Trabajo monográfico

El problema del número de clases de Gauss

La solución de Goldfeld-Oesterlé

Carolina Chiesa

Mayo 2023

Orientador:

Gonzalo Tornaría
Facultad de Ciencias, UDELAR

Licenciatura en Matemática
Universidad de la República
Montevideo, Uruguay

Resumen

Esta monografía está basada en el artículo [Oe] y su objetivo es entender la prueba dada por Goldfeld-Oesterlé al Problema de Gauss para el número de clases de ideales en cuerpos cuadráticos imaginarios.

Problema (Problema del número de clases de Gauss). *Dado $h \geqslant 1$, encontrar un algoritmo efectivo para determinar todos los cuerpos cuadráticos imaginarios con número de clases h.*

El Teorema de Goldfeld-Oesterlé da una cota inferior efectiva para $h(d)$, el número de clases del cuerpo cuadrático imaginario de discriminante d.

Teorema (Oesterlé).

$$h(d) > \tfrac{1}{7000}(\log|d|)\prod_{\substack{p|d\\ p\neq d}}\left(1-\tfrac{[2\sqrt{p}]}{p+1}\right).$$

Veremos primero algunos resultados básicos necesarios sobre cuerpos cuadráticos imaginarios y formas modulares, para finalmente introducirnos en la prueba.

Índice general

Introducción

Remontándonos al año 1640, Fermat enunció su Teorema sobre la suma de dos cuadrados.

TEOREMA 0.1. *Sea p un primo impar, entonces existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + y^2$ si y sólo si $p \equiv 1 \pmod 4$,*

Este fue el primero de varios de sus teoremas sobre representaciones de enteros como sumas de cuadrados, algunos de los que le siguieron fueron los siguientes:

TEOREMA 0.2. *Sea p un primo impar*

$$p = x^2 + 2y^2 \ x, y \in \mathbb{Z} \ \Leftrightarrow p \equiv 1, 3 \pmod 8$$

TEOREMA 0.3. *Sea p un primo impar*

$$p = x^2 + 3y^2 \ x, y \in \mathbb{Z} \Leftrightarrow p = 3 \ \acute{o} \ p \equiv 1 \pmod 3.$$

Los tres Teoremas enunciados arriba fueron probados por primera vez por Euler entre los años 1749 y 1763, y muchos otros teoremas del estilo fueron probados durante todo el siglo XVIII. En 1773 Lagrange publicó una prueba de los Teoremas de Fermat basadas en la teoría de formas cuadráticas binarias, que introdujo con conceptos como el discriminante y la relación de equivalencia de formas cuadráticas reducidas.

Dada una forma cuadrática $f(x, y) = ax^2 + bxy + cy^2$ con $a, b, c \in \mathbb{Z}$ de discriminante $d = b^2 - 4ac$ se dice que es *primitiva* si $\text{mcd}(a, b, c) = 1$, y se dice que representa al entero m si la ecuación $f(x, y) = m$ tiene solución entera. Si además se puede pedir $\text{mcd}(x, y) = 1$ entonces se dice que f *representa propiamente* a m. Bajo cambios de variables del tipo

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \qquad \alpha\delta - \beta\gamma = \pm 1$$

una forma sigue representando los mismos elementos; Lagrange define entonces la equivalencia entre formas cuadráticas de la siguiente manera:

DEFINICIÓN 0.4. Dos formas $f(x, y)$ y $g(x, y)$ son *equivalentes* si existen $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ con $\alpha\delta - \beta\gamma = \pm 1$ tales que $f(x, y) = g(\alpha x + \beta y, \gamma x + \delta y)$.

Si $\alpha\delta - \beta\gamma = 1$ entonces se dice que las formas son *propiamente equivalentes,* pero este concepto no fue introducido por Lagrange sino más adelante por Gauss. No es difícil ver que ser equivalentes y ser propiamente equivalentes son ambas relaciones de equivalencia, y que formas propiamente equivalentes también representan los mismos enteros. Usaremos la notación (a, b, c) para referirnos a la forma $f(x, y) = ax^2 + bxy + cy^2$ y $(a, b, c) \sim (A, B, C)$ para referirnos a formas propiamente equivalentes.

Cuando el discriminante d de una forma (a, b, c) es positivo la forma se dice *indefinida*, esto quiere decir que representa enteros positivos y negativos; en cambio cuando d es negativo la forma sólo representa enteros del mismo signo que a, en este caso se le dice *definida positiva* cuando $a > 0$ y *definida negativa* cuando $a < 0$. Toda forma primitiva definida positiva es propiamente equivalente a una única forma reducida.

DEFINICIÓN 0.5. Una forma primitiva definida positiva (a, b, c) es *reducida* si

$$|b| \leqslant a \leqslant c, \text{ y } |b| = a \text{ ó } a = c \Rightarrow b \geqslant 0.$$

DEFINICIÓN 0.6. Sea $d < 0$, $h(d)$ denota al número de clases de equivalencia de formas cuadráticas primitivas definidas positivas de discriminante d. Este número es finito y coincide con el número de formas reducidas de discriminante d.

En el árticulo 303 de *Disquisitiones Arithmeticae* Gauss conjetura que, fijando h, el número de discriminantes $d < 0$ tales que $h(d) = h$ es finito, y en el artículo 304 conjetura que el límite de $h(d)$ cuando $d \to \infty$ es infinito. Gauss también da una tabla para algunos números de clases fijos y conjetura que está completa, pero consideraba formas del tipo $ax^2 + 2bxy + cy^2$, que tienen discriminante par y en consecuencia corresponden a un problema más simple. La versión moderna del problema es la siguiente.

PROBLEMA (El problema del número de clases de Gauss). *Dado h, encontrar un algoritmo* efectivo *para determinar todos los discriminantes negativos con número de clases h.*

Hay una correspondencia entre el número de clases de formas cuadráticas de discriminante $d < 0$ y el número de clases de ideales en un cuerpo cuadrático imaginario de discriminante d, lo cual da otro enfoque al problema del número de clases de Gauss.
Dado un cuerpo cuadrático K imaginario de discriminante d y $\mathcal{O}_K$ su anillo de enteros, se definen los *ideales fraccionales* en $\mathcal{O}_K$ como los $\mathcal{O}_K-$submódulos finitamente generados, al conjunto de ideales fraccionales lo denotamos por $\mathrm{Fr}(\mathcal{O}_K)$. Si I es un ideal fraccional entonces existe $\alpha \in \mathcal{O}_K$ tal que αI es un ideal de $\mathcal{O}_K$. Si existe $b \in K^*$ tal que $I = b\mathcal{O}_K$ entonces se dice que el ideal fraccional I es principal y al conjunto de ideales fraccionales principales lo denotamos por $\mathrm{Pr}(\mathcal{O}_K)$. Decimos que dos ideales I, J son equivalentes $(I \sim J)$ si $I = PJ$ donde $P \in \mathrm{Pr}(\mathcal{O}_K)$.

DEFINICIÓN 0.7. Un entero $d \neq 1$ es un discriminante fundamental si satisface una de las siguientes condiciones:

(a) $d \equiv 1 \pmod 4$ y es libre de cuadrados.
(b) $d = 4k$, donde $k \equiv 2, 3 \pmod 4$ es libre de cuadrados.

Equivalentemente, los discriminantes fundamentales son los enteros que son discriminantes de cuerpos cuadráticos.

TEOREMA 0.8. *Dado $d < 0$ un discriminante fundamental. Hay una biyección entre clases de equivalencia de formas cuadráticas primitivas definidas positivas de discriminante d y clases de equivalencia de ideales fraccionales en un cuerpo cuadrático imaginario de discriminante d.*

A continuación se enuncian algunas de las contribuciones más importantes en relación al problema de número de clases de Gauss.

Dirichlet: Relaciona el número de clases de ideales en $\mathbb{Q}[\sqrt{d}]$ con el valor particular en $s = 1$ de una $L-$serie de Dirichlet, este resultado lo probó en 1839.

DEFINICIÓN 0.9. Dado un carácter de Dirichlet χ, su L-serie de Dirichlet asociada es

$$L(s,\chi) := \sum_{n=1}^{\infty} \chi(n)n^{-s} = \prod_{p} \left(1 - \chi(p)p^{-s}\right)^{-1}.$$

Notaremos por χ_d al carácter de Dirichlet asociado a un cuerpo cuadrático imaginario de discriminante d. Este carácter es el símbolo de Kronecker $\left(\frac{d}{\cdot}\right)$.

$L(s,\chi_d)$ converge para $\Re s > 1$ y se extiende por prolongación analítica a todo el plano complejo.

TEOREMA 0.10 (Dirichlet). *Sea $d < 0$ un discriminante fundamental. Entonces*

$$L(1,\chi_d) = \frac{2\pi h(d)}{w\sqrt{-d}},$$

donde w es el número de raíces de la unidad en K.

OBSERVACIÓN 0.11. *Como $h(d) \geqslant 1$ la $L-$serie anterior no se anula en $s = 1$. De ese resultado Dirichlet deduce la infinitud de los primos en progresiones aritméticas.*

Hecke, Landau: En 1918 se publicó el siguiente Teorema probado por Landau, pero que este atribuyó a Hecke.

TEOREMA 0.12 (Hecke). *Sea $d < 0$ un discriminante fundamental. Si $L(s,\chi_d) \neq 0$ para s real tal que $s > 1 - \frac{c}{\log|d|}$, entonces*

$$h(d) \geqslant c_1 \frac{\sqrt{|d|}}{\log|d|},$$

donde c, c_1 son ciertas constantes fijas.

Deuring: La hipótesis generalizada de Riemann (GRH) establece que los ceros no triviales de $L(s,\chi)$ se encuentran en $\Re s = \frac{1}{2}$. En 1933 Deuring probó

TEOREMA 0.13 (Deuring). *Si GRH es falsa entonces $h(d) \geqslant 2$ para $-d$ suficientemente grande.*

Mordell: En 1934 Mordell mejoró el resultado de Deuring, y en el mismo año Heilbronn hizo otro avance.

TEOREMA 0.14 (Mordell). *Si GRH es falsa, entonces* $\lim_{d\to-\infty} h(d) = \infty$.

TEOREMA 0.15 (Heilbronn). *Si RH es falsa, entonces* $\lim_{d\to-\infty} h(d) = \infty$.

Con este último resultado, Heilbronn probó junto a Linfoot que hay a lo sumo diez cuerpos cuadráticos imaginarios cuyo número de clases es 1, estos corresponden a los discriminantes $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$ y quizá, a un último discriminante fuera de esa lista.

Los resultados de Hecke, Deuring y Heilbronn combinados dan una prueba para la Conjetura de Gauss que no depende de la veracidad de la Hipótesis de Riemann, pero el método de estas pruebas no es efectivo, pues en caso de existir un cero de $L(s, \chi_d)$ localizado fuera de $\Re s = \frac{1}{2}$ dependerían de él.

Siegel: En 1935 dió una cota inferior para $h(d)$ que depende de una constante $c > 0$ que no puede ser calculada de forma efectiva.

TEOREMA 0.16. *Sea $d < 0$ un discriminante fundamental. Para todo $\varepsilon > 0$ existe $c > 0$ tal que*

$$h(d) > c|d|^{\frac{1}{2}-\varepsilon}.$$

Tatuzawa: En 1951 probó la siguiente versión del Teorema de Siegel,

TEOREMA 0.17 (Tatuzawa). *Sea $0 < \varepsilon < \frac{1}{11.2}$, si $|d| > e^{\frac{1}{\varepsilon}}$ entonces*

$$L(1, \chi_d) > 0.655|d|^{-\varepsilon}$$

excepto, a lo sumo, para un discriminante d.

La posible existencia de un discriminante para el que no valga la cota anterior hace que esta mejora de Tatuzawa al Teorema de Siegel también sea inefectiva, por lo que no resuelve el Problema de Gauss.

Heegner: Publicó en 1952 un artículo con lo que afirmaba era una prueba de la no existencia de un décimo cuerpo cuadrático imaginario con número de clases 1, lo que resolvería el Problema de Gauss para el número de clases 1. Sin embargo, su prueba contenía algunos errores y citaba —aunque no utilizaba— un trabajo de Weber que contenía resultados con pruebas incompletas, este fue el principal motivo por el cual no fue considerada como "esencialmente correcta" hasta el año 1967. Lamentablemente, Heegner falleció en 1965 sin ver su prueba ser aceptada. En 1969 Stark publicó la prueba de Heegner corregida.

Stark, Baker: Entre 1966 y 1967 resolvieron de forma independiente el Problema de Gauss para el número de clases 1. Stark probó que un décimo cuerpo cuadrático en el Teorema de Heilbronn-Linfoot no podría existir, de forma muy similar a la de Heegner. La solución de Baker, en cambio, utilizaba la independencia lineal de tres logaritmos.

Stark, Baker: En 1971 probaron, nuevamente de forma independiente, que no puede existir un decimonoveno cuerpo cuadrático imaginario con número de clases 2, ambos usaron el método de independencia lineal de logaritmos.

Goldfeld: En 1976 probó un Teorema que resuelve efectivamente el Problema de Gauss para el caso general, asumiendo que la Conjetura de Birch-Swinnerton-Dyer es

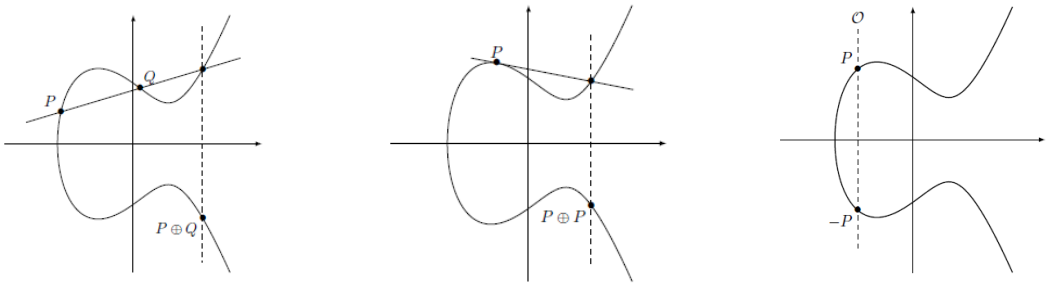

FIGURA 1. Ley de grupo

cierta para una curva de rango $g = 3$. Para entender el enunciado del Teorema de Goldfeld primero definimos algunos conceptos elementales de curvas elípticas.

Sea $E:\ y^2 = 4x^3 - ax - b$ una curva elíptica sobre $\mathbb{Q}$ de discriminante $\Delta = a^3 - 27b^2$ no nulo. El conjunto de sus puntos racionales se denota $E(\mathbb{Q})$ y es un grupo abeliano finitamente generado con la siguiente ley de grupo:

- El neutro 0 es el punto en infinito.
- Si $P = (x, y)$ su opuesto es $-P = (x, -y)$.
- La suma de tres puntos colineales es 0.

El *rango* g de $E(\mathbb{Q})$ se define como el número de generadores linealmente independientes de orden infinito en $E(\mathbb{Q})$, es decir, $E(\mathbb{Q}) = \mathbb{Z}^g \oplus T$ donde T es un subgrupo de torsión. El *conductor* de una curva elíptica es un entero asociado a ella cuyos divisores primos son los primos que dividen al discriminante de la curva. Si N denota al conductor de la curva E se define la $L-$serie de Hasse-Weil asociada a E como

$$L_E(s) = \prod_{p|N} \left(1 - t_p p^{-s}\right)^{-1} \prod_{p\nmid N} \left(1 - t_p p^{-s} + p^{1-2s}\right)^{-1},$$

donde $t_p = p + 1 - E(\mathbb{F}_p)$. Estos coeficientes están acotados por $|t_p| \leqslant 2\sqrt{p}$.

CONJETURA 0.1 (Birch-Swinnerton-Dyer). Sea g el rango de una curva elíptica $E/\mathbb{Q}$, entonces

$$L_E(s) \sim C_E(s-1)^g.$$

TEOREMA 0.18 (Goldfeld). *Sea $d < 0$ un discriminante fundamental y N tal que $\chi_d(N) = -1$. Si $L_E(s) \sim C_E(s-1)^g$ con g impar, entonces*

$$h(d) > \tfrac{c}{g^{4g}N^{13}} (\log|d|)^{g-2} e^{-21\sqrt{g\log\log|d|}},$$

donde c es una constante efectiva que no depende de E.

Existe una versión de este teorema para los casos $\chi_d(N) = 1$ y $\chi_d(N) = 0$. Para el primer caso, la proposición 1.37 nos da la cota $h \log N \geqslant \log \frac{d}{4}$. El segundo caso, en cambio, es más complicado de tratar. En la sección 2 del Capítulo 4 haremos un comentario sobre la prueba que da Oesterlé.

Observemos que por el Teorema anterior, para obtener una cota no trivial basta con encontrar una curva elíptica cuya $L-$serie tenga un cero de orden 3 en $s = 1$.

Gross-Zagier: En 1983 probaron un Teorema que da como corolario la existencia de una curva elíptica con un cero triple en $s = 1$, como requería el Teorema de Goldfeld. Combinando estos resultados se obtiene

TEOREMA 0.19 (Goldfeld-Gross-Zagier). *Para todo $\varepsilon > 0$ existe una constante $c > 0$ calculable de forma efectiva tal que $h(d) > c(\log |d|)^{1-\varepsilon}$.*

Oesterlé: En 1984 publica una prueba simplificada del Teorema de Goldfeld y calcula la constante para la curva elíptica E_0 que da el Corolario de Gross-Zagier.

TEOREMA 0.20 (Oesterlé).

$$h(d) > \frac{1}{7000}(\log |d|)\prod_{\substack{p|d \\ p\neq d}}\left(1 - \frac{[2\sqrt{p}]}{p+1}\right).$$

Watkins: En 2003 publicó su trabajo donde modifica las pruebas de Goldfeld-Oesterlé, mejorando la cota obtenida por Oesterlé, lo que le permite dar la clasificación completa de cuerpos cuadráticos imaginarios con número de clases hasta 100.

El objetivo de esta monografía es estudiar la prueba dada por Oesterlé en [Oe] al Teorema de Goldfeld, dividiremos entonces la estructura en cuatro capítulos.

En el primer capítulo veremos algunos resultados básicos sobre la teoría de cuerpos cuadráticos, posiblemente el resultado más importante aquí sea la correspondencia entre clases de ideales de un cuerpo cuadrático imaginario de discriminante d y clases de formas primitivas definidas positivas de discriminante d. Definiremos también la función ζ_K asociada a un cuerpo cuadrático y veremos algunas de sus propiedades, que serán necesarias más adelante.

En el segundo capítulo introducimos algunos resultados elementales sobre formas modulares, en particular necesitaremos usar la ecuación funcional para las L-series asociadas a las formas nuevas y a su cuadrado simétrico.

Luego de ver los preliminares necesarios en los dos capítulos anteriores, en el Capítulo 3 nos dedicaremos a estudiar la prueba de Oesterlé para el Teorema de Goldfeld. La prueba parte de asumir la existencia, para K un cuerpo cuadrático, de una constante M y dos series de Dirichlet ψ, G_K que cumplen ciertas propiedades, con esto asumido se busca acotar ciertas integrales que dependen de ψ, G_K, M y una constante U que se debe elegir convenientemente.

En el capítulo 4 vemos como Oesterlé define M, ψ y G_K que satisfacen las condiciones requeridas en la parte previa, y como finaliza la prueba utilizando la curva elíptica de conductor 37 dada por Gross-Zagier para computar la constante del Teorema de forma efectiva.

Capítulo 1

Cuerpos cuadráticos imaginarios y formas cuadráticas binarias

1. Cuerpos cuadráticos

Un cuerpo de números es una extensión de grado finito sobre $\mathbb{Q}$. Cuando el grado es dos se le denomina cuerpo cuadrático. Los cuerpos cuadráticos pueden escribirse como $K = \mathbb{Q}(\sqrt{m}) = \{a+b\sqrt{m} : \ a, b \in \mathbb{Q}\}$, donde $m \in \mathbb{Z}\backslash\{0, 1\}$ es un entero libre de cuadrados. Cuando $m > 0$ se dice que el cuerpo cuádratico es real y si $m < 0$ se dice imaginario. Se define el discriminante d_K del cuerpo cuadrático $Q(\sqrt{m})$ como m si $m \equiv 1 \pmod 4$ y $4m$ en otro caso.

Definición 1.1. Sea K un cuerpo cuadrático y $\alpha = a + b\sqrt{m} \in K$. Se definen el *conjugado, norma, traza* y *discriminante* de α como sigue,

$$\begin{aligned} \overline{\alpha} &:= a - b\sqrt{m} \in K \\ \mathrm{N}(\alpha) &:= \alpha\overline{\alpha} = a^2 - mb^2 \in \mathbb{Q} \\ \mathrm{Tr}(\alpha) &:= \alpha + \overline{\alpha} = 2a \in \mathbb{Q} \\ \mathrm{Disc}(\alpha) &:= (\alpha - \overline{\alpha})^2 = 4mb^2 \end{aligned}$$

Observación 1.2. *Si K es un cuerpo cuadrático y $\sigma : K \to K$ es un automorfismo que fija $\mathbb{Q}$, entonces $\sigma(\sqrt{m}) = \sqrt{m}$ o $\sigma(\sqrt{m}) = -\sqrt{m}$, luego existe un único automorfismo de cuerpos no trivial y el grupo de Galois de la extensión $K/\mathbb{Q}$ tiene dos elementos, $Gal(K/\mathbb{Q}) = \{id, \sigma\}$.*

Proposición 1.3.

(a) $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)\ \forall \alpha, \beta \in K$.
(b) $\mathrm{N}(\alpha) = 0 \Leftrightarrow \alpha = 0$.
(c) $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)\ \forall \alpha, \beta \in K$.
(d) $\mathrm{Disc}(\alpha) = 0 \Leftrightarrow \alpha \in \mathbb{Q}$.

Demostración. Una demostración se puede ver en [Tr, Prop. 4.1.3]. □

El anillo de enteros.

Definición 1.4. Dado K un cuerpo de números, $\alpha \in K$ es un *entero algebraico* si es raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$.

El conjunto de enteros algebraicos sobre un cuerpo de números K forma un anillo, que denotamos por $\mathcal{O}_K$. En particular, si K es un cuerpo cuadrático tenemos el siguiente teorema.

TEOREMA 1.5. *El anillo de enteros de un cuerpo cuadrático $K = \mathbb{Q}(\sqrt{m})$ está dado por*

$$\mathcal{O}_K = \begin{cases} \{a + b\sqrt{m} : \ a, b \in \mathbb{Z}\} \text{ si } m \equiv 2, 3 \pmod 4 \\ \{\frac{a+b\sqrt{m}}{2} : \ a \equiv b \pmod 2\} \text{ si } m \equiv 1 \pmod 4 \end{cases}$$

Además $\mathcal{O}_K = \mathbb{Z}[w_K]$, donde $w_K = \frac{d_K + \sqrt{d_K}}{2}$.

DEMOSTRACIÓN. Como todo $\alpha \in K$ satisface $\alpha^2 - \mathrm{Tr}(\alpha)\alpha + \mathrm{N}(\alpha) = 0$ tenemos la igualdad

$$\mathcal{O}_K = \{\alpha \in K : \ \alpha^2 - A\alpha + B = 0, \ A, B \in \mathbb{Z}\} = \{\alpha \in K : \ \mathrm{Tr}(\alpha), \mathrm{N}(\alpha) \in \mathbb{Z}\}.$$

Sea $\delta_0 := \begin{cases} \sqrt{m} \text{ si } m \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{m}}{2} \text{ si } m \equiv 1 \pmod 4 \end{cases}$, δ_0 es un entero algebraico, pues es raíz del polinomio $x^2 - m$ en el caso $m \equiv 2, 3 \pmod 4$ y de $x^2 - x + \frac{1-m}{4}$ en caso contrario; esto implica que $\mathbb{Z}[\delta_0] = \mathbb{Z} + \mathbb{Z}\delta_0 \subseteq \mathcal{O}_K$. Queremos ver la inclusión reversa.

Sea $\alpha = a + b\sqrt{m} \in \mathcal{O}_K$, por hipótesis $\mathrm{Tr}(\alpha) = 2a \in \mathbb{Z}$ y $\mathrm{N}(\alpha) = a^2 - b^2 m \in \mathbb{Z}$. Entonces $a = \frac{\mathrm{Tr}(\alpha)}{2}$ y $b = \frac{p}{q}$ con $p, q \in \mathbb{Z}$, $\mathrm{mcd}(p, q) = 1$, donde

$$4p^2 m = q^2(\mathrm{Tr}(\alpha)^2 - 4\,\mathrm{N}(\alpha)).$$

Como m es libre de cuadrados $q^2 \mid 4$, entonces $q = 1$ o $q = 2$, en cualquier caso $b = \frac{s}{2}$ con $s \in \mathbb{Z}$. Viendo esto módulo 4 tenemos que $\mathrm{Tr}(\alpha)^2 \equiv s^2 m \pmod 4$ y podemos distinguir en dos casos:

Caso 1: Si $m \not\equiv 1 \pmod 4$ entonces $\mathrm{Tr}(\alpha)^2 \equiv s^2 \equiv 0 \pmod 4$.
Luego $\mathrm{Tr}(\alpha) \equiv s \equiv 0 \pmod 2$ y $a, b \in \mathbb{Z}$.

