en otro caso} \end{cases}, \\
\zeta^{d_v}(k) &= \sum_{\substack{d \in \mathbb{Z}^\times \\ d \equiv d_v \pmod 4}} d^{-k}, \\
\sigma_0^{\hat{v}}(n) &= \sum_{\substack{m \in \mathbb{Z},\, m|n \\ n/m \equiv c_v \pmod 4}} sg(m).
\end{aligned}$$

Se puede probar que la función ζ^{d_v} es entera, y que en particular:

$$\zeta^{d_v}(1) = \frac{\pi i}{4} + \frac{\pi}{4}\cot\left(\frac{\pi d_v}{4}\right).$$

Como $g_1^{\hat{v}}$ es holomorfa y modular de peso 1 para $\Gamma(4)$ y además, a la luz de 2.23 sus coeficientes crecen como Cn (obsérvese que $|\sigma_0^{\hat{v}}(n)| < 2n+1$) concluimos que $g_1^{\hat{v}} \in \mathcal{M}_1(\Gamma(4))$.

Ahora bien, sea χ el único carácter no trivial módulo 4 y defínanse:

$$G_1^{\chi}(\tau) = \sum_{c \pmod 4} \sum_{d \pmod 4} \chi(c)\widehat{g_1^{(c,d)}}(\tau),$$

$$E_1^{\chi}(\tau) = 1 + c_1^{\chi}\sum_{n\geq 1}\left(\sum_{d|n}\chi(d)\right)q^n, \tag{2.25}$$

donde $c_1^{\chi} = \frac{2}{L(0,\chi)}$. La función E_1^{χ} es la serie de Eisenstein que buscamos, se puede probar que vale:

$$G_1^{\chi} \in \mathcal{M}_1(4,\chi), \quad G_1^{\chi}(\tau) = \frac{2C_1}{c_1^{\chi}}E_1^{\chi}(\tau).$$

2.4. Solución al problema

Sabemos que existe $\lambda \in \mathbb{C}$ tal que:

$$\theta_2(z) = \lambda E_1^{\chi}(z).$$

Como $r_2(0) = 1$ concluimos que $\lambda = 1$ y que por lo tanto $\theta_2 = E_1^{\chi}$. Además, si bien a priori desconocemos el valor de c_1^{χ}, como $r_2(1) = 4$ tenemos $c_1^{\chi} = 4$. Luego, como los coeficientes de θ_2 y E_1^{χ} son iguales concluimos:

$$r_2(n) = 4\sum_{d|n}\chi(d). \tag{2.26}$$

Una forma alternativa de escribir la fórmula es:

$$r_2(n) = 4\left(\sum_{\substack{d|n \\ d\equiv 1 \pmod 4}} 1 - \sum_{\substack{d|n \\ d\equiv 3 \pmod 4}} 1\right).$$

Observación 2.27. *Aplicando la fórmula a p primo, obtenemos:*

$$r_2(p) = \begin{cases} 8 \text{ si } p \equiv 1 \pmod 4 \\ 0 \text{ si } p \equiv 3 \pmod 4 \end{cases}$$

lo cual da una prueba alternativa del problema 1. Obsérvese que de hecho, las 8 *representaciones del caso* $p \equiv 1 \pmod 4$ *son esencialmente la misma. Más precisamente, dada una representación* $p = a^2 + b^2$*, debe tener* $ab \neq 0$ *y* $a \neq b$*, entonces* $(\pm a, \pm b)$ *y* $(\pm b, \pm a)$ *son las* 8 *representaciones de p como suma de cuadrados.*[1]

Observación 2.28 (**Fórmula de Leibniz**)**.** *De la información combinatoria de la función theta obtuvimos* $c_1^\chi = 4$ *lo cual tiene como consecuencia que* $L(0, \chi) = \frac{1}{2}$*. Recordamos que la L-función asociada al carácter* χ *se define como:*

$$L(s, \chi) = \sum_{n \geq 1} \chi(n) n^{-s} \text{ para } re(s) > 1,$$

y tiene continuación analítica a todo el plano complejo, de modo que $L(0, \chi)$ *tiene sentido. Además, la ecuación funcional que satisface vincula* $L(0, \chi)$ *con* $L(1, \chi)$*, de donde el valor de* $L(0, \chi)$ *implica la fórmula:*

$$L(1, \chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4}.$$

[1] Que un primo p, de ser representable como suma de dos cuadrados, puede ser representado de forma *esencialmente única* sigue también de que $\mathbb{Z}[i]$ es un DFU.

Capítulo 3

Modularidad de las funciones theta

En el presente capítulo generalizamos –siguiendo a [Iwa97]– las ideas del capítulo anterior. Dada una forma cuadrática Q definida positiva podemos definir una función theta $\Theta_Q(z)$. De hecho, no solo trabajaremos con la generalización directa de las funciones theta del capítulo anterior, sino que estudiaremos funciones theta *con peso*. El peso estará dado por una función esférica, por lo cual comenzamos definiendo estos objetos y probando un teorema que los caracteriza. Luego definiremos las funciones $\Theta_Q(z)$ y trabajando con ellas acabaremos probando que *para una forma cuadrática definida positiva en $2n$ variables, su función theta [con peso] es una forma modular de cierto peso en cierto espacio.*

3.1. Funciones esféricas

Una función $f : D \subseteq \mathbb{R}^r \to \mathbb{C}$ se dice de clase C^k si $f(x) = u(x) + iv(x)$ con $u, v : D \to \mathbb{C}$ de clase C^k.[1] Decimos que una función $f : D \subseteq \mathbb{R}^r \to \mathbb{C}$ es *armónica* si es de clase C^2 y satisface la ecuación de Laplace:

$$\Delta f = 0 \tag{3.1}$$

donde Δ denota al operador de Laplace:

$$\Delta = \sum_{i=1}^{r} \frac{\partial^2}{\partial x_i^2}. \tag{3.2}$$

[1] En este contexto, $\frac{\partial f}{\partial x_i} = \frac{\partial u}{\partial x_i} + i\frac{\partial v}{\partial x_i}$.

En la siguiente proposición reunimos algunas propiedades del Laplaciano que nos serán de utilidad en lo que sigue.

Proposición 3.3. *Sean $f, g : D \subseteq \mathbb{R}^n \to \mathbb{C}$ funciones suaves.*

a. *Vale*
$$\Delta(fg) = f\Delta(g) + \Delta(f)g + 2\sum_i \frac{\partial f}{\partial x_i}\frac{\partial g}{\partial x_i}.$$

b. *Si f y g son armónicas, $f+g$ es armónica.*

c. *Si f es armónica, entonces las derivadas parciales $\frac{\partial f}{\partial x_i}$ para $i = 1, ..., r$ son armónicas.*

Demostración. Para la parte (a), veamos primero que la igualdad es cierta para $F, G : D \to \mathbb{R}$. Tenemos:

$$\begin{aligned}\frac{\partial^2}{\partial x_i^2}(FG) &= \frac{\partial}{\partial x_i}\left(\frac{\partial F}{\partial x_i}G + F\frac{\partial G}{\partial x_i}\right)\\ &= \frac{\partial^2 F}{\partial x_i^2}G + 2\frac{\partial F}{\partial x_i}\frac{\partial G}{\partial x_i} + F\frac{\partial^2 G}{\partial x_i^2}.\end{aligned}$$

La identidad sigue de sumar en i. Ahora bien, si $f = u_1 + iv_1$ y $g = u_2 + iv_2$ tenemos que $fg = (u_1u_2 - v_1v_2) + i(u_1v_2 + v_1u_2)$. El resultado sigue de aplicar la identidad en cada uno de los cuatro términos.

La afirmación (b) sigue de la linealidad de la derivada . Por último, por el teorema de Schwarz Δ conmuta con $\frac{\partial}{\partial x_i}$, de donde sigue (c). □

A nuestros efectos, dada una matriz simétrica definida positiva A definimos el *operador de Laplace asociado a A*:

$$\Delta_A := \sum_{ij} \hat{a}_{ij}\frac{\partial^2}{\partial x_i \partial x_j} \tag{3.4}$$

donde $A^{-1} = (\hat{a}_{ij})_{i,j}$. Nótese que para $A = Id$ 3.4 es precisamente 3.2.

Diremos que f es *armónica respecto de A* si satisface la ecuación:

$$\Delta_A f = 0 \tag{3.5}$$

Definimos el elipsoide

$$\mathcal{E}_A := \{x \in \mathbb{R}^r : x^t A x \leq 1\},$$

a partir del cual definimos el *producto interno respecto de A*:

$$(f,g)_A := \int_{\mathcal{E}_A} f(x)\overline{g}(x)dx.$$

Recordamos que un polinomio $p \in \Bbbk[x_1,\ldots,x_k]$ se dice *homogéneo de grado* ν si cumple $p(\lambda x_1,\ldots,\lambda x_r) = \lambda^\nu p(x_1,\ldots,x_r)$. Si $\mathcal{P}$ denota al álgebra de polinomios $\Bbbk[x_1,...,x_r]$ y notamos $\mathcal{H}_\nu$ al conjunto conformado por los polinomios homogéneos de grado ν, subespacio vectorial de dimensión $\binom{\nu+r-1}{r-1}$, se tiene que:

$$\mathcal{P} = \bigoplus_\nu \mathcal{H}_\nu. \tag{3.6}$$

A una función armónica que a su vez es un polinomio homogéneo la llamamos *función esférica respecto de A*. El siguiente resultado nos da una caracterización de las funciones esféricas.

Teorema 3.7. *Sea f un polinomio homogéneo de grado ν. Son equivalentes:*

i. *f es una función esférica [respecto de A].*

ii. *f es ortogonal [respecto de A] a cualquier polinomio homogéneo de menor grado.*

iii. *f es de la siguiente forma:*

- *$f(x) =$ constante si $\nu = 0$,*
- *$f(x) =$ una forma lineal si $\nu = 1$,*
- *$f(x) =$ suma de formas $(u^tAx)^\nu$ donde $u \in \mathbb{C}^r$ es un vector isotrópico, es decir $u^tAu = 0$, si $\nu \geq 2$.*

Demostración.

Afirmación 3.8. *Basta con probar el teorema para $A = Id$.*

Sea R la matriz de la observación 1.17. Considérese $\tilde{f} : \mathbb{R}^r \to \mathbb{R}$, polinomio homogéneo de grado ν definido por $\tilde{f}(y) = f(Rx)$. La afirmación sigue de que f satisface (i), (ii) ó (iii) respecto de A si y solamente si $\tilde{f}$ satisface (i), (ii) ó (iii) respectivamente, pero respecto a Id.

Probada la afirmación nos disponemos a probar el Teorema 3.7. A la luz de la observación, lo haremos suponiendo $A = \mathrm{Id}$. Nótese que, por lo tanto, en lo que resta de la prueba *armónica* refiere a que se satisface 3.1.

Probemos que (iii) implica (i). Es claro que las funciones constantes y las formas lineales son armónicas. Para $\nu \geq 2$, para las expresiones de la forma $h(x) = (u^T x)^\nu$ vale:

$$\begin{aligned}\Delta h(x) &= \sum_{i=1}^{r} \frac{\partial^2}{\partial x_i^2}(u^t x)^\nu \\ &= \sum_{i=1}^{r} \nu u_i \frac{\partial}{\partial x_i}(u^t x)^{\nu-1} \\ &= \sum_{i=1}^{r} \nu(\nu-1) u_i^2 (u^t x)^{\nu-2} \\ &= \nu(\nu-1)(u^t x)^{\nu-2} \sum_{i=1}^{r} u_i^2.\end{aligned}$$

Pero como u es isotrópico tenemos $\sum_i u_i^2 = u^t u = 0$, así que $\Delta h = 0$. Concluimos que cualquier f que sea suma de estas expresiones será armónica por (b) de la proposición 3.3.

Ahora nos preparamos para probar que (i) implica (ii). A esos efectos, notemos ω_j a las $(r-1)$-formas diferenciales

$$\omega_j = (-1)^{j-1} dx_1 \dots \widehat{dx_j} \dots dx_r,$$

a partir de las cuales definimos $\omega = \sum_i x_i \omega_i$. Además para $j = 1, ..., r$ vale:

$$dx := dx_1 \dots dx_r = dx_j \omega_j = d(x_j \omega_j).$$

Observación 3.9. *Vale entonces* $d\omega = r dx$

Sea F una función suave y η_1 la $(r-1)$-forma diferencial $\eta_1 = F \cdot \omega$. Vemos que:

$$\begin{aligned}d\eta_1 &= d(F \cdot \omega) = d(F)\omega + F d\omega \\ &= \sum_i \frac{\partial F}{\partial x_i} dx_i \omega + rF dx \\ &= \sum_i \frac{\partial F}{\partial x_i} x_i dx + rF dx \\ &= (\delta F + rF) dx\end{aligned}$$

donde δ denota el operador diferencial de Euler $\delta = \sum_i x_i \frac{\partial}{\partial x_i}$.

Sea η_2 la $(r-1)$-forma diferencial $\eta_2 = (\delta F) \cdot \omega$. Aplicando la fórmula anterior, tenemos:

$$d\eta_2 = (\delta^2 F + r\delta F)dx. \tag{3.10}$$

Ahora bien, por un lado:

$$\begin{aligned}
\delta^2 F &= \delta\left(\sum_i \frac{\partial F}{\partial x_i} x_i\right) \\
&= \sum_i \delta\left(\frac{\partial F}{\partial x_i} x_i\right) \\
&= \sum_i \sum_j \left(\frac{\partial^2 F}{\partial x_j \partial x_i} x_i + \delta_{ij} \frac{\partial F}{\partial x_i}\right) x_j \\
&= \sum_{i,j} \frac{\partial^2 F}{\partial x_j \partial x_i} x_i x_j + \delta F.
\end{aligned}$$

Por otro lado, sea

$$g_i = \delta F x_i - \frac{\partial F}{\partial x_i}.$$

Obsérvese que vale:

$$\begin{aligned}
d(g_i\omega_i) &= d(\delta F x_i \omega_i) - d\left(\frac{\partial F}{\partial x_i}\omega_i\right) \\
&= d(\delta F) x_i \omega_i + \delta F d(x_i\omega_i) - d\left(\frac{\partial F}{\partial x_i}\omega_i\right) \\
&= \sum_j \left(\frac{\partial^2 F}{\partial x_j \partial x_i} x_j + \delta_{ij}\frac{\partial F}{\partial x_i}\right) x_i dx + \delta F dx - \frac{\partial^2 F}{\partial x_i^2} dx.
\end{aligned}$$

Así, para $g = g_1\omega_1 + ... + g_r\omega_r$:

$$dg = \left(\sum_{i,j} \frac{\partial^2 F}{\partial x_j \partial x_i} x_i x_j + (r+1)\delta F - \Delta F\right) dx.$$

Luego, partiendo de 3.10:

$$d\eta_2 = \delta^2 F + (r+1)\delta F - \Delta F dx + \Delta F dx$$

reconociendo dg:

$$d\eta_2 = \Delta F dx + dg.$$

El teorema de Stokes nos dice que –para una $(r-1)$-forma diferencial η– vale:

$$\int_{\mathcal{E}} d\eta = \int_{\partial\mathcal{E}} \eta,$$

lo cual aplicado a η_1 nos da:

$$\int_{\mathcal{E}} (\delta F + rF)dx = \int_{\partial\mathcal{E}} F\omega \tag{3.11}$$

y a η_2 –recordando que una forma exacta integra 0– nos da:

$$\int_{\mathcal{E}} \Delta F dx = \int_{\partial\mathcal{E}} (\delta F)\omega. \tag{3.12}$$

Ahora bien. Obsérvese que para un monomio $x = x_1^{\alpha_1}...x_r^{\alpha_r}$ de grado total ν vale $\delta(x) = \nu x$, por lo que para un polinomio homogéneo p de grado ν tenemos $\delta p = \nu p$. Combinando esta observación con 3.12, luego aplicando 3.11 vemos que:

$$\int_{\mathcal{E}} \Delta p dx = \nu(\nu + r) \int_{\mathcal{E}} p dx. \tag{3.13}$$

Ahora sí, probemos que (i) implica (ii) por inducción en ν. Suponemos que f es un polinomio homogéneo de grado ν tal que $\Delta f = 0$ y suponemos que g es otro polinomio homogéneo con $\deg(g) < \nu$. Recordando que las derivadas parciales de f son también armónicas (parte (c) de la Proposición 3.3) y que para estas sí tenemos probado que son perpendiculares a cualquier polinomio de grado menor (en particular, a las derivadas parciales de g), tenemos que:

$$\begin{aligned}\int_{\mathcal{E}} \overline{f} g dx &= c_1 \int_{\mathcal{E}} \Delta(\overline{f} g) dx \\ &= c_1 \int_{\mathcal{E}} \overline{f} \Delta g dx.\end{aligned}$$

Inductivamente:

$$\int_{\mathcal{E}} \overline{f} g dx = c_n \int_{\mathcal{E}} \overline{f} \Delta^n g dx.$$

Como el grado total de g decrece estrictamente cada vez que se le aplica Δ, existe n_o de modo que $\Delta^{n_o} g = 0$, de donde sigue que:

$$\int_{\mathcal{E}} \overline{f} g dx = 0$$

como queríamos probar.

