Tesis de Maestría

El Teorema de Gross–Zagier

Carolina Chiesa

Abril 2025

Orientador:

Gonzalo Tornaría
Facultad de Ciencias, UDELAR

Maestría en Matemática
Universidad de la República
Montevideo, Uruguay

Resumen

El Teorema de Gross-Zagier, de gran relevancia en la Teoría de números, establece una conexión entre ciertos objetos algebraicos: puntos de Heegner asociados a una curva elíptica, y ciertos objetos analíticos: derivadas de L-series de Rankin.

Una curva elíptica E tiene una L-serie asociada L_E. Si $L_E(1) = 0$, este teorema da una fórmula del tipo

$$L'_E(1) = \text{Cte} \cdot \text{h(P)}$$

donde P es un punto de Heegner, que representa un punto racional especial de la curva, y h(P) es su altura. La altura de un punto es no nula si y sólo si dicho punto tiene orden infinito, por lo que cuando la derivada no se anula la fórmula anterior implica la existencia de infinitos puntos racionales.

En mi tesis de maestría se presentan las técnicas empleadas en la prueba de Gross-Zagier, que puede esencialmente dividirse en dos partes. Por una parte, el método de Rankin permite expresar el valor de la L-serie en 1 como el producto interno de Petersson entre dos formas modulares de peso 2 para luego calcular sus coeficientes de Fourier. Por otra parte, empleando diversas técnicas el lado derecho puede manipularse localmente distinguiendo el caso arquimediano del no arquimediano.

Índice general

Introducción

Dear Bryan,

Working with Don Zagier, I think I've assembled a proof of the identity following conjecture 17.1 in my paper on Heegner points. Up to now we've been assuming that both N and D are prime, but I'd be surprised if the techniques didn't work in the general case. The method is more or less as I suggested in my letter of May 14; one uses Rankin's method to obtain explicit formulae for the derivatives of the L-series and stare at these long enough until one begins to see the local heights of Heegner points emerging. Something should actually be written down by the late Spring, and you'll get the first copy.

Two requests: would you mind if we referred to the identity and the resulting 17.1 in the next write-up as the conjecture of Birch (or of Birch/Stephens). I know you only make conjectures with lots of evidence, and only really believed it when $\chi^2 = 1$ and f came from an elliptic curve, but you were the one who discovered this amazing phenomenon, and without the security blanket of your evidence, I would never have dared a proof.

Second: could you send us some of your computations on $X_0(11)$, $X_0(17)$, and $X_0(19)$? The fun of the subject seems to me to be in the examples.

Best wishes,

Dick

Carta de Gross a Birch, 1º de diciembre de 1982.

El Teorema de Gross–Zagier, publicado en 1986 por Benedict Gross y Don Zagier, constituye un resultado de gran relevancia en la teoría de números. Este teorema relaciona la derivada de una L-serie asociada a una forma modular (o análogamente, a una curva elíptica) con la altura de un punto de Heegner, que es un punto en la curva modular de cierta forma asociado a una forma cuadrática.

Dada una curva elíptica E definida sobre un cuerpo de números K se define su rango algebraico como el rango del grupo $E(K)$ y su rango analítico como $\operatorname{ord}_{s=1} L_E(s)$, donde L_E es la L-serie asociada a E.

Una consecuencia fundamental de la fórmula de Gross–Zagier es que, dada una curva elíptica E sobre $\mathbb{Q}$, con rango analítico igual a 1, existe al menos un punto en la curva que no es de torsión; esto es, el rango algebraico de E es al menos 1.

Esto, junto con un resultado de Kolyvagin, da la siguiente relación:

rango analítico de $E \leq 1 \implies$ rango analítico de $E =$ rango algebraico de E .

El resultado recién mencionado es exactamente la Conjetura de Birch y Swinnerton-Dyer para curvas sobre $\mathbb{Q}$ con rango analítico igual a 0 o 1:

Conjetura (BSD, 1965). Sea E una curva elíptica definida sobre un cuerpo K, entonces $r_{\text{an}}(E) = r_{\text{alg}}(E)$.

La conjetura BSD es uno de los problemas abiertos más profundos de la Teoría de Números, específicamente en el estudio de las curvas elíptica y el Teorema de Gross–Zagier es crucial en la demostración del único caso sobre $\mathbb{Q}$ en el que está probada la conjetura.

Otra consecuencia relevante del teorema es la existencia de una L-serie asociada a una curva elíptica con un cero central de orden 3, esto, junto con un teorema de Goldfeld resuelve el problema del número de clases de Gauss: encontrar un algoritmo *efectivo* que determine todos los cuerpos cuadráticos imaginarios con un número de clases dado. El teorema de Goldfeld, que estudié en mi monografía de grado [1], establece lo siguiente:

Teorema 0.1 (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*

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

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

Observemos que la primera cota no trivial se obtiene con $g = 3$, por lo que una curva elíptica con un cero de orden 3 es exactamente lo que necesitaba Dorian Goldfeld para resolver por completo el problema.

Motivados entonces por su gran relevancia, el presente trabajo tiene como objetivo explorar y exponer las principales ideas y técnicas, que siguen vigentes hoy en día, involucradas en la prueba de este Teorema.

Estructura de la prueba.

Si D es el discriminante de un cuerpo cuadrático imaginario K, un punto de Heegner de discriminante D es un punto $x = (E \xrightarrow{\phi} E')$ en la curva modular $Y_0(N)$ donde ϕ tiene grado N y E, E' tienen multiplicación compleja por $\mathcal{O}_K$, el anillo de enteros de K. Consideremos $J = J_0(N)$ el Jacobiano de $X_0(N)$, aquí vive la parte algebraica del Teorema. El Jacobiano de $X_0(N)$ es una variedad abeliana de dimensión 1 y sus puntos sobre H, el cuerpo de clases de Hilbert, pueden verse como divisores en $X_0(N)$.

Por otra parte, hay una correspondencia $Cl_K \simeq \mathrm{Gal}(H/K)$ vía el Mapa de Artin. Si $\mathscr{A}$ denota una clase de ideales y $r_{\mathscr{A}}(n)$ el número de ideales de norma n en la clase $\mathscr{A}$, la L-serie asociada a la clase $\mathscr{A}$ se define como $L_{\mathscr{A}}(s) = \sum_{n\geq 0} r_{\mathscr{A}}(n)n^{-s}$; el teorema de Gross–Zagier relaciona esta L-serie con un elemento de $J(H)$ de la siguiente manera.

Teorema 0.2 (Gross–Zagier). *Sean f una forma modular de peso 2 para $\Gamma_0(N)$. Sea $c = (x) - (\infty) \in J(H)$ donde x es un punto de Heegner de discriminante D y sean $\mathscr{A}$ una clase de ideales en Cl_K y $\sigma_{\mathscr{A}} \in \mathrm{Gal}(H/K)$ el elemento que se corresponde con $\mathscr{A}$. La serie $g_{\mathscr{A}}(z) = \sum_{m\geq 1}\langle c, T_m c^{\sigma}\rangle q^m$ es una forma modular de peso 2 para $\Gamma_0(N)$ que*

satisface la fórmula

$$L'_{\mathscr{A}}(f,1) = \frac{8\pi^2}{u^2\sqrt{|D|}}(f, g_{\mathscr{A}})_{\Gamma_0(N)}$$

donde

- T_m *son correspondencias de Hecke en* $J(H)$.
- $\langle\ ,\ \rangle$ *es la altura en* $J(H) \times J(H)$.
- $u = |\mathcal{O}^\times|$.
-

$$L_{\mathscr{A}}(g_{\mathscr{A}}, s) := \sum_{\substack{n\geq 1 \\ gcd(n,ND)=1}} \left(\frac{D}{n}\right) n^{1-2s} L(g_{\mathscr{A}}, s) * L_{\mathscr{A}}(s).$$

Como corolario del Teorema anterior se obtiene una fórmula para $L'(f,1)$.

Corolario 0.3. *Bajo las hipótesis del Teorema anterior*

$$L'(f,1) = \frac{8\pi^2}{\mathrm{h}\sqrt{|D|}}\langle \tilde{c}_1, \tilde{c}_1\rangle (f,f)_{\Gamma_0(N)}$$

para cierto $\tilde{c}_1 \in J(H)$.

El objetivo de esta tesis es ilustrar la prueba dada por Gross–Zagier a su Teorema, para ello nos restringiremos al caso donde D y N son primos distintos, además, para garantizar la existencia de un punto de Heegner debemos pedir que N descomponga en K. La prueba puede dividirse en dos partes, una parte mayormente analítica en la que se construye la forma $g_{\mathscr{A}}$ y se calculan sus coeficientes de Fourier y otra parte que emplea técnicas mayormente algebraicas para calcular $\langle c, T_m c^\sigma\rangle$ como suma de las alturas locales, separando el caso arquimediano del no arquimediano.

El Capítulo 1 presenta los preliminares en formas modulares, curvas elípticas y álgebras de cuaterniones que necesitaremos a lo largo de la prueba.

El capítulo 2 da una breve introducción a puntos de Heegner ilustrando un ejemplo particular.

El Capítulo 3 se dedica a presentar la parte analítica de la prueba, comenzando por el Método de Rankin para construir $g_{\mathscr{A}}$ y culminando con el cálculo de sus coeficientes de Fourier.

El Capítulo 4 ilustra la parte algebraica de la prueba, el cálculo de las alturas locales arquimedianas requiere construir una función de Green apropiada mientras que el caso no arquimediano requiere emplear Teoría de la Intersección. En esta parte asumiremos los resultados que hacen uso de la geometría algebraica en la prueba. Luego de obtener las fórmulas de las alturas locales el problema queda reducido a hacer ciertos cálculos con normas en álgebras de cuaterniones.

En los Capítulos 3 y 4 habremos obtenido una fórmula para los coeficientes de $g_{\mathscr{A}}$ y una fórmula para la altura global; el Capítulo 5 cierra la prueba mostrando que estas fórmulas coinciden. Finalmente, mencionaremos algunas aplicaciones del Teorema.

Capítulo 1

Preliminares

1. Formas modulares

Trabajaremos con formas modulares de peso 2 para $\Gamma_0(N)$, por lo que esta sección se dedicará a presentar su definición y propiedades fundamentales. Las demostraciones pueden encontrarse en mi monografía de grado [1], y una referencia más completa es [4].

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

El grupo modular $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ actúa en el semiplano superior complejo $\mathcal{H}$ mediante transformaciones de Möbius.

Definición 1.1. Una forma modular de peso $k \in \mathbb{Z}$ 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 $\lim_{\mathrm{Im}(z)\to\infty} f(z)$.

Notemos $f|_k\gamma(z) := (cz+d)^{-k} f(\gamma(z))$, de forma que (2) puede reescribirse como

$$f|_k\gamma(z) = f(z).$$

Observación 1.2. *Observemos que como* $\mathrm{SL}_2(\mathbb{Z})$ *es generado por* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *y* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *basta con chequear la propiedad* (2) *en estas dos matrices.*

Las formas modulares admiten una expansión de Fourier de la forma $f(z) = \sum_{n=0}^{\infty} a_n q^n$, cuando $a_0 = 0$ (o lo que es equivalente $\lim_{\mathrm{Im}(z)\to\infty} f(z) = 0$) decimos que la forma es *cuspidal* y si además $a_1 = 1$ decimos que es *normalizada*. El conjunto de formas modulares de peso k forma un espacio vectoral complejo de dimensión finita que denotamos por $M_k(\mathrm{SL}_2(\mathbb{Z}))$, las formas cuspidales de peso k forman un subespacio vectorial de $M_k(\mathrm{SL}_2(\mathbb{Z}))$ al que denotamos $S_k(\mathrm{SL}_2(\mathbb{Z}))$.

Definición 1.3. El *subgrupo principal de congruencias* de nivel N es

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

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.

A nosotros nos interesará particularmente el subgrupo $\Gamma_0(N)$:

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

aunque más adelante también aparecerá el subgrupo $\Gamma_1(N)$:

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

Observación 1.4. *Todo subgrupo de congruencia tiene índice finito, $\Gamma(N)$ 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 $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Un concepto que usaremos todo el tiempo es el de *cúspide*, las cúspides de un subgrupo de congruencia son las clases de equivalencia de $\mathbb{Q} \cup \{\infty\}$ por la acción de Γ

Observación 1.5. *El número de cúspides siempre es finito. Por ejemplo, para el grupo modular hay una sola cúspide que se corresponde con el ∞. Para $\Gamma = \Gamma_0(N)$ con N primo hay dos cúspides: un número racional x está en la misma órbita que el 0 si y sólo si existen $a, b, c, d \in \mathbb{Z}$ tales que $\frac{b}{d} = x$ y $ad - Ncb = 1$ (esto es: $x = \frac{b}{d}$ con b, d coprimos y $N \nmid d$) y está en la misma órbita que el ∞ si y sólo si existen a, b, c, d como antes tales que $\frac{a}{Nc} = x$. Ahora es fácil notar que estos dos casos son disjuntos y que todo racional está en alguna de las dos órbitas.*

De la misma forma en que se define una forma modular para $\mathrm{SL}_2(\mathbb{Z})$ se puede definir una forma modular para un subgrupo de congruencia Γ.

Definición 1.6. Una función $f : \mathcal{H} \to \mathbb{C}$ 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) $f|_k\gamma(z)$ es holomorfa en ∞ para toda $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

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

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. Al espacio $S_k(\Gamma)$ se le puede equipar con un producto interno, llamado *Producto interno de Petterson* que se define como sigue:

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

donde $D(N)$ es un dominio fundamental para $\Gamma(N)$ y $\delta(f, g)$ es la forma diferencial $\delta(f, g) := y^k f(z)\overline{g(z)}\frac{dxdy}{y^2}$, donde $z = x + iy$. Al espacio de formas *débilmente modulares* (solo satisfacen (2)) que tienen crecimiento polinomial en las cúspides lo denotamos por $\tilde{M}_k(\Gamma)$, de forma análoga definimos $\tilde{S}_k(\Gamma)$. Estos espacios aparecerán en el Capítulo 3 ya que inicialmente tendremos la expansión de una forma *débilmente modular* g que permite expresar $L'(f, 1)$ en términos del producto de Petersson de $(f, g)_{\Gamma_0(N)}$; pero

no tendremos la expansión de una forma *modular* con esa propiedad hasta calcular su proyección holomorfa.

1.2. Operadores de Hecke.

Los operadores de Hecke vienen dados por dobles coclases de subgrupos de congruencia y serán fundamentales, pues descomponen nuestro espacio $M_2(\Gamma_0(N))$. Las formas nuevas serán los vectores propios para todos los operadores de Hecke.

Cuando en lugar de tener $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tenemos $\gamma \in \mathrm{GL}_2^+(\mathbb{Z})$ se define

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

y esta definición claramente extiende la antes vista.

Si Γ_1 y Γ_2 son dos subgrupos de congruencia de $\mathrm{SL}_2(\mathbb{Z})$, también podemos definir un operador $f|_k\Gamma_1\gamma\Gamma_2$ de la siguiente forma. Consideremos $\{\beta_j\} \subset \Gamma_1\gamma\Gamma_2$ un conjunto de representantes de las órbitas bajo la acción de Γ_1, es decir, $\Gamma_1\gamma\Gamma_2 = \bigcup_j \Gamma_1\beta_j$, definimos

$$f|_k\Gamma_1\gamma\Gamma_2 := \sum_j f|_k\beta_j.$$

Definición 1.7.