Caso 2: Si $m \equiv 1 \pmod 4$ entonces $\mathrm{Tr}(\alpha)^2 \equiv s^2 \pmod 4$.
Luego $\mathrm{Tr}(\alpha) \equiv s \pmod 2$ y, por lo tanto,

$$\alpha = a + b\sqrt{m} = \frac{\mathrm{Tr}(\alpha) + s\sqrt{m}}{2} \in \left\{ \frac{a + b\sqrt{m}}{2} : \ a \equiv b \pmod 2 \right\}.$$

Si escribimos $\mathrm{Tr}(\alpha) = s + 2k$, entonces vemos que

$$\alpha = \frac{s + 2k + s\sqrt{m}}{2} = k + s\frac{1 + \sqrt{m}}{2}.$$

La igualdad $\mathcal{O}_K = \mathbb{Z}[w_K]$ se deduce fácilmente a partir de la definición de d_K. □

PROPOSICIÓN 1.6. *Si $d_K < -4$, entonces el conjunto de unidades de $\mathcal{O}_K$ es $\{\pm 1\}$.*

DEMOSTRACIÓN. Siguiendo con la notación de la demostración previa, $x = a + b\delta_0 \in \mathcal{O}_K$ es una unidad si y sólo si $\mathrm{N}(x) = \pm 1$, esto es,

$$\mathrm{N}(x) = \mathrm{N}(a + b\delta_0) = a^2 + \mathrm{Tr}(\delta_0)ab + \mathrm{N}(\delta_0)b^2 = \pm 1.$$

Si $b = 0$ entonces $a^2 = 1$ y $x = \pm 1$, si $b \neq 0$ entonces dividimos entre b^2,

$$\frac{a^2}{b^2} + \mathrm{Tr}(\delta_0)\frac{a}{b} + \mathrm{N}(\delta_0) = \pm\frac{1}{b^2}.$$

Si $d_K < -4$, $\frac{-d_K}{4} > 1 \geqslant \pm\frac{1}{b^2}$, llegamos a una contradicción usando que $\frac{-d_K}{4}$ es el mínimo en $\mathbb{R}$ de la función $x^2 + \mathrm{Tr}(\delta_0)x + \mathrm{N}(\delta_0)$. □

Factorización única en ideales primos. Vamos a enunciar algunos resultados sobre cuerpos cuadráticos imaginarios que se pueden encontrar en [Cox, §5] o en [Tr, §4].

PROPOSICIÓN 1.7. *Si K es un cuerpo de números y $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_K$, entonces el anillo cociente $\mathcal{O}_K/\mathfrak{a}$ es finito.*

DEFINICIÓN 1.8. Dado un ideal $\mathfrak{a}$ no nulo de $\mathcal{O}_K$ se define su norma como $|\mathcal{O}_K/\mathfrak{a}\,|$.

PROPOSICIÓN 1.9. *Sea K un cuerpo cuadrático imaginario.*

(a) *Sean I y J dos ideales no nulos de $\mathcal{O}_K$. Si $I|J$ entonces* $\mathrm{N}(I) \mid \mathrm{N}(J)$.
(b) *Si $I \neq (0)$ entonces* $I\overline{I} = \mathrm{N}(I)\mathcal{O}_K$.
(c) *Sean I y J dos ideales no nulos de $\mathcal{O}_K$. Entonces* $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$.
(d) *Sea I un ideal, entonces existen $a, b, c \in \mathbb{Z}$ tales que $I = c(a\mathbb{Z} + (-b + \delta_0)\mathbb{Z})$ y* $\mathrm{N}(I) = c^2 a$.

TEOREMA 1.10. *Sea K un cuerpo de números. Su anillo de enteros $\mathcal{O}_K$ es un dominio de Dedekind, es decir, es Noetheriano, integralmente cerrado y sus ideales primos no nulos son maximales.*

OBSERVACIÓN 1.11. *Si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$ entonces $\mathcal{O}_K/\mathfrak{p}$ es un cuerpo, se le denomina cuerpo de residuos de $\mathfrak{p}$.*

Al ser dominios de Dedekind tienen factorización única en ideales:

TEOREMA 1.12. *Si K es un cuerpo de números, todo ideal no nulo $\mathfrak{a}$ de $\mathcal{O}_K$ se escribe de forma única como producto de ideales primos:*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_k.$$

Los ideales $\mathfrak{p}_i$ son exactamente los ideales primos de $\mathcal{O}_K$ que contienen $\mathfrak{a}$.

Regresando a cuerpos cuadráticos, si K es un cuerpo cuadrático de discriminante d_K podemos caracterizar la factorización de $(p) = p\mathcal{O}_K$ con $p \in \mathbb{Z}$ a partir del símbolo de Kronecker $\left(\frac{d_K}{p}\right)$. Recordemos que cuando p es un primo impar el símbolo de Kronecker coincide con el símbolo de Legendre, y cuando $p = 2$ lo extiende de la siguiente manera:

$$\left(\frac{d_K}{2}\right) = \begin{cases} 1 & \text{si } d_K \equiv 1 \pmod 8 \\ 0 & \text{si } d_K \equiv 0 \pmod 4 \\ -1 & \text{si } d_K \equiv 5 \pmod 8 \end{cases}$$

y tenemos la siguiente proposición,

PROPOSICIÓN 1.13. *Si K es un cuerpo cuadrático de discriminante d_K y $p \in \mathbb{Z}$ un primo, entonces*

(a) *Si $\left(\frac{d_K}{p}\right) = 1$ entonces existen ideales $\mathfrak{p} \neq \bar{\mathfrak{p}}$ en $\mathcal{O}_K$ tal que $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. En este caso decimos que p* descompone *en K.*
(b) *Si $\left(\frac{d_K}{p}\right) = 0$ entonces existe un ideal $\mathfrak{p}$ en $\mathcal{O}_K$ tal que $p\mathcal{O}_K = \mathfrak{p}^2$. Decimos que p* ramifica *en K.*
(c) *Si $\left(\frac{d_K}{p}\right) = -1$ entonces $p\mathcal{O}_K$ es un ideal primo en $\mathcal{O}_K$. Decimos que p es* inerte *en K.*

DEMOSTRACIÓN. Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$, $\mathfrak{p} \cap \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ que es distinto de (0) (contiene a $\mathrm{N}(\mathfrak{p})$). Entonces existe un único primo $p \in \mathbb{N}$ tal que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Por lo tanto, dado $\mathfrak{p}$ un ideal primo existe un único primo $p \in \mathbb{N}$ al que divide.

Sea $p \in \mathbb{N}$ primo y $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \dots$ la factorización en ideales primos, tomando norma $p^2 = \mathrm{N}(p\mathcal{O}_K) = \mathrm{N}(\mathfrak{p}_1)\,\mathrm{N}(\mathfrak{p}_2)\dots$, hay tres opciones: $\begin{cases} p \text{ inerte} & p\mathcal{O}_K = \mathfrak{p} \\ p \text{ ramifica} & p\mathcal{O}_K = \mathfrak{p}^2 \\ p \text{ descompone} & p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}} \end{cases}$.

No es difícil ver que la ecuación $x^2 - \mathrm{Tr}(\delta_0)x + \mathrm{N}(\delta_0) = 0$ tiene $1 + \left(\frac{d_K}{p}\right)$ soluciones en $\mathbb{Z}/p\mathbb{Z}$, pero también podemos ver que el número de soluciones es 0 si p es inerte, 1 si ramifica y 2 si descompone.

(a) Si p es inerte. Supongamos que existe una solución $x_0 \in \mathbb{Z}$ a la ecuación

$$x_0^2 - \mathrm{Tr}(\delta_0)x_0 + \mathrm{N}(\delta_0) \equiv 0 \pmod{p},$$

entonces $(x_0 - \delta_0)(x_0 - \overline{\delta_0}) = x_0^2 - \mathrm{Tr}(\delta_0)x_0 + \mathrm{N}(\delta_0) \in p\mathcal{O}_K$. Como $p\mathcal{O}_K$ es un ideal primo contiene a un factor de la izquierda, pongamos $\frac{x_0-\delta_0}{p} \in \mathcal{O}_K = \mathbb{Z}[\delta_0]$, pero esto es absurdo.

(b) Si p ramifica o descompone $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Por la parte 4 de 1.9

$$\mathfrak{p} = c(a\mathbb{Z} + (-b + \delta_0)\mathbb{Z}) \qquad \text{y} \qquad \mathrm{N}(p\mathcal{O}_K) = c^2 a,$$

como p es primo debe ser $c = 1$ y $a = p$, luego

$$\mathfrak{p} = p\mathbb{Z} + (-b + \delta_0)\mathbb{Z}, \qquad \bar{\mathfrak{p}} = p\mathbb{Z} + (-b + \overline{\delta_0})\mathbb{Z} = p\mathbb{Z} + (b - \mathrm{Tr}(\delta_0) + \delta_0)\mathbb{Z}.$$

y $x^2 - Tr(\delta_0)x + N(\delta_0) = (x - \delta_0)(x - \overline{\delta_0}) \equiv (x - b)(x - \mathrm{Tr}(\delta_0) + b) \pmod{p}$, por lo tanto, podemos observar que el número de soluciones módulo p a la ecuación es 1 si y solo si $x - b \equiv x - \mathrm{Tr}(\delta_0) + b \pmod{p}$ y 2 en caso contrario.

La condición $x - b \equiv x - \mathrm{Tr}(\delta_0) + b \pmod{p}$ es equivalente a la condición de ramificar, pues

$$\begin{aligned} \mathfrak{p} \subseteq \bar{\mathfrak{p}} \Leftrightarrow & p\mathbb{Z} + (-b + \delta_0)\mathbb{Z} \subseteq p\mathbb{Z} + (b - \mathrm{Tr}(\delta_0) + \delta_0) \\ \Leftrightarrow & \exists k, l \in \mathbb{Z} : \ -b + \delta_0 = kp + l(b - \mathrm{Tr}(\delta_0) + \delta_0. \end{aligned}$$

comparando coeficientes esto ocurre si y sólo si $l = 1$ y $-b = kp + \mathrm{Tr}(\delta_0) - b$, o equivalentemente si $b \equiv \mathrm{Tr}(\delta_0) - b \pmod{p}$.

□

OBSERVACIÓN 1.14. *Si p ramifica o descompone y $\mathfrak{p} \mid p\mathcal{O}_K$ entonces $\mathrm{N}(\mathfrak{p}) = p$. Si p es inerte entonces $\mathrm{N}(p\mathcal{O}_K) = p^2$.*

El grupo de clases de ideales. A continuación definiremos el grupo de clases de ideales, para lo cual requerimos de algunos resultados cuyas pruebas omitiremos, pero que pueden encontrarse en [Cox, §5].

DEFINICIÓN 1.15. Un *ideal fraccional* de $\mathcal{O}_K$ es un $\mathcal{O}_K$-submódulo no nulo $\mathfrak{a}$ de K tal que $d\mathfrak{a} = \{da : \ a \in \mathfrak{a}\}$ está contenido en $\mathcal{O}_K$ para algún $d \in \mathcal{O}_K$ no nulo.

PROPOSICIÓN 1.16. *Los ideales fraccionales son exactamente los $\mathcal{O}_K$-submódulos de K finitamente generados.*

DEFINICIÓN 1.17. Sea I un ideal fraccional, entonces existe $\alpha \in \mathcal{O}_K$ tal que αI es un ideal de $\mathcal{O}_K$. Se define la norma de I como $\mathrm{N}(I) := \frac{\mathrm{N}(\alpha I)}{\mathrm{N}(\alpha)}$, y el discriminante como $\Delta(I) := \det \begin{pmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{pmatrix}^2$, donde (α, β) es una $\mathbb{Z}$-base de I.

DEFINICIÓN 1.18. Un ideal fraccional $\mathfrak{a}$ se dice *principal* si existe $b \in K^*$, tal que $\mathfrak{a} = b\mathcal{O}_K$. Denotamos por $\mathrm{Pr}(\mathcal{O}_K)$ al conjunto de ideales fraccionales principales.

El conjunto de ideales fraccionales es un grupo libre generado por los ideales primos de $\mathcal{O}_K$, es decir que tiene factorización única en ideales primos:

TEOREMA 1.19. *El conjunto* $\mathrm{Fr}(\mathcal{O}_K)$ *de ideales fraccionarios de* $\mathcal{O}_K$ *es un grupo.*

TEOREMA 1.20. *Dado* $\mathfrak{a}$ *un ideal fraccional de* $\mathcal{O}_K$*, puede escribirse de forma única (salvo permutación) como producto de ideales primos distintos elevados a exponentes enteros.*

DEFINICIÓN 1.21. Se define el *grupo de clases de ideales* de K como el grupo cociente $\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Fr}(\mathcal{O}_K)/\mathrm{Pr}(\mathcal{O}_K)$. El *número de clases* del cuerpo cuadrático K es el orden de este grupo, lo denotamos por h_K.

2. Formas cuadráticas binarias

DEFINICIÓN 1.22. Dada una forma cuadrática binaria $f(x, y) = ax^2 + bxy + cy^2$ de discriminante $d_f = b^2 - 4ac$, se dice que es *primitiva* si $\mathrm{mcd}(a, b, c) = 1$.

DEFINICIÓN 1.23. Sea $m \in \mathbb{Z}$, se dice que una forma cuadrática binaria $f(x, y)$ representa m si existen $x, y \in \mathbb{Z}$ no ambos nulos tales que $m = f(x, y)$. Si además x e y son coprimos entonces se dice que f representa propiamente a m.

Si $f(x, y)$ es una forma cuadrática binaria y consideramos un cambio de variables del tipo

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \qquad \alpha\delta - \beta\gamma = \pm 1$$

entonces bajo este cambio de variable f sigue representando los mismos enteros.
Cuando el discriminante d_f de una forma $f(x, y)$ es positivo, esta representa enteros positivos y negativos, y se le llama *indefinida*. Cuando por el contrario el discriminante es negativo, como $4af(x, y) = (2ax + by)^2 - dy^2$, f representa sólo enteros del mismo signo que a. En el segundo caso, si $a > 0$ la forma es *definida positiva* y si $a < 0$ es *definida negativa*.

DEFINICIÓN 1.24. Dos formas $f(x, y)$ y $g(x, y)$ son *equivalentes* si existen $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ tales que $\alpha\delta - \beta\gamma = \pm 1$ y $f(x, y) = g(\alpha x + \beta y, \gamma x + \delta y)$. Si $\alpha\delta - \beta\gamma = 1$ entonces son *propiamente equivalentes.*

OBSERVACIÓN 1.25. *Dos formas equivalentes* f *y* g *tienen el mismo discriminante:*

$$d_f = (\alpha\delta - \beta\gamma) d_g (\alpha\delta - \beta\gamma) = d_g.$$

Se puede ver fácilmente que ser equivalentes y propiamente equivalentes son relaciones de equivalencia. Al conjunto de clases de equivalencia propia de formas primitivas definidas positivas de discriminante D le llamaremos $Cl(D)$ y denotaremos por $h(D)$ al número de clases $|Cl(D)|$.

Supongamos que $D \equiv 0, 1 \pmod 4$ es negativo y (a, b, c) y (a', b', c') son dos formas tales que $\operatorname{mcd}\left(a, a', \frac{b+b'}{2}\right) = 1$. Se define la *composición de Dirichlet* de (a, b, c) y (a', b', c') como sigue.

$$(a, b, c) \circ (a', b', c') = \left(aa', B, \frac{B^2 - D}{4aa'}\right),$$

donde $B \in \mathbb{Z}$ satisface

$$(a)\ B \equiv b \pmod{2a} \qquad (b)\ B \equiv b' \pmod{2a'} \qquad (c)\ B^2 \equiv D \pmod{4aa'}.$$

La composición de Dirichlet induce una operación binaria en $Cl(D)$ que le da estructura de grupo abeliano.

Definición 1.26. Una forma $f(x, y) = ax^2 + bxy + cy^2$ primitiva y definida positiva es *reducida* si

$$|b| \leqslant a \leqslant c \text{ y si } b = a \text{ ó } a = c \text{ entonces } b > 0.$$

Teorema 1.27. *Toda forma primitiva y definida positiva es propiamente equivalente a una única forma reducida.*

Demostración. Ver [Cox, Theorem 2.8]. □

Proposición 1.28. *Sea $f(x, y) = ax^2 + bxy + cy^2$ una forma reducida definida positiva de discriminante $d_f < 0$, entonces:*

(a) $a \leqslant \sqrt{\frac{-d_f}{3}}$

(b) $\frac{\sqrt{-d_f}}{2} \leqslant c \leqslant \frac{-d_f}{3a}$.

(c) *Si $f(x, y) = m$ con $m < c$, entonces $y = 0$.*

Demostración.

(a) $-d_f = 4ac - b^2 \geqslant 4a^2 - a^2 = 3a^2$, entonces $a \leqslant \sqrt{\frac{-d_f}{3}}$.

(b) $-d_f = 3ac + ac - a^2 \Rightarrow -d_f \geqslant 3ac$, por otro lado $c^2 \geqslant ca = \frac{b^2 - d_f}{4} \geqslant \frac{-d_f}{4}$, luego $c \geqslant \frac{\sqrt{-d_f}}{2}$.

(c) Sea $m = f(x, y)$ un entero representado por f, tal que $y \neq 0$.

Si $|y| \leqslant |x|$ entonces $|bxy| \leqslant ax^2$, luego

$$m = f(x, y) = ax^2 + bxy + cy^2 \geqslant ax^2 - ax^2 + cy^2 = cy^2 \geqslant c.$$

Si $|x| \leqslant |y|$ entonces $|bxy| \leqslant c|xy| \leqslant c(y^2 - 1)$, luego

$$m = f(x, y) = ax^2 + bxy + cy^2 \geqslant ax^2 - c(y^2 - 1) + cy^2 = ax^2 + c \geqslant c.$$

□

Observación 1.29. *Sea $f(x, y) = ax^2 + bxy + cy^2$, la única representación propia con $y = 0$ es $f(1, 0) = a$.*

TEOREMA 1.30. *Sea $T = \#\{p \text{ primo } : p \mid d_K\}$, entonces $2^{T-1} \mid h_K$.*

DEMOSTRACIÓN. Ver Prop. 3.11 en [Cox], la cual establece que $C(d)$ tiene exactamente $2^{\mu-1}$ elementos de orden menor o igual a 2, donde μ viene dado por una tabla que depende de d (mód 4) y d (mód 8).
Como en nuestro caso d_K es fundamental, la proposición mencionada establece que $\mu = T$. Como además el grupo $\mathrm{Cl}(d_K)$ es abeliano, el subconjunto de elementos de orden menor o igual a 2 es un subgrupo y por el Teorema de Lagrange $2^{T-1} \mid h_K$. □

3. Correspondencia entre $\mathrm{Cl}(d_K)$ y $\mathrm{Cl}(\mathcal{O}_K)$

Como es esperable, el número de clases de ideales de un cuerpo cuadrático K de discriminante d_K coincide con el número de clases de formas primitivas definidas positivas de discriminante d_K. A continuación veremos eso.

LEMA 1.31. *Sea $I \neq (0)$ un ideal fraccionario en un cuerpo cuadrático K, entonces*

$$\Delta(I) = \mathrm{N}(I)^2 d_K.$$

DEMOSTRACIÓN. Sabemos que $\mathcal{O}_K = [1, w_K]$, donde $w_K = \frac{d_K + \sqrt{d_K}}{2}$, y que existe $n \in \mathbb{N}$ tal que nI es un ideal de $\mathcal{O}_K$. Sea (α, β) una $\mathbb{Z}-$base de αI, entonces $\left(\frac{\alpha}{n}, \frac{\beta}{n}\right)$ es una $\mathbb{Z}$-base de I.
Además, existen $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ tales que $\alpha = a_1 + a_2 w_K$, $\beta = b_1 + b_2 w_K$, por lo tanto

$$det \begin{pmatrix} \frac{\alpha}{n} & \frac{\beta}{n} \\ \frac{\overline{\alpha}}{n} & \frac{\overline{\beta}}{n} \end{pmatrix}^2 = \frac{1}{n^4} \det \begin{pmatrix} 1 & w_K \\ 1 & \overline{w_K} \end{pmatrix}^2 \det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}^2 = d_K \frac{(a_1 b_2 - a_2 b_1)^2}{n^4}.$$

El término $\frac{(a_1 b_2 - a_2 b_1)^2}{n^4}$ es $\mathrm{N}(I)^2$, esto se deduce de la siguiente propiedad para grupos abelianos:
Si $G = \mathbb{Z} \oplus \mathbb{Z}$ y H es un subgrupo generado por $(a_1, a_2), (b_1, b_2)$ linealmente independientes, entonces

$$|G/H| = |a_1 b_2 - a_2 b_1|,$$

tomando $G = \mathcal{O}_K$ y $H = nI$.

□

Del Teorema 1.27 se puede deducir el siguiente,

TEOREMA 1.32. *El número $h(D)$ de clases de formas primitivas definidas positivas de discriminante D es finito e igual al número de formas reducidas de discriminante D.*

Con lo anterior estamos en condiciones de ver el teorema que establece la correspondencia entre $\mathrm{Cl}(\mathcal{O}_K)$ y $\mathrm{Cl}(d_K)$.

TEOREMA 1.33. *Sea K un cuerpo cuadrático imaginario de discriminante d_K.*

(1) *Si $f(x, y) = ax^2 + bxy + cy^2$ es una forma primitiva definida positiva de discriminante d_K, entonces*

$$I = \left[a, \frac{-b + \sqrt{d_K}}{2}\right] = \left\{ma + n\frac{-b + \sqrt{d_K}}{2} : \ m, n \in \mathbb{Z}\right\}$$

es un ideal de $\mathcal{O}_K$.

(2) *El mapa* $\phi : \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}(d_K)$ *dado por* $\phi([I]) = \left[\frac{\mathrm{N}(\alpha x-\beta y)}{\mathrm{N}(I)}\right]$, *donde* $[\alpha, \beta]$ *es una* $\mathbb{Z}-$*base de* I *orientada de forma positiva (esto quiere decir que* $\alpha\overline{\beta}-\overline{\alpha}\beta > 0$*), es un isomorfismo cuyo inverso está dado por el mapa*

$$[f(x, y)] \mapsto \left[\left[a, \frac{-b+\sqrt{d_K}}{2}\right]\right].$$

En consecuencia $h_K = h(d_K)$.

Demostración.

(1) Sabemos que $\mathcal{O}_K = \left[1, \frac{D_K+\sqrt{D_K}}{2}\right]$ por lo que basta ver:
   (a) $a\frac{d_K+\sqrt{d_K}}{2} \in I$
   (b) $\left(\frac{-b+\sqrt{d_K}}{2}\right)\left(\frac{d_K+\sqrt{d_K}}{2}\right) \in I$

   Veamos esto,
   (a) $a\frac{d_K+\sqrt{d_K}}{2} = \frac{ad_K+a\sqrt{d_K}}{2} = \frac{ad_K+ab+a(-b+\sqrt{d_K})}{2} = a\frac{d_K+b}{2} + a\frac{-b+\sqrt{d_K}}{2}$.
   Como $a \in \mathbb{Z}$ y $d_K \equiv b^2 \pmod 4 \Rightarrow d_K \equiv b \pmod 2$, entonces $a\frac{d_K+b}{2} \in \mathbb{Z}$ y por lo tanto $a\frac{d_K+\sqrt{d_K}}{2} \in I$.
   (b) $\left(\frac{-b+\sqrt{d_K}}{2}\right)\left(\frac{d_K+\sqrt{d_K}}{2}\right) = \frac{-bD+\sqrt{d_K}d_K-b\sqrt{d_K}+d_K}{4} = \frac{d_K-b^2}{4} + \frac{(d_K-b)(-b+\sqrt{d_K})}{4}$.
   Nuevamente, como $d_K \equiv b^2 \pmod 4$ entonces $\left(\frac{-b+\sqrt{d_K}}{2}\right)\left(\frac{d_K+\sqrt{d_K}}{2}\right) \in I$.

(2) Para ver que ϕ está bien definida hay que ver los siguientes tres items:
   (a) $\frac{\mathrm{N}(\alpha x+\beta y)}{\mathrm{N}(I)}$ es una forma cuadrática primitiva definida positiva de discriminante d_K.
   (b) El resultado es independiente de la base (α, β) tomada.
   (c) La imagen de una clase de ideales consiste en formas equivalentes.