Por último probaremos que (ii) implica (iii). Para esto, en $\mathcal{H}_\nu$ –espacio vectorial de dimensión finita– consideramos el conjunto

$$S_\nu = \{(u^t x)^\nu : u^t u = 0\}$$

que genera un subespacio vectorial

$$\mathcal{S}_\nu = \operatorname{span} S_\nu \subseteq \mathcal{H}_\nu$$

que es cerrado.

Observación 3.14. *Como ya probamos que (iii) implica (ii), tenemos que de hecho:*

$$\mathcal{S}_\nu \subseteq \mathcal{H}_\nu \cap \left(\bigcap_{\mu<\nu} \mathcal{H}_\mu^\perp \right).$$

Queremos probar que si $f \in \mathcal{H}_\nu$ perpendicular a cada $\mathcal{H}_\mu$ con $\mu < \nu$ y a todo polinomio en S_ν entonces es el polinomio nulo. De ese modo, tendremos que:

$$\mathcal{S}_\nu^\perp \cap \left(\mathcal{H}_\nu \cap \left(\bigcap_{\mu<\nu} \mathcal{H}_\mu^\perp \right) \right) = \{0\}.$$

De donde sigue la otra inclusión:

$$\mathcal{H}_\nu \cap \left(\bigcap_{\mu<\nu} \mathcal{H}_\mu^\perp \right) \subseteq \mathcal{S}_\nu.$$

Sea $g \in S_\nu$. Como g y sus derivadas parciales satisfacen (iii), entonces satisfacen (i) y (ii). Así:

$$\begin{aligned} \int_{\mathcal{E}} \overline{f} g dx &= c_1 \int_{\mathcal{E}} \Delta(\overline{f} g) dx \\ &= 2c_1 \int_{\mathcal{E}} \left(\sum_j \frac{\partial \overline{f}}{\partial x_j} \frac{\partial g}{\partial x_j} \right) dx \end{aligned}$$

pues $\Delta g = 0$ y $\deg(\Delta \overline{f}) < \deg f = \deg g$ por lo que $g \perp \Delta \overline{f}$.

Repitiendo lo anterior ν veces obtenemos que:

$$\begin{aligned} \int_{\mathcal{E}} \overline{f} g dx &= 2^\nu c_\nu \int_{\mathcal{E}} \left(\sum_{j_1,\ldots,j_\nu} \frac{\partial^\nu \overline{f}}{\partial x_{j_1} \cdots \partial x_{j_\nu}} \frac{\partial^\nu g}{\partial x_{j_1} \cdots \partial x_{j_\nu}} \right) \\ &= 2^\nu c_\nu vol(\mathcal{E}) \sigma \end{aligned}$$

pues como $\deg(f) = \deg(g) = \nu$ tenemos que las derivadas de orden ν necesariamente son constantes, de donde la suma en el integrando es realmente una constante σ.

Por un lado $\sigma = 0$, pues $f \perp g$ y $2^\nu c_\nu vol(\mathcal{E}) > 0$. Pero por otro, siendo f un polinomio homogéneo de grado ν tenemos que:

$$\nu f = \delta f = \sum_{j_1} x_{j_1} \frac{\partial f}{\partial x_{j_1}}.$$

Como las derivadas parciales de f son polinomios homogéneos de grado $\nu - 1$ (ó 0), vale:

$$(\nu - 1)\frac{\partial f}{\partial x_{j_1}} = \sum_{j_2} x_{j_2} \frac{\partial^2 f}{\partial x_{j_2} \partial x_{j_1}}$$

de donde:

$$\nu(\nu - 1) f = \sum_{j_1, j_2} x_{j_1} x_{j_2} \frac{\partial^2 f}{\partial x_{j_2} \partial x_{j_1}}.$$

Inductivamente:

$$\nu! f = \sum_{j_1, \ldots, j_\nu} x_{j_1} \ldots x_{j_\nu} \frac{\partial^\nu f}{\partial x_{j_1} \cdots \partial x_{j_\nu}}. \tag{3.15}$$

Para g, nótese que:

$$\frac{\partial^\nu g}{\partial x_{j_1} \cdots \partial x_{j_\nu}} = \nu! u_{j_1} ... u_{j_\nu}. \tag{3.16}$$

Conjugando la igualdad de 3.15 y evaluando en $u = (u_1, ..., u_r)$, luego reconociendo el miembro derecho de 3.16 obtenemos:

$$\overline{f}(u) = \frac{1}{\nu!} \sum_{j_1, \ldots, j_\nu} \frac{1}{\nu!} \frac{\partial^\nu g}{\partial x_{j_1} \cdots \partial x_{j_\nu}} \frac{\partial^\nu \overline{f}}{\partial x_{j_1} \cdots \partial x_{j_\nu}}.$$

Luego $\overline{f}(u) = \nu!^{-2}\sigma$, por lo que $f(u) = 0$. Tomando todos los elementos de S_ν, el razonamiento anterior nos da que $f(u) = 0$ siempre que $uu^t = 0$. Por lo tanto, f se anula en el conjunto algebraico $\mathcal{V}(p) = \{x \in \mathbb{C}^r : p(x) = 0\}$ donde $p(x) = \sum_i x_i^2$. Como $\mathbb{C}$ es algebraicamente cerrado, el ideal en $\mathbb{C}[x_1, \ldots, x_r]$ de los polinomios que se anulan en $\mathcal{V}(p)$ es, en virtud del Nullstellensatz de Hilbert, $\sqrt{\langle p \rangle}$. Es decir, tenemos $f \in \sqrt{\langle p \rangle}$ de donde existe n tal que vale $f^n \in \langle p \rangle$. Ahora bien:

a. Si $r = 1$, $p(x) = x^2$ y $f(x) = ax^\nu$ por lo que para $\nu \geq 2$ tenemos que $p \mid f$.

b. Si $r = 2$, $p(x, y) = x^2 + y^2$ se escribe como producto de dos irreducibles coprimos $p(x, y) = (x + iy)(x - iy)$. Como $p \mid f^n$, lo hace cada uno de sus factores irreducibles, de donde concluimos que $p \mid f$.

c. Si $r \geq 3$, entonces p es irreducible. Si consideramos a $p(x_1, \ldots, x_r) \in (\mathbb{C}[x_1, ..., x_{r-1}])[x_r]$, la irreducibilidad de p sigue de aplicar el criterio de Eisenstein. Para $r = 3$, tenemos que $p(x_1, x_2, x_3) = x_3^2 + (x_1^2 + x_2^2)$ y $x_1 + ix_2 \mid x_1^2 + x_2^2$ (pero $(x_1 + ix_2)^2 \nmid x_1^2 + x_2^2$), divide a 0 y no divide a 1. Para $r > 3$, por inducción el término independiente es irreducible, se aplica Eisenstein.

En cualquiera de los 3 casos considerados arriba, $p \mid f$ por lo que escribimos $f = ph$. Como f y p son homogéneos, h es homogéneo (y tenemos $\deg(h) = \nu - 2$), por lo que usando 3.11 junto con que $p_{|\partial\mathcal{E}} \equiv 1$, obtenemos:

$$\begin{aligned}\int_{\mathcal{E}} \overline{h} h dx &= k_1 \int_{\partial\mathcal{E}} \overline{h} h \omega \\ &= k_1 \int_{\partial\mathcal{E}} \overline{h} f \omega \\ &= k_2 \int_{\mathcal{E}} \overline{h} f dx \\ &= 0.\end{aligned}$$

Así $h = 0$, por lo que $f = 0$. El único caso que no fue cubierto es:

d. Si $r = 1$ y $\nu = 0, 1$.

Pero en este caso f es ax ó a para cierto $a \in \mathbb{C}$. Concluimos que (ii) implica (iii). □

Notamos $\mathcal{S}_\nu$ al *espacio de funciones esféricas de grado* ν. Enunciamos una consecuencia del teorema anterior.

Corolario 3.17. *Para $\nu \geq 2$, se tiene que:*

$$\dim_{\mathbb{C}} \mathcal{S}_v = \binom{\nu + r - 1}{r - 1} - \binom{\nu + r - 3}{r - 1}.$$

Demostración. Si bien por (ii) del teorema anterior

$$\mathcal{S}_\nu = \{f \in \mathcal{H}_\nu : f \perp \mathcal{H}_\mu \ \forall \mu < \nu\}$$

resulta que basta con que $f \perp \mathcal{H}_{\nu-2}$.

Para más detalles ver [Iwa97, Corolario 9.2]. □

3.2. Funciones theta

Sea $A \in M_r(\mathbb{Z})$ simétrica con forma cuadrática asociada Q definida positiva, y P una función esférica respecto de A de grado ν.

Definimos la *función theta con peso*:

$$\Theta(z, P) := \sum_{x \in \mathbb{Z}^r} P(x) e\left(Q(x)z\right).$$

Observación 3.18. *Si tomamos A la matriz asociada a la forma cuadrática $Q_r(x) = x_1^2 + \cdots + x_r^2$ y $P \equiv 1$ obtenemos la función θ_r definida en el Capítulo 2.*

Más aún, para una forma cuadrática definida positiva cualquiera, tomando $P \equiv 1$ obtenemos:

$$\Theta(z, P) = \sum_n r_Q(n) e^{2\pi i n z}, \quad z \in \mathbb{H}$$

donde como cabe esperar $r_Q(n) := \{x \in \mathbb{Z}^n : Q(x) = n\}$. Así generalizamos la definición de función theta asociada al problema de los r cuadrados a una forma cuadrática Q en general.

Proposición 3.19. *La función theta con peso es una función holomorfa en todo el semiplano superior.*

Demostración. Supongamos primero que P es constante, digamos $P(x) = k$.

Observación 3.20. *Como Q es definida positiva, existen constantes positivas c_o, c_1 tales que:*

$$c_o Q_r(x) \leq Q(x) \leq c_1 Q_r(x),$$

consecuencia de que todas las normas en $\mathbb{R}^r$ son equivalentes.

A la luz de la observación:

$$\begin{aligned}|\Theta(z,P)| &\leq |k| \sum_{x\in\mathbb{Z}^r} |e(Q(x)z)| \\ &= |k| \sum_{x\in\mathbb{Z}^r} e^{2\pi Q(x)\,\mathrm{im}(z)} \\ &\leq |k| \sum_{x\in\mathbb{Z}^r} e^{2\pi c_1 Q_r(x)\,\mathrm{im}(z)} \\ &= |k| \sum_n r_r(n) e^{2\pi c_1 n\ \mathrm{im}(z)},\end{aligned}$$

por lo que la prueba es la misma que dimos para θ_r en 2.6.

Sea P ahora de grado $\nu > 0$. Podemos suponer que $P(x) = (u^t Ax)^\nu$ – pues en virtud del Teorema 3.7 una función esférica arbitraria es suma de polinomios de este tipo, y la suma de funciones holomorfas es holomorfa.

Antes de proceder observamos dos cosas:

i. Para $x \in \mathbb{R}^r$, $|x| = (Q_r(x))^{1/2}$.

ii. $T(x) = u^t Ax$ es una transformación lineal, luego $|T(x)| \leq ||T||_{op}|x|$.

$$\begin{aligned}|\Theta(z,P)| &\leq \sum_{x\in\mathbb{Z}^r} |P(x)e(Q(x)z)| \\ &= \sum_{x\in\mathbb{Z}^r} |P(x)| e^{2\pi Q(x)\,\mathrm{im}(z)} \\ &\leq \sum_{x\in\mathbb{Z}^r} |P(x)| e^{2\pi c_1 Q_r(x)\,\mathrm{im}(z)} \\ &\leq C_o \sum_{x\in\mathbb{Z}^r} |x|^\nu e^{2\pi c_1 Q_r(x)\ \mathrm{im}(z)} \\ &= C_o \sum_n e^{2\pi c_1 n\ \mathrm{im}(z)} \sum_{\substack{x\in\mathbb{Z}^r \\ Q_r(x)=n}} |x|^\nu \\ &=\leq C_o \sum_n r_r(n) n^{\nu/2} e^{2\pi c_1 n\ \mathrm{im}(z)}.\end{aligned}$$

Luego usando la cota $r_r(n) < Cn^r$ tenemos:

$$|\Theta(z,P)| \leq C_1 \sum_n n^{\hat{k}} e^{2\pi c_1 n\ \mathrm{im}(z)}$$

donde $\hat{k} = r + \frac{\nu}{2}$. Nuevamente, la prueba es la misma que en 2.6. □

Si bien A es entera, no lo es necesariamente A^{-1}. Sin embargo, para $N \in \mathbb{Z}_{\geq 1}$ bien elegido –por ejemplo $N = |A|$– la matriz $A^* = NA^{-1}$ también es entera. Para cualquier N que cumpla lo anterior se tiene que $|A||A^*| = N^r$, de donde $N^r \equiv 0 \pmod{|A|}$ lo que implica que $\mathrm{rad}(|A|) \mid N$ (donde el radical de un entero k es el producto de todos los primos que lo dividen; el radical del ideal $\langle k \rangle \triangleleft \mathbb{Z}$ –al que notamos $\sqrt{\langle k \rangle}$– es el ideal $\langle \mathrm{rad}(k) \rangle$, lo que explica la denominación).

Ejemplo 3.21. *La forma cuadrática Q_r tiene matriz asociada*

$$A_r = \begin{pmatrix} 2 & & \\ & \ddots & \\ & & 2 \end{pmatrix}.$$

Su inversa no es entera, pero sí lo es la matriz $A_r^* = 2A_r^{-1}$. Así que en este caso se deberá tomar $N \equiv 0 \pmod 2$.

Proposición 3.22. *Sea A simétrica, definida positiva (no necesariamente entera) y sea P una función esférica respecto de A de grado ν. Para $z \in \mathbb{H}$ y $x \in \mathbb{C}^r$ tenemos:*

$$\sum_m P(m+x) e\left(Q(m+x)z\right) = \frac{i^{-\nu}}{\sqrt{|A|}} \left(\frac{i}{z}\right)^k \sum_m P^*(m) e\left(\frac{-1}{z} Q^*(m) + m^T x\right).$$

En particular (para $x = 0$):

$$\Theta_A(z, P) = i^{-\nu} |A|^{1/2} \left(\frac{i}{z}\right)^k \Theta_{A^{-1}}(-z^{-1}, P^*)$$

donde $P^*(x) := P(A^{-1}x)$ es esférica respecto de A^{-1}, $Q^*(x) = \frac{1}{2} x^t A^{-1} x$ y $k = \frac{r}{2} + \nu$.