- El operador de Hecke del primer tipo u operador diamante $\langle d\rangle$ se define para d coprimo con N de la siguiente manera

  $$\langle d\rangle f = f|_k\gamma,$$

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

  Cuando $\gcd(d, N) > 1$ se define $\langle d\rangle$ como el operador nulo.
- El operador de Hecke T_p de segundo tipo se define para p primo como

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

Proposición 1.8. *Los operadores de Hecke conmutan entre sí:*

$$\langle d\rangle T_p = T_p\langle d\rangle \qquad \langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle = \langle de\rangle \qquad T_pT_q = T_qT_p$$

Definición 1.9. Sea $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ un carácter, se define el espacio $M_k(N, \chi)$ como

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

Proposición 1.10. *$M_k(\Gamma_1(N))$ se descompone como $M_k = \bigoplus_\chi M_k(N,\chi)$.*

Y lo mismo ocurre con $\tilde{M}_k(\Gamma_0(N))$ y con el conjunto de las formas débilmente modulares cuspidales $\tilde{S}_k(\Gamma_0(N))$.

1.3. Formas nuevas.

Si $M \mid N$ entonces $S_k(\Gamma_0(M)) \subseteq S_k(\Gamma_0(N))$, pero cuando además $d|\frac{N}{M}$ existe otra inmersión de $S_k(\Gamma_0(M))$ en $S_k(\Gamma_0(N))$ que consiste en el mapa

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

DEFINICIÓN 1.11. Sea $\gamma_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$. Para $d \mid N$ podemos definir el mapa

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

- El subespacio de *formas viejas de nivel* N es
$$S_k(\Gamma_1(N))^{\text{old}} := \sum_{p|N} i_p\left(S_k(\Gamma_1(Nd^{-1}))^2\right),$$
informalmente podemos decir que son las formas en $S_k(\Gamma)$ que provienen de niveles más bajos.
- El subespacio de *formas nuevas de nivel* N es
$$S_k(\Gamma_1(N))^{\text{new}} := \left(S_k(\Gamma_1(N))^{\text{old}}\right)^{\perp}.$$

PROPOSICIÓN 1.12. *Los operadores de Hecke respetan la descomposición de* $S_k(\Gamma_0(N))$ *en formas nuevas y viejas:* $S_k(\Gamma_1(N))^{\text{old}}$ *y* $S_k(\Gamma_1(N))^{\text{new}}$ *son estables por* $\langle n\rangle$ *y* T_n*, para todo* $n \in \mathbb{Z}^+$.

COROLARIO 1.13. $S_k(\Gamma_1(N))^{new}$ *tiene una base ortonormal de vectores propios para los operadores de Hecke* $\langle n\rangle$ *y* T_n.

DEFINICIÓN 1.14. 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 1.15. *La L-serie asociada a una forma nueva* f*,*

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

converge para $\operatorname{Re} s > k/2 + 1$ *y admite un producto de Euler de la forma*

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

PROPOSICIÓN 1.16. *Sea* f *una forma nueva de peso* 2 *para* $\Gamma_0(N)$*, entonces su L-serie completada* $\Lambda(s) = N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(f,s)$ *se extiende a una función entera y satisface una ecuación funcional* $\Lambda(f, 2-s) = \pm\Lambda(f,s)$.

PROPOSICIÓN 1.17. *Sea* f *una forma nueva en* $S_2(N,\chi)^{new}$ *y* ψ *un carácter de Dirichlet primitivo módulo* r*. Existe un entero* $N_\psi \geq 1$ *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 llamamos* twist de f por ψ.

PROPOSICIÓN 1.18. *Si* $\gcd(N,d) = 1$*, entonces* $f \otimes \chi_d$ *tiene carácter* χ *y nivel* Nd^2*. Además* $a_n(f \otimes \chi_d) = a_n(f)\chi_d(n)$ *para todo* $n \geq 1$ *y la constante* ε *para la ecuación funcional es*

$$\varepsilon(f \otimes \chi_d) = \chi_d(-N)\varepsilon(f).$$

1.4. Series de Eisenstein.

El producto interno de Petersson permite descomponer el espacio de formas modulares de un peso dado como $M_k(\Gamma) = S_k(\Gamma) \bigoplus \mathscr{E}_k(\Gamma)$, donde $\mathscr{E}_k(\Gamma) \coloneqq S_k(\Gamma)^{\perp}$. En $\mathrm{SL}_2(\mathbb{Z})$ el espacio $\mathscr{E}_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ con $k \geq 2$ es generado por las series de Eisenstein

$$G_{2k}(\tau) = \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(m+n\tau)^{2k}}.$$

donde la notación $\sum'$ significa que sumamos sobre los pares $(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. Observemos que

$$G_{2k}(\tau) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}} \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ \gcd(m,n)=1}}{}' \frac{1}{(m\tau+n)^{2k}} = \zeta(2k) \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ \gcd(m,n)=1}}{}' \frac{1}{(m\tau+n)^{2k}}$$

a $E_{2k}(\tau) \coloneqq \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ \gcd(m,n)=1}}{}' \frac{1}{(m\tau+n)^{2k}}$ se le denomina la serie de Eisenstein *normalizada* de peso $2k$ para $\mathrm{SL}_2(\mathbb{Z})$, y esta serie solo converge para $k > 1$. Dar bases para $\mathscr{E}_k(\Gamma)$ cuando $k = 0, 1$ o 2 requiere más trabajo, en la próxima sección aparecerá una serie de Eisenstein de peso 2 que estará directamente relacionada con otra función fundamental: la $\wp$ de Weierstrass, a lo largo de esta tesis nos encontraremos con otras series de Eisenstein de pesos 0 y 1, por ejemplo, la serie

$$E_{N,\varepsilon,s}(z) = \frac{1}{2} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ c\equiv 0 \pmod N \\ \gcd(d,N)=1}} \frac{\varepsilon(d)}{(cz+d)} \frac{y^s}{|cz+d|^{2s}}$$

converge absolutamente para $\operatorname{Re} s > \frac{1}{2}$ y define una serie de Eisenstein de peso 1 y carácter ε para $\Gamma_0(N)$ y la serie

$$E_{N,s}(z) = \sum_{\gamma\in\Gamma_0(N)} \operatorname{Im}(\gamma(z))^s$$

es una serie de Eisenstein de peso 0 para $\Gamma_0(N)$, más aún, como $\tilde{\mathscr{E}}_0(\Gamma_0(N))$ tiene dimensión 1 lo genera.

2. Curvas elípticas

En esta sección introduciremos las nociones básicas sobre curvas elípticas y daremos algunas pruebas que nos ayuden a entender mejor estos objetos y en particular ayuden a esclarecer las construcciones con Puntos de Heegner que iremos viendo a lo largo de los próximos capítulos. Para más detalles se puede consultar [4]Ch. I y [15] como libros introductorios y [14] para una lectura más avanzada.

2.1. Primeras definiciones.

Una *curva elíptica* es una curva de género 1 con un punto racional distinguido O. Una curva C/k con un punto racional es de género 1 si y sólo es isomorfa a una curva dada por una ecuación, llamada de Weierstrass, de la forma

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

con $a_1, a_2, a_3, a_4, a_6 \in k$. En consecuencia también podemos definir una curva elíptica como la curva dada por una ecuación de Weierstrass con el punto racional distinguido $O = (0 : 1 : 0)$ en infinito.

Las curvas elípticas admiten una ley de grupo donde el punto distinguido O es el neutro, una *isogenía* entre dos curvas elípticas es un homomorfismo de grupos no trivial.

El mapa multiplicar por $n \in \mathbb{N}$:

$$[n] : E(k) \to E(k), \quad [n](P) = nP = P \oplus \cdots \oplus P$$

es una isogenía, a los puntos en el kernel de este mapa los denotamos por $E[n](k)$ y los llamamos *puntos de n-torsión*. Se puede ver que $E[n](k)$ es un subgrupo finito de $E(k)$, más aún, su cardinal divide a n^2 y si $\mathrm{char}(k) \nmid n$ es exactamente n^2.

Cuando una curva elíptica E tiene una isogenía $\phi : E \to E$ que no es un mapa de multiplicación por n, decimos que E tiene *multiplicación compleja*.

2.2. Reducción módulo p.

Las curvas elípticas definidas sobre $\mathbb{Q}$ admiten un modelo definido por una ecuación corta de Weierstrass de la forma

$$E : y^2 = x^3 + ax + b$$

dado un modelo de esta forma para E podemos reducir sus coeficientes módulo un primo p, a la curva reducida la denotamos por $\tilde{E}$ y definimos el tipo de reducción de E dependiendo de $\tilde{E}$. Cuando p divide al discriminante $\Delta_E = -16(4a^3 + 27b^2)$ la curva que obtenemos tiene una singularidad (y por lo tanto no define una curva elíptica), en estos casos diremos que E tiene *mala reducción* en p, en otro caso diremos que tiene *buena reducción* y además subclasificamos de la siguiente forma

- Buena reducción: si E no tiene singularidades.
  - Si $\tilde{E}(\overline{\mathbb{F}}_p)$ tiene p-torsión no trivial entonces resulta que $\tilde{E}[p](\mathbb{F}_p) \simeq \mathbb{Z}/p\mathbb{Z}$ y en este caso diremos que E tiene reducción *ordinaria*.
  - Si $\tilde{E}(\overline{\mathbb{F}}_p)$ tiene p-torsión trivial diremos que E tiene reducción *supersingular*
- Mala reducción: E tiene una singularidad
  - Si la singularidad es un *nodo*, es decir, hay dos rectas tangentes al punto, diremos que E tiene reducción multiplicativa. En este caso $\tilde{E}(\overline{\mathbb{F}}_p) \simeq \overline{\mathbb{F}}_p^*$. Si

las tangentes están definidas sobre $\mathbb{F}_p$ diremos además que la reducción es *multiplicativa split*, en otro caso diremos que es *multiplicativa non-split*.
- Si la singularidad es una *cúspide*, hay una sola recta tangentes al punto, diremos que E tiene reducción aditiva. En este caso $\tilde{E}(\overline{\mathbb{F}}_p) \simeq \overline{\mathbb{F}}_p$.

2.3. La L-serie asociada a una curva elíptica.

Sea $p \nmid \Delta_E$, definimos $N_p(E)$ como la cantidad de puntos en la curva reducida,

$$N_p(E) = \#\{(x,y) \in \mathbb{F}_p^2 : \ y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}\}$$

y $a_p := p - N_p(E)$. La L-serie asociada a E es

$$L_E(s) = \prod_p L_p(E,s)$$

donde

$$L_p(E,s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s}) & \text{si } E \text{ tiene buena reducción en } p \\ 1 & \text{si } E \text{ tiene reducción aditiva en } p \\ 1 + p^{-s} & \text{si } E \text{ tiene reducción multiplicativa split en } p \\ 1 - p^{-s} & \text{si } E \text{ tiene reducción multiplicativa non-split en } p \end{cases}$$

Esta L-serie tiene buenas propiedades como la convergencia para $\operatorname{Re} s$ suficientemente grande y una ecuación funcional, de hecho, el teorema de Modularidad nos dice que L_E coincide con la L-serie de una forma modular de peso 2!

2.4. Tres teoremas sobre $E(\mathbb{Q})$.

Los siguientes teoremas son resultados que describen la estructura de $E(\mathbb{Q})$.

Teorema 1.19 (Mordell–Weil, 1901). *$E(\mathbb{Q})$ es finitamente generado: $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$ con $r < \infty$ y T, denotanto la torsión de E, finitamente generado.*

Teorema 1.20 (Mazur, 1978). *Los posibles subgrupos de torsión de $E(\mathbb{Q})$ son*

$$\begin{cases} \mathbb{Z}/N\mathbb{Z} & \text{donde } N \in \{1,\dots,10,12\} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & \text{donde } N \in \{1,\dots,4\} \end{cases}$$

El teorema de Mazur es un resultado muy profundo, una exposición de su prueba puede encontrarse en [6, tesisCGallardo].

Por otra parte, el teorema de Nagell-Lutz describe los puntos de torsión de cualquier curva no singular dada por una ecuación de Weierstrass con coeficientes enteros.

Teorema 1.21 (Nagell–Lutz, 1935-1937). *Sea $P = (x,y)$ un punto de torsión en una curva no singular dada por una ecuación*

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

con coeficientes enteros, entonces $x, y \in \mathbb{Z}$ o P tiene orden 2 y $4x, 8y \in \mathbb{Z}$.

En la siguiente sección veremos una descripción topológica de las curvas elípticas.

2.5. Curvas elípticas como toros complejos.

Un *retículo* en $\mathbb{C}$ es un conjunto $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ donde $\{\omega_1, \omega_2\}$ es una base para $\mathbb{C}/\mathbb{R}$, los *toros complejos* son los cocientes $\mathbb{C}/\Lambda$. Algebraicamente un toro complejo es un grupo abeliano con la suma compleja, analíticamente, veremos que es una superficie de Riemann.

PROPOSICIÓN 1.22. *Sean Λ y Λ' dos retículos con bases $\{\omega_1, \omega_2\}$ y $\{\omega_1', \omega_2'\}$ respectivamente. Entonces $\Lambda = \Lambda'$ si y sólo si existe $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ tal que $(\omega_1', \omega_2') = \gamma \begin{pmatrix}\omega_1 \\ \omega_2\end{pmatrix}$.*

La proposición anterior nos deja el siguiente corolario,

COROLARIO 1.23. *Sea $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ una función holomorfa entre toros complejos tal que $\varphi(z + \Lambda) = mz + b + \Lambda'$ y $m\Lambda \subseteq \Lambda'$. Entonces son equivalentes:*

(1) φ es un homomorfismo de grupos.
(2) $b \in \Lambda'$ y $\varphi(z + \Lambda) = mz + \Lambda'$.
(3) $\varphi(0) = 0$.

En particular existe un homomorfismo no trivial si y sólo si existe $m \in \mathbb{C}$ no nulo tal que $m\Lambda = \Lambda'$.

Con esto, podemos restringirnos a tomar bases $\{\omega_1, \omega_2\}$ orientadas de forma que $\omega_1/\omega_2 \in \mathcal{H}$, más aún, podemos considerar que $\omega_1 = 1$ y $\omega_2 = \tau \in \mathcal{H}$. La proposición anterior nos dice que cada toro complejo determina un punto $\tau \in \mathcal{H}$ y que este punto es único a menos de actuar por $\mathrm{SL}_2(\mathbb{Z})$.

El teorema que queremos ver es el siguiente:

TEOREMA 1.24. *Dada una curva elíptica E, existe un réticulo Λ tal que $\mathbb{C}/\Lambda$ y E son isomorfos como superficies de Riemann. Además, dicho isomorfismo es único a menos de homotecia.*

Comencemos definiendo la función de Weierstrass para Λ, esta será la función que nos dará la curva elíptica que queremos.

DEFINICIÓN 1.25. La función $\wp$ de Weierstrass es la serie

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

Esta es una función par, además, si derivamos obtenemos la serie

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

que es una función Λ periódica, lo que quiere decir que $\wp'_\Lambda(z + \omega_i) - \wp'_\Lambda(z) = 0$ para $i = 1, 2$ y por lo tanto $\wp_\Lambda(z + \omega_i) - \wp_\Lambda(z)$ es constante. Si evaluamos en $z = \frac{-\omega_i}{2}$ llegamos a $\wp_\Lambda(\frac{-\omega_i}{2}) - \wp_\Lambda(\frac{\omega_i}{2}) = 0$ y concluimos que $\wp_\Lambda$ también es Λ-periódica.