   Veámoslo.
   (a)

$$\frac{\mathrm{N}(\alpha x - \beta y)}{\mathrm{N}(I)} = \frac{(\alpha x - \beta y)(\overline{\alpha} x + \overline{\beta} y)}{\mathrm{N}(I)} = \frac{Ax^2 - Bxy + Cy^2}{\mathrm{N}(I)},$$

   donde $A = \alpha\overline{\alpha}, B = -\beta\overline{\alpha} - \overline{\beta}\alpha, C = \beta\overline{\beta}$.
   Como $\alpha, \beta, \alpha + \beta \in I$ su norma es divisible por $\mathrm{N}(I)$, de esta forma $\mathrm{N}(I)$ divide a A, B, C y por lo tanto $\frac{\mathrm{N}(\alpha x-\beta y)}{\mathrm{N}(I)}$ es una forma cuadrática binaria con coeficientes enteros. El discriminante de $q(x, y)$ es $\frac{B^2-4AC}{\mathrm{N}(I)^2} = d_K$ por el lema previo, y resta ver que es una forma primitiva.
   Recordemos que $d_K = m$ con $m \equiv 1 \pmod 4$ o $d_K = 4m$ con $m \not\equiv 1 \pmod 4$, donde m es un entero libre de cuadrados, por lo tanto el único posible divisor común de A, B, C es 2 en el segundo caso. Como $4|d_K \Rightarrow \left(\frac{d_K}{2}\right) = 0$, entonces $(2) = t^2$, luego

$$(\alpha) = t^u\mathfrak{a}(\beta) = t^v\mathfrak{b}I = t^{\min(u,v)}J$$

   donde $\mathfrak{a}, \mathfrak{b}$ y J son coprimos con (2), luego $A = \frac{\mathrm{N}(\alpha)}{\mathrm{N}(I)}$ o $B = \frac{\mathrm{N}(\beta)}{\mathrm{N}(I)}$ es impar.

(b) Si $\{\alpha,\beta\}$ y $\{\gamma,\delta\}$ son dos $\mathbb{Z}-$bases positivamente orientadas de I, entonces

$$\alpha = p\gamma + q\delta \qquad \beta = r\gamma + s\delta \qquad p,s,q,r \in \mathbb{Z}$$

y se ve fácilmente que $ps - qr = 1$.

(c) Si $c \in K^*$, entonces $\{c\alpha, c\beta\}$ es una base de cI y $\frac{\mathrm{N}(xc\alpha - yc\beta)}{\mathrm{N}(cI)} = \frac{\mathrm{N}(c)\,\mathrm{N}(x\alpha - y\beta)}{\mathrm{N}(c)\,\mathrm{N}(I)}$, por lo tanto ϕ está bien definida.

Ahora queremos ver que ϕ es biyectiva.

Observación 1.34. *Si I es un ideal fraccional de $\mathcal{O}_K$ con $\mathbb{Z}-$base $\{\alpha,\beta\}$ entonces $\phi([I]) = [ax^2 + bxy + cy^2]$ donde*

$$a = \frac{\alpha\overline{\alpha}}{\mathrm{N}(I)} \qquad b = \frac{-\alpha\overline{\beta} - \overline{\alpha}\beta}{\mathrm{N}(I)} \qquad c = \frac{\beta\overline{\beta}}{\mathrm{N}(I)}$$

El mapa $\psi : Cl(d_K) \to Cl(\mathcal{O}_K)$ dado por $[f(x,y)] = \left[\left[a, \frac{-b+\sqrt{d_K}}{2}\right]\right]$ también está bien definido, veamos esto.

Sean $f(x,y) = ax^2 + bxy + cy^2$ y $g(x,y) = a'x^2 + b'xy + c'y^2$ dos formas equivalentes, esto quiere decir que $f(x,y) = g(px + qy, rx + sy)$ para ciertos p,q,r,s enteros que satisfacen $ps - qr = 1$. Sean τ y τ' las raíces en el semiplano superior de $f(x,1)$ y $g(x,1)$ respectivamente, como $a, a' \geqslant 0$ entonces $\tau = \frac{-b+\sqrt{d_K}}{2a}$ y $\tau' = \frac{-b'+\sqrt{d_K}}{2a'}$.

Entonces $\left[a, \frac{-b+\sqrt{d_K}}{2}\right] = a[1,\tau]$, y por lo tanto para ver que ψ está bien definida basta ver que $f \sim g \Leftrightarrow [1,\tau] = \lambda[1,\tau']$, lo cual veremos en dos pasos:

(1)$f \sim g \Leftrightarrow \tau' = \frac{p\tau+q}{r\tau+s}$:

$$0 = f(\tau,1) = g(p\tau + q, r\tau + s) = (r\tau + s)^2 g\left(\frac{p\tau+q}{r\tau+s}, 1\right)$$

Además $\Im\frac{p\tau+q}{r\tau+s} = (ps - qr)|r\tau + s|^2\Im\tau$ y por lo tanto τ y τ' están en el mismo semiplano.

(2)$\tau' = \frac{p\tau+q}{r\tau+s} \Leftrightarrow [1,\tau] = \lambda[1,\tau']$, *donde* $\lambda = r\tau + s \in K^*$*:*

$$\lambda[1,\tau] = [r\tau + s, p\tau + q] = [1,\tau] \text{ porque } ps - qr = 1.$$

Recíprocamente, si $\lambda[1,\tau'] = [1,\tau]$ entonces $\lambda = r\tau + s$ y $\lambda\tau' = p\tau + q$ y debe ser $ps - rq = 1$.

Por último queremos ver que ϕ y ψ son inversos.

Sea $f(x,y) = ax^2 + bxy + cy^2$ una forma cuadrática definida positiva de discriminante d_K e $I = \left[a, \frac{-b+\sqrt{d_K}}{2}\right]$. Entonces $\mathrm{N}(I) = \mathrm{N}([a, a\tau])$, y como $[a, a\tau]$ tiene índice a en $[1, a\tau] = \mathcal{O}_K$ resulta $\mathrm{N}(I) = a$. Luego,

$$\begin{aligned}\phi([I]) &= \frac{a^2}{a}x^2 - \frac{-b + \sqrt{D} - b - \sqrt{d_K}}{2a}xy + \left(\frac{-b+\sqrt{d_K}}{2}\right)\left(\frac{-b-\sqrt{d_K}}{2}\right)y^2 \\ &= ax^2 + bxy + \frac{b^2 - d_K}{4a} \\ &= ax^2 + bxy + cy^2.\end{aligned}$$

Por otra parte, si I es un ideal fraccional, podemos escribirlo como $I = [\alpha, \beta]$ con $\alpha > 0$ y $\beta = k + \frac{d+\sqrt{d_K}}{2}$, y como vimos antes $\mathrm{N}(I) = \alpha$.
Luego $\phi([I]) = ax^2 + bxy + cy^2$ donde

$$a = \frac{\alpha^2}{\alpha} = \alpha \qquad b = -2k - d_K \qquad c = \frac{k^2 + kD + (d_K^2 - d_K)}{4\alpha}$$

Finalmente $\psi \circ \phi([I]) = \left[\left[\alpha, \frac{2k+d_K+\sqrt{d_K}}{2}\right]\right] = [[\alpha, \beta]]$.

□

4. Las funciones ζ y ζ_K

La $L-$serie de Dirichlet asociada al carácter χ es $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, que converge para $\Re(s) > 1$. En particular tenemos la función zeta de Riemann, que es la L-serie asociada al carácter trivial: $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Definición 1.35. La función zeta del cuerpo cuadrático imaginario K se define como $\zeta_K(s) := \zeta(s)L(s, \chi)$, donde χ es el símbolo de Kronecker $\left(\frac{-d_K}{\cdot}\right)$.

Definición 1.36. La función zeta parcial de una clase de ideales $\mathcal{C}$ se define como $\zeta(\mathcal{C}, s) := \sum_{\mathfrak{c} \in \mathcal{C}} \mathrm{N}(\mathfrak{c})^{-s}$.

Existe $\mathfrak{a}' \in \mathcal{C}^{-1}$ tal que todo $\mathfrak{a} \in \mathcal{C}$ cumple que $\mathfrak{a}\mathfrak{a}' = \alpha\mathcal{O}_K$, $\alpha \in K$, tomando norma: $\mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{a}') = \mathrm{N}(\alpha\mathcal{O}_K) = \mathrm{N}(\alpha)$, luego

$$\zeta(\mathcal{C}, s) = \mathrm{N}(\mathfrak{a}')^s \sum_{\alpha : \mathfrak{a}' | \alpha\mathcal{O}_K} \mathrm{N}(\alpha)^{-s}.$$

Ahora, $\alpha\mathcal{O}_K = \beta\mathcal{O}_K$ si y sólo si $\alpha = b\beta$, donde $b \in \mathcal{O}_K$ satisface que $\mathrm{N}(b) = 1$. Y por la correspondencia vista en la parte anterior,

$$\zeta(\mathcal{C}, s) = \sum_{\alpha:\ a' | \alpha\mathcal{O}_K} \frac{\mathrm{N}(a')^s}{\mathrm{N}(\alpha)} = w^{-1} \sum_{(m,n) \in \mathbb{Z}^2 \setminus (0,0)} q(m, n)^{-s}, \tag{1}$$

donde w^{-1} es la cantidad de unidades en $\mathcal{O}_K$. Si $d_K < -4$ entonces $w = 2$, para $d_K = 4$, $w = 4$ y para $d_K = 3$, $w = 6$.
Para $d_K < 4$ tenemos lo siguiente,

$$\zeta_K(s) = \prod_p (1 - p^{-s})^{-1} \prod_p (1 - \chi(p)p^{-s})^{-1} \tag{2}$$

$$= \prod_{p:\chi(p)=1} (1 - p^{-s})^{-2} \prod_{p:\chi(p)=0} (1 - p^{-s})^{-1} \prod_{p:\chi(p)=-1} (1 - p^{-s})^{-1}(1 + p^{-s})^{-1} \tag{3}$$

$$= \prod_{\mathfrak{p}} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-s} \tag{4}$$

$$= \sum_{\mathfrak{n} \text{ ideal de } \mathcal{O}_K} \mathrm{N}(\mathfrak{n})^{-s} \tag{5}$$

$$= \sum_{\mathcal{C}\in Cl(\mathcal{O}_K)} \sum_{\mathfrak{c}\in\mathcal{C}} \mathrm{N}(\mathfrak{c})^{-s} \tag{6}$$

$$= \sum_{q\in Q^{red}_{d_K}} \frac{1}{2} \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} q(m,n)^{-s} \tag{7}$$

$$= \sum_{q\in Q^{red}_{d_K}} \left(\sum_{m\in\mathbb{N}} q(m,0)^{-s} + \sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} q(m,n)^{-s} \right) \tag{8}$$

$$= \sum_{q\in Q^{red}_{d_K}} \left(a(q)^{-s} \sum_{m\in\mathbb{N}} m^{-2s} + \sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} q(m,n)^{-s} \right) \tag{9}$$

$$= \sum_{q\in Q^{red}_{d_K}} \left(a(q)^{-s}\zeta(2s) + \sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} q(m,n)^{-s} \right), \tag{10}$$

donde

(4) se obtiene a partir de (3) aplicando la observación 1.14.

(5) se sigue de la factorización única en ideales de $\mathcal{O}_K$.

(7) es la igualdad 1, observar que en este caso $w = 2$.

En (9) usamos que $q(m,-n) = q(-m,n)$ y separamos en representaciones con $y = 0$ y con $y \neq 0$.

Si ahora queremos calcular $\frac{\zeta_K(s)}{\zeta(2s)}$ tenemos lo siguiente

$$\frac{\zeta_K(s)}{\zeta(2s)} = \prod_p \frac{(1-p^{-2s})}{(1-p^{-s})(1-\chi(p)p^{-s})} = \prod_p \frac{1+p^{-s}}{(1-\chi(p)p^{-s})},$$

y por otra parte

$$\begin{aligned}
\frac{\zeta_K(s)}{\zeta(2s)} &= \sum_{q\in Q^{red}_{d_K}} \left(a(q)^{-s} + \frac{1}{\zeta(2s)} \sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} q(m,n)^{-s} \right) \\
&= \sum_{q\in Q^{red}_{d_K}} \left(a(q)^{-s} + \frac{1}{\zeta(2s)} \sum_{d=1}^{\infty} \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{N}^* \\ \mathrm{mcd}(m,n)=d}} q(m,n)^{-s} \right) \\
&= \sum_{q\in Q^{red}_{d_K}} \left(a(q)^{-s} + \frac{1}{\zeta(2s)} \sum_{d=1}^{\infty} d^{-2s} \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{N}^* \\ \mathrm{mcd}(m,n)=1}} q(m,n)^{-s} \right) \\
&= \sum_{q\in Q^{red}_{d_K}} \left(a(q)^{-s} + \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{N}^* \\ \mathrm{mcd}(m,n)=1}} q(m,n)^{-s} \right).
\end{aligned}$$

PROPOSICIÓN 1.37.

(a) *Si p descompone en $\mathcal{O}_K$ entonces* $p^h \geqslant \frac{d_K}{4}$.

(b) *Si escribimos* $\frac{\zeta_K(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \nu_n n^{-s}$ *entonces* $\sum_{n \leqslant \frac{\sqrt{d_K}}{2}} \nu_n \leqslant h$.

DEMOSTRACIÓN.

(a) Como p descompone existen ideales $\mathfrak{p} \neq \bar{\mathfrak{p}}$ tales que $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ y $\mathrm{N}(\mathfrak{p}) = \mathrm{N}(\bar{\mathfrak{p}}) = p$. $\mathfrak{p}^h$ es un ideal principal de $\mathcal{O}_K$ y por lo tanto está generado por un elemento de la forma $\frac{a+b\sqrt{d_K}}{2}$, pues recordemos que $\mathcal{O}_K = [1, \frac{d_K+\sqrt{d_K}}{2}]$. Como $\mathfrak{p} \neq \bar{\mathfrak{p}}$ tenemos que $b \neq 0$, luego

$$p^h = \mathrm{N}(\mathfrak{p})^h = \frac{a^2 + |d_K| b^2}{4} \geqslant \frac{|d_K|}{4}.$$

(b) Por 1.28 sabemos que una forma $q(x, y)$ representa (propiamente) a $a(q)$, $c(q)$ y enteros mayores a $c(q) \geqslant \frac{\sqrt{|d_K|}}{2}$. Como $d_K < -4$ es un discriminante fundamental, es decir $d_K \equiv 1 \pmod 4$ y libre de cuadrados o $d_K = 4m$ con m libre de cuadrados, entonces $\frac{\sqrt{d_K}}{2}$ no es entero y la desigualdad es estricta: $c(q) > \frac{\sqrt{|d_K|}}{2}$. Vimos que

$$\frac{\zeta_K(s)}{\zeta(2s)} = \sum_{q \in Q_{d_K}^{red}} \left(a(q)^{-s} + \sum_{\substack{(m,n) \in \mathbb{Z} \times \mathbb{N}^* \\ \mathrm{mcd}(m,n)=1}} q(m,n)^{-s} \right), \tag{11}$$

por la desigualdad anterior los elementos de la forma $q(m, n)^{-s}$ corresponderían a sumandos n^{-s} con $n \geqslant c(q) > \frac{\sqrt{|d_K|}}{2}$. Entonces tenemos lo siguiente:

$$\sum_{n \leqslant \frac{\sqrt{|d_K|}}{2}} \nu_n n^{-s} = \sum_{\substack{q \in Q_{d_K}^{red} \\ a(q) \leqslant \frac{\sqrt{|d_K|}}{2}}} a(q)^{-s} = \sum_{n \leqslant \frac{\sqrt{|d_K|}}{2}} \#\{q : a(q) = n\} n^{-s},$$

es decir

$$\sum_{n \leqslant \frac{\sqrt{|d_K|}}{2}} \nu_n = \#\left\{ q : a(q) \leqslant \frac{\sqrt{|d_K|}}{2} \right\} \leqslant h. \tag{12}$$

De hecho, por 1.28 podemos observar que las formas que no están en $\left\{ q : a(q) \leqslant \frac{\sqrt{|d_K|}}{2} \right\}$ son exactamente aquellas tales que $\frac{\sqrt{|d_K|}}{2} < a(q) \leqslant \sqrt{\frac{|d_K|}{3}}$.

□

OBSERVACIÓN 1.38. *Por 1.37* (b) *tenemos que*

$$\frac{\zeta_K(s)}{\zeta(2s)} = \prod_p \left(\frac{1 + p^{-s}}{1 - \chi(p) p^{-s}} \right) = \sum_{n=0}^{\infty} \nu_n n^{-s},$$

donde

$$\sum_{n \leqslant \frac{\sqrt{|d_K|}}{2}} \nu_n \leqslant h.$$

Podemos ver entonces que el hecho de que el número de clases $h = h_K$ sea "pequeño" para un cuerpo K de discriminante "grande" se traduce en que hay muchos primos pequeños tales que $\frac{1+p^{-s}}{1-\chi(p)p^{-s}} = 1$. Esto igualdad se da si y sólo si $\chi(p) = 1$, es decir, si p es inerte.

Si definimos la función de Liouville $\lambda : \mathbb{N}^* \to \{-1, 1\}$ como la función completamente multiplicativa tal que $\lambda(p) = -1$ para p primo, entonces lo anterior se traduce como "hay muchos primos pequeños tales que $\lambda(p) = \chi(p)$".

Capítulo 2

Formas modulares de peso 2

1. Formas modulares de peso k para subgrupos de congruencia.

A $G = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ se le llama grupo modular, actúa en $\hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ de la siguiente forma:

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

Es fácil ver que en el semiplano superior $\mathcal{H} : \{z \in \mathbb{C} : \Im(z) > 0\}$ se satisface que $\Im\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{\Im(z)}{|cz+d|^2}$, por lo tanto $\mathcal{H}$ es estable bajo la acción del grupo modular.

Definición 2.1. Sea $k \in \mathbb{Z}$. Una forma modular de peso k para $\mathrm{SL}_2(\mathbb{Z})$ es una función $f : \mathcal{H} \to \mathbb{C}$ que satisface

(1) f es holomorfa en $\mathcal{H}$.

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

(3) f es holomorfa en ∞, esto quiere decir que existe $\lim_{Im(z)\to\infty} f(z)$.

Observación 2.2. $\mathrm{SL}_2(\mathbb{Z})$ *es generado por* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *y* $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *y por lo tanto la condición* (2) *en 2.1 se satisface si y sólo si* $f(z+1) = f(z)$ *y* $f(-1/z) = z^k f(z)$.
En particular, las formas modulares sobre $\mathrm{SL}_2(\mathbb{Z})$ *son* $\mathbb{Z}-$*periódicas, lo que implica que admiten una expansión de Fourier de la forma* $f(z) = \sum_{n=-\infty}^{\infty} a_n q^n$, *donde* $q = e^{2\pi i z}$. *Como son funciones holomorfas en* ∞ *se satisface que* $a_n = 0$ *para* $n < 0$.

Definición 2.3. Sea $f(z) = \sum_{n=0}^{\infty} a_n q^n$ una forma modular de peso k en $\mathrm{SL}_2(\mathbb{Z})$, se dice *cuspidal* si $a_0 = 0$ y *normalizada* si $a_1 = 1$.

Es fácil ver que el conjunto de formas modulares de peso k, denotado por $M_k(\mathrm{SL}_2(\mathbb{Z}))$ forma un espacio vectorial complejo. La condición de ser holomorfa en ∞ hace que la dimensión de este espacio vectorial sea finita. Por otra parte, el producto de una forma modular de peso k y otra de peso l es una forma modular de peso $k+l$.

Las formas cuspidales de peso k forman un subespacio vectorial de $M_k(\mathrm{SL}_2(\mathbb{Z}))$ al que denotamos $S_k(\mathrm{SL}_2(\mathbb{Z}))$. Observar que la condición de ser cuspidal es equivalente a $\lim_{\Im(z)\to\infty} f(z) = 0$.

Sea N un entero positivo. El subgrupo principal de congruencias de nivel N es

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

DEFINICIÓN 2.4. Un subgrupo Γ de $\mathrm{SL}_2(\mathbb{Z})$ es un *subgrupo de congruencia* si existe $N \in \mathbb{Z}^+$ tal que $\Gamma(N) \subseteq \Gamma$. N es el *nivel de congruencia* de Γ.

OBSERVACIÓN 2.5. *Todo subgrupo de congruencia tiene índice finito, pues* $\Gamma(N)$ *es el kernel del homomorfismo natural* $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$*, luego* $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N)$ *es isomorfo a* $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Dos tipos de subgrupos de congruencia importantes son Γ_0 y Γ_1:

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

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

Análogo a 2.1 se puede definir una forma modular de peso k en un subgrupo de congruencia Γ.

DEFINICIÓN 2.6. Sea $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Definimos el operador $[\gamma]_k$ en las funciones $f : \mathcal{H} \to \mathbb{C}$ como

$$f[\gamma]_k(z) := (cz + d)^{-k} f(\gamma(z)).$$

DEFINICIÓN 2.7. $f : \mathcal{H} \to \mathbb{C}$ es una forma modular de peso k para Γ si

(1) f es holomorfa en $\mathcal{H}$.

(2) $f(\gamma(z)) = (cz + d)^k f(z)$ para $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

(3) $f[\gamma]_k(z) := (cz + d)^{-k} f(z)$ es holomorfa en ∞ para toda $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Si además $f[\gamma]_k$ tiene coeficiente de Fourier $a_0 = 0$ para toda $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ entonces se dice que f es *cuspidal*.

La tercera condición en la definición previa no permite asociar una única expansión de Fourier a f. Si por ejemplo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ lleva ∞ en s racional , y $\beta := \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$, entonces $\pm\gamma\beta$ también lo hace. Además $f[\pm\gamma\beta](z) = (\pm 1)^k f[\gamma](z + j)$, por lo tanto $f[\gamma]$ y $f[\gamma\beta]$ son ambas holomorfas en ∞ pero pueden tener expansión de Fourier distintas. A pesar de esto se puede observar que la definición de cuspidal está bien dada y al conjunto de formas cuspidales de peso k en un subgrupo de congruencia Γ lo denotamos por $S_k(\Gamma)$. Como antes, el conjunto de formas modulares de peso k en Γ, denotado por $M_k(\Gamma)$, forma un espacio vectorial complejo de dimensión finita y $S_k(\Gamma)$ es un subespacio vectorial.

OBSERVACIÓN 2.8. $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$*, y por lo tanto*

$$M_k(\Gamma_0(N)) \subset M_k(\Gamma_1(N)).$$

2. Operadores de Hecke

A continuación introduciremos resumidamente dos tipos de operadores en $M_k(\Gamma_1(N))$ que serán fundamentales más adelante, al asociar L-series a las funciones modulares y ver algunas de sus propiedades.

Sean Γ_1 y Γ_2 dos subgrupos de congruencia en $\mathrm{SL}_2(\mathbb{Z})$ y $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. El conjunto $\Gamma_1\alpha\Gamma_2$ es una clase lateral doble y el grupo Γ_1 actúa en $\Gamma_1\alpha\Gamma_2$ por multiplicación a izquierda, con lo cual obtenemos una partición $\Gamma_1\alpha\Gamma_2 = \cup_j \Gamma_1\beta_j$, donde los β_j son representantes de las órbitas.

Vamos a extender la definición 2.6 para $\gamma \in \mathrm{GL}_2^+(\mathbb{Z})$.

Definición 2.9. Sea $f : \mathcal{H} \to \mathbb{C} \in M_k(\Gamma(N))$ y $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{Z})$, definimos

$$f[\gamma]_k(z) := \det(\gamma)^{k-1}(cz+d)^{-k} f(\gamma z).$$

Sean Γ_1 y Γ_2 dos subgrupos de congruencia de $\mathrm{SL}_2(\mathbb{Z})$, y $\{\beta_j\} \subset \Gamma_1\gamma\Gamma_2$ un conjunto de representantes de las órbitas bajo la acción de Γ_1, definimos

$$f[\Gamma_1\gamma\Gamma_2]_k(z) := \sum_j f[\beta_j]_k.$$

Observación 2.10. *$\Gamma_1(N)$ es normal en $\Gamma_0(N)$ ya que es el kernel del mapa $\psi : \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$ dado por $\psi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = d \pmod N$. El mapa anterior también es sobreyectivo, por lo que induce un isomorfismo $\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^*$.*

Es fácil ver que

$$\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) = \left\{ \gamma \in \mathrm{M}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix} \pmod N \text{ y } \det\gamma = p \right\}.$$

Cuando $p \mid N$ un conjunto de representantes consiste en $\beta_j = \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$ $0 \leqslant j < p$.

En caso de que $p \nmid N$ hay una coclase extra, un representante es $\beta = \begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ donde $mp - Nn = 1$. Para mas detalles ver [D-S, §5].

Definición 2.11. Sea d tal que $mcd(d, N) = 1$, un operador de Hecke del primer tipo u operador diamante es

$$\langle d \rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N)) \qquad \text{dado por} \qquad \langle d \rangle f = f[\gamma]_k,$$

para cualquier $\gamma = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$ tal que $\delta \equiv d \pmod N$.

Definición 2.12. Para p primo, se definen los operadores de Hecke del segundo tipo

$$T_p : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N)) \qquad T_p f = f\left[\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)\right]_k.$$

Proposición 2.13. *Los operadores de Hecke están bien definidos y conmutan entre sí,*

(1) $\langle d \rangle T_p = T_p \langle d \rangle$.
(2) $\langle d \rangle \langle e \rangle = \langle e \rangle \langle d \rangle = \langle de \rangle$.
(3) $T_p T_q = T_q T_p$.