Lema 3.23. *Se cumple que*

$$\int_{\mathbb{R}} e\left(\frac{1}{2} y^2 z - yu\right) dy = \left(\frac{i}{z}\right)^{1/2} e\left(-\frac{u^2}{2z}\right).$$

Demostración (del lema). Escríbase $e\left(\frac{1}{2} y^2 z - yu\right) = e^{\frac{\pi i}{z}(yz-u)^2} e^{-\frac{\pi i}{z} u^2}$, luego:

$$\int_{\mathbb{R}} e\left(\frac{1}{2} y^2 z - yu\right) dy = e\left(-\frac{u^2}{2z}\right) \int_{\mathbb{R}} e^{\frac{\pi i}{z}(yz-u)^2} dy.$$

Por lo tanto el resultado sigue de calcular la integral:

$$\int_{\mathbb{R}} e^{\frac{\pi i}{z}(yz-u)^2} dy,$$

equivalentemente:

$$\int_{\mathbb{R}} e^{-\pi(yz\alpha-u\alpha)^2} dy$$

donde $\alpha = (iz)^{-1/2}$.

Repitiendo el argumento del Lema 2.15 aplicado al paralelogramo de vértices 0, R, $R+u/z$ y u/z nos da:

$$\int_{\mathbb{R}} e^{-\pi(yz\alpha-u\alpha)^2} dy = \int_{\mathbb{R}} e^{-\pi(z\alpha)^2 y^2} dy.$$

Afirmación 3.24. *Si $\omega \in \mathbb{C}$ con $re(\omega) > 0$, entonces:*

$$\int_{\mathbb{R}} e^{-\pi\omega y^2} dy = \omega^{-1/2} \int_{\mathbb{R}} e^{-\pi y^2} dy; \tag{3.25}$$

Observando que $z\alpha = (z/i)^{1/2}$ tiene parte real positiva sigue de la observación:

$$\int_{\mathbb{R}} e^{-\pi(yz\alpha)^2} dy = \left(\frac{i}{z}\right)^{1/2} \int_{\mathbb{R}} e^{-y^2} dy$$

donde la integral de la derecha da 1 como vimos en el lema 2.15, lo cual concluye la prueba del lema.

Nos resta probar la afirmación. Para eso, sea:

$$F(\omega) = \int_{\mathbb{R}} e^{-\pi\omega y^2} dy. \tag{3.26}$$

En estos términos la afirmación 3.24 se escribe:

$$F(\omega) = \omega^{-1/2} F(1), \quad re(\omega) > 0 \tag{3.27}$$

fórmula que ya sabemos cierta para $\omega \in \mathbb{R}^+$ –pues sigue del cambio de variable $x = \sqrt{\omega}y$– pero que tiene sentido en una cierta región Ω. Hilando

más fino, si $\Omega = \{\omega \in \mathbb{C} : Re(\omega) > 0\}$:

$$\begin{aligned}\left|\int_{\mathbb{R}} e^{-\pi\omega y^2} dy\right| &\leq \int_{\mathbb{R}} |e^{-\pi\omega y^2}| dy \\ &= \int_{\mathbb{R}} e^{-\pi Re(\omega) y^2} dy \\ &= (Re(\omega))^{-1/2} \int_{\mathbb{R}} e^{-\pi y^2} dy < \infty.\end{aligned}$$

Por lo tanto, queda definida $F : \Omega \to \mathbb{C}$ dada por 3.26. Obsérvese que también $\omega^{-1/2}$ está bien definido en todo Ω.

Afirmamos que F es holomorfa, para lo cual invocamos al teorema de Morera: si F es continua[2] e integra 0 en todo triángulo $T \subseteq \Omega$ sigue que F es holomorfa. Ahora bien:

$$\oint_T F(z)dz = \oint_T \left(\int_{\mathbb{R}} e^{-\pi z y^2} dy\right) dz.$$

El teorema de Tonelli aplicado a $f(t, z) = |e^{-\pi z t^2}|$ nos dice que como:

$$\begin{aligned}\oint_T \int_{\mathbb{R}} |f(t, z)| dt dz &= \left(\int_{\mathbb{R}} e^{-\pi y^2} dy\right) \left(\oint_T (Re(\omega))^{-1/2} d\omega\right) \\ &< \infty\end{aligned}$$

f es integrable, luego el Teorema de Fubini justifica el cambio del orden de integración y:

$$\oint_T F(z)dz = \int_{\mathbb{R}} \left(\oint_T e^{-\pi z y^2} dz\right) dy.$$

Pero la función del integrando, como función de z, es holomorfa y por tanto $\oint_T e^{-\pi z y^2} dz = 0$. Luego

$$\oint_T F(z)dz = 0$$

para todo triángulo $T \subseteq \Omega$ de donde sigue que $F : \Omega \to \mathbb{C}$ es holomorfa.

Como los miembros izquierdo y derecho de 3.27 son funciones holomorfas en Ω y coinciden en $\mathbb{R}^+ \subseteq \Omega$ concluimos –en virtud del principio de identidad– que son iguales. □

[2] que lo es, la integral converge absolutamente por lo que podemos intercambiar el límite con la integral.

Demostración (de la Proposición 3.22). Consideramos $f(x) = e(Q(x)z)$ y aplicaremos sumación de Poisson. Para eso tenemos que calcular:

$$\hat{f}(v) = \int_{\mathbb{R}^r} f(x)e(-x^t v)dx.$$

A esos efectos, sea R la matriz de la observación 1.17. El cambio de variable $y = Rx$ nos da $Q(x) = \frac{1}{2}y^t y$, si u es el vector que cumple $v = R^t u$ tenemos $x^t Av = y^t u$, y $dx = |R|^{-1}dy$ donde $|R|^2 = |A|$. Sustituyendo:

$$\hat{f}(v) = |R|^{-1} \int_{R^r} e\left(\frac{1}{2}y^t yz - y^t u\right) dy.$$

Como $v^t w = \sum_{i=1}^r v_i w_i$, tenemos que $\frac{1}{2}y^t yz - y^t u = \sum_{i=1}^r \left(\frac{1}{2}y_i^2 z - y_i u_i\right)$, lo cual nos permite escribir la integral como producto de integrales en cada coordenada:

$$\hat{f}(v) = |R|^{-1} \prod_{i=1}^r \int_{\mathbb{R}} e\left(\frac{1}{2}y_i^2 z - y_i u_i\right) dy_i.$$

Ahora simplemente aplicamos el Lema 3.23 a cada factor:

$$\hat{f}(v) = |R|^{-1} \left(\frac{i}{z}\right)^{r/2} \prod_{i=1}^r e\left(-\frac{u_i^2}{2z}\right).$$

Calculando el producto y reconociendo $u^t u$:

$$\hat{f}(v) = |R|^{-1} \left(\frac{i}{z}\right)^{r/2} e\left(-\frac{u^t u}{2z}\right).$$

Ahora deshacemos el cambio de variable, en particular: $\frac{1}{2}u^t u = \frac{1}{2}(R^{-1}v)^t R^{-1}v = \frac{1}{2}v^t R^{-1t} R^{-1}v = \frac{1}{2}v^t A^{-1}v =: Q^*(v)$. Además $|R| = |A|^{1/2}$:

$$\hat{f}(v) = |A|^{-1/2} \left(\frac{i}{z}\right)^{r/2} e\left(-\frac{1}{z}Q^*(v)\right).$$

Ahora sí, aplicando sumación de Poisson obtenemos:

$$\sum_m e\left(Q(m+x)z\right) = |A|^{-1/2} \left(\frac{i}{z}\right)^{r/2} \sum_m e\left(-\frac{1}{z}Q^*(m) + m^t x\right). \quad (3.28)$$

Así hemos probado la afirmación para $P \equiv 1$.

Para obtener el resultado para P genérico, por el teorema 3.7 basta con

probarlo para $(c^tAx)^\nu$ donde c es isotrópico si $\nu \geq 2$ y arbitrario en cualquier otro caso. Sea L el operador:

$$L = \sum_j c_j \frac{\partial}{\partial x_j}.$$

Se cumple que $L(Q(x)) = x^tAc$, $L^2(Q(x)) = c^tAc$ y $L^m(Q(x)) = 0\ \forall m \geq 3$.

El resultado seguirá de aplicar L^ν a ambos miembros de la igualdad 3.28.

Por un lado:

$$L\left(\sum_m e\left(Q(m+x)z\right)\right) = 2\pi iz \sum_m e\left(Q(m+x)z\right) c^tA(x+m).$$

Luego:

$$L^2\left(\sum_m e\left(Q(x+m)z\right)\right) = (2\pi iz)^2 \sum_m e\left(Q(x+m)z\right)\left(c^tA(x+m)\right)^2.$$

Inductivamente:

$$L^\nu\left(\sum_m e\left(Q(x+m)z\right)\right) = (\pi iz)^\nu \sum_m e\left(Q(x+m)z\right)\left(c^tA(x+m)\right)^\nu.$$

Recordando que $P(x) = (c^tAx)^\nu$ tenemos que lo anterior nos dice que el resultado de aplicar L^ν al miembro izquierdo de 3.28 nos da:

$$(2\pi iz)^\nu \sum_m P(x+m) e\left(Q(m+x)z\right).$$

Ahora, hacemos lo mismo en el derecho. Se tiene:

$$L\left(\sum_m e\left(-\frac{1}{z}Q^*(m) + m^tx\right)\right) = 2\pi i \sum_m e\left(-\frac{1}{z}Q^*(m) + m^tx\right) c^Tm.$$

Aplicando L nuevamente:

$$L^2\left(\sum_m e\left(-\frac{1}{z}Q^*(m) + m^tx\right)\right) = (2\pi i)^2 \sum_m e\left(-\frac{1}{z}Q^*(m) + m^tx\right)(c^tm)^2.$$

Inductivamente:

$$L^\nu\left(\sum_m e\left(-\frac{1}{z}Q^*(m)+m^tx\right)\right)=(2\pi i)^\nu\sum_m e\left(-\frac{1}{z}Q^*(m)+m^tx\right)(c^tm)^\nu.$$

Obsérvese que $P^*(m)=P(A^{-1}m)=(c^tA(A^{-1}m))^\nu=(c^tm)^\nu$, luego, aplicar L^ν al miembro derecho de 3.28 da:

$$|A|^{-1/2}\left(\frac{i}{z}\right)^{r/2}(2\pi i)^\nu\sum_m P^*(m)e\left(-\frac{1}{z}Q^*(m)+m^tx\right).$$

Igualando las expresiones anteriores y dividiendo entre $(2\pi iz)^\nu$ concluimos. □

3.3. Funciones theta congruentes

En lo que sigue trabajaremos con las *funciones theta congruentes*:

$$\Theta(z;h)=\sum_{m\equiv h\ (\text{mód }N)}P(m)e\left(\frac{Q(m)}{N^2}z\right) \tag{3.29}$$

para $h\in\mathbb{Z}^r$, N entero positivo.

Observación 3.30. *Las funciones $\Theta(\ \cdot\ ;h):\mathbb{H}\to\mathbb{C}$ son holomorfas. En efecto, la suma que define a $\Theta(z;h)$ es una subsuma de $\Theta(z/N^2)$.*

Obsérvese que, por homegeneidad, valen:

$$\Theta(z;0)=N^\nu\Theta(z)\ ,\quad \Theta(z;-h)=(-1)^\nu\Theta(z,h),$$

donde aquí, como en lo que resta de la sección, no hacemos referencia en la notación a la matriz A o a la función esférica P, salvo que alguna aclaración sea necesaria.

Como $\Theta(z;h)$ depende de h módulo N, es natural considerar el conjunto:

$$\mathcal{H}=\{h\ (\text{mód }N):Ah\equiv 0\ (\text{mód }N)\}.$$

Lema 3.31. *$\mathcal{H}$ es un grupo abeliano finito (con la suma) de orden $|A|$.*

Demostración. Que $\mathcal{H}$ es un grupo abeliano finito con la suma es claro.

Probaremos la afirmación sobre el cardinal primero asumiendo que A es triangular superior con $a_{ii} > 0$. Sea $\mathcal{B} = [0,1)^r$ y consideremos el paralelepípedo $\mathcal{P} = A\mathcal{B}$.

Sea

$$f : \mathcal{P} \to \prod_{i=1}^{i=r} [0, a_{ii}), \quad f(x_1, \ldots, x_r) = (x_1 \text{ mód } a_{11}, \ldots, x_r \quad \text{mód } a_{rr}).$$

Afirmamos que f es una biyección. En efecto, dado $y = (y_1, ..., y_r)$ en la imagen la ecuación $a_{rr}x_r = y_r \mod a_{rr}$ tiene exactamente una solución para $x_r \in [0,1)$. Luego, la ecuación $a_{(r-1)(r-1)}x_{r-1} + a_{(r-1)r}x_r = y_{r-1}$ mód $a_{(r-1)(r-1)}$, como x_r fue determinado en la ecuación anterior, tiene exactamente una solución $x_{r-1} \in [0,1)$. Inductivamente, encontramos $x = (x_1, ..., x_r) \in [0,1)^r$ de modo que $f(Ax) = y$ y como vimos, este es único. Además, f restringe a una biyección entre $\mathcal{P} \cap \mathbb{Z}^r$ y $\mathcal{C} \cap \mathbb{Z}^r$ (donde estamos llamando $\mathcal{C}$ al codominio de f). Los vectores imagen y preimagen difieren por múltiplos enteros de los a_{ii} (que son también enteros), luego en $f(p_1, ..., p_r) = (y_1, ..., y_r)$ vale $(p_1, ..., p_r) \in \mathcal{P} \cap \mathbb{Z}^r$ si y solamente si $(y_1, ..., y_r) \in \mathcal{C} \cap \mathbb{Z}^r$. Así $|\mathcal{P} \cap \mathbb{Z}^r| = |\mathcal{C} \cap \mathbb{Z}^r| = |A|$.

Los vectores enteros $h \in N\mathcal{B}$ con $Ah \equiv 0 \pmod N$ se corresponden son imagen de vectores con coordenadas enteras en $\mathcal{P}$. Esto sigue de que:

$$\begin{aligned} Ah \equiv 0 \pmod N &\iff Ah = Nv \;\; v \in \mathbb{Z}^r \\ &\iff h = NA^{-1}v \;\; v \in \mathbb{Z}^r. \end{aligned}$$

Por lo tanto, tenemos que $|\mathcal{H}| = |\mathcal{P} \cap \mathbb{Z}^r| = |A|$.

Nótese que el final del argumento anterior no hizo uso de las condiciones que impusimos sobre A. Por lo tanto, para tener el caso general solamente necesitamos probar $|\mathcal{P} \cap \mathbb{Z}^r| = |A|$. Luego el argumento del párrafo anterior nos da $|\mathcal{H}| = |A|$.

Ahora en toda generalidad, como A es una matriz invertible sobre $\mathbb{Q}$, podemos escribir $A = UB$ con $U, B \in \mathcal{M}_r(\mathbb{Z})$, B triangular superior con entradas positivas en la diagonal y U de determinante 1 (de modo que $U^{-1} \in \mathcal{M}_r(\mathbb{Z})$), descomposición llamada *forma normal de Hermite*. Los puntos enteros en

$\mathcal{P}_A$ están en biyección con los de $\mathcal{P}_B$; vía $x \mapsto U^{-1}x$ y $y \mapsto Uy$ (dado que U y U^{-1} son matrices enteras) y le aplicamos el "caso particular" a $\mathcal{P}_B$:

$$|\mathcal{H}| = |\mathcal{P}_A \cap \mathbb{Z}^r| = |\mathcal{P}_B \cap \mathbb{Z}^r| = |B| = |A|.$$

□

En la siguiente proposición describimos los carácteres del grupo $\mathcal{H}$.