DEFINICIÓN 1.26. La serie de Eisenstein de peso k para Λ es

$$G_k(\Lambda) = \sum_{\omega \in \Lambda}{}' \frac{1}{\omega^k}.$$

Esta serie de Eisenstein está bien definida y es absolutamente convergente para $k > 2$.

PROPOSICIÓN 1.27. *$\wp_\Lambda(z)$ está bien definida en $\mathbb{C}-\Lambda$, es una función meromorfa con un polo doble en cada $\omega\in\Lambda$. Además, es una función par y periódica con periodos ω_1 y ω_2.*

DEMOSTRACIÓN. Consideremos el disco $C_R=\{z\in\mathbb{C}:|z|\leq R\}$. La intersección $\Lambda\cap C_R$ es finita. Consideremos ahora $\omega\in\Lambda-C_R$, es fácil ver que existe $M_R\in\mathbb{R}$ tal que

$$\left|\frac{1}{(z-\omega)^2}\right|\leq\frac{M_R}{|\omega|^2}.$$

Entonces

$$\left|\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right|=\left|\frac{2z\omega-z^2}{\omega^2(z-\omega)^2}\right|=\left|\frac{z(2\omega-z)}{\omega^2(z-\omega^2)}\right|\leq\frac{M_R(2+R/|\omega|)}{|\omega|^3}\leq\frac{3M_RR}{|\omega|^3},$$

lo cual implica que $\wp_\Lambda$ converge absolutamente y uniformemente en $C_R-\Lambda$ para todo $R\geq 0$, de donde vemos que es meromorfa. Además, poniendo $z=\omega$ vemos que hay un polo cuyo orden es 2 para todo $\omega\in\Lambda\cap C_R$. La paridad de $\wp_\Lambda$ es clara,

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

Para ver la periodicidad de $\wp_\Lambda$ consideremos su derivada,

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

que es Λ-periódica. Como $\wp'_\Lambda(z+\omega)-\wp'_\Lambda(z)=0$ para todo $z\in\mathbb{C}-\Lambda$, $\omega\in\Lambda$ resulta que $\wp_\Lambda(z+\omega_i)-\wp_\Lambda(z)$ es constante, evaluando en $z=\frac{-\omega_i}{2}$ llegamos a que es 0, y por lo tanto tiene periodos ω_i para $i=1,2$. ■

PROPOSICIÓN 1.28 (La expansión de Laurent).
Para $z\in C_R$ donde $R:=\min\{|\omega|:\omega\in\Lambda-\{0\}\}$

$$\wp_\Lambda(z)=\frac{1}{z^2}+\sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n}.$$

DEMOSTRACIÓN.

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

Si le restamos $\frac{1}{\omega^2}$ nos queda

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

y sumando sobre ω

$$\wp_\Lambda(z)=\frac{1}{z^2}+\sum_{\omega\in\Lambda}{}'\sum_{n=1}^{\infty}\frac{(n+1)z^n}{\omega^{n+2}}=\frac{1}{z^2}+\sum_{n=1}^{\infty}(n+1)G_{n+2}(\Lambda)z^n.$$

Finalmente, como $\wp_\Lambda$ es una función par, los coeficientes n-ésimos son nulos para n impar. ■

TEOREMA 1.29. *El par* $(\wp_\Lambda, \wp'_\Lambda)$ *satisface la igualdad*

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

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

Además, la cúbica que satisface: $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ *se descompone como* $y^2 = 4(x-e_1)(x-e_2)(x-e_3)$ *donde* $e_1 = \wp_\Lambda(\frac{\omega_1}{2})$, $e_2 = \wp_\Lambda(\frac{\omega_2}{2})$, $e_3 = \wp_\Lambda(\frac{\omega_1+\omega_2}{2})$ *son todos distintos.*

DEMOSTRACIÓN. De la expansión de Laurent alrededor del origen obtenemos que $\wp'_\Lambda(z) = \frac{-2}{z^3} + 6G_4(\Lambda)z + 20G_6(\Lambda) + O(z^5)$. Si ahora elevamos al cuadrado nos queda $[\wp'_\Lambda(z)]^2 = \frac{4}{z^6} - \frac{24G_4(\Lambda)}{z^2} - 80G_6(\Lambda) + O(z^2)$ y por otra parte $4[\wp_\Lambda(z)]^3 = \frac{4}{z^6} + \frac{36G_4(\Lambda)}{z^2} + 60G_6(\Lambda) + O(z^2)$. Restando ambas cosas

$$[\wp'_\Lambda(z)]^2 - 4[\wp_\Lambda(z)]^3 - \frac{60G_4(\Lambda)}{z^2} = -140G_6(\Lambda) + O(z^2).$$

El lado izquierdo de esta igualdad no tiene polos en $z = 0$ y por lo tanto no tiene polos en el paralelogrado de vértices $\{0, \omega_1, \omega_2, \omega_1 + \omega_2\}$, al ser $\wp_\Lambda$ y su derivada funciones Λ-periódicas esto implica que el lado izquierdo es holomorfo y está acotado, por lo tanto es constante.

Nos resta ver que los e_i son las raíces de $4x^3 - g_2(\Lambda)x + g_3(\Lambda)$ y son distintos. Como $\wp_\Lambda$ es par, $\wp'_\Lambda$ es impar y por lo tanto

$$\wp'_\Lambda\left(\frac{\omega_i}{2}\right) = -\wp'_\Lambda\left(\frac{-\omega_i}{2}\right) = -\wp'_\Lambda\left(\omega_i - \frac{\omega_i}{2}\right) = -\wp'_\Lambda\left(\frac{\omega_i}{2}\right) = 0,$$

de donde los e_i son raíces, para ver que son distintas consideremos las funciones $g_i(z) = \wp_\Lambda(z) - e_i$ con las respectivas raíces $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$. Como la derivada también se anula allí, son ceros de orden al menos 2, si $e_1 = e_2$ entonces $\wp_\Lambda$ tendría un cero de orden al menos 4, pero sus ceros son de orden 2. ■

OBSERVACIÓN 1.30. *El discriminante de* $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, $g_2(\Lambda)^3 - 27g_3(\Lambda)^2$ *es no nulo porque el polinomio tiene tres raíces distintas.*

Lo que acabamos de ver muestra que el mapa $z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z))$ definido en $\mathbb{C} - \Lambda$ envía puntos en el toro complejo a pares de puntos en $\mathbb{C}^2$ que satisfacen la ecuación de una curva elíptica (pues es una cónica no singular). Este mapa se puede extender a todo $\mathbb{C}$ si enviamos los puntos en el retículo al punto O de la curva elíptica, ahora tenemos que ver dos cosas:

1. El mapa anterior es un isomorfismo entre superficies de Riemann.
2. El mapa anterior es un isomorfismo de grupos.

TEOREMA 1.31. *Sea* $E : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$. *El mapa* $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}) \subseteq \mathbb{P}^2(\mathbb{C})$ *definido por* $\phi(z+\Lambda) = (\wp_\Lambda(z), \wp'_\Lambda(z))$ *para* $z \neq 0 + \Lambda$ *y* $\phi(0+\Lambda) = O$ *es un isomorfismo entre superficies de Riemann y un isomorfismo de grupos.*

DEMOSTRACIÓN. Ya vimos que el mapa está bien definido, veamos ahora que es biyectivo. Para ver la inyectividad supongamos que $\phi(z_1) = \phi(z_2)$, la función $\wp_\Lambda$ es de orden 2 (la cantidad de soluciones a $\wp_\Lambda(z) = 0$ contadas con multiplicidad en un paralelogramo es igual a la cantidad de polos, y los polos de $\wp_\Lambda$ son los $\omega \in \Lambda$ con orden

2), como $\wp_\Lambda(z) - \wp_\Lambda(z_1)$ se anula en z_1, z_2 y $-z_1$ esto quiere decir que al menos dos de estas raíces son congruentes módulo Λ.

- Si $2z_1 \in \Lambda$: $\wp_\Lambda(z) - \wp_\Lambda(z_1)$ tiene un cero doble en z_1 y se anula en z_2, por lo tanto $z_1 - z_2 \in \Lambda$.
- Si $z_2 + z_1 \in \Lambda$: $\wp'_\Lambda(z_2) = \wp'_\Lambda(-z_1) = -\wp'_\Lambda(z_1)$, como por hipótesis $\wp'_\Lambda(z_2) = \wp'_\Lambda(z_1)$ esto implica que las derivadas se anulan y por lo tanto $z_2 - z_1 \in \Lambda$.

Para ver la sobreyectivad tomemos un punto en E. Si el punto es O tiene preimagen 0. Si el punto es $(x, y) \in \mathbb{C}^2$, sabemos que existe z tal que $\wp_\Lambda(z) = x$ porque $\wp_\Lambda$ tiene orden 2, luego $y = (\wp'_\Lambda(x))$ y $y = (-\wp'_\Lambda(z))$ satisfacen la ecuación.

Para ver que ϕ es holomorfa solo resta ver que lo es en 0; $\wp_\Lambda$ y $\wp'_\Lambda$ tienen polos en 0, tomemos $z \neq 0$ arbitrario y veamos la curva proyectivamente.

$$\phi(z + \Lambda) = (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1) = (z^3\wp_\Lambda(z) : z^3\wp'_\Lambda(z) : z^3),$$

si ahora tomamos límite $z \to 0$ vemos que $\lim_{z\to 0} \phi(z) = (0 : -2 : 0) = (0 : 1 : 0) = O$. Si queremos probar que ϕ es un isomorfismo, por el teorema de la función inversa basta ver que es inyectivo con derivada no nula; ya vimos que es inyectivo.

Los ceros de $\wp'_\Lambda(z)$ son $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$ y estos son ceros de $g(z) = \wp_\Lambda(z) - e_i$ $i = 1, 2, 3$ respectivamente, y tienen orden 2. Si derivamos $g'(z) = \wp'_\Lambda(z)$ y $g''(z) = \wp''_\Lambda(z)$, y al tener ceros de orden 2 esto implica que $g'' \neq 0$ y por lo tanto ϕ' y ϕ'' no tienen ceros en común. Esto prueba que ϕ es efectivamente un isomorfismo de Superficies de Riemann, para terminar la prueba del teorema queremos ver que preserva la Ley de grupo.

Por definición $\phi(0 + \Lambda) = O$, la ley de grupo en E está caracterizada porque la suma de tres puntos colineales en la curva da O, tenemos que probar que ϕ respeta esta estructura. Tomemos dos puntos en $\mathbb{C}/\Lambda$: $z_1 + \Lambda, z_2 + \Lambda$ y la recta por los puntos $\phi(z_1 + \Lambda), \phi(z_2 + \Lambda)$ en el plano complejo: $ax + by + c = 0$. Distinguimos dos casos

1. Si $b \neq 0$ la función $a\wp_\Lambda(z) + b\wp'_\Lambda(z) + c = 0$ tiene un polo triple en $0 + \Lambda$.
2. Si $b = 0$ la función $a\phi_\Lambda(z) + c = 0$ tiene un polo doble en $0 + \Lambda$.

En 1. se puede ver que hay un tercer punto $z_3 + \Lambda$ tal que $z_1 + z_2 + z_3 + \Lambda = 0 + \Lambda$. En 2. se puede poner $z_3 = 0$ y se satisface lo mismo. ■

3. La curva modular

A partir de ahora usaremos los términos "curva elíptica" y "toro complejo" indistintamente. Diremos que dos curvas elípticas son equivalentes si, como en Corolario 1.36, $m\Lambda = \Lambda'$, esto claramente da una clase de equivalencia de curvas elípticas complejas. El mismo corolario dice que cada toro complejo determina un punto τ en el semiplano superior que es único a menos de actuar por $\mathrm{SL}_2(\mathbb{Z})$, consideremos entonces la relación de equivalencia en $\mathcal{H}$ dada por esta acción. Hay una biyección entre las primeras clases de equivalencia y las segundas: las clases de isomorfismo de curvas elípticas se corresponden con las clases de equivalencia del semiplano superior bajo la acción del grupo modular.

Definimos el *espacio de moduli*

$$S_0(N) = \{(E, C) : \ E \text{ curva elíptica y } C \text{ un subgrupo cíclico de } E \text{ de orden } N\}/\sim,$$

donde $(E, C) \sim (E', C')$ si existe un isomorfismo $\phi : E \to E'$ tal que $\phi(C) = C'$. Notaremos por $[E, C]$ a un elemento de $S_0(N)$, observemos que es equivalente dar un elemento $[E, C]$ en el espacio de moduli $S_0(N)$ que dar una isogenía $\phi : E \to E'$ de grado N. A lo largo de los siguientes capítulos usaremos la segunda descripción, pero la primera ilustra mejor la prueba del teorema que veremos a continuación.

La curva modular para $\Gamma_0(N)$ es $Y_0(N) = \Gamma_0(N) \setminus \mathcal{H} = \{\Gamma_0(N)\tau \ : \tau \in \mathcal{H}\}$.

Teorema 1.32. *Se cumple que* $S_0(N) = \{[\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] : \tau \in \mathcal{H}\}$.

Además, dos elementos en $S_0(N)$, $[E_\tau, \langle 1/N + \Lambda_\tau\rangle]$ *y* $[E_{\tau'}, \langle 1/N + \Lambda_{\tau'}\rangle]$ *son iguales si y sólo si* $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. *Concluimos que el mapa* $\psi_0 : S_0(N) \to Y_0(N)$ *dado por* $\psi_0([E_\tau, \langle 1/N + \Lambda_\tau\rangle]) = \Gamma_0(N)\tau$ *es una biyección.*

Demostración. Sea $[E, C]$ un elemento de $S_0(N)$, ya vimos que E es isomorfa a un toro complejo $\mathbb{C}/\Lambda_{\tau'}$ y por lo tanto un generador de C se puede escribir como $g = \frac{c\tau'+d}{N} + \Lambda'_\tau$ con $\gcd(c, d, N) = 1$. Sean $a, b \in \mathbb{Z}$ tales que $ad - bc \equiv 1 \pmod N$ y consideremos $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, a menos de cambiar los representantes de $a, b, c, d \mod N$ podemos asumir que $\Gamma \in \mathrm{SL}_2(\mathbb{Z})$. Observemos que tomando $\tau = \gamma\tau'$ obtenemos que

$$(c\tau' + d)\Lambda_\tau = (c\tau + d)(\mathbb{Z} \oplus \mathbb{Z}\tau) = (cz + d)\mathbb{Z} + (a\tau' + b)\mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}\tau = \Lambda_{\tau'}$$

y por lo tanto el mapa multiplicar por $c\tau' + d$ es un isomorfismo de $\mathbb{C}/\Lambda_\tau$ en $\mathbb{C}/\Lambda_{\tau'}$ que envía $\frac{1}{N} + \Lambda_\tau$ en g.