Demostración. Ver [D-S] 5.2.4. □

DEFINICIÓN 2.14. Sea $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ un carácter, definimos el espacio $M_k(N,\chi)$ como

$$M_k(N,\chi) = \{f \in M_k(\Gamma_1(N)) : \langle d\rangle f = \chi(d) f \ \forall d \in (\mathbb{Z}/N\mathbb{Z})^*\}.$$

$M_k(\Gamma_1(N))$ se descompone como $M_k = \bigoplus_\chi M_k(N,\chi)$.

PROPOSICIÓN 2.15. *Sea $f \in M_k(\Gamma_1(N))$, como $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \in \Gamma_1(N)$, f tiene periodo 1 y admite una expansión de Fourier de la forma*

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

(a) *Si $\mathbb{1}_N : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$ es el carácter trivial, entonces $T_p f$ tiene expansión de Fourier*

$$\begin{aligned} T_p f(z) &= \sum_{n=1}^{\infty} a_{np}(f) q^n + \mathbb{1}_N(p) p^{k-1} \sum_{n=0}^{\infty} a_n(\langle p\rangle f) q^{np} \\ &= \sum_{n=1}^{\infty} a_{np}(f) q^n + \mathbb{1}_N(p) p^{k-1} a_{n/p}(\langle p\rangle f) q^n. \end{aligned}$$

(b) *Si $f \in M_k(N,\chi)$ entonces $T_p f \in M_k(N,\chi)$ y*

$$T_p f(z) = \sum_{n=0}^{\infty} \left(a_{np}(f) + \chi(p) p^{k-1} a_{n/p}(f)\right) q^n$$

DEMOSTRACIÓN.

(a) Sea $0 \leqslant j < p$ y $\beta_j = \begin{pmatrix}1 & j\\ 0 & p\end{pmatrix}$, entonces

$$\begin{aligned} f[\beta_j]_k(z) &= p^{k-1} p^{-k} f\left(\frac{z+j}{p}\right) \\ &= \frac{1}{p} \sum_{n=0}^{\infty} a_n(f) e^{\frac{2\pi i n(z+j)}{p}} \\ &= \frac{1}{p} \sum_{n=0}^{\infty} a_n(f) q_p^n \mu_p^n, \end{aligned}$$

donde $q_p = e^{\frac{2\pi i z}{p}} = q^{\frac{1}{p}}$ y $\mu_p = e^{\frac{2\pi i j}{p}}$. Como

$$\sum_{j=0}^{p-1} e^{\frac{2\pi i n j}{p}} = \begin{cases} p & \text{si } p \mid N \\ 0 & \text{si } p \nmid N \end{cases},$$

entonces

$$\sum_{j=0}^{p-1} f[\beta_j]_k(z) = \sum_{n \equiv 0 \pmod p} a_n(f) e^{\frac{2\pi i n z}{p}} = \sum_{n=0}^{\infty} a_{np}(f) q^n.$$

Si $p \mid N$ esto es $T_p f$, en caso contrario existen m, n tales que $mp - Nn = 1$ y $T_p f$ incluye el término

$$f\left[\begin{pmatrix} m & n \\ N & p \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right]_k (z) = \langle p\rangle f[\beta_j](z) = p^{k-1}\langle p\rangle f(pz),$$

de donde se deduce (a).

(b) es inmediato de (a) observando que $\langle d\rangle T_p f = T_p(\langle d\rangle f) = \chi(p)T_p f$.

□

Las definiciones de $\langle d\rangle$ y T_p se pueden extender en general a $\langle n\rangle, T_n$ para cualquier $n \in \mathbb{Z}^+$.

Definición 2.16.

- Si $mcd(n, N) = 1$ entonces $\langle n\rangle$ queda determinado por $n \pmod N$.
- Si $mcd(n, N) > 1$ entonces $\langle n\rangle$ es el operador nulo.

Definición 2.17.

- $T_1 = 1$ es la identidad.
- Sea $r \geqslant 2$, T_{p^r} se define de forma inductiva como $T_{p^r} = T_p T_{p^{r-1}} - p^{r-1}\langle p\rangle T_{p^{r-2}}$.
- La definición se extiende a cualquier $n = \prod p_i^{r_i}$ de forma multiplicativa:

$$T_n = \prod T_{p_i{}^{r_i}}.$$

3. Formas nuevas

Se puede ver que si $M \mid N$ entonces $S_k(\Gamma_1(M)) \subseteq S_k(\Gamma_1(N))$, además, si $d|\frac{N}{M}$ existe otra inmersión de $S_k(\Gamma_1(M))$ en $S_k(\Gamma_1(N))$ que consiste en el mapa

$$f(z) \mapsto f[\gamma_d]_k(z) = d^{k-1} f(dz),\ \gamma_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}.$$

El mapa anterior es inyectivo, lineal, y lleva formas en $S_k(\Gamma_1(M))$ en $S_k(\Gamma_1(N))$. Las *formas viejas* distinguen las formas en $S_k(\Gamma(N))$ que "provienen" de niveles más bajos.

Dado un subgrupo de congruencia Γ existe un producto interno en el espacio de formas cuspidales de peso k en Γ llamado *Producto interno de Petersson*, que es definido como sigue:

Definición 2.18. Sean $f, g \in S_k(\Gamma_1(N))$, se define su Producto interno de Petersson como

$$\langle f, g\rangle := \frac{1}{[G : \Gamma(N)]} \int_{D_0(N)} \delta(f, g),$$

donde $D_0(N)$ es un dominio fundamental para $\Gamma(N)$ y, escribiendo $z = x + iy$, $\delta(f, g)$ es la forma diferencial $\delta(f, g) := y^{k-2} f(z)\overline{g(z)}dxdy$

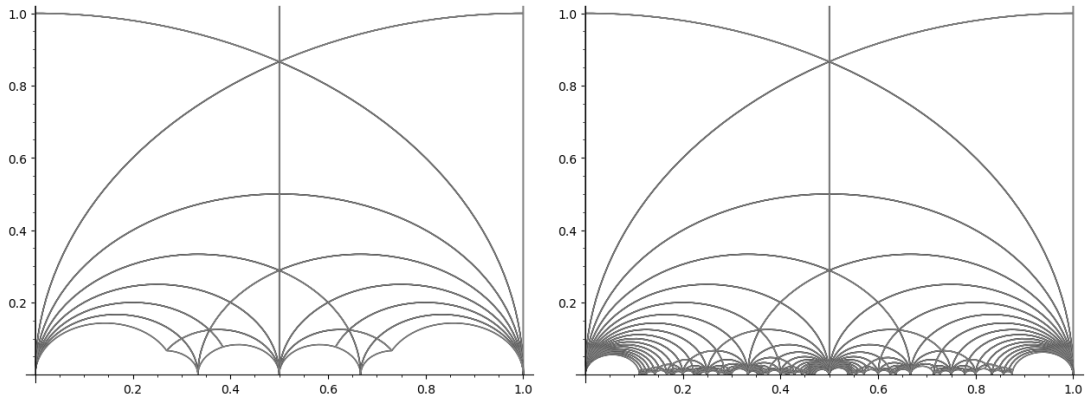

FIGURA 1. Dominios fundamentales para $\Gamma_0(13)$ (izq.) y $\Gamma_1(17)$ (der.)

DEFINICIÓN 2.19. Si $d \mid N$, consideramos $\gamma_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$. Se define el mapa i_d como sigue,

$$i_d : \left(S_k(\Gamma_1(Nd^{-1}))\right)^2 \to S_k(\Gamma_1(N)), \quad \text{tal que } (f,g) \mapsto f + g[\gamma_d]_k.$$

El subespacio de *formas viejas de nivel* N es

$$S_k(\Gamma_1(N))^{old} := \sum_{p|N} i_p \left(S_k(\Gamma_1(Nd^{-1}))^2\right),$$

y el subespacio de *formas nuevas de nivel* N es

$$S_k(\Gamma_1(N))^{new} := \left(S_k(\Gamma_1(N))^{old}\right)^{\perp}.$$

Los operadores de Hecke respetan la descomposición de $S_K(\Gamma_1(N))$ en formas nuevas y viejas. Este resultado junto con los siguientes se pueden encontrar en [D-S, §5].

PROPOSICIÓN 2.20. *Los subespacios $S_k(\Gamma_1(N))^{old}$ y $S_k(\Gamma_1(N))^{new}$ son estables por los operadores de Hecke $\langle n \rangle$ y T_n, para todo $n \in \mathbb{Z}^+$.*

COROLARIO 2.21. *$S_k(\Gamma_1(N))^{old}$ y $S_k(\Gamma_1(N))^{new}$ tienen base ortonormal de valores propios para los operadores de Hecke $\langle n \rangle$ y T_n con $mcd(n,N) = 1$.*
En el caso de las formas nuevas, se puede (no es inmediato) eliminar la condición $mcd(n,N) = 1$.

DEFINICIÓN 2.22. Una *forma nueva* es $f \in S_k(\Gamma_1(N))^{new}$ normalizada tal que es un vector propio para todos los operadores de Hecke $\langle n \rangle$ y T_n, $n \in \mathbb{Z}^+$ (basta pedirlo para n coprimo con N).

PROPOSICIÓN 2.23. *Sea $f(z) = \sum_{n=0}^{\infty} a_n q^n$ una forma nueva, entonces $a_n a_m = a_{nm}$ para todo $m, n \in \mathbb{Z}^+$ tal que $mcd(m,n) = 1$.*
Si $f \in M_k(N,\chi)$ entonces $a_{p^n} = a_p(f) a_{p^{n-1}} - \chi(p) p^{2k-1} a_{p^{n-2}}$.

Demostración. Como f es un vector propio para todo n coprimo con N existen $\lambda(n)$ y $\mu(n)$ tales que $\langle n\rangle f = \lambda(n)f$ y $T_n f = \mu(n)f$. Asumamos el siguiente resultado, *Afirmación:* el mapa $n \mapsto \lambda(n)$ define un carácter de Dirichlet χ tal que $f \in M_k(N,\chi)$. De la afirmación y la proposición previa se deduce la igualdad

$$\mu(n)a_1 f = a_1(T_n f) = a_n(f).$$

Cuando f es normalizada, esto se reduce a $\mu(n) = a_n$ si $mcd(n,N) = 1$. El resultado se sigue de 2.17. □

Proposición 2.24. *Si* $f = \sum_{n=0}^{\infty} a_n q^n \in S_k(\Gamma_1(N),\chi)$ *es una forma nueva entonces su L-serie asociada* $L(f,s) := \sum_{n=1}^{\infty} a_n n^{-s}$ *converge para* $\Re s > k/2+1$ *y admite un producto de Euler*

$$L(f,s) = \prod_p (1 - a_p p^{-s} + \chi(p)p^{k-1-2s})^{-1}.$$

Demostración. Consideremos la función holomorfa definida en el disco unitario $D = \{z : \mid z \mid < 1\}$ dada por $g(z) = \sum_{n=1}^{\infty} a_n z^n$. Por Cauchy

$$a_n = \frac{1}{2\pi i}\int_{|z|=r} g(z) z^{-n}\frac{dz}{z}.$$

Fijando $y = \frac{1}{n}$ y haciendo el cambio de variables $z = e^{2\pi i(x+iy)}$ nos queda

$$a_n = \int_{x=0}^{x=1} f(x+iy)e^{-2\pi i n(x+iy)}dx = e^{2\pi}\int_{x=0}^{x=1} f(x+iy)e^{-2\pi i n x}dx.$$

Como f es cuspidal debe cumplir que $\lim_{\Im z\to\infty} |f(z)|\Im z^{k/2} = 0$, como además $|f(z)|\Im z^{k/2}$ es continua, esto implica que es acotada. Existe entonces $C \in \mathbb{R}$ tal que $|a_n| \leqslant Cn^{k/2}$ y $a_n n^{-s} = O(n^{k/2-\Re s})$, esto implica que f converge absolutamente para $\Re s > k/2+1$.

Consideremos ahora $P(S) = \prod_{p<S}\left(\sum_{m=0}^{\infty} a_{p^m}p^{-ms}\right)$. Como los coeficientes son multiplicativos, si A consiste en los números cuyos factores primos son menores a S entonces $P(S) = \sum_{n\in A} a_n n^{-s}$. Luego

$$|L(f,s) - P(S)| = \left|\sum_{n\in\mathbb{N}\setminus A} a_n n^{-s}\right| \leqslant \sum_{n\geqslant S} a_n n^{-s}$$

y como $L(f,s)$ converge la suma de la derecha tiene límite 0 cuando $S\to\infty$. Deducimos que $P(S)$ converge absolutamente a $L(f,s)$.

Sea $X = p^{-s}$, resta ver que $\sum_{m=0}^{\infty} a_{p^m}X^n = (1 - a_p(f)X + \chi(p)p^{k-1}X^2)^{-1}$, lo cual equivale a ver que la serie

$$\psi(X) = \sum_{m=0}^{\infty} a_{p^m}(f)X^n(1 - a_p(f)X + \chi(p)p^{k-1}X^2)$$

es constante igual a 1. Usando la proposición 2.15

$$\psi(X) = a_1 + a_pX - a_1a_pX + \sum_{m=2}^{\infty} \left(a_{p^m} + a_{p^{m-2}}\chi(p)p^{k-1} - a_{p^{m-1}}a_p \right) X^m = a_1 = 1.$$

□

El caso que nos interesa es el de formas modulares $f \in S_k(\Gamma_0(N))$ de peso 2 que son formas nuevas, es decir, son normalizadas y autovectores para todos los T_n y $\langle n \rangle$, los resultados vistos para $\Gamma_1(N)$ permanecen válidos para $\Gamma_0(N)$ (esto no es algo inmediato), vamos a asumir también que estas formas modulares satisfacen la siguiente propiedad:

(P) *Si f es una forma nueva de peso 2 para $\Gamma_1(N)$, entonces existe $\varepsilon \in \{-1, 1\}$ tal que* $f(\frac{-1}{N\tau}) = -\varepsilon N\tau^2 f(\tau)$.

Proposición 2.25. *Sea $f = \sum_{n=1}^{\infty} a_n q^n$ una forma nueva de peso 2 para $\Gamma_0(N)$. Entonces*

(a) $|a_p| \leqslant 2\sqrt{p}$ *para todo p primo.*
(b) *Si $p^2 \mid N$ entonces $a_p = 0$.*
(c) *Si $p \mid N$ y $p^2 \nmid N$ entonces $a_p = \pm 1$.*

Demostración. La parte (a) es un caso particular de la Conjetura de Ramanujan-Petersson

$$a_n(f) = O(n^{\frac{k-1}{2}+\varepsilon}) \ \forall \varepsilon > 0,$$

que fue probada por Deligne a partir de las Conjeturas de Weil en el año 1974 [Del]. Las partes (b) y (c) son más sencillas, [Ogg, Theorem 1]. □

Observación 2.26. *En la prueba de 2.24 obtuvimos la cota $|a_n| \leqslant Cn^{\frac{k}{2}}$, lo cual implica la convergencia uniforme de $L(f, s)$ para $\Re s > \frac{k}{2} + 1$. La proposición 2.25 mejora esta cota para el caso particular de las formas nuevas de peso 2. Ahora tenemos $|a_p| \leqslant 2\sqrt{p}$ y por lo tanto $L(f, s)$ converge para $\Re s > \frac{3}{2}$*

Proposición 2.27. *Sea f en las hipótesis de la proposición anterior.*
La función $s \mapsto N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(f, s)$ se extiende a una función entera $\Lambda(f, s)$ que satisface la ecuación funcional $\Lambda(f, 2 - s) = \varepsilon\Lambda(f, s)$.

Demostración.

Afirmación. *Si $\Re s > \frac{3}{2}$ entonces*

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

Prueba de la afirmación: $\Gamma(s)$ converge para s con parte real positiva y $L(f,s)$ para s con $\Re s > \frac{3}{2}$, por lo tanto el término de la izquierda converge absolutamente, luego

$$\begin{aligned}(2\pi)^{-s}\Gamma(s)L(f,s) &= (2\pi)^{-s}\sum_{n=0}^{\infty} a_n n^{-s}\int_0^\infty e^{-t}t^s\,\frac{dt}{t}\\ &= \sum_{n=0}^{\infty} a_n \int_0^\infty e^{-2\pi tn}t^s\,\frac{dt}{t} \qquad \text{(integrando por partes)}\\ &= \int_0^\infty \sum_{n=0}^{\infty} a_n e^{-2\pi tn}t^s\,\frac{dt}{t}\\ &= \int_0^\infty f(it)t^s\,\frac{dt}{t}.\end{aligned}$$

□

Por la afirmación tenemos que

$$\begin{aligned}\Lambda(f,s) &= N^{s/2}\int_0^\infty f(it)t^s\frac{dt}{t}\\ &= \int_0^\infty f\left(\frac{it}{\sqrt{N}}\right)t^s\frac{dt}{t}\\ &= \int_0^1 f\left(\frac{it}{\sqrt{N}}\right)t^s\frac{dt}{t} + \int_1^\infty f\left(\frac{it}{\sqrt{N}}\right)t^s\frac{dt}{t}\\ &= \int_0^1 \varepsilon f\left(\frac{i}{\sqrt{N}t}\right)t^{s-2}\frac{dt}{t} + \int_1^\infty f\left(\frac{it}{\sqrt{N}}\right)t^s\frac{dt}{t}\\ &= \int_1^\infty \varepsilon f\left(\frac{it}{\sqrt{N}}\right)t^{2-s}\frac{dt}{t} + \int_1^\infty f\left(\frac{it}{\sqrt{N}}\right)t^s\frac{dt}{t}\\ &= \int_1^\infty f\left(\frac{it}{\sqrt{N}}\right)\left(t^s+\varepsilon t^{2-s}\right)\frac{dt}{t}\end{aligned}$$

Como $f\left(\frac{it}{\sqrt{N}}\right)$ tiene orden $e^{-2\pi t/\sqrt{N}}$ cuando $t\to\infty$ esta integral converge en todo el plano complejo. □

Proposición 2.28. *Sea $f = \sum_{n=1}^{\infty} a_n(f)q^n \in M_k(N,\chi)$ una forma nueva normalizada de peso 2 y nivel N y ψ un carácter de Dirichlet primitivo módulo r. Entonces existe un entero $N_\psi \geqslant 1$ y una forma modular $f\otimes\psi$ de peso 2, nivel N_ψ y carácter $\chi\psi^2$ tales que $a_p(f\otimes\psi) = a_p(f)\psi(p)$ para todo primo p.*
Claramente $f\otimes\psi$ está determinada de forma única, le llamaremos torsión de f por ψ.

Demostración. Notemos por $G(\psi)$ a la suma de Gauss $\sum_{u \pmod r}\psi(u)\mathrm{e}(\frac{u}{r})$, donde $\mathrm{e}(m) = e^{2\pi im}$. Como ψ es un carácter primitivo, entonces $G(\psi)\neq 0$ y cumple la siguiente igualdad:

$$G(\overline{\psi})\psi(n) = \sum_{u \pmod r}\overline{\psi}(u)\mathrm{e}\left(\tfrac{nu}{r}\right). \tag{13}$$

Luego,

$$\begin{aligned}(f\otimes\psi)(z) := \sum_{n=0}^{\infty}\psi(n)a_n(f)q^n &= \sum_{n=0}^{\infty} a_n(f)\mathrm{e}(nz)G(\overline{\psi})^{-1}\sum_{u \pmod r}\overline{\psi}(u)\mathrm{e}(\tfrac{un}{r})\\ &= G(\overline{\psi})^{-1}\sum_{u \pmod r}\overline{\psi}(u)\sum_{n=0}^{\infty}a_n(f)\mathrm{e}\left(n(z+\tfrac{u}{r})\right)\\ &= \sum_{u \pmod r}\overline{\psi}(u)f(z+\tfrac{u}{r}).\end{aligned}$$

Sea $\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \Gamma_0(M)$, entonces

$$\gamma z + \frac{u}{r} = \begin{pmatrix}1 & \frac{u}{r}\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} z = \begin{pmatrix} a+\frac{uc}{r} & b - \frac{bcdu}{r} - \frac{cd^2u^2}{r^2}\\ c & d - \frac{cd^2u}{r}\end{pmatrix}\begin{pmatrix}1 & \frac{d^2u}{r}\\ 0 & 1\end{pmatrix} z.$$

Si c es el conductor de χ y $M = \mathrm{mcm}\{N, cr, r^2\}$, de lo anterior se deduce que

$$\begin{aligned}(f\otimes\psi)[\gamma](z) &= \sum_{u \pmod r}\overline{\psi}(u)f\left(\gamma z + \frac{u}{r}\right)\\ &= \sum_{u \pmod r}\overline{\psi}(u)\chi\left(d - \frac{cd^2u}{r}\right)f\left(z+\frac{d^2u}{r}\right)\\ &= \chi(d)\sum_{u \pmod r}\overline{\psi}(d^2u)f\left(z+\frac{d^2u}{r}\right)\\ &= \chi(d)\psi(d^2)\sum_{u \pmod r}\overline{\psi}(d^2u)f\left(z+\frac{d^2u}{r}\right)\\ &= \chi(d)\psi(d^2)(f\otimes\psi)(z),\end{aligned}$$

esto significa que $f\otimes\psi$ es una forma modular de peso k, nivel M y carácter $\chi\psi^2$. □

Proposición 2.29. *Si* $\mathrm{mcd}(N, d^2)$ *es libre de cuadrados, entonces* $f\otimes\chi_d$ *tiene carácter* χ *y nivel* $N_{\chi_d} = \mathrm{mcm}(N, d^2)$. *Además se cumple que* $a_n(f\otimes\chi_d) = a_n(f)\chi_d(n)$ *para todo* $n \geqslant 1$ *y la constante* ε *para la ecuación funcional viene dada por la fórmula*

$$\varepsilon(f\otimes\chi) = \chi_d(-N_1)\varepsilon(f)\prod_{p\mid N_2} -a_p(f), \tag{14}$$

donde $N = N_1N_2$ *y* $N_2 = \mathrm{mcd}(N, d)$.

Demostración. Se puede encontrar una prueba de esto en [D-S] §5. □

Observación 2.30. *Si* $\mathrm{mcd}(N, d) = 1$ *la fórmula anterior se reduce a*

$$\varepsilon(f\otimes\chi_d) = \chi_d(-N)\varepsilon(f). \tag{15}$$

DEFINICIÓN 2.31. Recordemos que la función de Liouville es $\lambda : \mathbb{N}^* \to \{\pm 1\}$ completamente multiplicativa tal que vale -1 en los primos. Dada $f = \sum_{n=0}^{\infty} a_n q^n$ una forma nueva normalizada de peso 2, nivel N y carácter χ. Vamos a definir las siguientes L-series:

(1) $L(f \otimes \lambda, s) := \sum_{n=1}^{\infty} a_n \lambda(n) n^{-s}$ y
(2) $L(\mathrm{Sym}^2 f, s) := \prod_p (1 - \chi(p)p^{1-s})^{-1} L(f, s/2) L(f \otimes \lambda, s/2)$.