Proposición 3.32. *Los caracteres de $\mathcal{H}$ están dados por $\psi_h : \mathcal{H} \to \mathbb{C}^\times$,*

$$\psi_h(l) = e(N^{-2}h^tAl).$$

Demostración. En efecto,

i. Si $g \equiv 0 \pmod N$) entonces vale $g = Ng'$ y $h^tAg = Nh^TAg'$ y como $h^tAg' = (g'^tAh)^t$ concluimos que $h^tAg \equiv 0 \pmod{N^2}$ de donde $\psi_h(g) = 1$.

ii. Vale $\psi_h(l + l') = \psi_h(l)\psi_h(l')$ pues $e(x + y) = e(x)e(y)$.

iii. Los ψ_h efectivamente definen mapas $\mathcal{H} \to \mathbb{C}^\times$. Si $l \equiv l' \pmod N$, entonces $\psi_h(l) = \psi_h(l' + g)$ para cierto $g \equiv 0 \pmod N$) y de aplicar (ii) seguida por (i) tenemos $\psi_h(l) = \psi_h(l')$.

De lo anterior sigue que $\{\psi_h\}_{h\in\mathcal{H}}$ son caracteres de $\mathcal{H}$. Además vale que $\psi_h = \psi_{h'}$ si y solamente si $h \equiv h' \pmod N$).

Supongamos que $\psi_h = \psi_{h'}$, luego para todo $l \in \mathcal{H}$ vale:

$$\begin{aligned} \psi_h(l) &= \psi_{h'}(l) \\ e(N^{-2}h^tAl)) &= e(N^{-2}h'^tAl) \\ e(N^{-2}(h - h')^tAl)) &= 1 \end{aligned}$$

de donde:

$$(h - h')^tAl \equiv 0 \pmod{N^2} \ \ \forall l \in \mathcal{H}.$$

Ahora bien, razonando como en el lema anterior:

$$Al \equiv 0 \pmod N \iff l = NA^{-1}v, \ v \in \mathbb{Z}^r.$$

Definimos pues los $l_i = NA^{-1}e_i$ y tenemos:

$$\begin{aligned}(h-h')^T A l_i &\equiv 0 \text{ (mód } N^2)\\ (h-h')^T A(NA^{-1}e_i) &\equiv 0 \text{ (mód } N^2)\\ (h-h')^T e_i &\equiv 0 \text{ (mód } N)\\ h_i - h'_i &\equiv 0 \text{ (mód } N).\end{aligned}$$

Concluimos pues que $h - h' \equiv 0$ (mód N) como queríamos probar.

Recíprocamente, si $h \equiv h'$ (mód N) es fácil ver que $\psi_h = \psi'_h$: valen $\psi_g = 1$ para $g \equiv 0$ (mód N) y $\psi_{h+h'} = \psi_h \psi_{h'}$ (argumentando como en (i) y (ii)) de donde sigue que $\psi_h = \psi_{h'}$.

Como $\mathcal{H} \cong \widehat{\mathcal{H}}$ y $|\{\psi_h\}_{h\in\mathcal{H}}| = |\mathcal{H}|$ concluimos que los ψ_h son todos los caracteres de $\mathcal{H}$. □

Obsérvese que tenemos la siguiente simetría: $\psi_h(g) = \psi_g(h)$. Sin explicitarlo nos servimos de ella para probar que si $h \equiv h'$ (mód N) entonces $\psi_h = \psi_{h'}$ (pues eso es equivalente, simetría mediante, a que $\psi_l(h) = \psi_l(h')$ para todo $l \in \mathcal{H}$). A la luz de esta observación, a partir de ahora notaremos $\psi(h, g) := \psi_h(g)$.

Proposición 3.33. *Sea $h \in \mathcal{H}$. Entonces:*

$$\Theta(z+2;h) = e\left(\frac{2Q(h)}{N^2}\right)\Theta(z;h). \tag{3.34}$$

Además, si diag(A) *es par:*

$$\Theta(z+1;h) = e\left(\frac{Q(h)}{N^2}\right)\Theta(z;h). \tag{3.35}$$

Demostración. Escribiendo $m = h + vN$ tenemos:

$$Q(m) = Q(h) + N^2 Q(v) + N h^t A v \tag{3.36}$$

de donde:

$$m^t A m \equiv h^t A h \text{ (mód } N^2)$$

pues $v^t(Ah) \equiv 0$ (mód N).

Luego

$$\begin{aligned}\Theta(z+2;h) &= \sum_{m\equiv h \pmod N} P(m)e\left(\frac{Q(m)}{N^2}(z+2)\right)\\ &= \sum_{m\equiv h \pmod N} P(m)e\left(\frac{Q(m)}{N^2}z\right)e\left(\frac{2Q(m)}{N^2}\right)\\ &= e\left(\frac{2Q(h)}{N^2}\right)\sum_{m\equiv h \pmod N} P(m)e\left(\frac{Q(m)}{N^2}z\right).\end{aligned}$$

Así que probamos 3.34. Ahora bien, si $\mathrm{diag}(A)$ es par vale siempre que $v^tAv \equiv 0$ (mód 2), por lo que de 3.36 deducimos:

$$Q(m) \equiv Q(h) \text{ (mód } N^2),$$

de donde:

$$\begin{aligned}\Theta(z+1;h) &= \sum_{m\equiv h \pmod N)} P(m)e\left(\frac{Q(m)}{N^2}(z+1)\right)\\ &= \sum_{m\equiv h \pmod N)} P(m)e\left(\frac{Q(m)}{N^2}z\right)e\left(\frac{Q(m)}{N^2}\right)\\ &= e\left(\frac{Q(h)}{N^2}\right)\sum_{m\equiv h \pmod N} P(m)e\left(\frac{Q(m)}{N^2}z\right).\end{aligned}$$

□

Proposición 3.37. *Sea $h \in \mathcal{H}$. Entonces vale:*

$$\Theta(-1/z;h) = i^{-\nu}|A|^{-1/2}(-iz)^k \sum_{l\in\mathcal{H}} \psi(h,l)\Theta(z;l).$$

Demostración. Aplicamos la proposición 3.22 a $x = N^{-1}h$. El miembro izquierdo de dicha igualdad es:

$$\sum_m P\left(\frac{h+Nm}{N}\right)e\left(\frac{1}{N^2}Q(h+Nm)z\right).$$

Por ser P homogéneo de grado ν, esta expresión no es más que $N^{-\nu}\Theta(z;h)$. Por su parte, el miembro derecho es:

$$\frac{i^{-\nu}}{\sqrt{|A|}}\left(\frac{i}{z}\right)^k \sum_m P^*(m)e\left(\frac{-1}{z}Q^*(m) + N^{-1}m^th\right),$$

donde como en la proposición $k = \nu + \frac{r}{2}$.

Por la correspondencia

$$v = NA^{-1}m,\ m \in \mathbb{Z}^r \longleftrightarrow Av \equiv 0 \pmod{N}, v \in \mathbb{Z}^r$$

vale

$$\frac{i^{-\nu}}{\sqrt{|A|}} \left(\frac{i}{z}\right)^k \sum_{Av \equiv 0 \pmod{N}} P^*(N^{-1}Av) e\left(-\frac{1}{z} Q^*(N^{-1}Av) + N^{-2}(Av)^t h\right).$$

Obsérvese que $P^*(N^{-1}Av) = N^{-\nu}P(v)$, $Q^*(N^{-1}Av) = N^{-2}Q(v)$ y además $(Av)^t h = v^t Ah$. Luego la expresión anterior se torna:

$$\frac{i^{-\nu}}{\sqrt{|A|}} \left(\frac{i}{z}\right)^k N^{-\nu} \sum_{Av \equiv 0 \pmod{N}} P(v) e\left(\frac{-1}{N^2 z} Q(v) + N^{-2} v^t Ah\right).$$

Dividiendo ambas expresiones entre $N^{-\nu}$ y luego evaluando en $-1/z$:

$$\Theta(-1/z; h) = \frac{i^{-\nu}}{\sqrt{|A|}} (-iz)^k \sum_{Av \equiv 0 \pmod{N}} P(v) e\left(\frac{z}{N^2} Q(v)\right) e\left(N^{-2} v^t Ah\right).$$

Separando la última suma en clases módulo N:

$$\Theta(-1/z; h) = \frac{i^{-\nu}}{\sqrt{|A|}} (-iz)^k \sum_{l \in \mathcal{H}} \sum_{\substack{v \equiv l \pmod{N} \\ Av \equiv 0 \pmod{N}}} P(v) e\left(\frac{z}{N^2} Q(v)\right) e\left(N^{-2} v^t Ah\right)$$

sigue el resultado. □

Las dos proposiciones anteriores nos dan fórmulas de transformación para la acción por S y T. Más precisamente: en 3.33 vemos cómo se relaciona $\Theta(T^2 z; h)$ con $\Theta(z; h)$, y que si además $\mathrm{diag}(A)$ es par entonces tenemos una relación entre $\Theta(Tz; h)$ y $\Theta(z; h)$; en 3.37 obtenemos una fórmula que nos permite escribir $\Theta(Sz; h)$ como combinación lineal de las $\Theta(z; l)$ con $l \in \mathcal{H}$. Buscamos ahora fórmulas de transformación por otras matrices $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

A esos efectos, sea $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Supongamos $d \neq 0$. Cambiando α por $-\alpha$ (pues ambas actúan del mismo modo en $\mathbb{H}$) podemos asumir $d > 0$. Asumamos también que una de las siguientes dos condiciones se cumple:

$$b \equiv c \equiv 0 \ (\text{ mód } 2), \tag{3.38}$$

$$\mathrm{diag}(A) \equiv 0 \ (\text{ mód } 2). \tag{3.39}$$

Sea

$$\gamma = \alpha S = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}.$$

Como $d\gamma \cdot z = b - (dz - c)^{-1}$ vale:

$$\Theta(\gamma \cdot z; h) = \sum_{m \equiv h \pmod{N}} P(m) e\left(\frac{Q(m)}{N^2}\left(\frac{b}{d} - \frac{1}{d(dz-c)}\right)\right).$$

Ahora bien, $e\left(\frac{bQ(m)}{dN^2}\right)$ depende de m módulo dN. En efecto,

- Si se cumple 3.38 entonces $b = 2b'$. Ahora sea $m' = m + dNg$, luego:

$$\begin{aligned} \frac{bQ(m')}{dN^2} &= \frac{2b'Q(m')}{dN^2} \\ &= \frac{b'(2Q(m) + 2d^2N^2Q(g) + 4dNm^tAg)}{dN^2}, \end{aligned}$$

  y como $m \equiv h \pmod{N}$ entonces $Am \equiv 0 \pmod{N}$ y por tanto $m^tAg \equiv 0 \pmod{N}$ de donde

$$2d^2N^2Q(g) + 4dNm^tAg \equiv 0 \pmod{dN^2}.$$

- Si se cumple 3.39, entonces x^tAx es siempre par. Por lo tanto, escribiendo $m' = m + dNg$:

$$\frac{bQ(m')}{dN^2} = \frac{b(Q(m) + d^2N^2Q(g) + 2dNm^tAg)}{dN^2},$$

  luego, de forma análoga a la del caso anterior,

$$d^2N^2Q(g) + 2dNm^tAg \equiv 0 \pmod{dN^2}$$

Por lo tanto, podemos separar la suma anterior en las distintas clases módulo dN:

$$\begin{aligned} \Theta(\gamma z; h) &= \sum_{\substack{g \pmod{dN} \\ g \equiv h \pmod{N}}} \sum_{m \equiv g \pmod{N}} P(m) e\left(\frac{bQ(m)}{dN^2}\right) e\left(\frac{-dQ(m)}{(dN)^2(dz-c)}\right) \\ &= \sum_{\substack{g \pmod{dN} \\ g \equiv h \pmod{N}}} e\left(\frac{bQ(g)}{dN^2}\right) \sum_{m \equiv g \pmod{N}} P(m) e\left(\frac{-dQ(m)}{(dN)^2(dz-c)}\right). \end{aligned}$$

Ahora bien, reconocemos en la suma sobre m a la función theta asociada a la matriz dA y la clase g (mód dN) (obsérvese que $(dA)g = d(Ag) \equiv 0$ (mód dN))) evaluada en el punto $-1/(dz-c)$. Podemos aplicarle la proposición 3.37, obteniendo:

$$\frac{(i(c-dz))^k}{i^\nu d^{r/2}|A|^{1/2}} \sum_{\substack{l \ (\text{mód } dN) \\ Al \equiv 0 \ (\text{mód } N)}} e\left(\frac{l^t Ag}{dN^2}\right) \sum_{m \equiv l \ (\text{mód } dN)} P(m) e\left(\frac{Q(m)}{dN^2}(dz-c)\right).$$

Ahora bien, argumentando como antes (discutiendo según se cumple 3.38 o 3.39) tenemos que $cQ(m) \equiv cQ(l)$ (mód dN^2), luego:

$$\frac{(i(c-dz))^k}{i^\nu d^{r/2}|A|^{1/2}} \sum_{\substack{l \ (\text{ mód } dN) \\ Al \equiv 0 \ (\text{mód } N)}} e\left(\frac{l^t Ag}{dN^2} - \frac{cQ(l)}{dN^2}\right) \sum_{m \equiv l \ (\text{mód } dN))} P(m) e\left(\frac{Q(m)z}{N^2}\right).$$

Sustituyendo esto en la expresión que teníamos para $\Theta(\gamma z; h)$ obtenemos:

$$\Theta(\gamma z; h) = \frac{(i(c-dz))^k}{i^\nu d^{r/2}|A|^{1/2}} \sum_{\substack{l \ (\text{mód } dN) \\ Al \equiv 0 \ (\text{mód } N)}} \varphi(h,l) \sum_{m \equiv l \ (\text{mód } dN)} P(m) e\left(\frac{Q(m)z}{N^2}\right)$$

donde:

$$\varphi(h,l) = \sum_{\substack{g \ (\text{mód } dN) \\ g \equiv h \ (\text{mód } N)}} e\left(\frac{bQ(g) + l^t Ag - cQ(l)}{dN^2}\right).$$

Si cambiamos g por $g + cl$, de modo que ahora g recorre las clases módulo dN de vectores $\equiv h - cl$ obtenemos que el sumando pasa a ser:

$$e\left(\frac{bQ(g) + cQ(l)(bc+1) + g^t Al(bc+1)}{dN^2}\right),$$

pero como $ad - bc = 1$, así:

$$e\left(\frac{bQ(g) + adcQ(l) + adg^t Al}{dN^2}\right).$$

Así:

$$\begin{aligned}\varphi(h,l) &= \sum_{\substack{g \pmod{dN} \\ g\equiv h-cl \pmod{N}}} e\left(\frac{bQ(g)+adcQ(l)+adg^tAl}{dN^2}\right) \\ &\overset{*}{=} \sum_{\substack{g \pmod{dN} \\ g\equiv h-cl \pmod{N}}} e\left(\frac{bQ(g)+adh^tAl-acQ(l)}{dN^2}\right) \\ &= e\left(\frac{ah^tAl-acQ(l)}{N^2}\right)\varphi(h-cl,0) \\ &= e\left(\frac{-acQ(l)}{N^2}\right)e\left(\frac{ah^tAl}{N^2}\right)\varphi(h-cl,0)\end{aligned}$$

donde en (*) usamos que $g \equiv h - cl \pmod{N}$, luego

$$adg^tAl - ad(h-cl)^tAl = adNv^tAl \equiv 0 \pmod{dN^2}.$$

Terminamos reconociendo el segundo factor del producto:

$$\varphi(h,l) = e\left(\frac{-acQ(l)}{N^2}\right)\psi(ah,l)\varphi(h-cl,0) \tag{3.40}$$

Por definición $\varphi(h,l)$ depende de $h \pmod{N}$, y de esto último vemos que también depende solamente de $l \pmod{N}$, por lo que agrupando los sumandos según las clases módulo N:

$$\Theta(\gamma z;h) = \frac{(i(c-dz))^k}{i^\nu d^{r/2}|A|^{1/2}}\sum_{h'\in\mathcal{H}}\varphi(h,h')\Theta(z;h').$$

Ahora bien, recordemos que $\gamma = \alpha S$. Por lo que $\gamma S = -\alpha$ (nuevamente, la acción de α y $-\alpha$ en el semiplano superior es la misma). Así, cambiando z por Sz:

$$\Theta(\alpha z;h) = \frac{\left(\frac{i}{z}(cz+d)\right)^k}{i^\nu d^{r/2}|A|^{1/2}}\sum_{h'\in\mathcal{H}}\varphi(h,h')\Theta(Sz;h').$$

Pero ahora podemos aplicar a cada uno de los $\Theta(Sz;h')$ la proposición 3.37:

$$\Theta(\tau z;h) = \frac{\left(\frac{i}{z}(cz+d)\right)^k}{i^{2\nu}d^{r/2}|A|}(-iz)^k\sum_{h'\in\mathcal{H}}\varphi(h,h')\sum_{l\in\mathcal{H}}\psi(h,l)\Theta(z;l).$$

Por un lado,

$$\left(\frac{i}{z}(cz+d)\right)^k(-iz)^k = (cz+d)^k.$$

Cuya verificación diferimos al lema 3.49, pues $k \in \frac{1}{2}\mathbb{Z}$.