Ahora supongamos que $\tau, \tau' \in \mathcal{H}$ son tales que $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$, entonces $\tau = \gamma\tau'$ con $\gamma \in \Gamma_0(N)$. Como $c \equiv 0 \pmod N$ y $\gcd(d, N) = 1$,

$$(c\tau' + d)\Lambda_\tau = \Lambda_{\tau'} \qquad (c\tau' + d)\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{d}{N} + \Lambda_{\tau'}.$$

Concluimos que $[\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau\rangle] = [\mathbb{C}/\Lambda_{\tau'}, \langle \frac{1}{N} + \Lambda_{\tau'}\rangle]$. Con argumentos similares se puede ver que si $[\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau\rangle] = [\mathbb{C}/\Lambda_{\tau'}, \langle \frac{1}{N} + \Lambda_{\tau'}\rangle]$ entonces $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. ■

Acabamos de ver una biyección entre el espacio de moduli $S_0(N)$ y la curva modular $Y_0(N) = \Gamma_0(N)/\mathcal{H}$, pero de hecho se le puede dar a ambos espacios estructuras de Superficie de Riemann, de forma que son isomorfos como superficies de Riemann. La curva modular se puede compactificar, a la curva compactificada la denotamos $X_0(N)$, esta es Hausdorff, conexa, compacta y también se le puede dar estructura de una Superficie de Riemann. A veces haremos abuso de notación y escribiremos $E \xrightarrow{\phi} E' \in Y_0(N)$.

4. Álgebras de cuaterniones

En esta sección presentaremos algunas nociones básicas sobre álgebras de cuaterniones. Nos basaremos en las notas [17, FMC] escritas por Gonzalo Tornaría para la AGRA II, 2015, una referencia extensa sobre el tema es [19].

El álgebra de *cuaterniones de Hamilton* es el álgebra sobre $\mathbb{R}$ con base $\{1, i, j, k\}$ donde $i^2 = j^2 = k^2 = ijk = -1$. Esta construcción se puede generalizar a cualquier cuerpo de característica distinta de 2.

Definición 1.33. Dado un cuerpo K con $\mathrm{char}(K) \neq 2$ y $a, b \in F^*$ definimos el álgebra de cuaterniones $(a, b)_K$ como el álgebra con base $1, i, j, k$ donde la multiplicación viene determinada por las relaciones

$$i^2 = a, \qquad j^2 = b, \qquad k = ij = -ji.$$

Una K-álgebra es *central* si su centro es K y *simple* si no tiene ideales bilateros no triviales. No es difícil probar que la definición anterior es equivalente a la siguiente:

Definición 1.34. Un álgebra de cuaterniones sobre K es un álgebra central simple de dimensión 4 sobre K.

Es decir, $(a, b)_K$ es una K-álgebra central simple de dimensión 4 y recíprocamente un álgebra de cuaterniones sobre K tiene la forma $(a, b)_K$ para un par de elementos no nulos de K. Esta última definición es la usual y es válida incluso en característica 2.

Ejemplo 1.35.

- El álgebra de cuaterniones de Hamilton $(-1, -1)_{\mathbb{R}}$ es un álgebra de división.
- Las matrices 2×2 sobre $\mathbb{R}$ forman un álgebra de cuaterniones.

De hecho, a menos de isomorfismo estas son las únicas álgebras de cuaterniones sobre $\mathbb{R}$, y vale en general que toda álgebra de cuaterniones sobre un cuerpo K es un álgebra de división o es isomorfa a $M_2(K)$.

4.1. Clasificación de álgebras de cuaterniones.

Ya mencionamos la clasificación sobre $\mathbb{R}$, sobre $\mathbb{C}$ no hay álgebras de división no triviales por lo que toda álgebra es isomorfa a $M_2(\mathbb{C})$, lo mismo ocurre en cuerpos finitos, la siguiente pregunta que surge naturalmente es qué ocurre con $\mathbb{Q}$ y para responder esto haremos un estudio local.

Las posibles completaciones de $\mathbb{Q}$ son $\mathbb{Q}_p$ con p primo o $\mathbb{Q}_\infty = \mathbb{R}$. Sea v un lugar para $\mathbb{Q}$, esto es, $v \in \{p : \text{ primo}\} \cup \{\infty\}$ y sea D un álgebra de cuaterniones sobre $\mathbb{Q}$, la localización de D en v es la extensión de escalares a $\mathbb{Q}_v$: $D_v := D \otimes \mathbb{Q}_v$.

Comencemos con el lugar arquimediano ∞, el álgebra D_∞ puede ser isomorfa a $H = (-1, -1)_{\mathbb{R}}$ o a $M_2(\mathbb{R})$. En el primer caso decimos que D es *definida* y en el segundo caso que es *indefinida*. De forma similar tenemos el siguiente Teorema:

Teorema 1.36 (Clasificación local). *Hay* exactamente *dos álgebras de cuaterniones sobre $\mathbb{Q}_v$ a menos de isomorfismo: $M_2(\mathbb{Q}_v)$ y un álgebra de división.*

Definición 1.37. Decimos que un álgebra de cuaterniones D ramifica en v si D_v es isomorfa a un álgebra de división.

La ramificación de un álgebra de cuaterniones la determina a menos de isomorfismos.

PROPOSICIÓN 1.38. *Dos álgebras de cuaterniones son isomorfas si y sólo si ramifican en los mismos lugares.*

Además, la ramificación es un número finito y par, y tenemos la siguiente clasificación global.

TEOREMA 1.39 (Clasificación global). *La ramificación de D es un conjunto finito de cardinal par. Más aún, dado un conjunto de lugares finito de cardinal par, existe un álgebra de cuaterniones sobre $\mathbb{Q}$ con esa ramificación y esta es única a menos de isomorfismo.*

Este resultado se extiende a cualquier cuerpo de números de la siguiente manera. Sea K un cuerpo de números.

DEFINICIÓN 1.40. Un lugar de K es un ideal primo en $\mathcal{O}_K$ o una inmersión $K \hookrightarrow \mathbb{R}$ o $K \hookrightarrow \mathbb{C}$.

Las definiciones de localización y ramificación son analogas.

TEOREMA 1.41. *Sea D es un álgebra de cuaterniones sobre K, entonces D ramifica en un conjunto finito par de lugares que no contiene ningún lugar complejo. Además, dado un conjunto lugares no complejos de cardinal par existe un álgebra de cuaterniones que ramifica en dicho conjunto y dicha álgebra es única a menos de isomorfismo.*

4.2. Revisitando la clasificación de curvas elípticas.

DEFINICIÓN 1.42. Un retículo en un álgebra de cuaterniones D es un $\mathbb{Z}$-submódulo libre de rango 4. Un orden en D es un retículo que además es un subanillo de D.

Consideremos E/k una curva elíptica y $\mathrm{End}_k(E) = \{\alpha : E \to E : \alpha \text{ es una isogenía sobre } k\}$, este anillo (con la suma punto a punto y la composición) de endomorfismos es isomorfo o bien a $\mathbb{Z}$, a un orden en un cuerpo cuadrático imaginario o a un orden en un álgebra de cuaterniones y esta clasificación se corresponde con la que vimos en 2.2.

PROPOSICIÓN 1.43. *Sea E/k una curva elíptica y $\mathrm{End}_k(E)$ su anillo de endomorfismos. Entonces*

1. *Si $\mathrm{char}(k) = 0$, entonces $\mathrm{End}_k(E) \simeq \mathbb{Z}$ o $\mathrm{End}_k(E) \simeq \mathcal{O}$, un orden en un cuerpo cuadrático imaginario.*
2. *Si $\mathrm{char}(k) \neq 0$, entonces hay dos opciones para $\mathrm{End}_k(E)$.*

$$\mathrm{End}_k(E) \simeq \mathcal{O} \quad o \quad \mathrm{End}_k(E) \simeq R$$

donde $\mathcal{O}$ es un orden en un cuerpo cuadrático imaginario y R es un orden maximal en un álgebra de cuaterniones.

Observemos que cuando $k = \mathbb{Q}$ o $k = \mathbb{C}$ la parte 1 de la proposición anterior nos dice que E/k tiene multiplicación compleja si $\mathrm{End}_k(E) \simeq \mathcal{O}$.

COROLARIO 1.44 (Clasificación de curvas elípticas). *Sea E/k una curva elíptica sobre k un cuerpo de característica p. Entonces ocurre exactamente una de las siguientes opciones.*

- $\mathrm{End}_k(E) \otimes \mathbb{Q} \simeq \mathbb{Q}$.
- $\mathrm{End}_k(E) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{D})$.

- $\mathrm{End}_k(E) \otimes \mathbb{Q} \simeq B_{p,\infty}$, *el álgebra de cuaterniones ramificada en* $\{p, \infty\}$.

En el tercer caso de la proposición diremos que la curva tiene reducción *supersingular*, en caso contrario diremos que tiene reducción *ordinaria.* No es difícil ver que la definición que vimos antes coincide con esta.

Capítulo 2

Puntos de Heegner

DEFINICIÓN 2.1. Un *punto de Heegner* de discriminante D en $Y_0(N) \subseteq X_0(N)$ es un punto $x = (E \xrightarrow{\phi} E')$ donde ϕ tiene grado N y E, E' son curvas elípticas con multiplicación compleja, que además tienen el mismo anillo de endomorfismos $\mathcal{O}_K$, el anillo de enteros de un cuerpo cuadrático imaginario de discriminante D.

Tenemos una condición necesaria y suficiente para la existencia de puntos de Heegner de discriminante D: existen si y sólo si existe un ideal entero $\mathfrak{n} \subseteq \mathcal{O}$ tal que $\mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$, por lo que en general asumimos que estamos bajo la Hipótesis de Heegner

(HH) Existe un ideal $\mathfrak{n} \subseteq \mathcal{O}$ tal que $\mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$.

A los ideales que satisfacen esa condición le llamamos *primitivos de norma* N.

PROPOSICIÓN 2.2. *Hay una biyección*

$$\left\{\begin{array}{c}\textit{Puntos de Heegner}\\ \textit{en } X(\mathbb{C})\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{Pares } (\mathscr{A},\mathfrak{n}) : \mathscr{A} \in Cl_K\\ \mathfrak{n} \textit{ ideal primitivo de norma } N \textit{ en } \mathcal{O}\end{array}\right\}$$

Dada por $(\mathbb{C}/\mathfrak{a}, \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}) \hookleftarrow ([\mathfrak{a}], \mathfrak{n})$

DEMOSTRACIÓN. Consideremos $\mathfrak{a}$ un ideal (fraccional) de Cl_K y $\mathfrak{n}$ un ideal primitivo de norma N. Las curvas elípticas $E = \mathbb{C}/\mathfrak{a}$ y $E' = \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$ tienen multiplicación compleja por $\mathcal{O}$ y la identidad en $\mathbb{C}$ induce una isogenía $id : E \to E'$ entre ellas con núcleo $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \simeq \mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$.

Observemos que otro par $(\mathfrak{a}', \mathfrak{n}')$ en las mismas hipótesis definen el mismo punto de Heegner si y solo si $\mathbb{C}/\mathfrak{a} = \mathbb{C}/\mathfrak{a}'$ y $\mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1} = \mathbb{C}/\mathfrak{a}'\mathfrak{n}'^{-1}$, y esto ocurre si y sólo si existe $\lambda \in K^*$ tal que $\mathfrak{a} = \lambda\mathfrak{a}'$ y $\mathfrak{n} = \mathfrak{n}'$. Por otro lado, dado un punto de Heegner $x = (E \xrightarrow{\phi} E')$ de discriminante D, podemos escribir $E = \mathbb{C}/\Lambda$ y $E' = \mathbb{C}/\Lambda'$, y a menos de reescalar Λ y Λ' podemos asumir que están en K y que por lo tanto son ideales fraccionales $\mathfrak{a}$ y $\mathfrak{b}$ respectivamente con $\mathfrak{a} \subseteq \mathfrak{b}$. Como el núcleo de la isogenía es un grupo cíclico de orden N isomorfo a $\mathfrak{b}/\mathfrak{a}$ resulta que $n = \mathfrak{a}\mathfrak{b}^{-1}$ es un ideal primitivo de orden N. ■

Hay una correspondencia entre ideales primitivos de norma N y soluciones $\beta \in \mathbb{Z}/2N\mathbb{Z}$ a la ecuación $\beta^2 \equiv D \pmod{4N}$ que viene dada por

$$\beta \mapsto \mathfrak{n} = N\mathbb{Z} + \frac{\beta + \sqrt{|D|}}{2}\mathbb{Z}.$$

Esta correspondencia sumada a la correspondencia entre curvas elípticas con multiplicación compleja por $\mathcal{O}$ y soluciones a ecuaciones cuadráticas de discriminante D nos dan la siguiente proposición.

PROPOSICIÓN 2.3. *Hay una biyección*

$$\{(\mathscr{A},\mathfrak{n}) : \mathscr{A} \in Cl_K, \mathfrak{n} \text{ ideal primitivo en } \mathcal{O}\}$$
$$\updownarrow$$
$$\Gamma_0(N)\backslash \left\{ \begin{array}{c} \text{Soluciones } \tau\in\mathcal{H} \text{ a una ecuación cuadrática primitiva} \\ Ax^2+Bx+C=0 \\ \text{de discriminante } D \text{ tal que } N|A,\ A>0 \end{array} \right\}$$

DEMOSTRACIÓN. Sea x un punto de Heegner, por la proposición anterior se corresponde con un par $([\mathfrak{a}],\mathfrak{n})$ donde $\mathfrak{a}$ y $\mathfrak{n}$ son ideales en $\mathcal{O}$ con $\mathfrak{n}$ primitivo de norma N. Podemos asumir (reescalando) que tenemos una base orientada $\langle\omega_1,\omega_2\rangle$ de $\mathfrak{a}$ tal que $\langle\omega_1,\omega_2/N\rangle$ es una base de $\mathfrak{a}\mathfrak{n}^{-1}$, de esta forma $\tau = \frac{\omega_1}{\omega_2} \in \mathcal{H}$ satisface una ecuación cuadrática con coeficientes enteros primitiva de discriminante D, ya que está en K y lo mismo ocurre con $N\tau$. Como $N\tau$ también satisface una ecuación cuadrática resulta que $N \mid A$ y $\gcd(A/N, B, CN) = 1$. De hecho, podemos escribir $\mathfrak{a} = A\mathbb{Z} + \frac{B+\sqrt{D}}{2}$ y por lo tanto $\mathfrak{a}\mathfrak{n}^{-1} = \frac{A}{N}\mathbb{Z} + \frac{B+\sqrt{D}}{2}\mathbb{Z}$.

Recíprocamente, si $\tau \in \mathcal{H}$ satisface una ecuación cuadrática de discriminante D entonces $E = \mathbb{C}/\Lambda_\tau$ tiene multiplicación compleja por $\mathcal{O}$, ya vimos que existe un ideal fraccional $\mathfrak{a}$ tal que $E = \mathbb{C}/\mathfrak{a}$, la clase de B en $\mathbb{Z}/2N\mathbb{Z}$ es invariante módulo $\Gamma_0(N)$ y determina un ideal $\mathfrak{n}$ de norma N, la condición sobre A implica que $E = \mathbb{C}/\mathfrak{n}\mathfrak{a}^{-1}$ también es una curva elíptica por lo que la isogenía $(E \xrightarrow{\phi} E')$ corresponde a un punto de Heegner. ■

1. Acciones sobre puntos de Heegner

Se puede ver que $\mathbb{C}/\mathcal{O}$ está definido sobre H, el cuerpo de clases de Hilbert de K, que se define como la máxima extensión abeliana no ramificada de K. Por lo tanto los puntos de Heegner $x \in X_0(N)(\mathbb{C})$ son puntos racionales en $X_0(N)(H)$. El mapa de Artin da una biyección entre $\mathrm{Gal}(H/K)$ y Cl_K (ver Th. 5 3 en [2]) para cualquier cuerpo de numéros K, como en nuestro caso K es un cuerpo cuadrático imaginario la teoría CM nos da el siguiente resultado.