PROPOSICIÓN 2.32. *Si $f = \sum_{n=0}^{\infty} a_n q^n$ es una forma nueva de peso 2, nivel N y carácter χ, entonces*

$$L(\mathrm{Sym}^2 f, s) = \prod_p (1 + \chi(p)p^{1-s})^{-1} \sum_{n=1}^{\infty} a_n^2 n^{-s}.$$

DEMOSTRACIÓN. Sea $f = \sum_{n=1}^{\infty} a_n q^n$ una forma nueva normalizada de peso 2 y carácter χ para $\Gamma_0(N)$. Podemos escribir

$$L(f, s/2) = \prod_p \left(1 - \alpha_p p^{-s/2}\right)^{-1} \left(1 - \beta_p p^{-s/2}\right)^{-1},$$

donde $\alpha_p \beta_p = \chi(p)p$ y $\alpha_p + \beta_p = a_p$. Como la función λ es completamente multiplicativa y $\lambda(p) = -1$ para todo primo p, esto implica que

$$L(f \otimes \lambda, s/2) = \prod_p \left(1 + \alpha_p p^{-s/2}\right)^{-1} \left(1 + \beta_p p^{-s/2}\right)^{-1}$$

Pongamos $X = p^{-s}$,

$$\begin{aligned} L(f, s/2) L(f \otimes \lambda, s/2) &= \prod_p \left(1 - \alpha_p^2 X\right)^{-1} \left(1 - \beta_p^2 X\right)^{-1} \\ &= \prod_p \left(1 - (\alpha_p^2 + \beta_p^2)X + \alpha_p^2 \beta_p^2 X^2\right)^{-1} \\ &= \prod_p \left(1 - (a_p^2 - 2\chi(p)p)X + \chi^2(p)p^2 X^2\right)^{-1} \end{aligned}$$

Por otra parte, tenemos las siguientes relaciones:

$$a_{p^n} = a_p a_{p^{n-1}} - \chi(p) p a_{p^{n-2}} \qquad n \geqslant 2. \tag{1}$$

$$\chi(p) p a_{p^{n-3}} = a_p a_{p^{n-2}} - a_{p^{n-1}} \qquad n \geqslant 3. \tag{2}$$

Elevando al cuadrado ambos lados en (1) y (2) tenemos

$$a_{p^n}^2 = (a_p^2 - \chi(p)p) a_{p^{n-1}}^2 - \chi(p)p(a_p^2 - \chi(p)p) a_{p^{n-2}}^2 + \chi(p)^3 p^3 a_{p^{n-3}}^2. \tag{3}$$

La L-serie $\sum_{n=1}^{\infty} a_n^2 n^{-s}$ puede escribirse como

$$\sum_{n=1}^{\infty} a_n^2 n^{-s} = \prod_p \sum_{j \geqslant 0} a_{p^j}^2 p^{-js}.$$

Para probar la proposición querremos ver que

$$(1+\chi(p)pX)^{-1}\sum_{j\geqslant 0} a_{p^j}^2 X^j = \left(1-a_p^2X+\chi(p)^2p^2X^2+2\chi(p)pX\right)^{-1}(1-\chi(p)pX)^{-1},$$

lo cual equivale a ver

$$\sum_{j=0}^{\infty} a_{p^j}^2 X^j\,(1-\chi(p)pX)\left(1-a_p^2X+\chi(p)^2p^2X^2+2\chi(p)pX\right) = (1+\chi(p)pX). \tag{4}$$

El término de la izquierda en 4 es

$$\begin{aligned}
&\sum_{j=0}^{\infty} a_{p^j}^2 X^j\left(1+(\chi(p)p-a_p^2)X+(a_p^2\chi(p)p-\chi(p)^2p^2)X^2-\chi(p)^3p^3X^3\right)\\
=&\sum_{j=0}^{\infty}\left(a_{p^j}^2X^j+a_{p^j}^2(\chi(p)-a_p^2)X^{j+1}+a_{p^j}^2(a_p^2\chi(p)p-\chi(p)^2p^2)X^{j+2}-a_{p^j}^2\chi(p)^3p^3X^{j+3}\right)\\
=&A(X)+B(X),
\end{aligned}$$

donde

$$\begin{aligned}
A(X) &= 1+(a_p^2+\chi(p)p-a_p^2)X+(a_{p^2}^2+a_p^2(\chi(p)p-a_p^2)+(a_p^2\chi(p)p-\chi(p)^2p^2))X^2\\
&= 1+\chi(p)pX+(a_{p^2}^2+a_p^2(\chi(p)p-a_p^2)+(a_p^2\chi(p)p-\chi(p)^2p^2))X^2\\
&= 1+\chi(p)pX+\left(a_{p^2}^2-(a_p^2-\chi(p)p)^2\right)^2\\
&= 1+\chi(p)p \qquad \text{(por (1))}.\\
B(X) &= \sum_{j\geqslant 3}\left(a_{p^j}^2+a_{p^{j-1}}^2(\chi(p)-a_p^2)+a_{p^{j-2}}^2(a_p^2\chi(p)p-\chi(p)^2p^2)-a_{p^{j-3}}^2\chi(p)^3p^3\right)X^j.\\
&= 0 \qquad \text{(por (3))}.
\end{aligned}$$

□

Proposición 2.33. *Si N es un entero libre de cuadrados, entonces la función*

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

se extiende a una función entera que satisface la ecuación funcional

$$\Lambda(\mathrm{Sym}^2 f,3-s) = \Lambda(\mathrm{Sym}^2 f,s).$$

Demostración. [1].

Sea $f(z)=\sum_{n=1}^{\infty} a_n q^n$, y escribamos $z=x+iy$, entonces

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} f(z)^2dx = \sum_{n=1}^{\infty} a_n^2 e^{-4\pi ny},$$

[1]La prueba para un caso más general se encuentra en [Ogg]

y, por lo tanto,

$$\int_{-\infty}^{\infty}\int_{-\frac{1}{2}}^{\frac{1}{2}} y^{s-1}f(z)^2dxdy = \sum_{n=1}^{\infty} a_n^2 e^{-4\pi ny}\int_0^{\infty}\frac{y}{4\pi n}^{-s}e^{-y}\frac{dy}{y} \tag{1}$$

$$= (4\pi)^{-s}\Gamma(s)\sum_{n=1}^{\infty} a_n^2 n^{-s}, \tag{2}$$

Ahora, $D = \{x+iy \in \mathbb{C} \ : \ |x| \leqslant \frac{1}{2}\}$ es un dominio fundamental para el grupo de traslaciones $T = \left\{\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} \ : \ n \in \mathbb{Z}\right\}$, y podemos escribirlo como unión de clases laterales a derecha de T.
$T\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \left\{\begin{pmatrix}a+nc & b+nd\\ c & d\end{pmatrix} \ : \ n \in \mathbb{Z}\right\} = T\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ si y sólo si $(c,d) = \pm(c',d')$, por lo tanto hay una correspondencia entre clases laterales derechas de T en $\Gamma_0(N)$ y pares (c,d) asociados a matrices en $\Gamma_0(N)$, de forma que se pueden elegir los pares $(0,1)$ y (c,d) con $c>0, N \mid d$ y $\text{mcd}(c,d)=1$ como representantes, denotemos por $\mathcal{C}$ a este conjunto de representantes.

Observando que $\Im(\gamma z)^s = \frac{\Im(z)^s}{|j(\gamma,z)|^{2s}}$ deducimos que $\delta(f,\bar{f}) := |f|^2(z)dxdy$ es invariante por la acción de $\Gamma_0(N)$ y

$$\int_D y^s f^2(z)dxdy = \int_{D_0} f^2(z)y^s F_N(z,s)dxdy, \tag{3}$$

donde D_0 es un dominio fundamental para $\Gamma_0(N)$ y

$$F_N(z,s) = \sum_{(c,d)\in\mathcal{C}} |cz+d|^{-2s} = 1 \sum_{\substack{m\in\mathbb{Z}^+\\ \text{mcd}(mN,n)=1}} |mNz+n|^{-2s}.$$

Sea ahora

$$\zeta_N(s) = \prod_{p\nmid N}(1-p^{-s})^{-1} = \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}^+\\ \text{mcd}(n,N)=1}} n^{-s}$$

Si $\mu(d)$ denota a la función de Möbius tenemos que $\sum_{d|n}\mu(d) = \begin{cases}1 & n=1\\ 0 & n>1\end{cases}$, luego

$$\begin{aligned}
2\zeta_N(2s)F_N(z,s) &= \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\ \text{mcd}(n,N)=1}} |mNz+n|^{-2s}\\
&= {\sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}}' \sum_{d|\text{mcd}(n,N)} \mu(d)|mNz+n|^{-2s}\\
&= \sum_{d|n} {\sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}}' \mu(d)|mNz+dn|^{-2s}
\end{aligned}$$

$$= \sum_{d|n} \mu(d) d^{-2s} G\left(\tfrac{Nz}{d}, s\right),$$

donde $G(z,s) = \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}}{}' |mz+n|^{-2s}$.

Definamos ahora $L_{f^2}(s) := \zeta_N(2(s-1)) \sum_{n=1}^{\infty} a_n^2 n^{-s}$. Multiplicando (1) y (3) por $2\zeta_N(2(s-1))$ tenemos

$$2(4\pi)^{-s}\Gamma(s)L_{f^2}(s) = \sum_{d|N} \mu(d) d^{-2(s-1)} \int_{D_0(N)} y^{s-1} \delta(f,\bar{f}) G\left(\tfrac{Nz}{d}, s-1\right). \tag{4}$$

La función $I(z,s) := \left(\frac{y}{\pi}\right)^s \Gamma(s) G(z,s)$ es una función entera excepto por polos simples de residuo 1 en $s=0$ y $s=1$. Además satisface las ecuaciones funcionales

$$I(z,s) = I(z,1-s) \qquad\qquad I(\gamma(z),s) = I(z,s) \text{ para toda } \gamma \in G.$$

Multiplicando (4) por $\left(\frac{N}{\pi}\right)^{s-1}\Gamma(s-1)$ llegamos a

(5)

$$\phi(s) := (2\pi)^{-2(s-1)} N^{s-1}\Gamma(s)\Gamma(s-1)L_{f^2}(s) = 2\pi \sum_{d|N} \frac{\mu(d)}{d^{s-1}} \int_{D_0(N)} \delta(f,\bar{f}) I\left(\frac{Nz}{d}, s-1\right).$$

Supongamos que p es un primo que divide a N y sea $\beta = \begin{pmatrix} sp & -r \\ N & p \end{pmatrix} \in \Gamma_0\left(\frac{N}{p}\right)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, entonces

1. Como f un autovector para todos los operadores de Hecke y además es normalizada, la proposición 2.23 implica que $f[\beta]_k = a_p f$.
2. N es libre de cuadrados, entonces por la proposición 2.25 si $p \mid n$, $a_p = \pm 1$.
3. $\delta(f,\bar{f}) \circ \beta = a_p^2 \delta(f,\bar{f}) = \delta(f,\bar{f})$.
4. $\beta^{-1}D_0$ es un dominio fundamental para $\beta^{-1}\Gamma_0(N)\beta = \Gamma_0(N)$.

Podemos deducir que, para $d \mid \frac{N}{p}$,

$$\begin{aligned}\int_{D_0(N)} I\left(\frac{Nz}{pd}, s-1\right)\delta(f,\bar{f}) &= a_p^2 \int_{D_0(N)} I\left(\frac{Nz}{d}, s-1\right)\delta(f,\bar{f}) \\ &= \int_{D_0(N)} I\left(\frac{Nz}{d}, s-1\right)\delta(f,\bar{f}),\end{aligned}$$

luego

$$\phi(s) = (2\pi)(1-a_p^2 p^{1-s}) \sum_{d|\frac{N}{p}} \mu(d) d^{1-s} \int_{D_0(N)} I\left(\frac{Nz}{d}, s-1\right)\delta(f,\bar{f}).$$

Repitiendo esto para cada primo $p \mid N$ y recordando que $a_p^2 = 1$,

$$\phi(s) = (2\pi)\prod_{p|N}(1-p^{1-s}) \int_{D_0(N)} I\left(Nz, s-1\right)\delta(f,\bar{f}).$$

Si definimos $\phi^+(s) := \prod_{p|N}(1-p^{1-s})^{-1}\phi(s)$, lo anterior significa que ϕ^+ satisface la ecuación funcional

$$\phi^+(s) = \phi^+(3-s).$$

La función Γ satisface la *fórmula de duplicación de Legendre*:

$$\Gamma(z)\Gamma(z+1) = 2^{1-2s}\sqrt{\pi}\Gamma(2z),$$

aplicando esta fórmula con $z = \frac{s-1}{2}$ tenemos

$$\begin{aligned}\phi^+(s) &= (2\pi)^{-2(s-1)}N^{s-1}\Gamma(s)\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s-1}{2}\right)2^{s-2}\pi^{-1/2}\zeta(s-1)\Lambda(\mathrm{Sym}^2 f, s)\\ &= \pi N^{-1}N^s(2\pi)^{-s}\Gamma(s)\pi^{\frac{-s}{2}}\Gamma\left(\frac{s}{2}\right)\Lambda(\mathrm{Sym}^2 f, s)\xi(s-1)\\ &= \Lambda(\mathrm{Sym}^2 f, s)\pi N^{-1}N^s\xi(s-1)\end{aligned}$$

donde $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ satisface la ecuación funcional $\xi(s) = \xi(1-s)$, con lo cual $\Lambda(\mathrm{Sym}^2 f, s)$ debe cumplir

$$\Lambda(\mathrm{Sym}^2 f, s) = \Lambda(\mathrm{Sym}^2 f, 3-s).$$

□

Observación 2.34. *En la demostración anterior*

$$L_{f^2}(s) = \prod_{p\nmid N}(1-p^{1-s})^{-1}L(\mathrm{Sym}^2 f, s) = \prod_{p|N}(1-p^{1-s})\zeta(s-1)L(\mathrm{Sym}^2 f, s)$$

y vimos que

$$\begin{aligned}\phi(s) :=& (2\pi)^{-2(s-1)}N^{s-1}\Gamma(s)\Gamma(s-1)L_{f^2}(s)\\ =& (2\pi)\prod_{p|N}(1-p^{1-s})\int_{D_0(N)} I(Nz, s-1)\delta(f, \bar{f}).\end{aligned}$$

Como $I(Nz, s-1)$ tiene polos simples de residuo 1 en $s=2$ observamos que $\phi(s)$ tiene un polo simple en $s=2$ de residuo $(2\pi)\prod_{p|N}(1-p^{-1})\int_{D_0(N)}\delta(f,\bar{f})$. Por otra parte, $\zeta(s-1)$ también tiene un polo simple de residuo 1 en $s=2$. Deducimos entonces que

$$L(\mathrm{Sym}^2 f, 2) = 2(2\pi)^{-3}\int_{D_0(N)}\delta(f,\bar{f}) \neq 0.$$

Capítulo 3

Demostración de Oesterlé al Teorema de Goldfeld

Sea K un cuerpo cuadrático imaginario de discriminante $-d < -4$ y $\chi_d = (\frac{-d}{\cdot})$ su carácter asociado, que coincide con el símbolo de Kronecker. Llamémosle h al número de clases $h_K = h(-d)$.

Dadas dos series de Dirichlet $A = \sum_{n=1}^{\infty} a_n n^{-s}$ y $B = \sum_{n=1}^{\infty} b_n n^{-s}$ escribimos $A \ll B$ cuando $|a_n| \leqslant |b_n|$ para todo $n \geqslant 1$. Para la demostración del Teorema de Goldfeld vamos a considerar dos series de Dirichlet ψ y G, y una constante $M \in \mathbb{R}_{>0}$ que satisfagan las siguientes 4 condiciones.

(C1)

$$\psi(s) \ll \zeta(2s-1)^2 \qquad \text{y} \qquad G(s) \ll \left(\frac{\zeta_K(s-\frac{1}{2})}{\zeta(2s-1)}\right)^2$$

En particular, esto implica que ψ converge para $\Re s > 1$ y G converge para $\Re s > \frac{3}{2}$.

(C2) G admite un Producto de Euler de la forma $\prod_p G_p$ con $G_p(s) = \frac{(1+\alpha p^{-s})(1+\beta p^{-s})}{(1+\alpha' p^{-s})(1+\beta' p^{-s})}$, donde $\alpha, \alpha', \beta, \beta' \in \mathbb{C}$ tienen módulo menor o igual a $\sqrt{p}$.

(C3) Sea $\gamma(s) = M^s \Gamma(s)^2$. La función $\varphi(s) = d^s \gamma(s)\psi(s)G(s)$ se extiende a una función entera que decrece rápidamente en cada banda vertical, satisface la ecuación funcional $\varphi(s) = \varphi(2-s)$ y admite un cero de orden al menos 3 en $s = 1$. De la ecuación funcional se deduce que el orden del cero en $s = 1$ es al menos 4.

(C4) ψ admite una extensión holomorfa sobre un entorno del semiplano $\mathcal{H}_1 := \{s \in \mathbb{C} : \ \Re s \geqslant 1\}$, con un cero simple en $s = 1$. La función $\gamma\psi$ decrece rápidamente en infinito sobre cada banda vertical en $\mathcal{H}_1$

En principio se asume la existencia de ψ, G y M. En el capítulo 4 veremos que si f es una forma modular de peso 2 y nivel N tal que su L-serie asociada tiene un cero de orden al menos 3 en $s = 1$, entonces podemos tomar

$$\begin{aligned} \psi(s) &= L(f,s)L(f\otimes\lambda,s) = \frac{L(\mathrm{Sym}^2 f, 2s)}{\zeta(2s-1)}, \\ G_K(s) &= L(f\otimes\chi_d,s)L(f\otimes\lambda,s)^{-1}, \\ M &= \frac{N}{4\pi^2} \end{aligned}$$

donde ψ que satisfacen las condiciones **(C1)-(C4)** para todo cuerpo cuadrático K con discriminante coprimo a N tal que $\chi_d(N) = -1$.

El Teorema de Gross-Zagier implica la existencia de dicha forma modular y junto con el Teorema de Goldfeld esto da una cota efectiva para el número de clases de cuerpos cuadráticos en la familia descrita anteriormente. El resultado se extiende para la familia de todos los cuerpos cuadráticos imaginarios.

1. Igualdad fundamental

PROPOSICIÓN 3.1. *Sea* $w(s) = \frac{1}{2\pi i} d^{s-1}\gamma(s)\psi(s)G(s)(s-1)^{-3}$. *Para* $\sigma > \frac{3}{2}$

$$J := \int_{\sigma-i\infty}^{\sigma+i\infty} w(s)ds = 0.$$

DEMOSTRACIÓN. Sea $K > 0$, consideremos el dominio simplemente conexo

$$\Delta_K = \{z = x + iy \in \mathbb{C} \ : \ 1 \leqslant x \leqslant \sigma, \ -K \leqslant y \leqslant K\}$$

Por el Teorema de los residuos

$$\int_{\sigma-iK}^{\sigma+iK} w(s)ds + \int_{\sigma+iK}^{1+iK} w(s)ds + \int_{1+iK}^{1-iK} w(s)ds + \int_{1-iK}^{\sigma+iK} w(s)ds = \int_{\partial\Delta_K} w(s)ds = 0$$

De aplicar la condición **(C3)** y tomar límite $K \to \infty$ resulta

$$\int_{\sigma-i\infty}^{\sigma+i\infty} w(s)ds = \int_{1-i\infty}^{1+i\infty} w(s)ds.$$

Observar que $w(s) = \frac{1}{2\pi i d}\varphi(s)(s-1)^{-3}$. Por la ecuación funcional que satisface φ es claro que $w(2-s) = -w(s)$ y por lo tanto $J = -J = 0$. □

Sea $U \geqslant 1$ una constante real, definimos

$$G(U,s) := \prod_{p<U} G_p(s),$$

y

$$G(U,s)^* := G(s) - G(U,s) = G(U,s)\left(-1 + \prod_{p\geqslant U} G_p(s)\right),$$

donde recordamos que G_p son los factores de Euler de G dados por la condición **(C2)**. Ahora definimos las integrales $J(U)$ y $J(U)^*$ de forma análoga a J en la proposición previa,

$$J(U) := \int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-1}\gamma(s)\psi(s)G(U,s)(s-1)^{-3}\frac{ds}{2\pi i}.$$

$$J(U)^* := \int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-1}\gamma(s)\psi(s)G(U,s)^*(s-1)^{-3}\frac{ds}{2\pi i}.$$

Por la condición **(C4)** la función $\gamma\psi$ es holomorfa en el dominio de integración. Como además $G(U,s)$ tiene una cantidad finita de factores, esto implica que $J(U)$ y $J(U)^*$ convergen, y la proposición previa implica que $J(U) = -J(U)^*$.

2. La integral J(U)

Dado $\eta \leqslant \frac{1}{4}$, por la condición **(C4)** existe $\tilde{\eta}$ tal que ψ se extiende a una función holomorfa en el dominio $\Delta := \{s \in \mathbb{C} : \ 1-\eta \leqslant \Re s \leqslant 1, \ -\tilde{\eta} \leqslant \Im s \leqslant \tilde{\eta}\} \cup \mathcal{H}_1$ representado en la siguiente imagen.

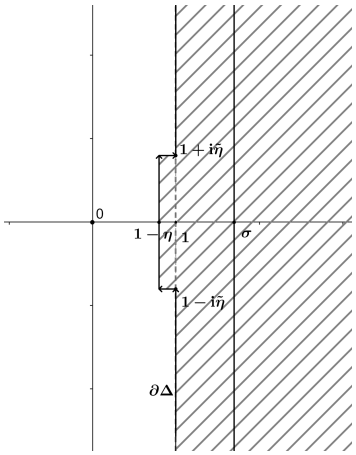

FIGURA 1. Dominio Δ.

En particular ψ es holomorfa en la región delimitada por $\partial\Delta$ y la recta $\{s : \Re s = \sigma\}$.

PROPOSICIÓN 3.2. *Sea* $J_\Delta(U) := \int_{\partial\Delta} d^{s-1}\gamma(s)\psi(s)G(U,s)(s-1)^{-3}\frac{ds}{2\pi i}$, *entonces*

$$J(U) - J_\Delta(U) = C_1 G(U,1)\left(\log d + \frac{G'(U,1)}{G(U,1)} + C_2\right),$$

donde C_1 *es el valor de la función* $s \mapsto \frac{\gamma(s)\psi(s)}{s-1}$ *en* $s=1$ *y* C_2 *el valor de la derivada logarítmica en el mismo punto.*

DEMOSTRACIÓN. Por el Teorema de los residuos y un argumento análogo al de la proposición 3.1

$$J(U) - J_\Delta(U) = 2\pi i \sum_{p_k \text{ polos}} \operatorname{Res}(p_k).$$

Sea $f(s)$ una función holomorfa y $F(s) = \frac{f'(s)}{f(s)}$ su derivada logarítmica, entonces, dado un punto a

$$f(s) = f(a)\left(1 + F(a)(s-a) + O\left((s-a)^2\right)\right)$$

Luego

$$\operatorname{Res}\left(\frac{f(s)}{(s-a)^2}, a\right) = f(a)F(a).$$

La proposición se sigue de aplicar lo anterior a $f(s) = d^{s-1}\frac{\gamma(s)\psi(s)}{s-1}G(U,s)$ en $a=1$, pues el cero de $\gamma(s)\psi(s)$ en $s=1$ es simple y $\gamma\psi$ es holomorfa en el resto de los puntos, al igual que $G(U,s)$.
Entonces

$$\operatorname{Res}\left(\frac{f(s)}{(s-1)^2}, 1\right) = f(1)F(1),$$

donde

$$f(1) = \lim_{s\to 1} \frac{\gamma(s)\psi(s)}{s-1} G(U,1) = C_1 G(U,1)$$

y

$$F(1) = \left.\frac{(d^{s-1})'}{d^{s-1}}\right|_{s=1} + C_2 + \left.\frac{G'(U,s)}{G(U,s)}\right|_{s=1} = \log d + C_2 + \frac{G'(U,1)}{G(U,1)}.$$

□

PROPOSICIÓN 3.3. *Existe una constante $C_3 > 0$ que sólo depende de M y ψ, tal que*

$$|J_\Delta(U)| \leqslant C_3 \sup_{s\in\partial\Delta} |G(U,s)|.$$

DEMOSTRACIÓN. Podemos tomar

$$C_3 = \int_{\partial\Delta} |\gamma(s)\psi(s)(s-1)^{-3}| \frac{ds}{2\pi},$$

que converge por **(C3)**. □

3. Algunos lemas

LEMA 3.4. *Sean $m \in \mathbb{Z}$, $m \geqslant 2$ y $a, \sigma \in \mathbb{R}$ tales que $a < \sigma$.*
Entonces la función $I : \mathbb{R}^*_{>0} \to \mathbb{C}$ dada por $I(x) = \int_{\sigma-i\infty}^{\sigma+i\infty} x^{-s}(s-a)^{-m} \frac{ds}{2\pi i}$ es real positiva. Si además $a \geqslant 0$, entonces I es decreciente y convexa.

DEMOSTRACIÓN. Veremos que

$$I(x) = \begin{cases} \frac{x^{-a}|\log x|^{m-1}}{(m-1)!} & \text{si } x \leqslant 1 \\ 0 & \text{si } x \geqslant 1 \end{cases}$$

Es claro que $I(x)$ es positiva y si $a \geqslant 0$ entonces es decreciente. Además I es C^2 y como x^{-a} es convexa como función en x, resulta que $x \mapsto I(x)$ también lo es.
Si $x > 1$ entonces el integrando tiene una singularidad evitable en $s = a$, y si $x \leqslant 1$ entonces tiene un polo en $s = a$ de orden m y residuo

$$\mathrm{Res}(a) = \frac{1}{(m-1)!}\left[\frac{d^{m-1}}{ds^{m-1}} x^{-s}\right]_{s=a} = x^{-a}\frac{|\log x|^{m-1}}{(m-1)!}.$$

En cualquier caso, por el Teorema de los Residuos es suficiente ver que

$$\lim_{R\to\infty} \int_{C_R} x^{-s}(s-a)^{-m} ds = 0,$$

donde C_R es la semicircunferencia dada por $C_R = \{z \in \mathbb{C} : \ |z| = R, \ \text{ y } \Re s < \sigma\}$.
Pero haciendo el cambio de variables $u = s - a$ tenemos que

$$\left|\int_{C_R} x^{-s}(s-a)^{-m} ds\right| = x^{-a}\left|\int_{C_R} x^{-u}u^{-m} du\right| \leqslant x^{-a}\int_{C_R} x^{\Re s} R^{-m},$$

y esta última integral es $O(x^{-R}R^{-m} + R^{-m})$, que tiende a 0 cuando $R \to \infty$ independientemente del valor de x. □

Sean a, σ y m en las hipótesis del Lema 3.4 y $\mu_1, \dots, \mu_r$ medidas no negativas sobre $\mathbb{R}_+^*$ tales que

$$\mu_i([0,y)) \ll y \text{ cuando } y \to \infty, \qquad \text{y } \mu_i([0,y)) \ll e^{\frac{-1}{y}} \text{ cuando } y \to 0. \tag{6}$$

Observemos que la función $t \mapsto t^{-\sigma}$ es integrable. Para $1 \leqslant j \leqslant r$ y s con $\Re(s) = \sigma$ definimos $\hat{\mu}_j(s) := \int_{\mathbb{R}_+^*} t^{-s} d\mu_j$ y $J(x) = \int_{\sigma-i\infty}^{\sigma+i\infty} \hat{\mu}_1(s) \dots \hat{\mu}_r(s) x^{-s} (s-a)^{-m} \frac{ds}{2\pi i}$.