Por otro, definiendo:

$$\Phi(h,l) = \sum_{h' \in \mathcal{H}} \varphi(h,h')\psi(h',l)$$

lo que hemos probado es que hemos demostrado que:

$$\Theta(\tau z; h) = \frac{(cz+d)^k}{i^{2\nu} d^{r/2} |A|} \sum_{l \in \mathcal{H}} \Phi(h,l)\Theta(z;l).$$

Para continuar, supondremos que también se satisface una de las siguientes dos condiciones:

$$c \equiv 0 \ (\text{mód } 2N) \tag{3.41}$$

$$c \equiv 0 \ (\text{mód } N) \text{ y } \operatorname{diag}(NA^{-1}) \equiv 0 \ (\text{mód } 2) \tag{3.42}$$

Observación 3.43. *Si se cumple 3.41, entonces $c = 2c'$ con $c' \equiv 0$ (mód N) y por tanto para $l \in \mathcal{H}$*

$$cQ(l) = c'(2Q(l)) \equiv 0 \ (\text{mód } N^2)$$

Si se cumple 3.42, para $l \in \mathcal{H}$ sea $v \in \mathbb{Z}^r$ tal que $Al = Nv$. Luego $NA^{-1}v = l$, y la condición sobre la diagonal de NA^{-1} nos dice que la forma cuadrática asociada a NA^{-1} es entera. En particular

$$Q(l) = Q(NA^{-1}v) = N^2 Q(A^{-1}v) = N^2 v^t A^{-1} v = N v^t (NA^{-1}) v \equiv 0 \ (\text{mód } N).$$

A la luz de la observación, se cumpla 3.41 o 3.42 tenemos que $cQ(l) \equiv 0$ (mód N^2) de donde 3.40 se simplifica a:

$$\varphi(h,l) = \psi(ah,l)\varphi(h,0).$$

Luego, tenemos:

$$\begin{aligned}\Phi(h,l) &= \varphi(h,0) \sum_{h' \in \mathcal{H}} \psi(ah,h')\psi(h',l) \\ &= \begin{cases} \varphi(h,0)|A| & \text{si } l \equiv -ah \ (\text{ mód } N) \\ 0 & \text{si no} \end{cases}\end{aligned}$$

que sigue de la ortogonalidad de los caracteres junto con el hecho de que $|\mathcal{H}| = |A|$.

Sustituyendo esto en la fórmula que teníamos para $\Theta(\alpha z; h)$:

$$\Theta(\alpha z; h) = \frac{(cz+d)^k}{i^{2\nu} d^{r/2}} \varphi(h,0) \Theta(z; -ah),$$

de donde sigue:

$$\Theta(\alpha z; h) = \frac{(cz+d)^k}{d^{r/2}} \varphi(h,0) \Theta(z; ah). \tag{3.44}$$

Nos resta calcular

$$\varphi(h,0) = \sum_{\substack{g \pmod{dN} \\ g \equiv h \pmod{N}}} e\left(\frac{bQ(g)}{dN^2}\right).$$

Como $ad - bc = 1$, entonces $ad = 1 + bc \equiv 1$ (mód N) (tanto en 3.41 como en 3.42 estamos suponiendo que $c \equiv 0$ (mód N)), por lo que podemos escribir $g = adh + xN$ con x variando libremente módulo d.

$$\varphi(h,0) = e\left(\frac{a^2 bdQ(h)}{N^2}\right) \sum_{x \pmod{d}} e\left(\frac{bQ(x)}{d}\right).$$

Nuevamente, como $ad = 1 + bc$ tenemos que

$$adQ(h) = Q(h) + bcQ(h).$$

Ahora bien, si suponemos 3.41 entonces $bc \equiv 0$ (mód $2N$) de donde sigue que $bcQ(h) \equiv 0$ (mód N^2). Si suponemos 3.42 este también es el caso: pues $bc \equiv 0$ (mód N) pero la condición adicional sobre la diagonal de NA^{-1} nos da $Q(h) \equiv 0$ (mód N). Por lo tanto, tenemos que

$$adQ(h) - Q(h) \equiv 0 \pmod{N^2}$$

y sustituyendo esto en la identidad que tenemos para $\varphi(h,0)$ obtenemos:

$$\varphi(h,0) = e\left(\frac{abQ(h)}{N^2}\right) G. \tag{3.45}$$

donde

$$G = \sum_{x \pmod{d}} e\left(\frac{bQ(x)}{d}\right) \tag{3.46}$$

es la *suma de Gauss* asociada a la forma cuadrática $Q(x)$, la cual calcularemos en la siguiente sección haciendo uso de una suposición adicional:

$$d \equiv 1 \text{ (mód 2)} \tag{3.47}$$

Esta suposición nos permite dar otra expresión para G del siguiente modo:

- Como $(d, 2) = 1$, $(d, c) = 1$ (pues $ad - bc = 1$) y $(d, |A|) = 1$ (tenemos $ad \equiv 1$ (mód N) por lo que $(d, N) = 1$, pero habíamos observado que todo factor primo de $|A|$ aparece en la factorización de N): tenemos que $(d, 2c|A|) = 1$;
- Cambiando x por $2cx$ (permutando los x módulo d por ser $(d, 2c) = 1$) y $bc = -1 + ad \equiv -1$ (mód d) tenemos:

$$G = \sum_{x \text{ (mód } d)} e\left(\frac{-4cQ(x)}{d}\right) \tag{3.48}$$

Cerramos la sección probando el siguiente lema:

Lema 3.49. *Sean $c, d \in \mathbb{Z}$ con $d > 0$. Para $k \in \frac{1}{2}\mathbb{Z}$ vale:*

$$\left(\frac{1}{-iz}(cz + d)\right)^k (-iz)^k = (cz + d)^k.$$

Demostración. Cuando $k \in \mathbb{Z}$ es claro, pero como $k \in \frac{1}{2}\mathbb{Z}$ necesitamos verificar el caso $k = \frac{1}{2}$.

La raíz cuadrada es una función holomorfa en $\mathbb{C}\backslash\{x + iy : y = 0, x < 0\}$. Consideremos las funciones

$$f(z) = \left(\frac{1}{-iz}(cz + d)\right)^{1/2} (-iz)^{1/2} \quad , \quad g(z) = (cz + d)^{1/2}.$$

Obsérvese que si $z \in \mathbb{H}$, entonces:

$$re\left(\frac{1}{-iz}(cz + d)\right) = \frac{d \cdot \text{im}(z)}{|z|^2} > 0, \quad re(-iz) = \text{im}(z) > 0$$

por lo que $f : \mathbb{H} \to \mathbb{C}$ es holomorfa.

Por otra parte:

$$\text{im}(cz + d) = c \cdot \text{im}(z) = 0 \iff c = 0$$

por lo que discutimos según dos casos:

i. $c \neq 0$

ii. $c = 0$.

En el primer caso $g : \mathbb{H} \to \mathbb{C}$ es holomorfa y observamos que para $z = it$ con $t > 0$ vale:

$$\begin{aligned} f(it) &= \left(\frac{1}{i(it)}(cit+d)\right)^{1/2}(-i(it))^{1/2} = \left(\frac{1}{t}(cit+d)\right)^{1/2} t^{1/2} \\ &= \frac{1}{t^{1/2}}(cit+d)^{1/2}t^{1/2} = (cit+d)^{1/2} = g(it). \end{aligned}$$

Luego, en virtud del principio de identidad para funciones holomorfas concluimos que $f = g$ en $\mathbb{H}$.

En el caso $c = 0$, verificamos la igualdad directamente:

$$\left(\frac{d}{-iz}\right)^{1/2}(-iz)^{1/2} = d^{1/2}\left(\frac{1}{-iz}\right)^{1/2}(-iz)^{1/2} = d^{1/2}(-iz)^{-1/2}(-iz)^{1/2} = d^{1/2}.$$

□

3.4. Sumas de Gauss

El objetivo de esta sección es probar:

Proposición 3.50. *Sea d un entero positivo tal que $(d, 2c|A|) = 1$. Entonces:*

$$G = \left(\frac{|A|}{d}\right)\left(\overline{\varepsilon}_d\left(\frac{2c}{d}\right)\sqrt{d}\right)^r \tag{3.51}$$

donde G es la suma 3.48 y:

$$\varepsilon_d = \left(\frac{-1}{d}\right)^{1/2} = \begin{cases} 1 & \text{si } d \equiv 1 \text{ (mód 4)} \\ i & \text{si } d \equiv -1 \text{ (mód 4)} \end{cases}$$

Daremos la prueba una vez probados los lemas que necesitaremos para la demostración.

Lema 3.52. *Sea $N \in \mathbb{Z}_{>0}$. Entonces:*

$$\sum_{t \text{ (mód } N)} e\left(\frac{t^2}{N}\right) = \varepsilon_N N^{1/2}$$

para

$$\varepsilon_N = \frac{1 + i^{-N}}{1 - i}.$$

Demostración. Llamemos S_N a la suma que pretendemos calcular. Notando $f(x) = e(x^2/N)$, tenemos:

$$\begin{aligned} S_N &= \sum_{t=0}^{N-1} f(t) \\ &= \sum_{t=0}^{N}{}' f(t) \end{aligned}$$

donde el $'$ en la suma anterior quiere decir que los términos $f(0)$ y $f(N)$ están sumados multiplicados por un factor de $1/2$.

Luego, sumación de Poission nos da:

$$S_N = \sum_{v=-\infty}^{\infty} \int_0^N f(x)e(vx)dx. \tag{3.53}$$

Ahora bien:

$$\begin{aligned} \int_0^N f(x)e(vx)dx &= \int_0^N e\left(\frac{x^2}{N} + vx\right) dx \\ &= \int_0^N e\left(\frac{x^2 + vNx}{N}\right) dx \\ &= N\int_0^1 e\left(N(u^2 + vu)\right) du \\ &= N\int_0^1 e\left(N(u^2 + vu)\right) du \\ &= N\int_0^1 e\left(N\left(\left(u + \frac{1}{2}v\right)^2 - \frac{1}{4}v^2\right)\right) du \\ &= Ne\left(-\frac{1}{4}v^2\right)\int_0^1 e\left(N\left(u + \frac{1}{2}v\right)^2\right) du \\ &= Ne\left(-\frac{1}{4}v^2\right)\int_{\frac{1}{2}v}^{\frac{1}{2}v+1} e\left(Ny^2\right) dy. \end{aligned}$$

Obsérvese que:

$$e\left(-\frac{1}{4}v^2\right) = \begin{cases} 1 & \text{si } v \equiv 0 \text{ (mód 2)} \\ i^{-N} & \text{si } v \equiv 1 \text{ (mód 2)} \end{cases}.$$

Separando en casos y escribiendo $v = 2k$ o $v = 2k + 1$ según corresponda, sustituyendo en 3.53 obtenemos:

$$\begin{aligned} S_N &= N \sum_{k=-\infty}^{\infty} \int_k^{k+1} e(Ny^2)dy + Ni^{-N} \sum_{k=-\infty}^{\infty} \int_{k+\frac{1}{2}}^{k+\frac{3}{2}} e(Ny^2)dy \\ &= N(1 + i^{-N}) \int_{\mathbb{R}} e(Ny^2)dy \\ &= N^{1/2}(1 + i^{-N}) \int_{\mathbb{R}} e(y^2)dy. \end{aligned}$$

Concluimos del siguiente modo: vimos que $S_N = CN^{1/2}(1 + i^{-N})$ para una constante C –una integral que habría que calcular– pero sabemos que $S_1 = 1$. Luego:

$$1 = C(1 + i^{-1}),$$

de donde

$$C = \frac{1}{1 - i}.$$

□

Lema 3.54. *Consideremos la suma de Gauss*

$$g(n, c) = \sum_{t \ (\text{ mód } c)} e\left(\frac{nt^2}{c}\right). \tag{3.55}$$

Si vale $(c, 2n) = 1$ *entonces:*

$$g(n, c) = \left(\frac{n}{c}\right) \varepsilon_c c^{1/2}$$

donde

$$\varepsilon_c = \begin{cases} 1 & \text{si } c \equiv 1 \ (\text{ mód } 4) \\ i & \text{si } c \equiv -1 \ (\text{ mód } 4) \end{cases}$$

Observación: El Lema 3.52 es un caso particular del que acabamos de enunciar. Más precisamente, nos dice que:

$$g(1, c) = \varepsilon_c c^{1/2}.$$

Demostración. Sea $c = c_o c_1^2$ donde c_o es libre de cuadrados. Ahora bien, en (3.25) t recorre $\{0, 1, ..., c-1\}$. Dividiendo t entre $c_o c_1$ tenemos $t = c_o c_1 q + r$

donde $0 \leq r < c_o c_1$ y $0 \leq q < c_1$. Es equivalente que t recorra $\{0, 1, ..., c-1\}$ a que q recorra $\{0, \ldots, c_1 - 1\}$ y r recorra $\{0, \ldots, c_o c_1 - 1\}$. Por lo tanto:

$$g(n,c) = \sum_{\substack{r \pmod{c_o c_1} \\ q \pmod{c_1}}} e\left(\frac{nq^2 c_o^2 c_1^2}{c}\right) e\left(\frac{2nc_o c_1 qr}{c}\right) e\left(\frac{nr^2}{c}\right).$$

Obsérvese que en cada sumando el primer factor es 1 –pues $c = c_o c_1^2$– y que podemos simplificar el segundo término, obteniendo:

$$g(n,c) = \sum_{r \pmod{c_o c_1}} e\left(\frac{nr^2}{c}\right) \sum_{q \pmod{c_1}} e\left(\frac{2nqr}{c_1}\right).$$

La suma sobre q da, por ortogonalidad de caracteres (pues $(c, 2n) = 1$), c_1 si $r \equiv 0$ (mód c_1) y 0 en otro caso. Luego:

$$\begin{aligned} g(n,c) &= \sum_{r \pmod{c_o c_1}} e\left(\frac{nr^2}{c}\right) c_1 \delta(\{r \equiv 0 \text{ (mód } c_1)\}) \\ &= c_1 \sum_{r \pmod{c_o}} e\left(\frac{nr^2}{c_o}\right) \\ &= c_1 g(n, c_o). \end{aligned}$$

A la luz de lo anterior, debemos calcular la suma $g(n, c_o)$ para c_o libre de cuadrados.