TEOREMA 2.4. *Si K es un cuerpo cuadrático imaginario y $\mathfrak{a}$ es un ideal propio en $\mathcal{O}_K$, entonces $H = K(j(\mathfrak{a}))$ y el mapa $\varphi : Cl_K \to \mathrm{Gal}(H/K)$ dado por $\mathfrak{b} \mapsto \sigma$ donde $j(\mathfrak{a})^\sigma = j(\mathfrak{a}\mathfrak{b}^{-1})$ es biyectivo.*

Queremos estudiar la acción del grupo de Galois sobre los puntos de Heegner y para eso usamos la identificación de la proposición 2.2.

- **Conjugación compleja:** actúa en el par $([\mathfrak{a}],\mathfrak{n})$ como $\overline{([\mathfrak{a}],\mathfrak{n})} = ([\overline{\mathfrak{a}}],\overline{\mathfrak{n}}) = ([\mathfrak{a}]^{-1}, N\mathfrak{n}^{-1})$.
- **Gal(H/K)**: actúa en Cl_K por multiplicación a derecha, $([\mathfrak{a}],\mathfrak{n})^{\varphi(\mathfrak{b})} = ([\mathfrak{a}\mathfrak{b}^{-1}],\mathfrak{n})$
- **Involución canónica:** La involución canónica $\omega_N : Y_0(N)(\mathbb{C}) \to Y_0(N)(\mathbb{C})$ es la inducida por la involución $\omega_N(z) = -\frac{1}{Nz}$ definida en $\mathcal{H}^*$. Esta acción envía una base del retículo asociado a E en una de E' mediante la isogenía dual. En pares $([\mathfrak{a}],\mathfrak{n})$ correspondientes a un punto de Heegner la acción es $\omega_N(([\mathfrak{a}],\mathfrak{n})) = ([\mathfrak{a}\mathfrak{n}^{-1}],\overline{\mathfrak{n}})$.
- **Involuciones de Atkin-Lehner:** por cada $p \mid N$ hay una involución $\omega_p : Y_0(N)(\mathbb{C}) \to Y_0(N)(\mathbb{C})$ inducida por cualquier matriz $W_p \in \begin{pmatrix} p\mathbb{Z} & \mathbb{Z} \\ N\mathbb{Z} & p\mathbb{Z} \end{pmatrix}$ de

determinante p, en pares $([\mathfrak{a}], \mathfrak{n})$ la acción se ve como $\omega_p(([\mathfrak{a}], \mathfrak{n})) = ([\mathfrak{a}\mathfrak{p}^{-k}], \mathrm{m})$ donde $\mathfrak{n} = \mathfrak{p}^k\mathfrak{m}$ siendo $\mathfrak{p}$ el único divisor de p que también divide a $\mathfrak{n}$.

El *Jacobiano* de una superficie de Riemann X de género g es el cociente

$$J(X) = \Omega^1_{\mathrm{hol}}(X)^\wedge / H^1(X, \mathbb{Z}),$$

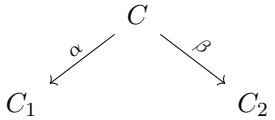
tiene estructura de toro complejo de dimensión g y $X \hookrightarrow J(X)$. Nosotros trabajaremos en el Jacobiano $J(X)$ de la curva modular $X = X_0(N)$. La correspondencia de Abel permite identificar $J(H)$ con el cociente $\mathrm{Div}^0(X)/P(X)$ de divisores de grado 0 módulo divisores principales en X.

Estamos interesados en dos elementos específicos en $J(X)$, los que se corresponden con

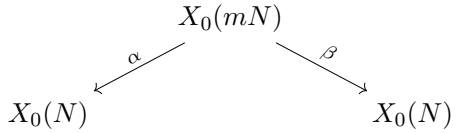
$$c = (x) - (\infty) \qquad \text{y} \qquad d = (x) - (0)$$

siendo x un punto de Heegner de discriminante D. Particularmente nos interesa calcular $T_m(c)$ y $T_m(d)$, donde T_m son correspondencias de Hecke definidas en $J(H)$.

Una correspondencia entre dos curvas C_1 y C_2 es una curva C junto con un par de mapas $\alpha : C \mapsto C_1$, $\beta : C \mapsto C_2$ que representamos mediante el diagrama



Las correspondencias de Hecke se definen para $m \geq 1$ coprimo con N mediante un diagrama



Como $\gcd(m, N) = 1$, si $\phi : E \mapsto E'$ es una Nm-isogenía su núcleo es un subgrupo cíclico de orden mN, como $\gcd(m, N) = 1$ se puede descomponer como suma directa de un subgrupo de orden m y otro de orden N. Podemos suponer sin pérdida de generalidad (reescalando retículos) que $E' = E/C_m \oplus C_N$. El mapa α se olvida de C_m y β cocienta por él, más precisamente,

$$\alpha([E, E/C_m \oplus C_N]) = [E, E/C_N]$$

$$\beta([E, E/C_m \oplus C_N]) = [E/C_m, E/(C_m \oplus C_N)/C_m].$$

Los mapas α y β inducen mapas α^*, β_* en los divisores de grado 0

$$[E, E/C_N] \overset{\alpha^*}{\to} \sum_{C_m \leq E} [E, E/C_m \oplus C_N] \overset{\beta_*}{\to} \sum_{C_m \leq E} [E/C_m, E/(C_m \oplus C_N)/C_m]$$

y $\alpha^* \circ \beta_*$ induce un mapa en el jacobiano. En resumen tenemos una acción en $J(H)$ dada por

$$T_m((x)) = \sum_{C \in S} (x_C)$$

donde S es el conjunto de subgrupos de E cíclicos de orden m y $x_C = [E/C, E'/\phi(C)]$.

2. Alturas locales y altura global

En la expresión algebraica de la fórmula de Gross–Zagier nos aparece el término $\langle c, T_m c^\sigma \rangle$, este símbolo corresponde a la altura de Nerón–Tate, que es una forma cuadrática en $J(H)$. La altura de Nerón–Tate admite una descomposición como suma de alturas locales en divisores con soporte disjuntos, resultado que fue probado por Nerón.

El soporte de un divisor $d = \sum_{y \in X} m_y(y)$ es el conjunto $\mathrm{Sop}(d) = \{y \in X : \ m_y \neq 0\}$. Denotemos por

$$\mathrm{Div}^0_{RP}(X) \coloneqq \{(a,b) \in \mathrm{Div}^0(X) \times \mathrm{Div}^0(X) : a, b \text{ con soporte disjuntos.}\}$$

al conjunto de pares de divisores con soporte disjunto, allí estarán bien definidas las alturas locales.

Para cada lugar v en H existe una valuación $|\cdot|_v : H_v^\times \to \mathbb{R}_{>0}$, denotemos por H_v al completado. Para todo $\alpha \in H^\times$ se cumple la fórmula del producto

$$\prod_v |\alpha|_v = 1.$$

Dado un lugar v se define el símbolo de altura local $\langle\ ,\ \rangle_v : \mathrm{Div}^0_{RP}(X/H_v)$ como la única función que cumple

1. Es biaditiva y simétrica.
2. Es continua.
3. Si $a = \sum_P m_P P$ y $b = \mathrm{div}(f)$ entonces $\langle a, b\rangle_v = \sum_P m_P \log |f(P)|_v$.

No es obvio que existe una función con esas características aunque sí es fácil ver que si existe es única, ya que dados dos símbolos su resta está bien definida sobre $J(H_v) \times J(H_v)$ que es compacto, y es un mapa continuo y aditivo que toma valores reales, por lo tanto es la función nula.

La suma de estos símbolos locales en divisores con soporte disjunto coinciden con el símbolo global: $\langle a, b\rangle = \sum_v \langle a, b\rangle_v$. Como los símbolos locales $\langle a, b\rangle_v$ valen 0 para casi todo lugar v la suma es finita, además, por la fórmula del producto la altura global queda invariante al sumarle a a un ideal principal, es decir, está bien definida en $J(H)$.

3. Ejemplo: La curva 83a1

En su artículo [21], Zagier utiliza la curva elíptica [13, 37.a1] como ejemplo para ilustrar los elementos que aparecen en el Teorema de Gross–Zagier. Intentemos hacer algo similar pero utilizando la curva elíptica [13, 83.a1] Consideremos la curva elíptica $E/\mathbb{Q}$ dada por $y^2 + xy - y = x^3 + x^2 + x$. El discriminante de E es $\Delta = -83$, su conductor es $N = 83$ y su j invariante es $j = \frac{47^3}{83}$.

La curva E sobre $\mathbb{C}$.

El cambio de variable $y \mapsto 2y + x$ seguido de $y \mapsto y + 1$ nos da la forma reducida $E : y^2 = 4x^3+5x^2+6x+1$, el polinomio $4x^3+5x^2+6x+1$ tiene una raíz real $\gamma \approx -0.1929$, y dos raíces complejas conjugadas $\alpha \approx -0.5286 + 1.0083i$, $\beta \approx -0.5286 - 1.0083i$ y como se ve en la figura 1 $E(\mathbb{R})$ tiene una sola componentes, es decir $E(R) \simeq S^1$. Los periodos

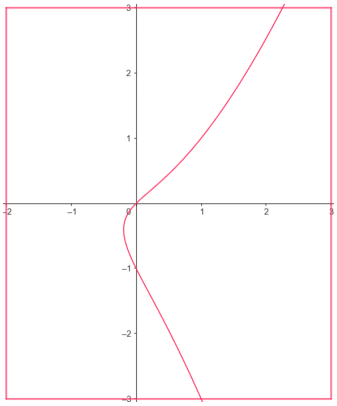


FIGURA 1. $E(\mathbb{R})$

real y complejo de E son respectivamente

$$\omega_1 = \int_{E(\mathbb{R})} \frac{dx}{y} = 2\int_{\gamma}^{\infty} \frac{dx}{\sqrt{|4x^3+5x^2+6x+1|}} \approx 3.3744689,$$
$$\omega_2 = \int_{E(\mathbb{R})} \frac{dx}{y} = 2\int_{\beta}^{\gamma} \frac{dx}{\sqrt{|4x^3+5x^2+6x+1|}} \approx 1.68723445 + 1.95716430i.$$

La curva E sobre $\mathbb{Q}$.

El punto $P_0 = (0,0) \in E(\mathbb{Q})$ tiene orden infinito, esto se puede ver fácilmente. Por ejemplo, por el Teorema de Mazur, podríamos calcular $P \dots 12P$ y ver que no dan ∞, pero por Nagell-Lutz basta con calcular hasta $5P$ ya que $4P = (\frac{-3}{16}, \frac{-31}{64})$ no tiene coordenadas enteras (ni son de la forma $(\frac{m}{4}, \frac{n}{8})$ con m, n enteors) y por lo tanto no tiene orden finito. Más aún, los únicos puntos enteros en E son

$$\begin{array}{lll} P_0 = (0,0) & 2P_0 = (1,-3) & 3P_0 = (4,7) \\ -P_0 = (0,-1) & -2P_0 = (1,1) & -3P_0 = (4,-12). \end{array}$$

No tan fácilmente se puede ver que de hecho E es libre de torsión y P_0 genera el grupo de Mordell-Weil, es decir, $E(\mathbb{Q}) = \langle P_0 \rangle \cong \mathbb{Z}$. Podemos calcular la altura de P_0 con un algoritmo dado por Tate, tal como lo hace Zagier en el artículo antes citado, sin embargo, para el propósito de entender E nos basta con aproximarla mediante

$$\tilde{h}(P_0) = \lim_{n\to\infty} h_{\text{naive}}(2^n P_0)$$

donde $h_{\text{naive}}(\frac{p}{q}, y) = \text{máx}\{|p|, |q|\}$.

Las alturas convergen rápidamente, después de 10 iteraciones obtenemos la aproximación $\tilde{h}(P_0) \approx 0.17729229$. Para calcular la altura en otro punto basta con observar que $h(nP_0) = n^2 h(P_0)$.

La curva E módulo p.

Como $\Delta = -83$ en $p = 83$ hay mala reducción, para cualquier otro primo p el grupo $E(\mathbb{F}_p)$ es finito de orden $N_p(E)+1$ donde $N_p(E)$ denota la cantidad de soluciones módulo

p a $y^2 - y \equiv x^3 - x \pmod{p}$ y agregamos el ∞. La L-serie de Dirichlet asociada a E es

$$L_E(s) = (1 + 83^{-s})^{-1} \prod_{p \neq 83} (1 + a_p p^{-s} + p^{1-2s})^{-1}$$

donde $a_p = p - N_p(E)$. Para los primos hasta 100 tenemos la siguiente tabla

p	a_p	$N_p(E)$	p	a_p	$N_p(E)$	p	a_p	$N_p(E)$
2	-1	4	29	-7	37	67	-2	70
3	-1	5	31	5	27	71	2	70
5	-2	8	37	-11	49	73	0	74
7	-3	11	41	-2	44	79	14	66
11	3	9	43	-8	52	83	-1	85
13	-6	20	47	0	48	89	0	90
17	5	13	53	6	48	97	-8	106
19	2	18	59	5	55	89	4	86
23	-4	28	61	5	57	97	4	94

Modularidad

Por el Teorema de Wiles ahora sabemos que E es modular, si calculamos a_n para $n \leq 10$ obtenemos

$$L_E(s) = 1 - \frac{1}{2^s} - \frac{1}{3^s} - \frac{1}{4^s} - \frac{2}{5^s} + \frac{1}{6^s} - \frac{3}{7^s} + \frac{3}{9^s} - \frac{2}{10^s} + \dots$$

y hay una única forma modular comenzando con esos coeficientes: [13, 83.2.a.a] , que debe ser la que corresponde a E.

El Teorema de Modularidad fue probado luego del Teorema de Gross–Zagier, pero hay herramientas que permiten probar la modularidad de cualquier curva particular sin acudir a él. De hecho, Zagier da dos pruebas distintas de la modularidad de E, una empleando técnicas analíticas y la otra algebraicas. Probablemente la prueba más sencilla computacionalmente sea la analítica, esta es la que veremos a continuación

Llamemos f a la forma modular $83.2.a.a$ que es nuestra candidata, resulta que f es la única forma modular nueva de peso 2 en Γ, donde Γ es el subgrupo de SL_2 generado por $\Gamma_0(37)$ y $W_{83} = \begin{pmatrix} 0 & \frac{-1}{\sqrt{83}} \\ \sqrt{83} & 0 \end{pmatrix}$. Consideremos el mapa $\phi : \mathcal{H} \to \mathbb{C}$ dado por

$$\phi(\tau) = 2\pi i \int_{\tau}^{i\infty} f(z)dz.$$

Es claro que $\phi' = -2\pi i f$ y como f es una forma modular de peso 2 para Γ tenemos que $\phi(\gamma\tau) - \phi(\tau) = C_\gamma$ es constante para toda $\gamma \in \Gamma$. La imagen del mapa $\gamma \mapsto C_\gamma$ es un retículo Λ' con $g_2(\Lambda')$ y $g_3(\Lambda')$ enteros (esto es consecuencia de Eichler-Shimura). El subgrupo de congruencia $\Gamma_0(83)$ admite un generador con 16 elementos y es fácil calcular $\phi(\gamma\tau) - \phi(\tau)$ para este conjunto y para W_{83}, lo que nos permite aproximar una base del retículo y posteriormente dar con exactitud (pues son números enteros) $g_2 = 5076$ y $g_3 = 42984$, concluyendo que $\mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda'$, pues otro modelo para E es $E : y^2 = 4x^3 - 5076x - 42984$. Ahora, lo que obtuvimos fue un isomorfismo

$$\Gamma\backslash\mathcal{H} \simeq \mathbb{C}/\Lambda$$

y esto significa que E es modular.