LEMA 3.5. *J es una función positiva definida sobre $\mathbb{R}_+^*$.*

DEMOSTRACIÓN.

$$J(x) = \int_{\sigma-i\infty}^{\sigma+i\infty} \int_{\mathbb{R}_+^*} t_1^{-s} d\mu_1 \dots \int_{\mathbb{R}_+^*} t_r^{-s} d\mu_r x^{-s} (s-a)^{-m} \frac{ds}{2\pi i}$$

En primer lugar, debemos observar que la condición μ_j no negativa y $t \mapsto t^{-\sigma}$ integrable implica que cada μ_j es una medida σ-finita, además t^{-s} con $\Re s = \sigma$ y t^{-a} también son integrables respecto a cada μ_j y podemos aplicar el Teorema de Fubini.

$$J(x) = \int_{\mathbb{R}_+^*} \dots \int_{\mathbb{R}_+^*} t_r^{-s} \int_{\sigma-i\infty}^{\sigma+i\infty} t_1^{-s} \dots t_r^{-s} x^{-s} (s-a)^{-m} \frac{ds}{2\pi i} d\mu_1 \dots d\mu_r.$$

Por el Lema 3.4

$$J(x) = \int_{\mathbb{R}_+^*} \dots \int_{\mathbb{R}_+^*} I(xt_1 \dots t_r) d\mu_1 \dots d\mu_r.$$

Como la función $t \mapsto I(xt)$ es positiva por el Lema 3.4, entonces $J(x)$ es positiva. Por el mismo lema, si $a \geqslant 0$ la función $x \mapsto I(xt)$ es decreciente y convexa, luego $x \mapsto \int_{\mathbb{R}_+^*} I(xt)dt$ también lo es y más en general $J(x)$. □

LEMA 3.6. *Sean μ_j' medidas positivas definidas en $\mathbb{R}_+^*$ que satisfacen las mismas condiciones que las medidas μ_j, con $1 \leqslant j \leqslant r$. Para cada j se definen $\hat{\mu}_j'$ de forma análoga a $\hat{\mu}_j$, y J' análogo a J.*
Supongamos que $a \geqslant 0$ y $\int_0^x \int_0^{t_3} \int_0^{t_2} \mu_j([0,t_1]) dt_1 dt_2 dt_3 \leqslant \int_0^x \int_0^{t_3} \int_0^{t_2} \mu_j'([0,t_1]) dt_1 dt_2 dt_3$ para todo $x \geqslant 0$ y j ($1 \leqslant j \leqslant r$). Entonces $J \leqslant J'$.

DEMOSTRACIÓN. Por el Teorema de Fubini basta considerar el caso $r = 1$.

Como vimos antes $J(x) = \int_{R_+^*} I(xt) d\mu_1$ y $J'(x) = \int_{R_+^*} I(xt) d\mu_1'$. Ahora podemos aplicar partes cuatro veces,

$$J(x) =$$

$$\Big[I(xt)\mu([0,t])\Big]_0^\infty - \Big[xI'(xt) \int_0^t \mu([0,t_1])dt_1\Big]_0^\infty + \Big[x^2 I''(xt) \int_0^t \int_0^{t_2} \mu([0,t_1])dt_1 dt_2\Big]_0^\infty -$$

$$\Big[x^3 I'''(xt) \int_0^t \int_0^{t_3} \int_0^{t_2} \mu([0,t_1])dt_1 dt_2 dt_3\Big]_0^\infty + \int_0^\infty x^4 I''''(xt) \int_0^t \int_0^{t_3} \int_0^{t_2} \mu([0,t_1])dt_1 dt_2 dt_3 dt$$

Y tenemos un resultado análogo para $J'(x)$. La condición (6) implica que las evaluaciones en cero e infinito en los primeros 4 términos son todas nulas, mientras que la desigualdad de las integrales se deduce de la hipótesis y de observar en la prueba de 3.4 que $x^4 I''''(xt) \geqslant 0$, esto concluye la prueba del lema. □

A nosotros nos van a interesar dos casos, el primer caso en que las medidas μ_j son las imágenes por el homeomorfismo $t \mapsto t^{-1}$ de medidas de la forma $e^{-t}t^{-u-1}dt$, donde $u \leqslant \sigma$. Observar que en este primer caso $\mu_j(s) = \Gamma(s-u)$. El segundo caso es el de medidas de la forma $\sum_{n=0}^{\infty} a_n\delta_n$, donde δ_n es la medida de Dirac en el punto n y (a_n) es una sucesión de reales positivos tales que $\sum_{n=0}^{\infty} a_n n^{-\sigma}$ converge. En el segundo caso $\hat{\mu}_j(s) = \sum_{n=0}^{\infty} a_n n^{-s}$.

Ejemplo 3.7. Sea q una forma cuadrática binaria reducida de discriminante d, y sean

$$\mu = \sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} \delta_{q(m,n)}, \qquad \text{y} \qquad \mu' = \pi\delta_{\frac{\sqrt{d}}{2}} + \nu,$$

donde δ_x es la medida de Dirac en x y ν es la medida con densidad $\frac{\pi}{\sqrt{d}}$ respecto a la medida de Lebesgue μ_1 en $[\frac{\sqrt{d}}{2}, +\infty]$, es decir $\nu(A) = \int_A \frac{\pi}{\sqrt{d}} d\mu_1 = \frac{\pi}{\sqrt{d}}\mu_1$. Definamos ahora $N_q(x) := \#\{(m,n) \in \mathbb{Z}\times\mathbb{N}^* \ : \ q(m,n) \leqslant x\}$. En el capítulo 1 vimos que si $q(x,y) = ax^2 + bxy + cy^2$ es una forma reducida, entonces $N_q(x)$ es vació para $x < c$, también vimos que $\frac{\sqrt{d}}{2} < c \leqslant \frac{d}{3a}$. De la primera desigualdad se deduce que

$$\int_0^x N_q(t)dt = \begin{cases} 0 & \text{si } x < \frac{\sqrt{d}}{2} \\ \int_{\frac{\sqrt{d}}{2}}^x N_q(t)dt & \text{si } x \geqslant \frac{\sqrt{d}}{2}. \end{cases}.$$

Es fácil ver que $q(m,n) \leqslant x$ si y sólo si $\frac{(2am+bn)^2+dn^2}{4a} \leqslant x$, luego $0 < n \leqslant \sqrt{\frac{4ax}{d}}$ y $\frac{-\sqrt{4ax-dn^2}-bn}{2a} \leqslant m \leqslant \frac{\sqrt{4ax-dn^2}-bn}{2a}$. Ahora, fijo n hay a lo más $\frac{\sqrt{4ax-dn^2}}{a} + 1$ posibilidades para m, por lo que

(7)
$$N_q(x) \leqslant \sum_{n=1}^{\lfloor\sqrt{\frac{4ax}{d}}\rfloor} \left(\tfrac{\sqrt{4ax-dn^2}}{a} + 1\right)$$

(8)
$$\leqslant \sum_{n=0}^{\lfloor\sqrt{\frac{4ax}{d}}\rfloor} \tfrac{\sqrt{4ax-dn^2}}{a} - \tfrac{\sqrt{4ax}}{a} + \sqrt{\tfrac{4ax}{d}}$$

(9)
$$\leqslant \int_0^{\sqrt{\frac{4ax}{d}}} \tfrac{\sqrt{4ax-dt^2}}{a}dt + \tfrac{\sqrt{4ax}}{a} - \tfrac{\sqrt{4ax}}{a} + \sqrt{\tfrac{4ax}{d}} \text{ (pues el integrando es decreciente)}$$

(10)
$$= \tfrac{1}{a}\int_0^1 \tfrac{4ax}{d}\sqrt{1-u^2}du + \sqrt{\tfrac{4ax}{d}} \quad \left(\text{cambio de variables } u = t\sqrt{\tfrac{4ax}{d}}\right)$$

(11)
$$= \tfrac{\pi x}{\sqrt{d}} + \sqrt{\tfrac{4ax}{d}}.$$

Observemos que con los cálculos anteriores tenemos un término $\sqrt{\frac{4ax}{d}}$ que no puede ser eliminado, por lo que con ese método no podemos deducir que las médidas cumplen

la desigualdad

$$\int_0^x \mu([0,t])\,dt \leqslant \int_0^x \mu'([0,t])\,dt.$$

Esta desigualdad es parte de la hipótesis en la versión de Oesterlé del lema 3.6, que se encuentra en [Oe]. Oesterlé afirma que estas medidas cumplen la desigualdad, pero el artículo al que cita no fue publicado. Watkins remedia esto dando la versión enunciada del Lema 3.6 con integrales triples y probando que μ y μ' están en sus hipótesis.

PROPOSICIÓN 3.8. *Para todo $x \geqslant 0$ las medidas μ y μ' satisfacen*

$$\int_0^x \int_0^{t_3} \int_0^{t_2} \mu([0,t_1])\,dt_1dt_2dt_3 \leqslant \int_0^x \int_0^{t_3} \int_0^{t_2} \mu'([0,t_1])\,dt_1dt_2dt_3\,.$$

DEMOSTRACIÓN. Veremos un esbozo de la prueba, los detalles se pueden ver en [Wat].

Observemos primero que como $N_q(t) = 0$ para $t \leqslant \frac{\sqrt{d}}{2}$ ver la desigualdad anterior es igual a ver la siguiente,

$$\int_0^x \int_0^{t_3} \int_0^{t_2} N_q(t_1)\,dt_1dt_2dt_3 \leqslant \int_0^x \int_0^{t_3} \int_0^{t_2} \pi + \tfrac{\pi}{\sqrt{d}}(t_1 - \tfrac{\sqrt{d}}{2})\,dt_1dt_2dt_3. \tag{12}$$

Sea $\zeta_q(s) = \frac{1}{2} \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} q(m,n)^{-s}$, por (1) tenemos que

$$\sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} q(m,n)^{-s} = \zeta_q(s) - a(q)^{-s}\zeta(2s).$$

ζ_q satisface las siguientes propiedades:

(a) ζ_q converge para $\Re s > 1$ y se extiende de forma analítica a una función en el plano complejo excepto por un polo en $s = 1$ de residuo $\frac{\pi}{\sqrt{d}}$. Más aún, la función $\frac{\sqrt{d}}{2\pi}\Gamma(s)\zeta_q(s)$ es invariante por el cambio de variable $s \mapsto 1 - s$.
(b) Si $\Re s = \frac{3}{2}$ entonces $|\zeta_q(s)| \leqslant \frac{13}{a(q)^{\frac{3}{2}}}$.

Se puede ver que la integral de la izquierda en (12) es

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \left(\zeta_q(s) - a(q)^{-s}\zeta(2s)\right) \frac{x^{s+3}}{s(s+1)(s+2)(s+3)}\,ds.$$

Como $\zeta(2s)$ tiene ceros simples en los enteros negativos, el integrando tiene singularidades evitables en $s = -1, s = -2, s = -3$. Por otra parte, $\zeta_q(s)$ solo tiene un polo simple en $s = 1$ de residuo $\frac{\pi}{\sqrt{d}}$ y $\zeta(2s)$ tiene un polo simple en $s = \frac{1}{2}$ con residuo 1.

Si consideramos la región delimitada por $\Re s = \frac{-1}{2}$ y $\Re s = 2$ vemos que esta encierra los polos del integrando, los residuos son los siguientes:

$$\operatorname{Res}(s=0) = (\zeta_q(0) - \zeta(0))\,\frac{x^3}{6} = \left(\tfrac{1}{2} + \tfrac{1}{2}\right)\frac{x}{6}$$
$$\operatorname{Res}(s=\tfrac{1}{2}) = \left(-\frac{1}{a(q)^{\frac{1}{2}}}\right)\frac{8x^{\frac{7}{2}}}{105}$$
$$\operatorname{Res}(s=1) = \left(\frac{\pi}{\sqrt{d}}\right)\frac{x^4}{24}.$$

La idea es ahora cambiar el dominio de integración por $\Re s = -\frac{1}{2}$ en lugar de usar $\Re s = 2$, y luego acotar absolutamente los dos términos de la integral usando la ecuación funcional y la cota para ζ_q en $\Re s = \frac{3}{2}$ dadas en 3.7. La primera integral es

$$\left|\frac{1}{2\pi i}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty} \zeta_q(s)\frac{x^{s+3}}{s(s+1)(s+2)(s+3)}\,ds\right|$$
$$\leqslant \frac{d}{4\pi^2}\frac{2}{2\pi}\int_0^\infty \left|\frac{\Gamma(\frac{3}{2}+it)}{\Gamma(-\frac{1}{2}-it)}\right|\left|\frac{x^{\frac{5}{2}}13a(q)^{-\frac{3}{2}}}{(-\frac{1}{2}+it)(\frac{1}{2}+it)(\frac{3}{2}+it)(\frac{5}{2}+it)}\right| dt.$$

Por las propiedades de Γ esto es igual a

$$x^{\frac{5}{2}}a(q)^{-\frac{3}{2}}\frac{d}{4\pi^3}\int_0^\infty \frac{1}{\sqrt{\frac{9}{4}+t^2}\sqrt{\frac{25}{4}+t^2}}\,dt\,.$$

El valor de esta integral es aproximadamente $0.7981211 \leqslant \frac{4}{5}$, entonces se obtiene la cota $\frac{dx^{\frac{5}{2}}}{11a(q)^{\frac{3}{2}}}$.

Con un método similar podemos acotar la segunda integral,

$$\left|\frac{1}{2\pi i}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty} \zeta(2s)a(q)^{-s}\frac{x^{s+3}}{s(s+1)(s+2)(s+3)}ds\right| \leqslant \frac{1}{25}a(q)^{\frac{3}{4}}x^{\frac{9}{4}}.$$

Lo visto hasta ahora implica que el lado izquierdo de (12) es menor o igual a

$$\frac{x^3}{6} - \frac{8x^{\frac{7}{2}}}{a(q)^{\frac{1}{2}}105} + \frac{\pi x^4}{24\sqrt{d}} + \frac{dx^{\frac{5}{2}}}{11a(q)^{\frac{3}{2}}} + \frac{a(q)^{\frac{3}{4}}x^{\frac{9}{4}}}{25}.$$

Por otra parte, el lado derecho de (12) es exactamente

$$\int_0^x\int_0^{t_3}\int_0^{t_2} \pi + \tfrac{\pi}{\sqrt{d}}(t_1 - \tfrac{\sqrt{d}}{2})dt_1dt_2dt_3 = \frac{\pi(x-\frac{\sqrt{d}}{2})^3}{6} - \frac{\pi}{\sqrt{d}}\frac{(x-\frac{\sqrt{d}}{2})^4}{24}$$
$$= \frac{\pi x^4}{24\sqrt{d}} + \frac{\pi x^3}{12} - \frac{3\pi x^2\sqrt{d}}{16} + \frac{5\pi xd}{48} - \frac{7\pi d^{\frac{3}{2}}}{384}.$$

Para probar el lema basta ver entonces que la cota obtenida para el lado izquierdo es menor a la expresión obtenida para el derecho. Para eso separamos en dos casos, recordando que $a(q) \leqslant \sqrt{\frac{d}{3}}$ y $\frac{\sqrt{d}}{2} \leqslant 4$ (el otro caso es trivial).

- Cuando $x \leqslant \frac{9d}{4a(q)}$ entonces se puede refinar el argumento del inicio y obtener la siguiente desigualdad sin integrar tres veces

$$N_q(t_1) \leqslant \pi + \frac{\pi}{\sqrt{d}}\left(t_1 - \frac{\sqrt{d}}{2}\right) = \frac{\pi}{2} + \frac{\pi t_1}{\sqrt{d}}.$$

  Observemos que 7 nos da la desigualdad $N_q(t_1) \leqslant \frac{\pi t}{\sqrt{d}} + 3$, que no es suficiente.
- Cuando $x \geqslant \frac{9d}{4a(q)}$ entonces consideramos α y β tales que $a = \frac{\sqrt{d}}{\alpha}$ y $x = \beta\frac{d}{a}$. La desigualdad de las integrales triples se traduce a:

$$-\frac{8\alpha^4\beta^{\frac{7}{2}}}{105} + \frac{\alpha^3\beta^3}{6} + \frac{\alpha^4\beta^{\frac{5}{2}}}{11} + \frac{\alpha^{\frac{3}{2}}\beta^{\frac{9}{4}}}{25} \leqslant \frac{\pi\alpha^3\beta^3}{12} - \frac{3\pi\alpha^2\beta^2}{16} + \frac{5\pi\alpha\beta}{48} - \frac{7\pi}{384},$$

  que vale para todo que $\alpha \geqslant \sqrt{3}$ y $\beta \geqslant \frac{9}{4}$.

□

Acabamos de ver que μ y μ' están en las hipótesis del Lema 3.6. Finalmente observemos que para s con $\Re(s) = \sigma > 1$

$$\hat{\mu}(s) = \int_{\mathbb{R}_+^*} t^{-s} d \sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} \delta_{q(m,n)} = \sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} q(m,n)^{-s}$$

y

$$\begin{aligned}
\hat{\mu'}(s) = \int_{R_+^*} t^{-s} d\mu' &= \pi\left(\frac{\sqrt{d}}{2}\right)^{-s} + \frac{\pi}{\sqrt{d}}\int_{\frac{\sqrt{d}}{2}}^{+\infty} t^{-s}dt \\
&= \pi\left(\frac{\sqrt{d}}{2}\right)^{-s} + \frac{\pi}{\sqrt{d}}\frac{1}{s-1}\left(\frac{\sqrt{d}}{2}\right)^{1-s} \\
&= \pi\left(\frac{\sqrt{d}}{2}\right)^{-s}\left(1 + \frac{1}{2(s-1)}\right) \\
&= \pi\frac{s-\frac{1}{2}}{s-1}\left(\frac{\sqrt{d}}{2}\right)^{-s}.
\end{aligned}$$

Ejemplo 3.9. Consideremos las medidas

$$\nu = \sum_{n=1}^{\infty} \delta_n \qquad \text{y} \qquad \nu' = \delta_1 + \mu_1,$$

donde μ_1 es la medida de Lebesgue en $[1,\infty)$; y sean μ y μ' las imágenes vía $t \mapsto t^2$ de ν y ν' respectivamente.

Para $t \geqslant 0$ se tiene que $\nu([0,t]) \leqslant \nu'([0,t])$ y por lo tanto $\mu([0,t]) \leqslant \mu'([0,t])$ $\forall t > 0$, esto implica que nuevamente estamos en las hipótesis del Lema 3.6.

Sea s tal que $\Re(s) = \sigma > 1$, calculemos $\hat{\mu}(s)$ y $\hat{\mu'}(s)$.

$$\hat{\mu}(s) = \int_{\mathbb{R}_+^*} t^{-2s} d\nu = \sum_{n=0}^{\infty} t^{-2s}.$$
$$\hat{\mu'}(s) = \int_{\mathbb{R}_+^*} t^{-2s} d\nu' = 1 + \int_1^{\infty} t^{-2s} dt = 1 + \frac{1}{2s-1} = \frac{s}{s-\frac{1}{2}}.$$

4. Cota para J(U)*

A lo largo de esta sección vamos a asumir que $\sigma > 1$. Recordemos las definiciones de $J(U)$ y $J(U)^*$.

- $G(U,s) = \prod_{p<U} G_p(s)$
- $J(U) = \int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-1}\gamma(s)\psi(s)G(U,s)(s-1)^{-3}\frac{ds}{2\pi i}$
- $G(U,s)^* = G(s) - G(U,s)$
- $J(U)^* = \int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-1}\gamma(s)\psi(s)G(U,s)^*(s-1)^{-3}\frac{ds}{2\pi i}$

Haciendo el cambio de variables $s \mapsto s + \frac{1}{2}$ podemos escribir

$$J(U)^* = \int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}}\gamma(s+\tfrac{1}{2})\psi(\gamma+\tfrac{1}{2})G(U,s+\tfrac{1}{2})^*(s-\tfrac{1}{2})^{-3}\frac{ds}{2\pi i}.$$

Sea $H(x) = \int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}}\gamma(s+\frac{1}{2})x^{-s}(s-\frac{1}{2})^{-3}$, recordemos que $\gamma(s+\frac{1}{2}) = M^{s+\frac{1}{2}}\Gamma(s+\frac{1}{2})^2$. Observando que $\Gamma(s+\frac{1}{2}) = \hat{\mu}(s+\frac{1}{2})$ para $\mu = e^{-t}t^{-1}dt$ tenemos que $H(x) = J\left(\frac{x}{Md}\right)$ para $\mu_1 = \mu_2 = \mu$, por lo tanto podemos usar el Lema 3.5 para ver que H es una función positiva y decreciente en R_+^*.

Sea ahora $\varphi(s) = \sum_{n=0}^{\infty} a_n n^{-s}$ una serie de Dirichlet absolutamente convergente tal que $\psi(s+\frac{1}{2})G(U,s+\frac{1}{2})^* \ll \varphi(s)$, y tomemos $x = 1$. Como H es positiva,

$$\int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}}\gamma(s+\tfrac{1}{2})\varphi(s)(s-\tfrac{1}{2})^{-3}\frac{ds}{2\pi i} = \sum_{n=0}^{\infty}\int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}}\gamma(s+\tfrac{1}{2})a_n(s-\tfrac{1}{2})^{-3}\frac{ds}{2\pi i}.$$

Acotando término a término vemos que

$$|J(U)^*| \leqslant \int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}}\gamma(s+\tfrac{1}{2})\varphi(s)(s-\tfrac{1}{2})^{-3}. \tag{13}$$

El resultado anterior puede aplicarse al caso particular en que φ es el cuadrado de la serie $\zeta_K(s) = \sum_{q\in Q_d^{red}}\left(a(q)^{-s}\zeta(2s) + \sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} q(m,n)^{-s}\right)$ quitando los términos de la forma $a(q)^{-s}a(q')^{-s}\zeta(2s)^2$ donde $a(q)a(q') < U$, veamos esto.

Por la condición **(C1)** $\psi(s) \ll \zeta(2s-1)^2$ y $G(s) \ll \left(\frac{\zeta_K(s-\frac{1}{2})}{\zeta(2s-1)}\right)^2$, por lo tanto

$$\psi(s+\tfrac{1}{2})G(U,s+\tfrac{1}{2})^* \ll \zeta_K(s)^2 - \zeta(2s)^2 G(U,s+\tfrac{1}{2}) \ll \varphi$$

pues los módulos de los términos de $G(U, s+\frac{1}{2})$ están acotados por los de $\frac{\zeta_K(s)^2}{\zeta(2s)^2}$.

Como en el capítulo 1 vimos que

$$\frac{\zeta_K(s)}{\zeta(2s)} = \prod_p \frac{1+p^{-s}}{(1-\chi(p)p^{-s})} = \sum_{q\in Q_{d_K}^{red}} \left(a(q)^{-s} + \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{N}^* \\ mcd(m,n)=1}} q(m,n)^{-s} \right),$$

resulta que podemos quitarle a $\zeta_K(s)^2$ los elementos de la forma $a(q)a(q')\zeta(2s)^2$ con $a(q)a(q') < U$.

Proposición 3.10. *Recordemos que h corresponde al número de clases del cuerpo cuadrático K. Se cumple que*

$$|J(U)^*| \leqslant J_1 + J_2 + J_3,$$

donde

$$J_1 = h^2 \int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}} \gamma(s+\tfrac{1}{2}) U^{-s} s^2 (s-\tfrac{1}{2})^{-5} \tfrac{ds}{2\pi i} \tag{14}$$

$$J_2 = 2\pi h \int_{\sigma-i\infty}^{\sigma+i\infty} 2^s d^{\frac{s-1}{2}} \gamma(s+\tfrac{1}{2}) \frac{1}{s-1} \left(\sum_{q\in Q_d^{red}} a(q)^{-s} \right) \zeta(2s)(s-\tfrac{1}{2})^{-2} \frac{ds}{2\pi i} \tag{15}$$

$$J_3 = \pi^2 \frac{h^2}{\sqrt{d}} \int_{\sigma-i\infty}^{\sigma+i\infty} 2^{2s} \gamma(s+\tfrac{1}{2}) \frac{1}{(s-1)^2} (s-\tfrac{1}{2})^{-1} \frac{ds}{2\pi i} \tag{16}$$

Demostración. Ya vimos que $|J(U)^*| \leqslant \int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}} \gamma(s+\frac{1}{2}) \varphi(s) (s-\frac{1}{2})^{-3}$ para $\varphi(s)$ igual a $\zeta_K(s)$ eliminando los términos de la forma $a(q)^{-s}a(q')^{-s}\zeta(2s)^2$ tales que $a(q)a(q') < U$. Ahora separaremos φ en términos de la forma $a(q)^{-s}a(q')^{-s}\zeta(2s)^2$, $\sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} q(m,n) \sum_{(m',n')\in\mathbb{Z}\times\mathbb{N}^*} q'(m',n')$, y $a(q)^{-s}\zeta(2s) \sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} q(m,n)$. Por simplicidad les llamaremos términos de tipo 1, tipo 2 y tipo 3 respectivamente y notaremos φ_i a la suma sobre todos las formas $q, q' \in Q_d^{red}$ de elementos de tipo i.