Si p es un primo impar, el mapa $x \mapsto x^2$ de $(\mathbb{Z}/p\mathbb{Z})^\times$ en $(\mathbb{Z}/p\mathbb{Z})^\times$ es 2 a 1. Luego es fácil ver que, dado p primo (no necesariamente impar) e y fijo:

$$\#\{x \text{ (mód } p) : x^2 \equiv y \text{ (mód } p)\} = 1 + \left(\frac{y}{p}\right) \tag{3.56}$$

Ahora bien, y es cuadrado módulo c_o si y solamente si es cuadrado módulo p para todo p que divide a c_o. En efecto, si $x^2 \equiv y$ (mód c_o) entonces $x^2 \equiv y$ (mód p) para cualquier $p|c_o$. Recíprocamente, si existen $x_i^2 \equiv y$ (mód p_i) para cada p_i que divide a c_o, el x definido por $x \equiv x_i$ (mód p_i) para cada i, que existe y es único módulo c_o por el Teorema Chino de los restos, cumple que $x^2 \equiv y$ (mód c_o). Por lo tanto, de 3.56 obtenemos que para c_o libre de cuadrados e y fijo,

$$\#\{x \text{ (mód } c_o) : x^2 \equiv y \text{ (mód } c_o)\} = \prod_{p|c_o} \left(1 + \left(\frac{y}{p}\right)\right) = \sum_{d|c_o} \left(\frac{y}{d}\right). \tag{3.57}$$

Haciendo uso de esto:

$$\begin{aligned} g(n,c_o) &= \sum_{t \pmod{c_o}} e\left(\frac{nt^2}{c_o}\right) \\ &= \sum_{y \pmod{c_o}} e\left(\frac{ny}{c_o}\right) \#\{x \pmod{c_o} : x^2 \equiv y \pmod{c_o}\} \\ &= \sum_{d|c_o} \sum_{y \pmod{c_o}} \left(\frac{y}{d}\right) e\left(\frac{ny}{c_o}\right). \end{aligned}$$

Llamemos $S(d;n,c_o)$ a la suma interior, es decir:

$$S(d;n,c_o) = \sum_{y \pmod{c_o}} \left(\frac{y}{d}\right) e\left(\frac{ny}{c_o}\right).$$

Para d divisor propio de c_o, escríbase $y = dq + r$ (y notemos $C := c_o/d$):

$$\begin{aligned} S(d;n,c_o) &= \sum_{q=0}^{C-1} \sum_{r=0}^{d-1} \left(\frac{dq+r}{d}\right) e\left(\frac{n(dq+r)}{c_o}\right) \\ &= \sum_{q=0}^{C-1} e\left(\frac{ndq}{c_o}\right) \sum_{r=0}^{d-1} \left(\frac{r}{d}\right) e\left(\frac{nr}{c_o}\right) \\ &= \left(\frac{n}{d}\right) \sum_{q=0}^{C-1} e\left(\frac{ndq}{c_o}\right) \sum_{r=0}^{d-1} \left(\frac{nr}{d}\right) e\left(\frac{nr}{c_o}\right) \\ &= \left(\frac{n}{d}\right) \sum_{q=0}^{C-1} e\left(\frac{ndq}{c_o}\right) \sum_{x \pmod{d}} \left(\frac{x}{d}\right) e\left(\frac{x}{c_o}\right), \end{aligned}$$

llamamos $A(d)$ a la suma interior y tenemos:

$$\begin{aligned} S(d;n,c_o) &= \left(\frac{n}{d}\right) A(d) \sum_{q=0}^{C-1} e\left(\frac{nq}{C}\right) \\ &= 0 \end{aligned}$$

donde para la última igualdad sigue de la ortogonalidad de caracteres (usamos que $(n,C) = 1$).

Luego:

$$g(n,c_o) = \sum_{d|c_o} S(d;n,c_o) = S(c_o;n,c_o).$$

Pero

$$\begin{aligned} S(c_o; n, c_o) &= \sum_{y \pmod{c_o}} \left(\frac{y}{c_o}\right) e\left(\frac{ny}{c_o}\right) \\ &= \left(\frac{n}{c_o}\right) \sum_{y \pmod{c_o}} \left(\frac{ny}{c_o}\right) e\left(\frac{ny}{c_o}\right) \\ &= \left(\frac{n}{c_o}\right) \sum_{x \pmod{c_o}} \left(\frac{x}{c_o}\right) e\left(\frac{x}{c_o}\right) \\ &= \left(\frac{n}{c_o}\right) S(c_o; 1, c_o). \end{aligned}$$

Concluimos pues que:

$$g(n, c_o) = \left(\frac{n}{c_o}\right) g(1, c_o)$$

de donde sigue que en el caso general:

$$\begin{aligned} g(n, c) &= c_1 g(n, c_o) \\ &= \left(\frac{n}{c_o}\right) c_1 g(1, c_o) \\ &= \left(\frac{n}{c_o}\right) c_1 c_o^{1/2} \varepsilon_c. \end{aligned}$$

Observando que $c^{1/2} = c_o^{1/2} c_1$ y que

$$\left(\frac{n}{c}\right) = \left(\frac{n}{c_o}\right)\left(\frac{n}{c_1^2}\right) = \left(\frac{n}{c_o}\right)\left(\frac{n}{c_1}\right)^2 = \left(\frac{n}{c_o}\right)$$

concluimos la prueba del lema. □

Lema 3.58. *Sea p un primo impar y f una forma cuadrática sobre $\mathbb{Z}_p$. Entonces f es $\mathbb{Z}_p$-equivalente a una forma cuadrática diagonal. Es decir, si $A \in M_r(\mathbb{Z}_p)$ es la matriz asociada a f (i.e.: $f(x) = \frac{1}{2} x^t A x$), existen matrices $V \in \mathrm{GL}_r(\mathbb{Z}_p)$ y $D \in M_r(\mathbb{Z}_p)$ diagonal tal que*

$$V^t A V = D.$$

Demostración. Asociada a la matriz A también tenemos la forma bilineal $b(x, y) = x\widetilde{A}y$ que cumple $b(x, x) = f(x)$. La matriz A es $(2b(e_i, e_j))_{i,j}$ donde

estamos notando e_i al vector que tiene un 1 en la coordenada i-ésima y ceros en las otras.

Sea $R(f) = \{y \in \mathbb{Z}_p : f(x) = y\}$. Existe $\alpha \in R(f)$ de norma máxima[3], es decir:

$$\alpha \in R(f) : |\alpha|_p = \max_{x \in \mathbb{Z}_p^r}\{|f(x)|_p\}.$$

Hay dos opciones: o $\alpha = 0$ o $\alpha \neq 0$.

En el primer caso (recordar que $|0|_p = 1$) f solamente representa al 0 y por lo tanto, vemos que $b(x,y) = \frac{1}{2}(f(x+y) - f(x) - f(y)) = 0 \ \forall x, y \in \mathbb{Z}_p^r$. Luego la matriz A es la matriz nula y por tanto diagonal.

En el otro caso, sea $c \in \mathbb{Z}_p^r$ tal que $f(c) = \alpha$. Afirmamos que c es primitivo. Si no fuera el caso entonces $c = pc_o$ para $c_o \in \mathbb{Z}_p$ y por tanto $f(c_o) = \alpha/p^2 =: \alpha_o$. Pero $|\alpha_o|_p > |\alpha|_p$, lo cual sería una contradicción. Luego, por 1.15, existe una base de Z_p^r que comienza por c. Además, escribiendo a la forma cuadrática "en esa base", la matriz $(b_{ij})_{ij}$ -que tiene $b_{11} = 2\alpha$- cumple que b_{11} es mayor en valor absoluto p-ádico que cualquier otro elemento de la matriz. Como vale $2b(x,y) = f(x+y) - f(x) - f(y)$ y $p \neq 2$, se tiene:

$$\begin{aligned} |b(x,y)|_p &= |f(x+y) - f(x) - f(y)|_p \\ &\leq \max\{|f(x+y)|_p, |f(x)|_p, |f(y)|_p\} \\ &\leq |\alpha|_p \end{aligned}$$

lo cual nos da lo afirmado si lo aplicamos a $b(c_i, c_j)$ para la base $\{c = c_1, ..., c_r\}$.

Por lo tanto, combinando linealmente la fila 1 con las restantes podemos obtener ceros (haciendo la transformación que reemplaza fila_i por fila_i-$\frac{b_{1i}}{\alpha}\text{fila}_1$). Tenemos pues una matriz $V_1 \in \mathrm{GL}_r(\mathbb{Z}_p)$ con determinante invertible en $\mathbb{Z}_p$ pues es producto de una matriz cambio de base con la matriz recién descrita

[3]Los valores que toma la norma son $\{p^{-n} : n \in \mathbb{Z}_{\geq 0}\} \cup \{0\}$; cualquier subconjunto de este conjunto tiene máximo.

(que tiene determinante 1) de modo que se cumple:

$$V_1^t A V_1 = \begin{bmatrix} \alpha & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \widetilde{A} & \\ 0 & & & \end{bmatrix}$$

El resultado sigue por inducción. □

Lema 3.59 (de aproximación)**.** *Sea A una matriz entera simétrica con forma cuadrática asociada definida positiva. Para $d \in \mathbb{Z}_{>0}$ impar existe una matriz entera V con $(d, |V|) = 1$ y una matriz entera M diagonal módulo d tal que:*

$$V^t A V \equiv M \pmod{d}.$$

Demostración. Escribimos a d como producto de primos $d = p_1^{k_1} ... p_n^{k_n}$. Por el lema anterior, como los $p_i \neq 2$, existen matrices $V_i \in \mathrm{GL}_r(\mathbb{Z}_{p_i})$ de modo que $V_i^T A V_i = D_i$ con $D_i \in M_r(\mathbb{Z}_{p_i})$ diagonal. Esta igualdad nos da, proyectando sobre $p_i^{k_i}$:

$$\widetilde{V_i}^t A \widetilde{V_i} = \widetilde{D_i}$$

donde las matrices $\widetilde{A}$, $\widetilde{D_i} \in M_r(\mathbb{Z}/p_i^{k_i}\mathbb{Z})$ y $\widetilde{V_i} \in \mathrm{GL}_r(\mathbb{Z}/p_i^{k_i}\mathbb{Z})$.

Tenemos pues matrices $\{\widetilde{V_i}\}$, que definen por el Teorema Chino de los restos una matriz $\widetilde{V} \in M_r(\mathbb{Z}/d\mathbb{Z})$ de modo que $\widetilde{\pi_i}(\widetilde{V}) = \widetilde{V_i}$ –donde notamos $\widetilde{\pi_i} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/p_i^{k_i}\mathbb{Z}$ al morfismo inducido por la proyección de $\mathbb{Z}$ sobre $\mathbb{Z}/p_i^{k_i}\mathbb{Z}$. Para $V \in M_r(\mathbb{Z})$ tal que $V \equiv \tilde{V}$ (mód d), ponemos $M := V^t A V$ y se cumple que:

$$V^t A V \equiv M \pmod{d}$$

donde M es diagonal módulo d.

Que el determinante de V es coprimo con d puede verse del siguiente modo: las $\widetilde{V_i}$ eran invertibles módulo $p_i^{k_i}$, pues las matrices V_i eran invertibles; construimos pues una matriz entera V' repitiendo la construcción anterior con las $\{\widetilde{V_i}^{-1}\}$. Luego valdrá $VV' \equiv I$ (mód d), por lo que V es invertible módulo d, de donde sigue que $(|V|, d) = 1$. □

Ahora sí, nos disponemos a probar la Proposición 3.50.

Demostración. Por el Lema 3.59, existen matrices enteras V y M tales que:

$$V^t AV \equiv M \pmod{d}.$$

Como a su vez $(d, |V|) = 1$ podemos escribir $x = Vy \pmod{d}$ –observar que $x^t Ax = (Vy)^t AVy = y^t My$– obteniendo:

$$\begin{aligned} G &= \sum_{x \pmod{d}} e\left(\frac{-4cQ(x)}{d}\right) \\ &= \sum_{y \pmod{d}} e\left(\frac{-2cy^t My}{d}\right) \\ &= \sum_{y \pmod{d}} e\left(\frac{-2c(m_1 y_1^2 + ... + m_r y_r^2)}{d}\right) \\ &= \prod_{j=1}^{r} \left(\sum_{y_j \pmod{d}} e\left(\frac{-2cm_j y_j^2}{d}\right)\right). \end{aligned}$$

Como estamos suponiendo $(2c|A|, d) = 1$ y $|A| \equiv |M| \pmod{d}$, tenemos que $(2cm_j, d) = 1$ para $j = 1, ..., r$. Luego, cada factor del producto está en las hipótesis del Lema 3.54, por lo que:

$$\begin{aligned} G &= \prod_{j=1}^{r} \left(\frac{-2cm_j}{d}\right) \varepsilon_d d^{1/2} \\ &= \left(\frac{m_1 \cdots m_r}{d}\right) \left(\varepsilon_d \left(\frac{-1}{d}\right) \left(\frac{2c}{d}\right) d^{1/2}\right)^r. \end{aligned}$$

Usando nuevamente que $|A| \equiv |M| \pmod{d}$, por lo que $m_1 \cdots m_r = |A| + dk$, y que por otro lado

$$\varepsilon_d \left(\frac{-1}{d}\right) = \begin{cases} 1 & \text{si } d \equiv 1 \pmod{4} \\ -i & \text{si } d \equiv -1 \pmod{4} \end{cases}$$

concluimos que:

$$G = \left(\frac{|A|}{d}\right) \left(\overline{\varepsilon}_d \left(\frac{2c}{d}\right) \sqrt{d}\right)^r.$$

□

3.5. Modularidad de la función theta

La siguiente proposición es la culminación del trabajo de las últimas secciones:

Proposición 3.60. *Sea* $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *con* $d \equiv 1 \pmod 2$. *Supongamos además que una de las siguientes condiciones se cumple:*

i. $c \equiv 0 \pmod{2N}$ *y* $b \equiv 0 \pmod 2$,

ii. $c \equiv 0 \pmod{2N}$ *y* $\operatorname{diag}(A) \equiv 0 \pmod 2$, *ó*

iii. $c \equiv 0 \pmod N$ *y* $\operatorname{diag}(A) \equiv \operatorname{diag} NA^{-1} \equiv 0 \pmod 2$.

Entonces para $h \in \mathcal{H}$, $k = \nu + \frac{r}{2}$ *vale:*

$$\Theta(\alpha \cdot z; h) = e\left(\frac{abQ(h)}{N^2}\right) \vartheta(\alpha)(cz+d)^k \Theta(z; ah) \tag{3.61}$$

donde

$$\vartheta(\alpha) = \left(\frac{|A|}{d}\right)\left(\overline{\varepsilon_d}\left(\frac{2c}{d}\right)\right)^r \tag{3.62}$$

Demostración. Si $c = 0$ entonces $\alpha = \pm \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ y el resultado es 3.33.