BSD para E

La conjetura BSD predice la igualdad (para este caso particular, con torsión trivial)

$$L'_E(1) = \omega_1 h(P_0)$$

Sabiendo que $L_E = L_f$ podemos usar la L-serie completada

$$\tilde{L}_E = 83^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L_E(s)$$

y su forma integral

$$\tilde{L}_E(s) = \int_1^\infty f\left(\frac{i\tau}{\sqrt{83}}\right)(\tau^{s-1} - \tau^{1-s})d\tau$$

que permite extenderla de forma analítica a todo $\mathbb{C}$. Como la ecuación funcional para L_E nos dice que $L_E(1) = 0$ obtenemos la siguiente fórmula para la derivada en $s = 1$

$$L'_E(1) = \frac{2\pi}{\sqrt{83}}\tilde{L}'_E(1) = \frac{4\pi}{\sqrt{83}}\sum_{n=1}^{\infty} a_n \int_1^\infty e^{\frac{-2\pi n\tau}{\sqrt{83}}}\log\tau d\tau.$$

Si aproximamos el valor de la derivada usando los 20 primeros a_n llegamos a

$$L'_E(1) \approx 0.598267333,$$

que coincide con la aproximación $\omega_1 h(P_0) \approx 0.598267333$, tal como esperabamos.

Puntos de Heegner en E

El Teorema de Gross–Zagier nos dice que si P_D es un punto de Heegner de discriminante D para E entonces

$$h(P_D) = L'_E(1)L_{E,D}(1)$$

donde $L_{E,D}$ denota el twist de L_E por el símbolo de Kronecker $\left(\frac{\cdot}{D}\right)$. Dado que en este caso $P_0 = (0,0)$ es un generador de $E(\mathbb{Q})$ sabemos que $P_D = b(D)P_0$ para algún $b_D \in \mathbb{Z}$ y por lo tanto $h(P_D) = b(D)^2 h(P_0)$, entonces es fácil estimar $L_{E,D}(1)$ y finalmente determinar P_D a menos de signo. Por ejemplo, para $D = -8$ y $D = -15$ obtenemos $P_D = \pm P_0$. Si queremos encontrar exactamente el punto de Heegner debemos hacer los cálculos explícitamente, como haremos a continuación, pero un resultado muy interesante probado por Gross-Kohnen-Zagier es que el $b(n)$ coincide con los coeficientes de una forma modular de peso $\frac{3}{2}$, tal como lo sugiere comparar las tablas de $b(D)$ obtenidas por Zagier con las obtenidas del Teoremas de Waldspurger.

Para cada discriminante D que satisface la hipótesis de Heegner para E existen $2h_D$ elementos $\tau_i \in \mathcal{H}$ que corresponden a puntos de Heegner, estos son las soluciones de 2.3. El mapa ϕ nos envía dichos puntos a $\mathbb{C}/\Lambda$ y obtenemos puntos en $E(\mathbb{C})$

En principio los puntos que obtenemos en la curva no son puntos racionales sobre $\mathbb{Q}$, sino que están definidos sobre el cuerpo de clases de Hilbert H, pero módulo la acción de Γ son h_D puntos distintos $\phi(\tau_1), \ldots, \phi(\tau_{h_D})$ y la acción de $\mathrm{Gal}(H/\mathbb{Q}) \simeq Cl_K$ los permuta, entonces tenemos que el mapa

$$\mathcal{H} \to \Gamma\backslash\mathcal{H} \xrightarrow{\phi} \mathbb{C}/\Lambda \simeq E(\mathbb{C})$$

y al promediar

$$P_D = \frac{1}{2u}\sum_{i=1}^{2h_D}\phi(\tau_i)$$

tenemos un punto que está bien definido sobre $E(\mathbb{Q})$.

En nuestro ejemplo, el primer discriminante fundamental que satisface HH es -8, que tiene número de clases $h_{-8} = 1$. Las soluciones a ecuaciones cuadráticas $Ax^2 + Bx + C$ donde $83 \mid A$ y $B^2 \equiv -8 \pmod{4A}$ son $\tau_1 = \frac{18+i\sqrt{8}}{166}$ y $\tau_2 = \frac{18+i\sqrt{8}}{166}$, la aproximación

$$\phi(q) = -q + \frac{q^2}{2} + \frac{q^3}{3} + \frac{q^4}{4} + \frac{2q^5}{5} - \frac{q^6}{6} + \frac{3q^7}{7} - \frac{3q^8}{8} + \frac{2q^9}{9} - \frac{2q^{10}}{10} + O(q^{11})$$

nos da $\phi(\tau_2) = \phi(\tau_1) \approx 2.09178891706718 \in \mathbb{C}/\Lambda$, y se corresponden con el punto $(0,0) = P_0 \in E(\mathbb{Q})$. El promedio claramente nos da $P_{-8} = (0,0) \in E(\mathbb{Q})$.

El siguiente discriminante fundamental en satisfacer la hipótesis de Heegner es -15, en este caso el número de clases es 2 y obtenemos 4 puntos de Heegner

$$\tau_1 = \frac{-63 + i\sqrt{83}}{166} \overset{\phi}{\mapsto} 0.641341184435704 + 1.15711737544788i$$
$$\tau_2 = \frac{-103 + i\sqrt{83}}{166} \overset{\phi}{\mapsto} 0.641341184435704 - 1.15711737544788i$$
$$\tau_3 = \frac{-63 + i\sqrt{83}}{322} \overset{\phi}{\mapsto} -0.976730499878602 + 1.02851947199129i$$
$$\tau_4 = \frac{-63 + i\sqrt{83}}{322} \overset{\phi}{\mapsto} -0.976730499878602 + 1.02851947199129i$$

$P_{-15} = \frac{1}{2}\sum_{i=1}^{4} \phi(\tau_i) \approx 1.2527466487$ se corresponde con el punto $(0,-1) = -P_0 \in E(\mathbb{Q})$.

Capítulo 3

El método de Rankin

Comencemos con algunas definiciones que vamos a usar a lo largo del capítulo.

- K es un cuerpo cuadrático imaginario de discriminante $D < -4$, en particular el número de unidades en D es $\omega = 2$. Por simplicidad vamos a asumir que D es primo y distinto de 3.
- ε es el carácter de Dirichlet asociado a D: $\left(\frac{-D}{\cdot}\right)$.
- Cl_K es el grupo de clases de ideales, que tiene cardinal h.
- $\mathscr{A}$ representa una clase de ideales, $r_{\mathscr{A}}(n)$ denota la cantidad de ideales de norma n en la clase $\mathscr{A}$ y convenimos que $r_{\mathscr{A}}(0) = \frac{1}{\omega}$. $L_{\mathscr{A}}(s) = \sum_{n=0}^{\infty} r_{\mathscr{A}}(n) n^{-s}$ es la L-serie asociada a la clase de ideales $\mathscr{A}$ y $\theta_{\mathscr{A}}(z) = \sum_{n=0}^{\infty} r_{\mathscr{A}}(n) q^n$ la serie theta asociada.
- $f \in S_2^{\text{new}}(\Gamma_0(N))$ es una forma cuspidal en el espacio generado por formas nuevas de peso 2 y nivel N, que asumimos coprimo con D. $L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}$ es la L-serie asociada a f.
- $L^N(s,\varepsilon) := \sum_{\substack{n \geq 1 \\ \gcd(n,N)=1}} \varepsilon(n) n^{-s}$
- $E_{M,\varepsilon,s}(z) := \frac{1}{2} \sum_{\substack{(c,d) \in \mathbb{Z}^2 \\ c \equiv 0 \pmod{M} \\ \gcd(d,M)=1}} \frac{\varepsilon(d)}{(cz+d)} \frac{y^s}{|cz+d|^{2s}} \in \tilde{\mathscr{E}}_1(\Gamma_0(N), \varepsilon)$
- $E_s^D := \frac{1}{2} \sum_{\substack{(c,d) \in \mathbb{Z}^2 \\ D \mid c}} \frac{\varepsilon(d)}{(cz+d)} \frac{y^s}{|cz+d|^{2s}} \in \tilde{\mathscr{E}}_1(\Gamma_0(N), \varepsilon)$

Donde x e y refieren a la parte real e imaginaria de z respectivamente. No es dificil ver que L-serie de Rankin

$$L_{\mathscr{A}}(f,s) := L^N(2s - 2k + 1, \varepsilon) L(f,s) * L_{\mathscr{A}}(s)$$

converge absolutamente en $\operatorname{Re} s \geq \frac{3}{2}$. Además, mediante el método de Rankin se prueba que satisface una ecuación funcional, cuando su signo es positivo la L-serie se anula en $s = 1$. La primera parte de la prueba para la fórmula de Gross–Zagier consiste en calcular $L'_{\mathscr{A}}(f,1)$. El método de Rankin consiste en expresar $L_{\mathscr{A}}(f,s)$ como el producto de Petersson de f con el producto de una serie θ y una serie de Eisenstein. Este producto da una forma débilmente modular en $\Gamma_0(ND)$, al aplicarle el operador traza se obtiene una forma débilmente modular $\tilde{\phi}_s$ en $\Gamma_0(N)$ cuyo producto de Petersson con f sigue dando la L-serie $L_{\mathscr{A}}(f,s)$. La idea del Capítulo consiste en calcular los coeficientes de Fourier de $\tilde{\phi}_s$, ver que satisfacen una ecuación funcional y calcular el valor de su derivada en el centro, con eso se llega a una ecuación funcional para $L_{\mathscr{A}}(f,s)$. Finalmente se puede

reemplazar $\tilde{\phi_s}$ por una proyección que preserva el Producto de Petersson con f y que a diferencia de $\tilde{\phi_s}$ es holomorfa, esto permite dar una fórmula para $L'_{\mathscr{A}}(f,1)$.

Comencemos estudiando el primer paso de la prueba: el método de Rankin.

1. El método de Rankin

PROPOSICIÓN 3.1. *Para todo $\mathfrak{a} \in \mathscr{A}$ se cumple que*

$$\theta_{\mathscr{A}}(z) = \frac{1}{\omega} \sum_{\lambda \in \mathfrak{a}} q^{\frac{\mathrm{N}(\lambda)}{\mathrm{N}(\mathfrak{a})}}.$$

DEMOSTRACIÓN. El único elemento de norma 0 es $\lambda = 0$ y por lo tanto el coeficiente de q^0 coincide con el de la definición. Para ver que coinciden el resto de los coeficientes fijemos $\mathfrak{a} \in \mathscr{A}$ y observemos lo siguiente: $\mathfrak{a}\bar{\mathfrak{a}} = \mathrm{N}(\mathfrak{a})\, \mathcal{O}_K$ es un ideal principal, por lo que $\bar{\mathfrak{a}}^{-1} \in \mathscr{A}$.

Sea entonces $\mathfrak{b} \in \mathscr{A}$ de norma n. Como $\mathfrak{a}$ y $\bar{\mathfrak{b}}^{-1}$ están en la misma clase existe $\lambda \in K$ tal que $\mathfrak{a} = \lambda\bar{\mathfrak{b}}^{-1}$, luego $\lambda \in \mathfrak{a}$ y $\frac{\mathrm{N}(\lambda)}{\mathrm{N}(\mathfrak{a})} = \mathrm{N}(\bar{\mathfrak{b}}) = n$. Por otra parte, de la observación se sigue que dado $\lambda \in \mathfrak{a}$, $\lambda\bar{\mathfrak{a}}^{-1}$ es un ideal en la clase $\mathscr{A}$ de norma $\frac{\mathrm{N}(\lambda)}{\mathrm{N}(\mathfrak{a})}$, y es único a menos de multiplicar por un elemento invertible. Esto nos da una correspondencia entre los ideales de $\mathscr{A}$ de norma n y los elementos en $\mathfrak{a}$ de norma $n\,\mathrm{N}(\mathfrak{a})$ módulo $\mathcal{O}_K^\times$. ■

PROPOSICIÓN 3.2.

$$\frac{\Gamma(s+1)}{(4\pi)^{s+1}} L_{\mathscr{A}}(s+1) = (f, \theta_{\mathscr{A}} E_{\bar{s}})_{\Gamma_0(ND)}$$

donde $E_s(z) \coloneqq E_{ND,\varepsilon,s}(z)$

DEMOSTRACIÓN. Observemos que $f(x+iy) = \sum_{n=0}^{\infty} a_n e^{2\pi i n x} e^{-2\pi n y}$ y $\overline{\theta_{\mathscr{A}}(x+iy)} = \sum_{n=0}^{\infty} r_{\mathscr{A}}(n) e^{-2\pi i n x} e^{-2\pi n y}$, luego

$$f(x+iy)\overline{\theta_{\mathscr{A}}(x+iy)} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} a_m r_{\mathscr{A}}(n) e^{-2\pi i (n-m)x} e^{-2\pi (n-m) y}.$$

Si integramos en x, como $\int_0^1 e^{-2\pi i(n-m)x} dx$ se anula excepto si $n = m$, llegamos a la igualdad

$$\int_0^1 f(x+iy)\overline{\theta_{\mathscr{A}}(x+iy)} dx = \sum_{n=0}^{\infty} a_n r_{\mathscr{A}}(n) e^{-4\pi n y}.$$

De esta manera

$$\begin{aligned}\frac{\Gamma(s+1)}{(4\pi)^{s+1}}L_{\mathscr{A}}(s+1) &= \frac{\Gamma(s+1)}{(4\pi)^{s+1}}\sum_{n=1}^{\infty}\frac{a_n r_{\mathscr{A}}(n)}{n^{s+1}}\\ &= \frac{1}{(4\pi)^{s+1}}\int_0^{\infty}\sum_{n=1}^{\infty}\frac{a_n r_{\mathscr{A}}(n)}{n^{s+1}}y^{s+1}e^{-y}\,\frac{dy}{y}\\ &= \int_0^{\infty}\sum_{n=1}^{\infty}a_n r_{\mathscr{A}}(n)e^{-4\pi n y}y^{s+1}\,\frac{dy}{y}\\ &= \int_0^{\infty}\int_0^{1} f(x+iy)\overline{\theta_{\mathscr{A}}(x+iy)}y^{s+1}\,\frac{dxdy}{y}.\end{aligned}$$

El dominio de integración es un dominio fundamental para la acción del grupo Γ_∞, $\Gamma_\infty = \left\{\pm\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}, n\in\mathbb{Z}\right\}$ en $\mathcal{H}$ por lo que podemos reescribir la integral anterior como

$$\int_{\Gamma_\infty\backslash\mathcal{H}} f(z)\overline{\theta_{\mathscr{A}}(z)}y^{s+2}\,\frac{dxdy}{y^2}.$$