Observación 3.11.

(1) *Podemos cambiar los términos de tipo 1 por $U^{-s}\zeta(2s)^2$ pues φ eliminó los $a(q)a(q')$ menores a U.*
(2) *El Lema 3.6 aplicado al ejemplo 3.7 nos permite reemplazar $\sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}^*} q(m,n)$ por $\pi \frac{s-\frac{1}{2}}{s-1} 2^s d^{-\frac{s}{2}}$ para cada forma $q \in Q_d^{red}$, y el mismo lema aplicado al ejemplo 3.9 nos permite reemplazar $\zeta(2s)^2$ por $\left(\frac{s}{s-\frac{1}{2}}\right)^2$.*
(3) *Los dos puntos anteriores nos permiten reemplazar términos del tipo 1 por el término $U^{-s}s^2 \frac{1}{\left(s-\frac{1}{2}\right)^2}$, hay a lo más h^2 términos de este tipo.*
(4) *Análogamente, podemos reemplazar términos de tipo 2 por $a(q)\zeta(2s)\pi \frac{s-\frac{1}{2}}{s-1} 2^s d^{-\frac{s}{2}}$.*

(5) *Por último podemos reemplazar cada término del tipo 3 por* $\pi^2 \left(\frac{s-\frac{1}{2}}{s-1}\right)^2 2^{2s} d^{-s}$, *hay* h^2 *términos de este tipo.*

Aplicando la observación previa obtenemos lo siguiente:

(J1) Por el ítem 3

$$\int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}}\gamma(s+\tfrac{1}{2})\varphi_1(s)(s-\tfrac{1}{2})^{-3}\frac{ds}{2\pi i} \leqslant J_1.$$

(J2) Por el ítem 4

$$\int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}}\gamma(s+\frac{1}{2})\varphi_2(s)(s-\tfrac{1}{2})^{-3}\frac{ds}{2\pi i} \leqslant$$

$$\int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}}\gamma(s+\tfrac{1}{2})\left(\sum_{q\in Q_d^{red}} a(q)\right)\zeta(2s)\pi\frac{s-\frac{1}{2}}{s-1}2^s d^{-\frac{s}{2}}(s-\tfrac{1}{2})^{-3}\frac{ds}{2\pi i} \leqslant J_2.$$

(J3) Por el item 5

$$\int_{\sigma-i\infty}^{\sigma+i\infty} d^{s-\frac{1}{2}}\gamma(s+\tfrac{1}{2})\varphi_3(s)(s-\tfrac{1}{2})^{-3}\frac{ds}{2\pi i} \leqslant J_3,$$

de donde se deduce la proposición. □

Para finalmente hallar las cotas para J_1, J_2, J_3 necesitamos una proposición más.

PROPOSICIÓN 3.12. *Para todo* $x > 0$ *y* ε *tal que* $0 < \varepsilon \leqslant \frac{1}{2}$ *se satisfacen las siguientes desigualdades.*

(1)

$$\int_{\sigma-i\infty}^{\sigma+i\infty} x^s s^2 (s-\tfrac{1}{2})^{-5}\frac{ds}{2\pi i} \leqslant \left[\frac{1}{4!}\frac{\partial}{\partial s^4}(x^s s^2) + \frac{1}{3!}\frac{\partial}{\partial s^2}(x^s)\right]_{s=\frac{1}{2}}.$$

(2)

$$\int_{\sigma-i\infty}^{\sigma+i\infty} x^s \frac{1}{s-1}(s-\tfrac{1}{2})^{-2}\frac{ds}{2\pi i} \leqslant 4x.$$

(3)

$$\int_{\sigma-i\infty}^{\sigma+i\infty} x^s \frac{1}{(s-1)^2}(s-\tfrac{1}{2})^{-1}\frac{ds}{2\pi i} \leqslant \frac{x^{1+\varepsilon}}{\varepsilon}.$$

DEMOSTRACIÓN. Por simplicidad denotemos por F_i al integrando del ítem (i), para probar la proposición podemos aplicar en cada caso el Teorema de los Residuos. Observemos que de forma similar a lo que ocurre para el lema 3.4, cuando $x < 1$ las singularidades son evitables y las integrales nulas. Supongamos entonces que $x \geqslant 1$.

(1)

$$\begin{aligned}\int_{\sigma-i\infty}^{\sigma+i\infty} x^s s^2(s-\tfrac{1}{2})^{-5}\frac{ds}{2\pi i} &= \int_{D_R} x^s s^2(s-\tfrac{1}{2})^{-5}\frac{ds}{2\pi i} - \int_{\gamma R} x^s s^2(s-\tfrac{1}{2})^{-5}\frac{ds}{2\pi i} \\ &= (2\pi i)\mathrm{Res}\left(F_1, \tfrac{1}{2}\right) \text{ tomando límite } R\to\infty \\ &= \frac{1}{4!}\left[\frac{\partial}{\partial s^4}(x^s s^2)\right]_{s=\frac{1}{2}} \\ &\leqslant \left[\frac{1}{4!}\left(\frac{\partial}{\partial s^4}(x^s s^2)\right) + \frac{1}{3!}\frac{\partial}{\partial s^2}(x^s)\right]_{s=\frac{1}{2}}\end{aligned}$$

(2) De forma similar

$$\begin{aligned}\int_{\sigma-i\infty}^{\sigma+i\infty} x^s\frac{1}{s-1}(s-\tfrac{1}{2})^{-2}\frac{ds}{2\pi i} &= \mathrm{Res}\,(F_2,1) + \mathrm{Res}\left(F_2,\tfrac{1}{2}\right) \\ &= 4x + \left.\frac{\log x x^s(s-1)-x^2}{(s-1)^2}\right|_{s=\frac{1}{2}} \\ &= 4x - 2\log x\sqrt{x} - 4\sqrt{x} \\ &\leqslant 4x.\end{aligned}$$

(3) Como el integrando $F_3(s) = x^s\left(\frac{1}{(s-1)^2}\right)^2(s-\frac{1}{2})^{-1}$ no tiene polos en $\Re s > 1$ y las integrales sobre los segmentos $\{\sigma \geqslant \Re s \geqslant \sigma+\varepsilon,\ \Im s = \pm R\}$ tienden a 0 cuando $R\to\infty$, por el Teorema de los residuos la integral

$$\int_{\sigma-i\infty}^{\sigma+i\infty} F_3(s)\frac{ds}{2\pi i} = \int_{\sigma+\varepsilon-i\infty}^{\sigma+\varepsilon+i\infty} F_3(s)\frac{ds}{2\pi i}$$

es positiva. Sean

$$F_4(s) := x^s\frac{1}{(s-1)^2-\varepsilon^2}\left(s-\tfrac{1}{2}\right)^{-1}, I(s) := x^s\left(s-\tfrac{1}{2}\right)^{-1} = F_3(s)(s-1)^2 \quad ,$$

entonces,

$$\begin{aligned}\int_{\sigma-i\infty}^{\sigma+i\infty} F_3(s)ds &= \int_{\sigma+\varepsilon-i\infty}^{\sigma+\varepsilon+i\infty} \Re F_3(s)ds \\ &= \int_{\sigma+\varepsilon-i\infty}^{\sigma+\varepsilon+i\infty} \Re I(s)\Re\left(\frac{1}{(s-1)^2}\right) - \Im I(s)\Im\left(\frac{1}{(s-1)^2}\right)ds \\ &\leqslant \int_{\sigma+\varepsilon-i\infty}^{\sigma+\varepsilon+i\infty} \Re I(s)\Re\left(\frac{1}{(s-1)^2-\varepsilon^2}\right) - \Im I(s)\Im\left(\frac{1}{(s-1)^2}\right)ds \\ &= \Re\int_{\sigma+\varepsilon-i\infty}^{\sigma+\varepsilon+i\infty} F_4(s)\frac{ds}{2\pi i}ds \\ &= \int_{\sigma+\varepsilon-i\infty}^{\sigma+\varepsilon+i\infty} F_4(s)\frac{ds}{2\pi i}ds.\end{aligned}$$

Por último,

$$\begin{aligned}\int_{\sigma-i\infty}^{\sigma+i\infty} F_3(s)\frac{ds}{2\pi i} &\leqslant \int_{\sigma+\varepsilon-i\infty}^{\sigma+\varepsilon+i\infty} x^s \frac{1}{(s-1+\varepsilon)(s-1-\varepsilon)}(s-\tfrac{1}{2})^{-1}\frac{ds}{2\pi i}\\ &= \operatorname{Res}\left(F_4(s), 1+\varepsilon\right) + \operatorname{Res}\left(F_4(s), 1-\varepsilon\right)\\ &= x^{1+\varepsilon}\frac{(1+\varepsilon)^2}{2\varepsilon}(\tfrac{1}{2}+\varepsilon)^{-1} - x^{1-\varepsilon}\frac{(1-\varepsilon)^2}{2\varepsilon}(\tfrac{1}{2}-\varepsilon)^{-1}\\ &\leqslant x^{1+\varepsilon}\frac{(1+\varepsilon)^2}{2\varepsilon}(\tfrac{1}{2}+\varepsilon)^{-1}\\ &= \frac{x^{1+\varepsilon}}{\varepsilon+2\varepsilon^2}\\ &\leqslant \frac{x^{1+\varepsilon}}{\varepsilon}.\end{aligned}$$

□

Proposición 3.13.

(a) $J_1 \leqslant C_4\frac{h^2}{\sqrt{U}}\left(|\log\frac{dM}{U}|+3\right)^4$, *donde* $C_4 = \frac{M}{96}$.

(b) $J_2 \leqslant C_5 h \sum_{q\in Q_d^{red}} a(q)^{-1}$, *donde* $C_5 = \frac{2\pi^4}{3}M^{\frac{3}{2}}$.

(c) $J_3 \leqslant C_6\frac{h^2}{\sqrt{d}}$, *donde* $C_6 = 4\pi^2 \mathrm{e} M^{\frac{3}{2}}\sup(2,\log(4M))$

Demostración.

(a) Usando Fubini y la proposición previa

$$\begin{aligned}J_1 &= \tfrac{h^2}{\sqrt{d}}\int_{\sigma-i\infty}^{\sigma+i\infty}\Gamma^2(s+\frac{1}{2})\left(\frac{dM}{U}\right)^s s^2(s-\tfrac{1}{2})^{-5}\frac{ds}{2\pi i}\\ &= \tfrac{h^2}{\sqrt{d}}\int_0^\infty\int_0^\infty e^{-t_1}e^{-t_2}\frac{1}{\sqrt{t_1t_2}}\int_{\sigma-i\infty}^{\sigma+i\infty}\Gamma^2(s+\tfrac{1}{2})\left(\tfrac{t_1t_2dM}{U}\right)^s s^2(s-\tfrac{1}{2})^{-5}\frac{ds}{2\pi i}dt_1dt_2\\ &\leqslant \left[\tfrac{h^2}{\sqrt{d}}\int_0^\infty\int_0^\infty e^{-t_1}e^{-t_2}\frac{1}{\sqrt{t_1t_2}}\Big[\frac{1}{4!}\frac{\partial}{\partial s^4}\left(\left(\tfrac{dMt_1t_2}{U}\right)^s s^2\right)+\right.\\ &\qquad\left.\frac{1}{3!}\frac{\partial}{\partial s^2}\left(\frac{dMt_1t_2}{U}\right)^s\Big]_{s=\frac{1}{2}}dt_1dt_2\right]\\ &= \tfrac{h^2M}{U}\left[\frac{1}{4!}\frac{\partial}{\partial s^4}\left(\Gamma(s+\tfrac{1}{2})^2\left(\tfrac{dM}{U}\right)^{s-\frac{1}{2}}s^2\right)+\tfrac{1}{3!}\frac{\partial}{\partial s^2}\left(\Gamma(s+\tfrac{1}{2})^2\left(\tfrac{dM}{U}\right)^{s-\frac{1}{2}}\right)\right]_{s=\frac{1}{2}}\end{aligned}$$

Haciendo este último cálculo se ve que $J_1 \leqslant \frac{1}{96}P(\log\frac{dm}{U})$ donde P es un polinomio mónico de grado 4 y los coeficientes de sus monomios de grado d menor o igual a 3 están acotados por $\left(\frac{M}{96}\right)^d 3^{4-l}$, esto implica (a).

(b) Por Fubini

$$J_2 = \left[\frac{\pi h}{\sqrt{d}}\int_0^\infty\int_0^\infty e^{-t_1}e^{-t_2}\sqrt{t_1}\sqrt{t_2}\int_{\sigma-i\infty}^{\sigma+i\infty}\Big(\sum_{q\in Q_d^{red}} a(q)^{-s}\Big)\Big(\sum_{n=0}^{\infty} n^{-2s}\Big)\right.$$
$$\left.\Big(2M\sqrt{d}t_1t_2\Big)^s\,\frac{s}{s-1}(s-\frac{1}{2})^{-3}\frac{ds}{2\pi i}dt_1dt_2\right].$$

Como $\zeta(2s)$ y $\sum_{q\in Q_d^{red}} a(q)^{-s}$ convergen absolutamente, la integral conmuta con las sumas y por lo tanto, de aplicar la proposición previa resulta

$$J_2 = \pi h\int_0^\infty e^{-t}8\Big(\sum_{q\in Q_d^{red}} a(q)^{-1}\Big)\zeta(2)2Mtdt_1dt_2 = \frac{16\pi h}{\sqrt{d}}\Big(\sum_{q\in Q_d^{red}} a(q)^{-1}\Big)\gamma(\tfrac{3}{2})\zeta(2).$$

(c) Por Fubini J_3 es

$$J_3 = \frac{\pi^2}{4}\frac{h^2}{\sqrt{d}}\int_0^{\infty\,\int_0^\infty} e^{-t_1}e^{-t_2}\sqrt{t_1}\sqrt{t_2}\int_{\sigma-i\infty}^{\sigma+i\infty}(4Mt_1t_2)^s\Big(\frac{s}{s-1}\Big)^2(s-\tfrac{1}{2})^{-3}\frac{ds}{2\pi i}dt_1dt_2.$$

Por la proposición previa

$$J_3 \leqslant \frac{\pi^2}{4}\frac{h^2}{\sqrt{d}}\int_0^\infty\int_0^\infty e^{-t_1}e^{-t_2}\sqrt{t_1}\sqrt{t_2}\frac{4}{\varepsilon}(4Mt_1t_2)^{1+\varepsilon}dt = \frac{4\pi^2h^2}{\sqrt{d}}M^{\frac{3}{2}}\Gamma(\frac{3}{2}+\varepsilon)^2\frac{(4M)^\varepsilon}{\varepsilon}$$

para $\varepsilon \leqslant \frac{1}{2}$. Tomemos $\varepsilon = (\sup(2,\log(4M)))^{-1}$, en este caso

$$\Gamma(\frac{3}{2}+\varepsilon)^2 \leqslant 1 \qquad \text{y} \qquad (4M)^\varepsilon \leqslant \mathrm{e}$$

y eso concluye (c).

□

5. Elección de U

Fijemos $U = \Big(\frac{\sqrt{d}}{2}\Big)^{\frac{1}{\mathrm{m}}}$ donde m es el mínimo entero que satisface $\mathrm{m}^2+\mathrm{m} \geqslant \frac{h}{2}$ si $h \neq 4$ y $\mathrm{m} = \frac{3}{2}$ si $h = 4$.

Lema 3.14. *Existe a lo sumo un primo $p \leqslant U$ que descompone en K, y si tal primo existe entonces $p \geqslant \big(\frac{d}{4}\big)^{\frac{1}{h}}$.*

Sea q el divisor primo más grande de d, entonces $q \geqslant U$.

Demostración. Supongamos que existen p y p' en las hipótesis del lema. Entonces

$$\frac{1+p^{-s}}{1-p^{-s}}\frac{1+p'^{-s}}{1-p'^{-s}} \ll \prod_{p\text{ primo}}\frac{1+p^{-s}}{1-\chi(p)p^{-s}} = \frac{\zeta_K(s)}{\zeta(2s)}.$$

Observemos que $p^lp'^{l'} \leqslant \max\{p,p'\}^{l+l'} \leqslant \frac{\sqrt{d}}{2}$ para todo par $(l,l') \in \mathbb{N}^2$ tal que $l+l' \leqslant \lfloor \mathrm{m} \rfloor$ ($\lfloor \mathrm{m} \rfloor \neq \mathrm{m}$ solo si $h = 4$). Escribamos

$$\frac{1+p^{-s}}{1-p^{-s}}\frac{1+p'^{-s}}{1-p'^{-s}} = (1+p^s)(1+p'^s)\sum_{l=0}^{\infty}p^{-ls}\sum_{l'=0}^{\infty}p'^{-l's} =: \sum_{n=0}^{\infty}c_nn^{-s}$$

Por 1.37 (b) $\sum_{n\leqslant\frac{\sqrt{d}}{2}} c_n \leqslant h$.

Como los pares $(l,l') \in L = \{(0,0),(0,\lfloor m\rfloor),(\lfloor m\rfloor,0),(\lfloor m\rfloor-1,1),(1,\lfloor m\rfloor-1)\}$ satisfacen $l+l' \leqslant \lfloor m\rfloor$, tenemos que

$$\sum_{(l,l')\in L} c_{p^l p^{l'}} \leqslant h,$$

de donde

$$1+2\lfloor \mathrm{m}\rfloor+2\lfloor \mathrm{m}\rfloor+4\frac{\lfloor \mathrm{m}\rfloor(\lfloor \mathrm{m}\rfloor-1)}{2} \leqslant \sum_{(l,l')\in L} c_{p^l p^{l'}} \leqslant h.$$

Pero, por otra parte,

$$1+2\lfloor \mathrm{m}\rfloor+2\lfloor \mathrm{m}\rfloor+4\frac{\lfloor \mathrm{m}\rfloor(\lfloor \mathrm{m}\rfloor-1)}{2} = 1+2\lfloor \mathrm{m}\rfloor+2\lfloor \mathrm{m}\rfloor^2 > h$$

por hipótesis, lo cual lleva a una contradicción. La desigualdad $p \geqslant \left(\frac{d}{4}\right)^{\frac{1}{h}}$ para todo primo p que descompone fue probada en 1.37 (a), resta entonces ver la última parte del lema.

Sea q el mayor divisor primo de d, en 1.30 mencionamos la siguiente proposición:

$$\textit{Sea } T = \#\{p \textit{ primo } : p \mid d\} \text{ , entonces } 2^{T-1} \mid h,$$

de la cual se deduce que $T \leqslant 2m$, en caso contrario $2^{2m} \mid h \leqslant 2(m+m')$ y esta desigualdad solo se cumple para $m=0$. Como d ó $\frac{d}{4}$ es libre de cuadrados, debe existir un divisor primo mayor a $\left(\frac{d}{4}\right)^{\frac{1}{T}}$. □

LEMA 3.15. *Sea* $P(d) = \{p \textit{ primo } : p \mid d\}\backslash\{q\}$ *y* $V = \left(\frac{d}{4}\right)^{\frac{1}{h}}$. *Entonces*

(1) $1 \leqslant \sum_{q\in Q_d^{red}} a(q)^{-1} \leqslant \alpha_1 \prod_{p\in P(d)} \left(1+p^{-1}\right)$, *donde* $\alpha_1 = \left(1+\frac{h}{U}\right)\left(\frac{1+V^{-1}}{1-V^{-1}}\right)$.

(2) $|G(U,1) \geqslant \alpha_2 \prod_{p\in P(d)} |G_p(1)|$, *donde* $\alpha_2 = \left(\frac{1+V^{-\frac{1}{2}}}{1-V^{-\frac{1}{2}}}\right)^2$.

(3) $\Re\left(\frac{G'(U,1)}{G(U,1)}\right) \geqslant \sum_{p\in P(d)} \Re\left(\frac{G_p'(U,1)}{G_p(U,1)}\right) - \alpha_3$, *donde* $\alpha_3 = \frac{4V^{-\frac{1}{2}}}{1-V^{-1}}\log V$.

(4) $\sup_{s\in\Delta}\frac{|G(U,s)|}{|G(U,1)|} \leqslant \alpha_4 \prod_{p\in P(d)} (1-p^{-\frac{1}{4}})^{-2}$, *donde* $\alpha_4 = \frac{(1+V^{-\frac{1}{2}})^2}{(1-V^{\frac{1}{4}})^4}$.

DEMOSTRACIÓN.

(1) Ver [Oe, pág. 318].

(2) $|G(U,1)| = \prod_{p<U} |G_p(1)|$, por **(C1)** $|G_p(1)| \leqslant \frac{1+p^{-\frac{1}{2}}}{1-\chi(p)p^{-\frac{1}{2}}}$,y $|G_p(1)| \geqslant 1$ pues los $\alpha, \overline{\alpha}, \beta, \overline{\beta}$ tienen módulo menor o igual a $\sqrt{p}$. Luego,

$$|G(U,1)| = \prod_{p\in P(d)} |G_p(1)| \prod_{\substack{p\in P(d)\\ p>U}} |G_p(1)|^{-1} \prod_{\substack{p<U\\ \chi(p)=1}} |G_p(1)| \prod_{\substack{p<U\\ \chi(p)=-1}} |G_p(1)|$$
$$\geqslant \prod_{p\in P(d)} |G_p(1)| \prod_{\substack{p<U\\ \chi(p)=1}} |G_p(1)|^{-1}$$
$$\geqslant \prod_{p\in P(d)} |G_p(1)| \left(\frac{1-V^{-\frac{-1}{2}}}{1+V^{\frac{-1}{2}}}\right)^2,$$

esta última desigualdad se deduce de la condición **(C1)** y del lema 3.14, ya que

$$G(U,1) \ll \prod_{p<U} \left(\frac{1+p^{-\frac{1}{2}}}{1-\chi(p)p^{\frac{1}{2}}}\right)^2 \qquad \text{y} \qquad p \leqslant U \text{ descompone } \Rightarrow p > V.$$

(3)

$$\Re\frac{G'(U,1)}{G(U,1)} = \sum_{p<U} \left[\frac{d}{ds}\log|G_p(s)|\right]_{s=1}$$
$$\geqslant \sum_{p\in P(d)} \left[\frac{s}{ds}\log|G_p(s)|\right]_{s=1} + \left[\frac{d}{ds}\log|G_q(s)|^{-1}\right]_{s=1}$$
$$\geqslant \sum_{p\in P(d)} \left[\frac{s}{ds}\log|G_p(s)|\right]_{s=1} + \left[\frac{d}{ds}\log\left(\frac{1-q^{-s}}{1+q^{-s}}\right)^2\right]_{s=1}$$
$$\geqslant \sum_{p\in P(d)} \left[\frac{s}{ds}\log|G_p(s)|\right]_{s=1} + 2\left(\frac{1+q^{-1}}{1-q^{-1}}\right)\frac{(1+q^{-1})+(1-q^{-1})}{(1+q^{-1})^2}\log qq^{-1}$$
$$\geqslant \sum_{p\in P(d)} \left[\frac{s}{ds}\log|G_p(s)|\right]_{s=1} + \frac{4\log qq^{-1}}{(1-q^{-1})(1+q^{-1})}\log qq^{-s}$$
$$\geqslant \prod_{p\in P(d)} \Re\frac{G_p'(1)}{G_p(1)} + 4\frac{\log VV^{-\frac{1}{2}}}{1-V^{-1}}.$$

(4) Por la parte (a)

$$\frac{|G(U,s)|}{|G(U,1)|} \leqslant \frac{(1+V^{-\frac{1}{2}})^2}{(1+V^{-\frac{1}{4}})^2(1-V^{-\frac{1}{4}})^2} \prod_{p\in P(d)} \frac{|G_p(s)|}{|G_p(1)|} \prod_{\substack{p<U\\ p\notin P(d)}} |G_p(s)|.$$

Por el lema 3.14 y la condición **(C1)**

$$\frac{|G(U,s)|}{|G(U,1)|} \leqslant \frac{(1+V^{-\frac{1}{2}})^2}{(1+V^{-\frac{1}{4}})^2(1-V^{-\frac{1}{4}})^2} \frac{1+V^{\frac{1}{2}-s}}{1-V^{\frac{1}{2}-s}} \prod_{p\in P(d)} \frac{|G_p(s)|}{|G_p(1)|}.$$

Ahora recordemos que $s \in \Delta$ y $\Re s \geqslant \frac{3}{4}$ pues $\nu \leqslant \frac{1}{4}$. Podemos considerar $\Im s$ lo suficientemente pequeña, de forma que para $s \in \Delta$ se cumpla

$$\frac{|G(U,s)|}{|G(U,1)|} \leqslant \frac{(1+V^{-\frac{1}{2}})^2}{(1+V^{-\frac{1}{4}})^2(1-V^{-\frac{1}{4}})^2}\frac{1+V^{-\frac{1}{4}}}{1-V^{-\frac{1}{4}}}\prod_{p\in P(d)}(1-p^{-\frac{1}{4}}),$$

que es lo que deseamos.