Si $d > 0$ entonces el resultado sigue directamente del trabajo de las últimas dos secciones. Si $d < 0$ podemos cambiar α por $-\alpha$ y tenemos:

$$\Theta(-\alpha \cdot z; h) = e\left(\frac{abQ(h)}{N^2}\right) \vartheta(-\alpha)(-cz-d)^k \Theta(z; -ah).$$

El miembro izquierdo de la igualdad es $\Theta(\alpha z; h)$ pues $\alpha \cdot z = -\alpha \cdot z$. En el miembro derecho el primer factor es el mismo que el que se corresponde con α, en el segundo:

$$\begin{aligned}
\vartheta(-\alpha) &= \left(\frac{|A|}{-d}\right)\left(\overline{\varepsilon_{-d}}\left(\frac{-2c}{-d}\right)\right)^r \\
&= \left(\frac{|A|}{d}\right)\left(\overline{i\varepsilon_d}\,\mathrm{sg}(-2c)\left(\frac{-2c}{d}\right)\right)^r \\
&= \left(\frac{|A|}{d}\right)\left(\mathrm{sg}(c)i\,\overline{\varepsilon_d}\left(\frac{-2c}{d}\right)\right)^r \\
&= (\mathrm{sg}(c)i)^r \left(\frac{|A|}{d}\right)\left(\overline{\varepsilon_d}\left(\frac{-2c}{d}\right)\right)^r \\
&= (\mathrm{sg}(c)i)^r \vartheta(\alpha)
\end{aligned}$$

Esto junto con que $\Theta(z;-ah) = (-1)^\nu \Theta(z;h)$ nos da:

$$\begin{aligned}\Theta(\alpha\cdot z;h) &= e\left(\frac{abQ(h)}{N^2}\right)(\mathrm{sg}(c)i)^r\vartheta(\alpha)(-(cz+d))^k(-1)^\nu\Theta(z;ah)\\ &= e\left(\frac{abQ(h)}{N^2}\right)(-1)^{r/2}(-1)^\nu\vartheta(\alpha)(-(cz+d))^k\Theta(z;ah)\\ &= e\left(\frac{abQ(h)}{N^2}\right)\vartheta(\alpha)(-1)^k(-(cz+d))^k\Theta(z;ah)\\ &\overset{*}{=} e\left(\frac{abQ(h)}{N^2}\right)\vartheta(\alpha)(cz+d)^k\Theta(z;ah)\end{aligned}$$

donde en $(*)$ verificamos $(-1)^k(-(cz+d))^k = (cz+d)$ de forma análoga a la de la prueba del Lema 3.49 –recordando que estamos suponiendo $c \neq 0$. □

Teorema 3.63 (**Hecke, Schoenberg**). *Sea $Q : \mathbb{Z}^{2r} \to \mathbb{Z}$ una forma cuadrática entera definida positiva en $2r$ variables con matriz asociada A. Sea N un entero tal que NA^{-1} es entera y P una función esférica respecto de A de grado ν. Si A y NA^{-1} tienen ambas diagonal par, entonces la función $\Theta(z)$ es una forma modular $\mathcal{M}_k(N,\chi_D)$ para $k = \nu + r$ y carácter:*

$$\chi_D(\alpha) = \left(\frac{D}{d}\right) \;;\quad D = (-1)^r|A|.$$

Además, si $\nu > 0$ entonces $\Theta(z)$ es cuspidal.

Observación 3.64. *El Teorema de Hecke y Schoenberg como aparece por ejemplo en [BVdGHZ08] no refiere a funciones esféricas. El resultado enunciado aquí es un poco más fuerte, teniendo como caso $P = 1$ es al teorema en cuestión.*

Demostración. Que $\Theta(z)$ es holomorfa en $\mathbb{H}$ es el contenido de 3.19.

Como estamos en las hipótesis de (iii) de la Proposición 3.60, poniendo $h = 0$ obtenemos:

$$\Theta(\alpha\cdot z) = \vartheta(\alpha)(cz+d)^k\Theta(z)$$

para $\alpha = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \Gamma_0(N)$ con d impar.

Observación 3.65. *Como la forma cuadrática es en $2r$ variables, podemos simplificar 3.62:*

$$\begin{aligned}\vartheta(\alpha) &= \left(\frac{|A|}{d}\right)\left(\overline{\varepsilon_d}\left(\frac{2c}{d}\right)\right)^{2r} \\ &= \left(\frac{|A|}{d}\right)\left(\frac{-1}{d}\right)^{r}\end{aligned}$$

por lo que tenemos para $D = (-1)^r|A|$:

$$\vartheta(\alpha) = \chi_D(\alpha) = \left(\frac{D}{d}\right).$$

Nos resta probar que vale la misma fórmula de transformación para α con d par. Si $d \equiv 0$ (mód 2) entonces $2 \nmid c$ (pues $(c,d) = 1$) lo cual implica $2 \nmid N$ (pues $c \equiv 0$ (mód N)) y $2 \nmid |A|$ (pues $\operatorname{rad}(N) = \operatorname{rad}(|A|)$). En este caso se puede probar:

$$D = (-1)^r|A| \equiv 1 \text{ (mód 4)}.$$

Luego, si $D = D_o D_1^2$ con D_o libre de cuadrados, entonces por reciprocidad cuadrática χ_D es un carácter módulo D_o. Entonces, como $D_o = \operatorname{rad}(|A|)|N$, $\chi_D(d + kN) = \chi_D(d)$.

Sea $\gamma = \alpha T = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$ que tiene entrada inferior derecha impar, luego:

$$\Theta(\gamma \cdot z) = \chi_D(d+c)(cz + (c+d))^k \Theta(z)$$

Evaluando en $(z-1) = T^{-1}z$, recordando que $c \equiv 0$ (mód N) y usando 3.35:

$$\Theta(\alpha \cdot z) = \chi_D(d)(cz + d)^k \Theta(z).$$

Nos resta probar que $(\Theta[\gamma]_k)(z)$ es holomorfa en infinito para toda $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Para eso, consideremos las funciones theta congruentes $\Theta(z;h)$. Dada $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, por 1.19 podemos escribirla como producto de S y T, luego, en virtud de las Proposiciones 3.37 y 3.33 obtenemos

$$\Theta(\gamma \cdot z; h) = \sum_{h' \in \mathcal{H}} a_{h'} \Theta(z; h'). \tag{3.66}$$

Y por otro lado vale:

Afirmación 3.67. *Sea $h \in \mathcal{H}$. La función $\Theta(z;h)$ es holomorfa en infinito, y $\Theta(z;h) \to 0$ conforme $\operatorname{im}(z) \to \infty$ si $\nu > 0$.*

La afirmación sigue de que la serie que define a $\Theta(z;h)$ converge absolutamente en $\mathbb{H}_\sigma$ para $\sigma > 0$ –por hacerlo la que define a $\Theta(z)$, ver 3.19– así que para calcular el límite cuando $\mathrm{im}(z) \to \infty$ de $|\Theta(z;h)|$ podemos intercambiar el límite con la integral y ver que

$$\lim_{\mathrm{im}(z)\to\infty} |\Theta(z;h)| \leq P(0)$$

pues $Q(x) > 0$ salvo cuando $x = 0$.[4]

Luego aplicando esto a cada sumando de 3.66 obtenemos,

$$\lim_{\mathrm{im}(z)\to\infty} \Theta(\gamma \cdot z;h) < \infty,$$

(y vale 0 si $\nu > 0$).

Concluimos que $(\Theta[\gamma]_k)(z;h) = j(\gamma,z)^{-k}\Theta(\gamma \cdot z;h)$ es holomorfa en infinito para toda $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, y cuspidal si $\nu > 0$. □

[4]De hecho, se puede ver que *salvo* cuando $h \equiv 0$ (mód N) tenemos $\Theta(z;h) \to 0$ conforme $\mathrm{im}(z) \to \infty$, *incluso* cuando $\nu = 0$.

Capítulo 4

Fórmulas para sumas de cuadrados

Recordemos que en las primeras dos secciones del Capítulo 2 probamos:

$$\theta_{k+l}(z) = \theta_k(z)\theta_l(z),$$

así como que $\theta_2(z) \in \mathcal{M}_1(\Gamma_1(4))$. De hecho, a la luz de nuestro trabajo en las secciones subsiguientes del capítulo, pudimos probar que $\theta_2(z) \in \mathcal{M}_1(4, \chi)$ donde χ es el único carácter no-trivial módulo 4. Como consecuencia de esto tenemos:

$$\theta_{2k}(z) \in \mathcal{M}_k(4, \chi^k).$$

Alternativamente, podemos arribar a la misma conclusión si usamos el Teorema 3.63. Si consideramos la forma cuadrática Q_{2k} que tiene matriz asociada $A = 2\,\mathrm{Id}_{2k}$, tomando $N = 4$ tenemos que $NA^{-1} = 2\,\mathrm{Id}_{2k}$. El teorema nos dice que para la función theta con $P \equiv 1$ –$\Theta(z)$ es en este caso $\theta_{2k}(z)$– cumple:

$$\theta_{2k}(z) \in \mathcal{M}_k(4, \chi_D),$$

donde $D = (-1)^k 2^{2k}$ y por lo tanto:

$$\begin{aligned}\chi_D(\alpha) &= \left(\frac{D}{d}\right) \\ &= \left(\frac{-1}{d}\right)^k \\ &= \chi(\alpha)^k.\end{aligned}$$

De este modo, procediendo como en el Capítulo 2 se pueden obtener fórmulas para $r_{2k}(n)$. Es decir, construyendo una base del espacio de formas modulares y comparando los primeros coeficientes de estas con los $r_{2k}(n)$. En este capítulo nos contentaremos con recopilar algunas fórmulas, todas ellas en [Gla07] y presentadas en su mayoría como en [Iwa97].

Cabe observar lo siguiente: $\theta_{2k}(z) = f_{2k}(z) + s_{2k}(z)$ donde f_{2k} es una serie de Eisenstein y s_{2k} una forma cuspidal. Para los casos $k = 1, 2, 3, 4$ la parte cuspidal es trivial, por lo que las fórmulas obtenidas para $r_{2k}(n)$ involucran –como en el caso de $r_2(n)$– sumas de divisores de n. Para $k \geq 5$ el espacio $\mathcal{M}_{2k}(4, \chi^k)$ tiene formas cuspidales, lo cual hace que las fórmulas sean de naturaleza más intrincada.

En lo que sigue, si d es un divisor de n, notamos $d' = n/d$.

El caso $k = 1$, abordado en el Capítulo 2, tiene fórmula:

$$r_2(n) = 4 \sum_{d|n} \chi(d).$$

El caso $k = 2$ tiene fórmula:

$$r_4(n) = 8(2 + (-1)^n) \sum_{d|n, 2\nmid d} d.$$

Como $2 + (-1)^n > 0$ independientemente del valor de n, se puede recuperar de esta fórmula el *Teorema de Lagrange*:

Teorema 4.1 (**Lagrange**)**.** *Todo entero positivo puede expresarse como suma de cuatro cuadrados.*

El caso $k = 3$ tiene fórmula:

$$r_6(n) = 4 \left(4 \sum_{d|n} \chi(d') d^2 - \sum_{d|n} \chi(d) d^2 \right).$$

El caso $k = 4$ tiene fórmula:

$$r_8(n) = 16 \sum_{d|n} (-1)^{n-d} d^3.$$

El caso $k = 5$ tiene fórmula:

$$r_{10}(n) = \frac{4}{5}\left(\sum_{d|n}\chi(d)d^4 + 16\sum_{d|n}\chi(d')d^4 + 8G_4(n)\right),$$

donde

$$G_4(n) = \sum_{\substack{z\in\mathbb{Z}[i]\\ |z|=n}} z^4.$$

El caso $k = 6$ tiene fórmula:

$$r_{12}(n) = (-1)^{n-1}8\sum_{d|n}(-1)^{d+d'}d^5 + 4G_4'(n),$$

donde $G_4'(n)$ es análoga a $G_4(n)$ pero sumando sobre los cuaterniones de Hamilton, es decir[1]:

$$G_4'(n) = \sum_{\substack{(a,b,c,d)\in R_4(n)\\ z=a+bi+cj+dk}} z^4.$$

Dar fórmulas para $r_{2k+1}(n)$ es más delicado. Estos casos no están en las hipótesis del Teorema 3.63 presentado aquí; sí por ejemplo en las del Teorema 10.8 de [Iwa97, ver sección 10.4] que dice que θ_{2k+1} es una forma automorfa de peso medio entero. Sin embargo, Gauss había probado que:

$$r_3^*(n) = \begin{cases} 12h(-n) & \text{si } n \equiv 1, 2 \text{ (mód 4)} \\ 8h(-n) & \text{si } n \equiv 3 \text{ (mód 8)} \\ 0 & \text{en otro caso} \end{cases}.$$

Aquí $r_3^*(n)$ denota las representaciones *primitivas* de n como suma de 3 cuadrados (es decir, aquellas representaciones $a^2 + b^2 + c^2 = n$ donde $(a, b, c) = 1$). Por su parte $h(d)$ denota el número de clases de equivalencia propia de formas cuadráticas binarias primitivas definidas positivas de discriminante $d < 0$ (la equivalencia *propia* está dada por matrices de $\mathrm{SL}_2(\mathbb{Z})$).

Concluimos el capítulo con la siguiente observación referente a la asintótica de $r_k(n)$. Recordemos que $\theta_{2k} = f_{2k} + s_{2k}$ de donde

$$r_{2k}(n) = a_n(f_{2k}) + a_n(s_{2k}). \tag{4.2}$$

[1]La notación $R_k(n)$ es la del Capítulo 1, ver 2.2.

Se puede probar que los coeficientes de la forma cuspidal cumplen $|a_n(s_{2k})| < Cn^{k/2}$ [DS05, ver Teorema 5.9.1] mientras que si $f_{2k} \neq 0$, para n en ciertas clases de congruencia, se tiene que $a_n(f_{2k}) \gg n^{k-1}$. Así, para $k > 2$ los coeficientes de la serie de Eisenstein dominan conforme cuando $n \to \infty$. Es decir, si se conociera $f_{2k} \neq 0$ sus coeficientes darían una buena asintótica para los $r_{2k}(n)$. Por ejemplo, podemos afirmar que si $a_n(f_{2k}) > 0$ entonces $r_{2k}(n) > 0$ para n suficientemente grande.

Para el caso $k = 3$, un teorema de Siegel nos dice que:

$$|d|^{\frac{1}{2}-\varepsilon} \ll h(d) \ll |d|^{\frac{1}{2}+\varepsilon}, \quad d < 0, \varepsilon > 0,$$

lo cual nos permite dar una respuesta asintótica al problema en cuestión.

Capítulo 5

Epílogo

En lo que sigue $V = \mathbb{R}^n$. Recordamos que un retículo L es un $\mathbb{Z}$-submódulo de rango n tal que $L \otimes \mathbb{R} = V$. Se pueden elegir pues vectores v_1, ..., v_n de modo que todo $v \in L$ se escribe $v = \sum_i a_i v_i$ con $a_i \in \mathbb{Z}$.

Si en V consideramos una estructura de espacio cuadrático, existe una matriz definida positiva A es tal que:

$$Q(v) = \frac{1}{2} v^t A v \ , \quad B(v, w) = v^t \widetilde{A} w.$$

Llamamos a $\widetilde{A}$ de *matriz de Gram*. Si $\widetilde{A}'$ es la matriz de Gram asociada a otra base, vimos en el Capítulo 1 que $\widetilde{A}' = S^t \widetilde{A} S$ con $S \in \mathrm{GL}_n(\mathbb{Z})$.

Ejemplo 5.1. *En $V = \mathbb{R}^n$ con la estructura de espacio cuadrático usual, $L = \mathbb{Z}^n$ es un retículo con matriz de Gram* Id_n.