Si llamamos F a nuestro dominio fundamental, F puede ser escrito como $F=\bigcup_\gamma \gamma\mathscr{F}$ donde $\mathscr{F}$ es un dominio fundamental para la acción de $\Gamma_0(ND)$ sobre $\mathcal{H}$ esta integral es

$$\sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(ND)}\int_{\gamma\mathscr{F}} f(z)\overline{\theta_{\mathscr{A}}(z)}y^{s+2}\,\frac{dxdy}{y^2} = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(ND)}\int_{\mathscr{F}} f(\gamma z)\overline{\theta_{\mathscr{A}}(\gamma z)}\,\mathrm{Im}(\gamma z)^{s+2}\,\frac{dxdy}{y^2}.$$

Debido a la modularidad de f y $\theta_{\mathscr{A}}$ para $\Gamma_0(ND)$ y a la invarianza de la forma $\frac{dxdy}{y^2}$ bajo la acción de $\mathrm{SL}_2(\mathbb{Z})$ la integral anterior puede reescribirse como

$$\sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(ND)}\int_{\mathscr{F}}(cz+d)^2 f(z)\varepsilon(d)(c\bar{z}+d)\overline{\theta_{\mathscr{A}}(z)}\frac{y^{s+2}}{|cz+d|^{s+2}}\,\frac{dxdy}{y^2} = \int_{\mathcal{F}} f(z)\overline{\theta_{\mathscr{A}}(z)E_{\bar{s}}(z)}\,dxdy,$$

y este es el producto de Petersson $(f,\theta_{\mathscr{A}}E_{\bar{s}})_{\Gamma_0(ND)}$. ■

2. Cálculo de la traza

Recordemos la definición de E_s^D

$$E_s^D(z) := \frac{1}{2}\sum_{\substack{c,d\in\mathbb{Z}\\ D|c}}\frac{\varepsilon(d)}{cz+d}\frac{y^s}{|cz+d|^{2s}}\ ,$$

y definamos de forma similar E_s^1

$$E_s^1(z) := \frac{1}{2}\sum_{m,n\in\mathbb{Z}}\frac{\varepsilon(m)}{mz+n}\frac{y^s}{|mz+n|^{2s}}\ .$$

Definamos también $g_s^1(z) := \theta_{\mathscr{A}}(z)E_s^1(Nz)$ y $g_s^D(z) := \theta_{\mathscr{A}}(z)E_s^D(Nz)$.

El *operador traza* se define como

$$\begin{aligned} \mathrm{Tr}_N^M : M_2\left(\Gamma_0(M)\right) &\to M_2\left(\Gamma_0(N)\right) \\ g &\mapsto \sum_{\gamma\in\Gamma_0(M)\backslash\Gamma_0(N)} g|_{2k}\gamma \end{aligned}$$

este operador está bien definido y no depende del conjunto de representantes que tomemos, además preserva el producto interno de Petersson, como veremos en la siguiente proposición.

Proposición 3.3. Tr_N^{ND} *preserva el producto interno de Petersson: sea* $f \in S_2(\Gamma_0(N))$ *y* $g \in M_2(\Gamma_0(ND))$ *entonces* $(f,g)_{\Gamma_0(ND)} = (f, \mathrm{Tr}_N^{ND}(g))_{\Gamma_0(N)}$.

Demostración. Consideremos D_N un dominio fundamental para $\Gamma_0(N)$, la unión sobre las coclases $\bigcup_{\gamma\in\Gamma_0(ND)\backslash\Gamma_0(N)} \gamma D_N$ es un dominio fundamental para $\Gamma_0(ND)$, esta observación nos permite escribir el producto interno de Petersson como sigue

$$\begin{aligned} (f,g)_{\Gamma_0(ND)} &= \sum_{\gamma\in\Gamma_0(ND)\backslash\Gamma_0(N)} \int_{D_N} f(\gamma z)\overline{g(\gamma z)}\,\mathrm{Im}(\gamma z)^2\,\frac{dxdy}{y^2} \\ &= \sum_{\gamma\in\Gamma_0(ND)\backslash\Gamma_0(N)} \int_{D_N} f(\gamma z)\overline{g(\gamma z)}(cz+d)^{-2}\,dxdy \\ &= \int_{D_N} f(z) \sum_{\gamma\in\Gamma_0(ND)\backslash\Gamma_0(N)} g(z)|_2\gamma \\ &= (f, \mathrm{Tr}_N^{ND}(g))_{\Gamma_0(N)} \end{aligned}$$

■

Proposición 3.4.

$$(4\pi)^{-s-1}N^s L_{\mathscr{A}}(f, s+1) = (f, \mathrm{Tr}_N^{ND}(g_{\bar{s}}^D))_{\Gamma_0(N)}.$$

Demostración. El operador traza preserva el producto interno (3.3), lo cual, junto a la proposición 3.2 da la igualdad

$$(4\pi)^{-s-1}N^s L_{\mathscr{A}}(f, s+1) = (f, \mathrm{Tr}_N^{ND}\left(\theta_{\mathscr{A}} E_{\bar{s}}\right))_{\Gamma_0(N)}.$$

Notese que podemos reescribir E_s como $E_s(z) = \frac{1}{2} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ ND|c \\ \gcd(d,N)=1}} \frac{\varepsilon(d)}{(cz+d)} \frac{y^s}{|cz+d|^{2s}}$ donde reemplazamos la condición $\gcd(d, ND) = 1$ por $\gcd(d, N) = 1$, ya que $\varepsilon(d) = 0$ en otro caso. Además podemos eliminar la condición si usamos la función de Möbius,

$$
\begin{aligned}
E_s(z) &= \frac{1}{2} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ ND|c \\ \gcd(d,N)=1}} \sum_{e|\gcd(d,ND)} \mu(e) \frac{\varepsilon(d)}{(cz+d)} \frac{y^s}{|cz+d|^{2s}} \\
&= \frac{1}{2} \sum_{e|N} \mu(e) \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ ND|c\ , e|d}} \frac{\varepsilon(d)}{(cz+d)} \frac{y^s}{|cz+d|^{2s}} \\
&= \frac{1}{2} \sum_{e|N} \sum_{\substack{(c',d')\in\mathbb{Z}^2 \\ D|c'}} \frac{\varepsilon(d'e)}{c'N(Dz)+d'e} + \frac{y^s}{|c'N(dz)+d'e|} \\
&= \sum_{e|N} \frac{\mu(e)\varepsilon(e)}{e^{2s+1}} (N/e)^{-s} E_s^D\left(\frac{Nz}{e}\right)
\end{aligned}
$$

Consideremos $e \mid N$, $e > 1$. Cualquier conjunto de representantes para $\Gamma_0(ND)\backslash\Gamma_0(N)$ es también un sistema de representantes para $\Gamma_0(\frac{ND}{e})\backslash\Gamma_0(\frac{N}{e})$, por lo tanto los términos con $e > 1$ constituyen términos de nivel $\frac{N}{e}$ en $\mathrm{Tr}_N^{ND}(\theta_{\mathscr{A}} E_{\bar{s}})$; como f es ortogonal a las formas modulares de nivel estrictamente menor que N estos términos no contribuyen al producto interno. Finalmente observemos que los únicos términos que no se anulan en la suma anterior son los libres de cuadrados coprimos con D, lo que nos permite reemplazar $(f, \mathrm{Tr}_N^{ND}(\theta_{\mathscr{A}}(z) E_{\bar{s}}))_{\Gamma_0(N)}$ por $(f, \mathrm{Tr}_N^{ND}(\theta_{\mathscr{A}}(z) E_{\bar{s}}^D))_{\Gamma_0(N)}$. ■

Probar la ecuación funcional que queremos es equivalente a probar la ecuación funcional en los coeficientes A_m de $\mathrm{Tr}_N^{ND}(g_s^D) = \sum_{m=-\infty}^{\infty} A_m(s,y) e(nx)$, para calcular el desarrollo de Fourier tenemos que estudiar el desarrollo de $\theta_{\mathscr{A}}$ y el de E_s^D. Hay que estudiar entonces el comportamiento de ambas series en un conjunto de representantes de $\Gamma_0(ND)\backslash\Gamma_0(D)$ aunque por conveniencia se estudia el comportamiento en todo $\mathrm{SL}_2(\mathbb{Z})$.

Observación 3.5. *Las coclases de $\Gamma_0(ND)\backslash\Gamma_0(D)$ están en correspondencia con $\mathbb{P}^1(\mathbb{Z}/D\mathbb{Z})$. El mapa reducir módulo D*

$$\pi_D : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{D}$$

es sobreyectivo y $\Gamma_0(ND)$ es un subgrupo normal en $\Gamma_0(N)$ tal que $\mathrm{Ker}\,\phi \subset \Gamma_0(ND)$. Entonces

$$\Gamma_0(ND)\backslash\Gamma_0(N) \simeq \mathrm{SL}_2(\mathbb{Z}/D\mathbb{Z})/\pi_D(\Gamma_0(ND))$$

donde $\pi_D(\Gamma_0(ND)) = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{D} \in \mathrm{SL}_2(\mathbb{Z}/D\mathbb{Z}) \right\}$.

Sean $\gamma_c := \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$, $c = 0, \ldots, D-1$ *y* $\gamma_D = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, *observemos que los productos* $\gamma_j \begin{pmatrix} p & q \\ 0 & s \end{pmatrix} \equiv \begin{pmatrix} p & q \\ pc & qc+s \end{pmatrix}$ *generan todas las matrices en* $\mathrm{SL}_2(\mathbb{Z}/D\mathbb{Z})$ *con* $p \not\equiv 0 \pmod{D}$ *y γ_D genera el resto, por lo que $S = \{\gamma_c : c = 0, \ldots D\}$ es un conjunto de representantes de* $\mathrm{SL}_2(Z/D\mathbb{Z})/\pi_D(\Gamma_0(ND))$ *y está en clara biyección con* $\mathbb{P}^1(\mathbb{Z}/D\mathbb{Z})$.

PROPOSICIÓN 3.6. $E_s^D \in M_1(\Gamma_0(D), \varepsilon)$.

DEMOSTRACIÓN. Podemos reescribir $E_s^D(z)$ como

$$E_s^D = \frac{1}{2} L(\varepsilon, s) \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ D|c}} \frac{\varepsilon(d)}{cz+d} \frac{y^s}{|cz+d|^{2s}}$$

y

$$\sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ D|c}} \frac{\varepsilon(d)}{cz+d} \frac{y^s}{|cz+d|^{2s}} = \sum_{\gamma\in\Gamma_0(D)\backslash \mathrm{SL}_2(\mathbb{Z})} \varepsilon(d)\,\mathrm{Im}(z)^s|_1\gamma$$

es claramente débilmente modular para $\Gamma_0(D)$ con carácter ε. La convergencia se da para $\mathrm{Re}\, s > 1$. ■

PROPOSICIÓN 3.7. *Sea* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2$ *tal que* $D \nmid c$, *entonces*

$$E_s^D|_1\gamma(z) = \varepsilon(c) D^{-s-1} E_s^1\left(\frac{z + c^* d}{|D|}\right)$$

donde c^* *es el inverso de* c *módulo* D.

DEMOSTRACIÓN. Por definición

$$E_s^D(\gamma z) := \frac{1}{2} \sum_{\substack{m,n\in\mathbb{Z} \\ D|m}} \frac{\varepsilon(n)}{m(az+b)+n(cz+d)} \frac{y^s}{|m(az+b)+n(cz+d)|^{2s}}$$

Haciendo el cambio de variables $(m,n) \mapsto \gamma^{-1}(m,n) = (md - nc, an - bc)$ queda

$$E_s^D(\gamma z) = \frac{1}{2} \sum_{\substack{m,n\in\mathbb{Z} \\ D|md-nc}} \frac{\varepsilon(an-bm)}{mz+n} \frac{y^s}{|mz+n|^{2s}}$$

Y como $D \mid md - nc$ resulta que $c(an - bm) \equiv (ad - bc)m = m \pmod{D}$, es decir, $an - bm \equiv c^* m \pmod{D}$. Deducimos entonces que $\varepsilon(an - bm) = \varepsilon(c^* m) = \varepsilon(c)\varepsilon(m)$ y reemplazando esto en lo anterior

$$E_s^D|_1\gamma(z) = \frac{1}{2} \sum_{\substack{m,n\in\mathbb{Z} \\ D|md-nc}} \frac{\varepsilon(c)\varepsilon(m)}{mz+n} \frac{y^s}{|mz+n|^{2s}}$$

Finalmente observemos que la condición $D \mid md - nc$ es equivalente a la condición $nc = md - Dk$ para algún $k \in \mathbb{Z}$ con lo cual

$$\begin{aligned} E_s^D|_1\gamma(z) &= \frac{1}{2}\sum_{m,k\in\mathbb{Z}} \frac{\varepsilon(c)\varepsilon(m)}{mz + c^*md - Dk}\frac{y^s}{|mz - c^*md - Dk|^{2s}} \\ &= \frac{1}{2}\sum_{m,k\in\mathbb{Z}} |D|^{-s-1}\frac{\varepsilon(c)\varepsilon(m)}{m\left(\frac{z+c^*d}{|D|}\right) + k}\frac{y^s}{|m\left(\frac{z+c^*d}{|D|}\right) + k|^{2s}} \\ &= \frac{1}{2}|D|^{-s-1}E_s^1\left(\frac{z + c^*d}{|D|}\right). \end{aligned}$$

■

Antes de continuar con el estudio de $\theta_{\mathscr{A}}$ establezcamos algunas notaciones. Para $x \in \mathbb{C}$ denotaremos $e(x) = e^{2\pi ix}$. Para $a \in \mathbb{Z}/n\mathbb{Z}$ denotaremos a^* a su inverso módulo n, cuando existe, y $e_n(a) = e^{\frac{2\pi ia}{n}}$.

Proposición 3.8. $\theta_{\mathscr{A}} \in M_1(\Gamma_0(D), \varepsilon)$.

Proposición 3.9. *Sea* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$ *tal que* $D \nmid c$, *entonces*

$$\theta_A|_1\gamma = -\frac{i\varepsilon(c)}{\sqrt{|D|}}\theta_{\mathscr{A}}\left(\frac{z + c^*d}{|D|}\right)$$

donde c^* *es el inverso de* c *módulo* D.

Demostración. Veamos en primer lugar que podemos asumir $c = 1$.

Sea $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\gcd(c, D) = 1$ arbitraria, tomemos x tal que $cx \equiv d$ (mód D) y una matriz $\beta = \begin{pmatrix} * & * \\ 1 & x \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. El producto $\gamma\beta^{-1} = \begin{pmatrix} ax - b & * \\ cx - d & * \end{pmatrix}$ está en $\Gamma_0(D)$, y como $\theta_{\mathscr{A}} \in M_1(\Gamma_0(N), \varepsilon)$ si asumimos que la proposición se cumple para $c = 1$ tenemos que

$$\begin{aligned} \theta_{\mathscr{A}}|_\gamma(z) &= \theta_{\mathscr{A}}|_{\gamma\beta^{-1}\beta} \\ &= \varepsilon(ax - b)\theta_{\mathscr{A}}|_\beta \\ &= -\frac{i\varepsilon(ax - b)}{\sqrt{|D|}}\theta_{\mathscr{A}}\left(\frac{z + x}{|D|}\right) \\ &= -\frac{i\varepsilon(c)}{\sqrt{|D|}}\theta_{\mathscr{A}}\left(\frac{z + c^*d}{|D|}\right) \end{aligned}$$

donde en la última igualdad usamos dos veces que $x \equiv c^*d$ (mód D).