□

TEOREMA 3.16. *Existe una constante $C_8 > 0$ que depende de M y ψ pero no de G, K, h o d, tal que*

$$C_8 h \geqslant \text{ínf}\left\{1, \prod_{p\in P(d)}\left|\frac{G_p(1)}{1+p^{-1}}\right|\right\}\log d.$$

DEMOSTRACIÓN. Sabemos que $|J(U)^*| \leqslant J_1 + J_2 + J_3$, por la proposición 3.13 tenemos las siguientes desigualdades,

$$J_1 \leqslant C_4\frac{h^2}{\sqrt{U}}\left(|\log\frac{dM}{U}| + 3\right)^4 \qquad J_2 \leqslant C_5 h\sum_{q\in Q_d^{red}} a(q)^{-1} \qquad J_3 \leqslant C_6\frac{h^2}{\sqrt{d}}$$

Por la parte 1. del lema 3.15

$$\begin{aligned}|J(U)^*| &\leqslant J_1 + C_5 h\sum_{q\in Q_d^{red}} a(q)^{-1} + J_3 \leqslant C_6\frac{h^2}{\sqrt{d}}\\ &\leqslant C_5 h\prod_{p\in P(d)}(1+p^{-1})\left(\alpha_1 + \frac{C_4}{C_5}\frac{h}{\sqrt{U}}\left(|\log\frac{dM}{U}| + 3\right)^4 + \frac{C_6}{C_5}\frac{h}{\sqrt{d}}\right).\end{aligned}$$

Recordemos que

$$J(U) = C_1 G(U,1)\left(\log d + \Re\frac{G'(U,1)}{G(U,1)} + C_2\right) + J_\Delta(U)$$

donde $|J_\Delta| \leqslant C_3 \sup_{s\in\Delta}|G(U,s)|$, por las partes 2, 3 y 4 del lema previo

$$\begin{aligned}|J(U)| &\geqslant |C_1|\alpha_2\prod_{p\in P(d)}|G_p(1)|\left(\log d + \Re\frac{G'(U,1)}{G(U,1)} + C_2\right) + J_\Delta\\ &\geqslant |C_1|\alpha_2\prod_{p\in P(d)}|G_p(1)|\log d\left(1 + \frac{1}{\log d}\left[\sum_{p\in P(d)}\Re\frac{G_p'(1)}{G_p(1)} - \alpha_3 + C_2\right]\right) + J_\Delta\\ &\geqslant |C_1|\alpha_2\prod_{p\in P(d)}|G_p(1)|\log d\left(1 + \frac{1}{\log d}\left[\sum_{p\in P(d)}\Re\frac{G_p'(1)}{G_p(1)} - \alpha_3 + C_2 - \right.\right.\\ &\qquad\qquad\left.\left.\frac{C_3}{|C_1|}\sup_{s\in\Delta}\frac{G(u,s)}{G(U,1)}\right]\right)\\ &\geqslant |C_1|\alpha_6\log d\prod_{p\in P(d)}|G_p(1)|,\end{aligned}$$

donde

$$\alpha_6 := \alpha_2 \left(1 + \frac{1}{\log d}\left[\sum_{p\in P(d)} \Re\frac{G_p'(1)}{G_p(1)} - \alpha_3 + C_2 - \frac{C_3\alpha_4}{|C_1|}\prod_{p\in P(d)}(1-p^{-\frac{1}{4}})^{-2}\right]\right).$$

Sabemos que $T = \#P(d)$ es tal que $2^{T-1}|h$, en consecuencia está acotado por la vacuación 2-ádica de h, de esto se deduce que existe $\lambda_0 \in \mathbb{R}_+$ tal que para todo $\lambda \geqslant \lambda_0$, si $d \geqslant e^{\lambda h}$ entonces

$$\alpha_6 > 0 \qquad \text{y} \qquad \frac{\alpha_5}{\alpha_6} \leqslant 1 + C_7$$

donde C_7 es una constante efectivamente calculable que depende solamente de λ, ψ y M , y tiende a 0 cuando λ tiende a $+\infty$.
El teorema se sigue de la igualdad $J(U) = -J(U)^*$ tomando

$$C_8 = \sup\{\lambda, \frac{C_5}{|C_1|}(1 + C_7(\lambda))\}.$$

□

6. Conclusión

En este capítulo obtuvimos una cota para $h(d)$, asumiendo la existencia de ψ, M y G en las condiciones **(C1)**...**(C4)**. La constante obtenida en el Teorema 3.16 depende de ψ y M pero no del cuerpo cuadrático K o su discriminante d, ni tampoco de G.

En el capítulo siguiente veremos que si conocemos una forma nueva de peso 2 y nivel N con un cero de orden 3 en $s = 1$, entonces podemos definir ψ y M que dependen sólo de f. Además, para todo discriminante d tal que $\chi_d(N) = -1$ podemos definir G. Más precisamente, tendremos la siguiente Proposición.

Proposición. *Sea f una forma nueva de peso 2 y nivel N tal que $L(f, s)$ tiene un cero de orden al menos 3 en $s = 1$. Sea K un cuerpo cuadrático imaginario de discriminante d coprimo con N tal que $\chi_d(N) = -1$. Entonces la constante $M = \frac{N}{4\pi^2}$ y las series de Dirichlet $\psi(s) = L(f, s)L(f \otimes \lambda, s)$ y $G(s) = L(f \otimes \chi, s)L(f \otimes \lambda, s)^{-1}$ satisfacen las condiciones* **(C1)**,**(C2)**,**(C3)**,**(C4)**.

Esto quiere decir que si consideramos K en la familia $\mathcal{K}_N^-$ de los cuerpos cuadráticos imaginarios cuyo discriminante es coprimo con N y satisfacen $\chi_d(N) = -1$, de la existencia de ψ, M y G se deduce la existencia de una constante C_8 como en el Teorema 3.16 para K. Como C_8 no depende de K, la misma constante es válida para toda la familia.

Finalmente observemos que para cuerpos en K_N^-, la Proposición 2.25 implica que tenemos la cota $|G_p(1)| \geqslant 1 + p - \lfloor 2\sqrt{p}\rfloor$ para los factores de Euler de G. Ahora podemos aplicar el Teorema 3.16 a dicha familia para acotar el número de clases de forma efectiva, lo que obtenemos es el Teorema de Goldfeld para $\mathcal{K}_N^-$.

Teorema (Goldfeld). *Supongamos que existen M, ψ y G_K para todo $K \in \mathcal{K}_N^-$ que satisfacen las condiciones* **(C1)**-**(C4)**. *Entonces, para todo discriminante $-d$ de un cuerpo cuadrático imaginario en K_N^- existe una constante $C > 0$ efectivamente calculable, que depende sólo de M y ψ tal que*

$$\vartheta(d)\log d \leqslant Ch(-d);$$

donde

$$\vartheta(d) = \prod_{p \in P(d)} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right).$$

Capítulo 4

Construcción de una forma modular para el Teorema de Goldfeld

En el capítulo anterior vimos el Teorema 3.16, que asumiendo la existencia de series de M, ψ y G_K en las condiciones **(C1)-(C4)** establece la existencia de una constante C_8 que depende solo de M y ψ tal que

$$C_8 h \geqslant \text{ínf} \left\{ 1, \prod_{p \in P(d)} \left| \frac{G_p(1)}{1+p^{-1}} \right| \right\} \log d.$$

El último paso en el trabajo de Oesterlé en [Oe] es definir estos tres elementos asumiendo la existencia de una $L-$serie con un cero de orden al menos 3, esto último es un corolario del Teorema de Gross-Zagier.

1. Teorema de Oesterlé para la familia $\mathcal{K}_N^-$

Sea f una forma modular de peso 2 y nivel N, fijamos

$$M = \frac{N}{4\pi^2} \text{ y} \qquad \psi(s) = L(f,s)L(f \otimes \lambda, s).$$

Consideremos $\mathcal{K}_N^-$ el conjunto de cuerpos cuadráticos imaginarios de discriminante coprimo con N y tal que el carácter cuadrático asociado χ satisface $\chi(-N) = 1$. Para $K \in \mathcal{K}_N^-$ se define $G_K = L(f \otimes \chi, s)L(f \otimes \lambda, s)^{-1}$.

Observación 4.1. *Por lo visto en el capítulo 2*

$$G(1) = G(0) =$$

$$\prod_{p|Nd^2} (1 - a_p(f)\chi(p))^{-1} \prod_{p \nmid Nd^2} (1 - a_p(f)\chi(p) + p)^{-1} \prod_{p|N} (1 + a_p(f)) \prod_{p \nmid N} (1 + a_p(f) + p),$$

si p ramifica, como el discriminante es coprimo con N, $G_p(1) = 1 + a_p(f) + p$, además $a_p(f) \in \mathbb{Z}$ está acotado por $|a_p(f)| \leqslant 2\sqrt{p}$ (2.25) por lo que $|G_p(1)| \geqslant 1 + p - \lfloor 2\sqrt{p} \rfloor$.

Proposición 4.2. *Sea f una forma nueva de peso 2 y nivel N tal que $L(f,s)$ tiene un cero de orden al menos 3 en $s = 1$, y sea $K \in \mathcal{K}_N^-$. Entonces la constante $M = \frac{N}{4\pi^2}$ y las series de Dirichlet $\psi(s) = L(f,s)L(f \otimes \lambda, s)$ y $G(s) = L(f \otimes \chi, s)L(f \otimes \lambda, s)^{-1}$ satisfacen las condiciones* **(C1)**,**(C2)**,**(C3)**,**(C4)** *del Capítulo 3.*

Demostración.

(C1) Como $\mathrm{mcd}(N, d^2) = 1$ por 2.29 se tiene que

$$a_n(f \otimes \chi) = a_n(f)\chi(n) \qquad \text{y} \qquad a_n(f \otimes \lambda) = a_n(f)\lambda(f),$$

para todo $n > 0$. Además,

$$\psi(s) = L(\mathrm{Sym}^2 f, 2s) \prod_{p\nmid N}(1 - p^{1-2s}) = \sum_{n=0}^{\infty} a_n^2 n^{-2s} \prod_{p\nmid N} \frac{1 + p^{1-2s}}{1 - p^{1-2s}}.$$

Como $|a_p(f)| \leqslant 2\sqrt{p}$ para todo primo p,

$$\begin{aligned}\psi(s) &\ll 4 \sum_{n=0}^{\infty} n^{1-2s} \zeta(2s-1) \prod_{p|N} \frac{1 - p^{1-2s}}{1 + p^{1-2s}} \prod_{p\nmid N}(1 - p^{1-2s})^{-1} \\ &\ll \zeta(2s-1)^2.\end{aligned}$$

Finalmente

$$\begin{aligned}G_K(s) = \Bigg[&\prod_{p\nmid Nd^2} (1 - a_p(f)\chi(p)p^{-s})^{-1} \prod_{p\nmid Nd^2} (1 - a_p\chi(p)p^{-s} + p^{1-2s}) \\ &\prod_{p|N}(1 + a_p p^{-s}) \prod_{p\nmid N}(1 + a_p p^{-s} + p^{1-2s}) \Bigg] \\ \ll \Bigg[&\prod_{p\nmid Nd^2} (1 - \chi(p)p^{\frac{1}{2}-s})^{-1} \prod_{p\nmid Nd^2} (1 - \chi(p)p^{\frac{1}{2}-s} + p^{1-2s}) \\ &\prod_{p|N}(1 + a_p p^{\frac{1}{2}-s}) \prod_{p\nmid N}(1 + p^{\frac{1}{2}-s} + p^{1-2s}) \Bigg] \\ \ll &\left(\frac{\zeta_K(s - \frac{1}{2})}{\zeta(2s)} \right)^2.\end{aligned}$$

(C2) Es inmediato.

(C3) Se deduce de la ecuación funcional 2.27

$$d^s \gamma(s)\psi(s)G_K(s) = \Lambda(f, s)\Lambda(f \otimes \chi, s) = \varepsilon(f)\varepsilon(f \otimes \chi)\Lambda(f, 1-s)\Lambda(f \otimes \chi, 1-s).$$

El lado derecho tiene un cero de orden al menos 3 en $s = 1$ y por (15) el signo de la ecuación funcional es $\chi(-N)\varepsilon^2(f) = 1$, por lo tanto el orden del cero es al menos cuatro.

(C4) $\psi(s) = L(\mathrm{Sym}^2 f, 2s) \prod_{p\nmid N}(1 - p^{1-2s})$ satisface (2.33) y por lo tanto admite una extensión holomorfa sobre un entorno de $\mathcal{H}_1$. Además, por la observación 2.34 ψ tiene un cero simple en $s = 1$.

□

La proposición permite aplicar lo visto en el capítulo anterior a la familia $\mathcal{K}_N^-$ de cuerpos cuadráticos de discriminante coprimo con N que además satisfacen $\chi(-N) = 1$.

Recordemos que la constante C_8 en el teorema 3.16 está definida como

$$C_8 = \sup\{\lambda, \frac{C_5}{|C_1|}(1 + C_7)\},$$

donde C_1 es el valor de $\frac{\gamma(s)\psi(s)}{s-1}$ en $s = 1$, $C_5 = \frac{2\pi^4}{3}M^{\frac{1}{2}}$ y C_7 es una constante efectiva. El valor de C_1 es finito, pues ψ tiene un cero de orden simple en $s = 1$ y $\Gamma(1) = 1$. Observemos que

$$\begin{aligned}\frac{\gamma(s)\psi(s)}{s-1} &= \frac{M^s\Gamma^2(s)L(\mathrm{Sym}^2 f, 2s)\prod_{p\nmid N}(1-p^{1-2s})}{s-1} \\ &= \left(\tfrac{N}{4\pi^2}\right)^s\prod_{p\nmid N}(1-p^{1-2s})\frac{\Gamma^2(s)\Lambda(\mathrm{Sym}^2 f, 2s)N^{-2s}(2\pi)^{2s}\Gamma(2s)^{-1}\Gamma(s)^{-1}\pi^s}{s-1} \\ &= N^{-s}\Gamma(s)\Gamma(2s)^{-1}\pi^s\Lambda(\mathrm{Sym}^2 f, 2s)((s-1)\zeta(2s-1))^{-1}\prod_{p|N}(1-p^{-1})^{-1}.\end{aligned}$$

Como $\Gamma(2) = \Gamma(1) = 1$ y ζ tiene un polo simple con residuo simple en $s = 1$ esto nos queda

$$C_1 = \frac{\gamma(s)\psi(s)}{s-1} = N^{-1}\pi\prod_{p|N}(1-p^{-1})^{-1}\Lambda(\mathrm{Sym}^2 f, 2).$$

De la prueba de 2.33 se puede deducir el valor en $s = 1$ de $\Lambda(\mathrm{Sym}^2 f, 2s)$,

$$\Lambda(\mathrm{Sym}^2 f, 2) = 2N\int_{D_0} f(z)\overline{f(z)}dxdy,$$

luego

$$C_1 = 2\pi\prod_{p|N}\frac{p}{p-1}\int_{D_0} f(z)\overline{f(z)}dxdy$$

y por la definición de M

$$C_5 = \frac{\pi}{12}N^{\frac{3}{2}}.$$

El Teorema de Gross-Zagier, que no enunciaremos aquí, tiene como corolario el siguiente resultado:

COROLARIO 4.3. *Sea $E_0 : -139y^2 = x^3 + 4x^2 - 48x + 80$ la curva elíptica sobre $\mathbb{Q}$ de conductor $37 \cdot (139)^2$ y rango $g = 3$, su $L-$serie asociada $L_{E_0}(s)$ tiene un cero triple en $s = 1$.*

La $L-$serie anterior está asociada a la forma modular $f_1 = f_0 \otimes \chi_0$, donde $\chi_0 = \left(\frac{-139}{\cdot}\right)$ y f_0 es una forma nueva de peso 2 y nivel 37 tal que $f_0\left(\frac{-1}{37\tau}\right) = -37\tau^2 f_0(\tau)$. Haciendo los cálculos para la forma f_1 Oesterlé obtiene la cota $C = 7000$ en el Teorema de Goldfeld:

TEOREMA 4.4 (Oesterlé).

$$h(d) > \tfrac{1}{7000}(\log|d|)\prod_{\substack{p|d \\ p\neq d}}\left(1 - \tfrac{[2\sqrt{p}]}{p+1}\right).$$

Usando, en cambio, la curva elíptica 5077.a1 de conductor 5077 hallada por Brumer y Kramer, Oesterlé computa $C = 55$ para discriminantes coprimos con 5077. Para poder usar dicha curva era necesario mostrar su modularidad y que la L-serie tiene un cero de orden 3 en $s = 1$; lo cual probaron más adelante Oesterlé, Mestre y Serre.

2. Comentario sobre el caso general

Sea K un cuerpo cuadrático imaginario de discriminante $-d$ y carácter χ_d, y sean f_0, f_1 las formas modulares descritas anteriormente.

Cuando $\chi_d(-37) = -1$ (o equivalentemente $\chi(37) = 1$) la proposición 1.37 nos dice que $37^h \geqslant \frac{d}{4}$, tomando logaritmo, $h \log 37 \geqslant \log \frac{d}{4}$.

Cuando $\chi_d(-37) = 1$, como $d \in \mathcal{K}_N^-$ estamos en las hipótesis de la sección anterior.

Cuando $\chi_d(-37) = 0$, el resultado obtenido para la familia $\mathcal{K}_N^-$ puede ser modificado levemente de forma que valga cambiando la condición $\chi_d(-N) = -1$ por $\varepsilon(f \otimes \chi_d) = \varepsilon(f)$. En este caso se toma $\psi(s) = \prod_p \psi_p(s)$ la serie de Dirichlet tal que ψ_p es el $p-$ésimo factor de Euler de

$$\begin{cases} L(f \otimes \chi_d, s) & \text{si } p^2 \mid \operatorname{mcd}(N, d^2) \\ L(f, s)L(f \otimes \lambda, s) & \text{en otro caso} \end{cases},$$

$M = \frac{\sqrt{NN_\chi}}{4\pi^2 d}$, donde N_{χ_d} es el nivel de $f \otimes \chi_d$ y $G(s) = L(f, s)L(f \otimes \chi_d, s)\psi(s)^{-1}$.
Si se ve entonces que $\varepsilon(f_1 \otimes \chi_d) = \varepsilon(f)$ cuando $\chi_d(37) = 0$, se obtiene una cota efectiva para la familia de todos los cuerpos cuadráticos.

- $\varepsilon(f_0) = 1$ y $\varepsilon(f_1) = \chi_0(-37) = -1$.
- Si $\chi_d(-37) = 0$: $\varepsilon(f_1 \otimes \chi_d) = \varepsilon(f_0 \otimes \chi_0\chi_d) = -1$.

3. Resultados de Mark Watkins

Con los resultados de Oesterlé se dió la clasificación de cuerpos cuadráticos imaginarios para el número de clases $h = 3$, pero observemos que la cota dada por Goldfeld-Oesterlé es equivalente a

$$d \leqslant \exp\left(-C\theta(d)h(-d)\right),$$

es decir que es una cota exponencial para d. Con la cota de Oesterlé tenemos para $h(-d) \leqslant 100$

$$d \leqslant \exp\left(7000 \cdot 100 \prod_{p \leqslant 13} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right)^{-1}\right) \leqslant \exp 268800000.$$

Watkins modificó la técnica utilizada por Oesterlé para encontrar una cota efectiva en el Teorema de Goldfeld. En lugar de considerar la curva elíptica dada por Gross-Zagier o incluso la dada por Brumer-Kramer, utiliza funciones L de Dirichlet con ceros de parte imaginaria suficientemente pequeña. Con esta técnica, para $h \leqslant 100$ elimina la posibilidad de encontrar discriminantes d mayores a 2^{162} con número de clases h.

La tabla 1 corresponde a la clasificación dada por Watkins para $h \leqslant 100$, una observación es que no hay cuerpos con "número de clases pequeño" y un discriminante "excepcional" que sea anormalmente grande, lo cual es consistente con la Hipótesis de Riemann.

h	#	Mayor d_K	h	#	Mayor d_K	h	#	Mayor d_K	h	#	Mayor d_K	h	#	Mayor d_K
1	9	163	21	85	61483	41	109	296587	61	132	606643	81	228	1030723
2	18	427	22	139	85507	42	339	280267	62	323	647707	82	402	1446547
3	16	907	23	68	90787	43	106	300787	63	216	991027	83	150	1074907
4	54	1555	24	511	111763	44	691	319867	64	1672	693067	84	1715	1225387
5	25	2683	25	95	93307	45	154	308323	65	164	703123	85	221	1285747
6	51	3763	26	190	103027	46	268	462883	66	530	958483	86	472	1534723
7	31	5293	27	93	103387	47	107	375523	67	120	652723	87	222	1261747
8	131	6307	28	457	126043	48	1365	335203	68	976	819163	88	1905	1265587
9	34	10627	29	83	166147	49	132	393187	69	209	888427	89	192	1429387
10	87	13843	30	255	134467	50	345	389467	70	560	811507	90	801	1548523
11	41	15667	31	73	133387	51	159	546067	71	150	909547	91	214	1391083
12	206	17803	32	708	164803	52	770	439147	72	1930	947923	92	1248	1452067
13	37	20563	33	101	222643	53	114	425107	73	119	886867	93	262	1475203
14	95	30067	34	219	189883	54	427	532123	74	407	951043	94	509	1587763
15	68	34483	35	103	210907	55	163	452083	75	237	916507	95	241	1659067
16	322	31243	36	668	217627	56	1205	494323	76	1075	1086187	96	3283	1684027
17	45	37123	37	85	158923	57	179	615883	77	216	1242763	97	185	1842523
18	150	48427	38	237	289963	58	291	586987	78	561	1004347	98	580	2383747
19	47	38707	39	115	253507	59	128	474307	79	175	1333963	99	289	1480627
20	350	58507	40	912	260947	60	1303	662803	80	2277	1165483	100	1736	1856563

CUADRO 1. Tabla para $h \leqslant 100$

Bibliografía

[Ogg] A.P.Ogg. «On a Convolution of L-Series». En: *Inventiones mathematicae* 7 (1969), págs. 297-312.

[Cohn] Harvey Cohn. *Advanced number theory*. Courier Corporation, 1980. ISBN: 048664023X.

[Cox] David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Springer, 2013. ISBN: 9781118390184.

[Del] Pierre Deligne. «La conjecture de Weil : I». fre. En: *Publications Mathématiques de l'IHÉS* 43 (1974), págs. 273-307. URL: http://eudml.org/doc/103930.

[D-S] Fred Diamond y Jerry Shurman. *A First Course in Modular Forms*. Springer, 2005. ISBN: 978-0-387-27226-9.

[Gauss] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Trad. por Hugo Barrantes Campos, Michael Josephy y Angel Ruiz Zúñig. Academia Colombiana de Ciencias Exactas, Físicas y Naturales, 1995. ISBN: 958-9205-00-3.

[Gold] Dorian M. Goldfeld. «The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer». eng. En: *Bull. Amer. Math. Soc* 13 (1985), págs. 23-37. URL: https://www.ams.org/journals/bull/1985-13-01/S0273-0979-1985-15352-2/.

[I-K] Henryk Iwaniec y Emmanuel Kowalski. *Analytic number theory*. American Mathematical Society, 2004. ISBN: 0-8218-3633- 1.

[5077a1] The LMFDB Collaboration. *The L-functions and modular forms database, Home page of the Elliptic curve with LMFDB label 5077.a1*. mboxhttp://www.lmfdb.org/EllipticCurve/Q/5077/a/1. [Online; accessed 1 April 2023]. 2023.

[Mil] James S. Milne. *Algebraic Number Theory (v3.08)*. Available at www.jmilne.org/math/. 2020.

[Oe] Joseph Oesterlé. «Nombres de classes des corps quadratiques imaginaires». fre. En: *Séminaire Bourbaki* 26 (1985), págs. 309-323. URL: http://eudml.org/doc/110032.

[Sh] Goro Shimura. «On the Holomorphy of Certain Dirichlet Series». En: *Proceedings of The London Mathematical Society* (1975), págs. 79-98.

[Tr] Mak Trifković. *Algebraic Theory of quadratic numbers*. Wiley, 2013. ISBN: 978-1-4614-7716-7.

[Wat] Mark E. Watkins. «Class numbers of imaginary quadratic fields». En: *Math. Comput.* 73 (2003), págs. 907-938.