Restringiremos nuestra atención a aquellos retículos que son *enteros*, es decir que $b(v, w) \in \mathbb{Z}$ para $v, w \in L$. Decimos que un tal retículo es *par* si todos sus elementos cumplen $q(v) \equiv 0$ (mód 2).

Definimos el *discriminante* de L

$$\operatorname{disc} L = \det(\widetilde{A})$$

que es también el cuadrado del volumen del toro $\mathbb{R}^n / L$. Decimos que un retículo es *unimodular* cuando $\operatorname{disc}(L) = 1$.

Definimos el *retículo dual*:

$$L^{\#} = \{v \in \mathbb{R}^n : b(v, l) \in \mathbb{Z} \ \forall l \in L\}.$$

En el caso de los retículos enteros, $L \subseteq L^{\#}$. De hecho, $L = L^{\#}$ si y solamente si L es unimodular. Esto sigue del hecho que la matriz de Gram de $L^{\#}$ es $(\widetilde{A}\,^t)^{-1} = \widetilde{A}^{-1}$.

Dado un retículo L podemos asociarle una función theta:

$$\Theta_L(z) = \sum_n r_L(n) e^{2\pi i n z}, \;\; z \in \mathbb{H}.$$

Dados dos retículos $L_1 \subseteq \mathbb{R}^n$ y $L_2 \subseteq \mathbb{R}^m$, tenemos que

$$L_1 \oplus L_2 = \{(v_1, v_2) : v_1 \in L_1,\; v_2 \in L_2\} \subseteq \mathbb{R}^{n+m}$$

define un retículo cuya matriz de Gram es

$$\widetilde{A} = \begin{pmatrix} \widetilde{A_1} & 0 \\ 0 & \widetilde{A_2} \end{pmatrix}$$

donde $\widetilde{A_1}$ y $\widetilde{A_2}$ son las matrices de Gram de L_1 y L_2 respectivamente. Si L_1 y L_2 son unimodulares, entonces también lo es $L_1 \oplus L_2$. Lo mismo sucede respecto a la paridad. Además, repitiendo el razonamiento que dio la fórmula 2.7 en el Capítulo 1 obtenemos:

$$\Theta_{L_1 \oplus L_2}(z) = \Theta_{L_1}(z)\Theta_{L_2}(z). \tag{5.2}$$

La función theta asociada a un retículo L nos permite obtener información sobre el mismo. Comencemos viendo una consecuencia sorprendente de nuestro trabajo en el Capítulo 3.

Proposición 5.3. *Sea L un retículo unimodular par de rango n. Entonces $n \equiv 0$ (mód 8).*

Demostración. Supongamos primero que $n = 4$ (mód 8). Como L es par, $\Theta_L(Tz) = \Theta_L(z)$ por 3.35. En lo que respecta a la acción por S, la congruencia que satisface n nos da $\Theta_L(Sz) = -z^{n/2}\Theta(z)$ (ver 3.22). Usando estas dos identidades, vemos que:

$$\Theta_L(TSz) = -z^{n/2}\Theta_L(z).$$

De la igualdad anterior sigue que:

$$\begin{aligned} \Theta_L\left((TS)^2 z\right) &= -(TSz)^{n/2}\Theta_L(TSz) \\ &= \left(\frac{z-1}{z}\right)^{n/2} z^{n/2}\Theta_L(z) \\ &= (z-1)^{n/2}\Theta_L(z). \end{aligned}$$

Finalmente, calculamos:

$$\begin{aligned}\Theta_L\left((TS)^3 z\right) &= (TSz-1)^{n/2}\Theta_L(TSz)\\ &= -\left(\frac{1}{z}\right)^{n/2} z^{n/2}\Theta_L(z)\\ &= -\Theta_L(z).\end{aligned}$$

Pero $(TS)^3 = -Id$, así que $(TS)^3 z = z$ de donde habríamos probado que:

$$\Theta_L(z) = -\Theta_L(z)$$

lo cual supone un absurdo.

Para el caso general, si $n \not\equiv 0$ (mód 8) dividimos según si n es par o impar. Si n es par y $n \equiv 4$ (mód 8) entonces no hay nada que probar; en caso contrario $L \oplus L$ tiene rango $2n \equiv 4$ (mód 8) por lo cual obtenemos un absurdo aplicando el razonamiento anterior a este retículo. Si n es impar $L \oplus L \oplus L \oplus L$ tiene rango $4n \equiv 4$ (mód 8) y concluimos como en el caso anterior. □

Como corolario de la proposición, pues $\Theta_L(z)$ es holomorfa en $\mathbb{H}$ e ∞ por 3.19, obtenemos el siguiente corolario:

Corolario 5.4. *Sea L un retículo unimodular par. Entonces $\Theta_L(z)$ es una forma modular de peso $n/2$ para $\mathrm{SL}_2(\mathbb{Z})$.*

Obsérvese que la Proposición 5.3 no nos habla sobre la existencia de retículos unimodulares pares –pero nos da una condición que un tal retículo debe cumplir. Si notamos $v_n = \sum_i e_i = (1, \ldots, 1)$, definimos

$$D_n := \{x \in \mathbb{Z}^n : v_n \cdot x \equiv 0 \text{ (mód 2)}\}.$$

A partir de este definimos:

$$D_n^+ := D_n \cup \left(D_n + \frac{1}{2}v_n\right).$$

Si $n \equiv 0$ (mód 8) se puede probar que D_n^+ es un retículo unimodular par.

Cuando $n = 8$ el retículo definido coincide con el retículo E_8, denominación que proveniente de la clasificación de álgebras de Lie simples y complejas. Una

base posible para este retículo es $2e_1$ junto con $e_i + e_{i+1}$ para $i = 1, \ldots, 6$ y $\frac{1}{2}v_8$; con matriz de Gram:

$$\widetilde{A}_{E_8} = \begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 \end{pmatrix}$$

Su función theta es, en virtud del Corolario 5.4, una forma modular de peso 4 para $\mathrm{SL}_2(\mathbb{Z})$. Este es un espacio vectorial de dimensión 1 generado por la serie de Eisenstein $E_4(z)$ (ver 1.29):

$$E_4(z) = 1 + 240 \sum_{n \geq 1} \sigma_3(n) e^{2\pi i n z},$$

y como tanto $E_4(z)$ como $\Theta_{E_8}(z)$ tienen término constante 1, entonces son iguales. Vemos que por ejemplo en E_8 hay 240 vectores de norma $\sqrt{2}$.[1] Es importante observar que en el razonamiento anterior no usamos información sobre la construcción de E_8. Es decir, cualquier retículo L unimodular par de rango 8 tendrá $\Theta_L(z) = \Theta_{E_8}(z)$. Por desgracia, o por fortuna, esta observación no es muy útil: todo retículo unimodular par de rango 8 es, módulo una isometría, E_8. Esto puede deducirse, por ejemplo, de la *fórmula de la masa* como veremos a continuación.

Dos formas cuadráticas enteras están en el mismo *género* si son equivalentes sobre $\mathbb{R}$ y sobre $\mathbb{Z}_p$ para todo p. En términos de retículos, esto se traduce a que dos retículos están en el mismo género si son isomorfos sobre $\mathbb{R}$ y sobre $\mathbb{Z}_p$ para todo p. La *fórmula de la masa (Smith-Minkowski-Siegel)* dice que la *masa del género*

$$m(L) := \sum_{L' \in \mathrm{Gen}(L)} \frac{1}{\#\,\mathrm{Aut}(L')}$$

es un producto de factores locales (ver por ejemplo [CS88]).

En el caso de un retículo unimodular par de rango $n = 8k$, hay un solo

[1] Estos 240 vectores de norma $\sqrt{2}$ generan el *sistema de raíces* E_8.

género por lo que la suma recorre las clases de equivalencia de tales retículos (digamos C_n):

$$M_n = \sum_{L' \in C_n} \frac{1}{\#\operatorname{Aut}(L')}$$

A su vez, en este caso particular [Ser12, Capítulo V, 2.3] la fórmula de la masa dice que:

$$M_n = \frac{B_{2k}}{8k} \prod_{j=1}^{4k-1} \frac{B_j}{4j}.$$

Para el caso de E_8:

$$\begin{aligned} M_8 &= \frac{B_4}{8}\frac{B_2}{4}\frac{B_4}{8}\frac{B_6}{12} \\ &= \frac{-1/30}{8}\frac{1/6}{4}\frac{-1/30}{8}\frac{1/42}{12} \\ &= \frac{1}{696729600}. \end{aligned}$$

Pero la masa coincide con el aporte del término $\frac{1}{\#\operatorname{Aut}(E_8)}$, pues el grupo de autometrías de E_8 (que es el grupo de Weyl de tipo E_8) tiene precisamente 696729600 elementos. Así se concluye que C_8 consiste solamente de la clase de E_8: todo retículo unimodular par de rango 8 es isomorfo a E_8.

Para retículos unimodulares pares de rango $n = 16$, se produce el mismo fenómeno en cuanto a las funciones theta. Un tal retículo tiene por función theta a una forma modular de peso 8 para $\mathrm{SL}_2(\mathbb{Z})$, el cual es un espacio vectorial de dimensión 1 generado por la serie de Eisenstein $E_8(z)$:

$$E_8(z) = 1 + 480 \sum_{n \geq 1} \sigma_7(n) e^{2\pi i n z}.$$

Por lo tanto, si L es un retículo unimodular par de rango 16 tenemos que $\Theta_L(z) = E_8(z)$. Pero tenemos a disposición 2 retículos de este tipo: $L_1 = E_8 \oplus E_8$ y $L_2 = D_{16}^+$. Por el razonamiento anterior sabemos que sus funciones theta no tienen más opción que ser iguales, pero por otro lado por 5.2 nos dice que $\Theta_{L_1}(z) = E_4(z)^2$ de donde sigue la relación (pues los coeficientes de $\Theta_{L_1}(z)$ son los de $E_8(z)$):

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{i=1}^{n-1} \sigma(i)\sigma_3(n-i).$$

Si bien estos retículos son *isoespectrales* (i.e.: tienen la misma de vectores de norma $\sqrt{n}$ para todo n) se puede probar que no son isomorfos.[2] Esto nos da un ejemplo de retículos isoespectrales que no son isomorfos. Esto nos da una respuesta a la siguiente pregunta, que surge naturalmente al estudiar las funciones theta:

Problema 5.5. *Si Q, Q' son dos formas cuadráticas enteras en n variables con la misma función theta, ¿serán equivalentes?* [3]

La respuesta es, en general, *no*, como lo muestra el ejemplo de L_1 y L_2 con rango 16.

Más aún, en [Sch90] Schiemann da un ejemplo de formas cuadráticas definidas positivas en 4 variables que no son equivalentes si bien tienen la misma función theta. Conway y Sloane dan en [CS92] una familia de pares de retículos isoespectrales que tiene al ejemplo de Schiemann por caso particular. Que la pareja de retículos es isoespectral se prueba en [CS92] estableciendo una biyección que preserva norma entre los retículos de la pareja, mientras que en [Sch90] se usa la cota de Sturm para poder reducir la igualdad de las funciones theta –que son formas modulares– a la verificación de la coincidencia de finitos coeficientes.

Teniendo un ejemplo (L_1, L_2) de retículos isoespectrales no isométricos de rango n, podemos construir $\widetilde{L_i} = L_i \oplus \mathbb{Z}^m$, lo cual nos da un ejemplo $(\widetilde{L_1}, \widetilde{L_2})$ en rango mayor. Se puede probar que $\widetilde{L_1}$ y $\widetilde{L_2}$ no son isomorfos, mientras que son isoespectrales por 5.2. Por lo tanto, sabemos que la respuesta a la pregunta es negativa para $n \geq 4$.

El mismo Schiemann prueba en [Sch97] que en el caso de formas cuadráticas ternarias, la respuesta es afirmativa: encuentra una cota $b(f)$ de modo que si $r_f(n) = r_g(n)$ para todo $n \leq b(f)$ entonces f y g son equivalentes. Esto concluye la respuesta a la pregunta.

[2] Los vectores de norma $\sqrt{2}$ generan E_8, luego L_1 es generado por los 480 vectores de norma $\sqrt{2}$ que contiene. No sucede lo mismo con L_2: los 480 vectores de norma $\sqrt{2}$ generan el subretículo propio D_8.

[3] En términos de retículos: si L y L' son retículos de rango n con la misma función theta, ¿serán isomorfos?

Bibliografía

[BVdGHZ08] J. H. Bruinier, G. Van der Geer, G. Harder, and Don Zagier. *The 1-2-3 of modular forms: lectures at a summer school in Nordfjordeid, Norway*. Springer Science & Business Media, 2008.

[Cas08] J. W. S. Cassels. *Rational quadratic forms*. Courier Dover Publications, 2008.

[CS88] J. H. Conway and N. J. A. Sloane. *Low-dimensional lattices. IV. The mass formula. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 419(1857):259–286, 1988.

[CS92] J. H. Conway and N. J. A. Sloane. *Four-dimensional lattices with the same theta series. International Mathematics Research Notices*, 1992(4):93–96, 1992.

[Dav13] H. Davenport. *Multiplicative number theory*, volume 74. Springer Science & Business Media, 2013.

[DF94] P. De Fermat. *Oeuvres de Fermat*, volume 2. Gauthier-Villars, 1894.

[Dic20] L. E. Dickson. *History of the theory of numbers: Diophantine analysis*. Carnegie Institution of Washington, Washington DC, 1920.

[DS05] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics 228. Springer-Verlag New York, 2005.

[Elk09] N. Elkies. *Theta functions and weighted theta functions of euclidean lattices, with some applications*, 2009. `https://people.math.harvard.edu/~elkies/aws09.pdf`.

[Gla07] J. W. L. Glaisher. *On the numbers of representations of a number as a sum of* $2r$ *squares, where* $2r$ *does not exceed eighteen. Proceedings of the London Mathematical Society*, 2(1):479–490, 1907.

[Har99] G. H. Hardy. *Ramanujan: twelve lectures on subjects suggested by his life and work*, volume 136. American Mathematical Soc., 1999.

[Iwa97] H Iwaniec. *Topics in classical automorphic forms*, volume 17. American Mathematical Soc., 1997.

[JC22] J. Oaks J. Christianidis. *The Arithmetica of Diophantus: A Complete Translation and Commentary*. Scientific Writings from the Ancient and Medieval World. Routledge, 2022.

[Kit99] Y. Kitaoka. *Arithmetic of quadratic forms*, volume 106. Cambridge University Press, 1999.

[Lan87] S. Lang. *Elliptic Functions*. Springer-Verlag, 1987.

[Li23] C. Li. *From sum of two squares to arithmetic Siegel–Weil formulas. Bulletin of the American Mathematical Society*, 60(3):327–370, 2023.

[Roy17] R. Roy. *Elliptic and modular functions from Gauss to Dedekind to Hecke*. Cambridge University Press, 2017.

[Rud87] W. Rudin. *Real and complex analysis*. McGraw-HiII Book Company, 1987.

[Sch90] A. Schiemann. *Ein Beispiel positiv definiter quadratischer Formen der Dimension 4 mit gleichen Darstellungszahlen. Archiv der Mathematik*, 54(4):372–375, 1990.

[Sch97] A. Schiemann. *Ternary positive definite quadratic forms are determined by their theta series. Mathematische Annalen*, 308:507–517, 1997.

[Ser12] J. P. Serre. *A course in arithmetic*, volume 7. Springer Science & Business Media, 2012.

[Tor05] G. Tornaría. *The Brandt module of ternary quadratic lattices*. PhD thesis, University of Austin, 2005. `https://www.cmat.edu.uy/~tornaria/pub/tornaria_thesis.pdf`.

[Zac07] A. Zachary. *Theta Series as modular forms.* `http://zacharyabel.com/papers/Theta-Series-Mod_A07.pdf`, 2007.