Asumamos entonces $c = 1$. Como $\det\gamma = 1$ podemos escribir $\frac{az+b}{z+d}$ como $a + \mu$ donde $\mu = -\frac{1}{z+d}$, de forma forma

$$\theta_{\mathscr{A}}\left(\frac{az + b}{z + d}\right) = \frac{1}{2}\sum_{\lambda\in\mathfrak{a}} e\left(\frac{\mathrm{N}(\lambda)}{\mathrm{N}(\mathfrak{a})}\mu\right)$$

Por la fórmula de sumación de Poisson

$$\begin{aligned}\sum_{\lambda\in\mathfrak{a}} e(\mathrm{N}(\lambda)z) &= \frac{1}{\mathrm{N}(\mathfrak{a})\sqrt{D}}\sum_{\nu\in\mathfrak{a}'}\int_K e(\mathrm{N}(u)z)e^{-2\pi i\langle u,\nu\rangle}du\\ &= \frac{1}{\mathrm{N}(\mathfrak{a})\sqrt{D}}\sum_{\nu\in\mathfrak{a}'}\int_{\mathbb{R}^2} e(z(x^2-Dy^2)-(x\nu_1-Dy\nu_2))\,dxdy\\ &= \frac{1}{\mathrm{N}(\mathfrak{a})\sqrt{D}}\sum_{\nu\in\mathfrak{a}'}\int_{\mathbb{R}^2} e(x^2z-x\nu_1)e(-Dy^2z+Dy\nu_2)\,dxdy\end{aligned}$$

donde escribimos $\nu=\nu_1+i\sqrt{D}\nu_2$. Ahora podemos calcular cada integral en una variable y hacer el producto, si completamos cuadrados obtenemos que

$$\int_{\mathbb{R}} e(zx^2-xu)dx = \sqrt{\frac{i}{z}}e\left(\frac{-u^2}{z}\right)$$

y por lo tanto,

$$\sum_{\lambda\in\mathfrak{a}} e(\mathrm{N}(\lambda)z) = \frac{i}{\mathrm{N}(\mathfrak{a})\sqrt{D}z}\sum_{\nu\in\mathfrak{a}^{-1}\mathfrak{d}^{-1}} e\left(\frac{-\mathrm{N}(\nu)}{z}\right)$$

donde $\mathfrak{d}=\sqrt{D}\mathcal{O}_K$. Sustituyendo $z=\frac{\mu}{\mathrm{N}(\mathfrak{a})}$

$$\theta_{\mathscr{A}}\left(\frac{az+b}{z+d}\right) = -\frac{i}{\omega\sqrt{|D|}}(z+d)\sum_{\nu\in\mathfrak{a}^{-1}\mathfrak{d}^{-1}} e\left(\mathrm{N}(\nu)\,\mathrm{N}(\mathfrak{a}\mathfrak{d})\frac{(z+d)}{|D|}\right).$$

Denotemos por $\mathscr{D}$ a la clase de $\mathfrak{d}$, como $\theta_{\mathscr{A}}=\theta_{\mathscr{A}\mathscr{D}}=\theta_{\mathscr{A}^{-1}\mathscr{D}^{-1}}$ concluimos finalmente que

$$\theta_{\mathscr{A}}|_1\gamma = -\frac{i}{\sqrt{|D|}}\theta_{\mathscr{A}}\left(\frac{z+d}{|D|}\right).$$

■

Las proposiciones previas dan lugar al siguiente teorema.

Teorema 3.10. *Si $D\nmid N$ entonces*

$$\mathrm{Tr}_N^{ND}(g_s^D)(z) = g_s^D(z) - i\varepsilon(N)|D|^{-s-\frac{1}{2}}\tfrac{1}{|D|}\sum_{j=0}^{\infty} g_s^1\left(\frac{z+j}{D}\right)$$

Demostración. Sea $\gamma\in\Gamma_0(N)$ tal que $\gcd(c,D)=1$,

$$\begin{aligned}g_s^D|_2\gamma(z) &= (cz+d)\theta_{\mathscr{A}}(\gamma z)(cz+d)E_s^D\left(\frac{aNz+b}{cNz+d}\right)\\ &= \theta_A|_1\gamma(z)E_s^1|_1\gamma'(Nz)\end{aligned}$$

donde $\gamma'=\begin{pmatrix}a & bN\\ c/N & d\end{pmatrix}$. Por 3.7 y 3.9

$$\begin{aligned}\theta_A|_1\gamma(z)E_s^1|_1\gamma'(Nz) &= -\frac{i\varepsilon(c/N)\varepsilon(c)}{\sqrt{|D|}}E_s^1\left(\frac{Nz+(c/N)^*d}{|D|}\right)\theta_{\mathscr{A}}\left(\frac{z+c^*d}{|D|}\right)\\ &= -\frac{i\varepsilon(N)}{\sqrt{|D|}}g_s^D\left(\frac{z+c^*d}{|D|}\right).\end{aligned}$$

Por la observación 3.5 las coclases de $\Gamma_0(ND)\backslash\Gamma(N)$ están en correspondencia con $\mathrm{P}^1(\mathbb{Z}/D\mathbb{Z}) = \{(c:d)\}$ por lo que cada valor de c^*d determina una coclase y hay una coclase extra correspondiente a $c = 0$.

$$\begin{aligned}\mathrm{Tr}_N^{ND}(g_s^D)(z) &= \sum_{\gamma\in\Gamma_0(ND)\backslash\Gamma_0(D)} g_s^D(z)|_2\gamma \\ &= g_s^D(z) + \sum_{j=0}^{D-1} -\frac{i\varepsilon(N)}{|D|^{s+\frac{3}{2}}} g_s^1\left(\frac{z+j}{|D|}\right). \\ &= g_s^D(z) - i\varepsilon(N)|D|^{-s-\frac{1}{2}}\tfrac{1}{|D|}\sum_{j=0}^{\infty} g_s^1\left(\frac{z+j}{|D|}\right).\end{aligned}$$

■

Sea $\mathscr{E}_s(z) := E_s^D(Dz) - i\varepsilon(N)|D|^{-s-\frac{1}{2}}E_s^1(z)$, el teorema anterior nos da el siguiente corolario sobre $\mathscr{E}_s$.

Corolario 3.11. *Consideremos U_D el operador $f(z) \mapsto \frac{1}{|D|}\sum_{j=0}^{|D|-1} f\left(\frac{z+j}{|D|}\right)$. Entonces*

$$\mathrm{Tr}_N^{ND}(g_s^D) = (\theta_{\mathscr{A}}\mathscr{E}_s)|_{U_D}$$

Demostración.
Para probar la igualdad basta ver que $g_s^D(z) = \frac{1}{|D|}\sum_{j=0}^{\infty} E_s^D(z+j)\theta_{\mathscr{A}}(\frac{z+j}{D})$. Por una parte $E_s^D(z+j) = E_s^D(z)$ y por otra parte

$$\frac{1}{|D|}\sum_{j=0}^{|D|-1}\theta_{\mathscr{A}}\left(\frac{z+j}{|D|}\right) = \sum_{n\in\mathbb{Z}} r_{\mathscr{A}}(n)e^{\frac{2\pi inz}{|D|}}\left(\frac{1}{|D|}\sum_{j=0}^{|D|-1} e^{\frac{2\pi inj}{|D|}}\right)$$

La suma interna se anula para todo n coprimo con D, y vale $|D|$ en otro caso, por lo tanto lo anterior es igual a

$$\sum_{n\in\mathbb{Z}} r_{\mathscr{A}}(n|D|)e^{2\pi inz}$$

y como multiplicar por $\mathfrak{d}$ da una biyección entre ideales de norma $n|D|$ e ideales de norma n en la clase de $\mathscr{A}$ concluimos que esto es igual a $\theta_{\mathscr{A}}(z)$. ■

Observación 3.12. *La expansión de Fourier de $\mathscr{E}_s$ en x puede escribirse como $\mathscr{E}_s(z) = \sum_{n\in\mathbb{Z}} e_s(n,y)e(nx)$, donde $e_s(n,y)$ no dependen de x. Entonces*

$$\mathrm{Tr}_N^{ND}(g_s^D)(z) = \sum_{n\in\mathbb{Z}}\sum_{\substack{l\geq 0\\ Nn+l\equiv 0 \pmod D}} e_s(n,\tfrac{Ny}{|D|})r_{\mathscr{A}}(l)e^{-\frac{2\pi ly}{|D|}}e\left(\frac{Nn+l}{|D|}x\right) \tag{3.1}$$

3. Expansiones de Fourier

Si escribimos la expansión de Fourier de E_s^1 y E_s^D como

$$E_s^1(z) = \sum_{n\in\mathbb{Z}} e_s^1(n,y)e(nx), \qquad E_s^D(z) = \sum_{n\in\mathbb{Z}} e_s^D(n,y)e(nx)$$

la siguiente proposición describe los coeficientes de Fourier.

PROPOSICIÓN 3.13.

(a) Los coeficientes de Fourier de E_s^D vienen dados por

$$e_s^D(n,y) = \begin{cases} L(2s+1,\varepsilon)y^s & si\ n=0 \\ -i|D|^{-2s-\frac{1}{2}}y^{-s}\sum\limits_{\substack{m>0\\ m|n}}\varepsilon(\frac{n}{m})m^{-2s}V_s(ny) & si\ n\neq 0 \end{cases}$$

(b) Los coeficientes de Fourier de E_s^1 vienen dados por

$$e_s^1(n,y) = \begin{cases} V_s(0)L(2s,\varepsilon)y^{-s} & si\ n=0 \\ \sum\limits_{\substack{m|n\\ m>0}}\varepsilon(m)m^{-2s}V_s(ny)y^{-s} & si\ n\neq 0 \end{cases}$$

donde

$$V_s(t) = \int_{-\infty}^{\infty}\frac{e^{-2\pi xt}}{(x+i)(x^2+1)^2}dx$$

está definida para $\mathrm{Re}(s)>0$ *y* $t\in\mathbb{R}$.

DEMOSTRACIÓN. 1. Por sumación de Poisson

$$\sum_{l\in\mathbb{Z}}\frac{1}{(z+l)|z+l|^{2s}} = y^{-2s}\sum_{r\in\mathbb{Z}}V_s(ry)e^{2\pi irx}$$

Luego,

$$E_s^D = \tfrac{1}{2}\sum_{\substack{m,n\in\mathbb{Z}\\ D|n}}\frac{\varepsilon(n)}{(mz+n)|mz+n|^{2s}}y^s$$

$$= L(2s+1,\varepsilon)y^s + |D|^{-2s-1}y^s\sum_{m=1}^{\infty}\sum_{n\pmod D}\varepsilon(n)\sum_{l\in\mathbb{Z}}\frac{1}{(mz+\frac{n}{|D|}+l)\left|mz+\frac{n}{|D|}+l\right|^{2s}}$$

$$= L(2s+1,\varepsilon)y^s + |D|^{-2s-1}y^s\sum_{n\pmod D}\frac{\varepsilon(n)}{|D|m^{2s}}\sum_{r\in\mathbb{Z}}V_s(rmy)e(rmx)e(\tfrac{rn}{|D|})$$

La suma de Gauss $\sum\limits_{n\pmod{|D|}}\varepsilon(n)e\left(\frac{rn}{|D|}\right)$ vale $-i\varepsilon(r)\sqrt{|D|}$, sustituyendo en la igualdad anterior nos queda la siguiente fórmula para E_s^D,

$$E_s^D(z) = L(2s+1,\varepsilon)y^s - i|D|^{-2s-\frac{1}{2}}y^{-s}\sum_{m>0}\sum_{r\in\mathbb{Z}}\frac{\varepsilon(r)}{m^{2s}}V_s(rmy)e(rmx)$$

de donde se deduce (a).

2. De forma similar

$$E_s^D(z) = \tfrac{1}{2}\sum_{m,n\in\mathbb{Z}}\frac{\varepsilon(m)}{(mz+n)|mz+n|^{2s}}y^s$$

$$= y^s\sum_{m=1}^{\infty}\frac{\varepsilon(m)}{m^{2s}}\sum_{r\in\mathbb{Z}}V_s(rmy)e(rmx)$$

Sustituyendo en $r = 0$ obtenemos $e_s^D(0, y) = V_s(0)L(2s, \varepsilon)y^{-s}$ y en $n = rm$ nos da $e_s^D(n, y) = \sum_{\substack{m|n \\ m>0}} \frac{\varepsilon(n)}{m^{2s}} V_s(ny)y^{-s}$.

■

Corolario 3.14.

$$e_s(0, y) = L(2s + 1, \varepsilon)(|D|y)^s - \frac{i\varepsilon(N)}{\sqrt{|D|}} V_s(0)L(2s, \varepsilon)(|D|y)^{-s}$$

y para $n \neq 0$

$$e_s(n, y) = -\frac{i\varepsilon(N)}{\sqrt{|D|}} V_s(ny) \sum_{\substack{d|n \\ d>0}} \frac{\varepsilon(n, d)}{d^{2s}} (|D|y)^{-s}$$

donde

$$\varepsilon(n, d) = \begin{cases} \varepsilon(\frac{-Nn}{d}) & si\ D \mid d \\ \varepsilon(d) & si\ D \nmid d \end{cases}$$

Demostración. El resultado es inmediato para $n = 0$, para $n \neq 0$ la proposición anterior nos da

$$e_s(n, y) = -i|D|^{-s-\frac{1}{2}} V_s(ny)y^{-s} \left(\chi \sum_{\substack{m|\frac{n}{D} \\ m>0}} \varepsilon\left(\frac{n}{m|D|}\right) (m|D|)^{-2s} + \varepsilon(-N) \sum_{m|n} \varepsilon(m)\, m^{-2s} \right)$$

donde $\chi = 0$ si $D \nmid n$ y $\chi = 1$ si $D \mid n$. Si $D \nmid n$ la primera suma se anula y el resultado es claro, mientras que si $D \mid n$ podemos reescribir $e_s(n, y)$ como

$$e_s(n, y) = -i|D|^{-s-\frac{1}{2}} V_s(ny)y^{-s} \sum_{\substack{m|n \\ m>0}} \left(\varepsilon\left(\frac{n}{m}\right) m^{-2s} + \varepsilon(-Nm)\, m^{-2s} \right)$$

ya que si $m \mid n$ y $m \nmid \frac{n}{D}$ $m = D$ y $\varepsilon(\frac{n}{m}) = 0$, es decir, estamos agregando términos pero estos se anulan.

■

Proposición 3.15 (Propiedades de V_s).

(a) $V_s(0) = -\pi i 2^{-2s+1} \frac{\Gamma(2s)}{\Gamma(s)\Gamma(s+1)}$

(b) $V_s(t)$ *tiene continuación analítica y orden* $V_s(t) = t^{O(1)} e^{-2\pi|t|}$.

(c) $V_s^*(t) := (\pi|t|)^{-s-1}\Gamma(s+1)V_s(t)$ *es una función entera en* s *y satisface la ecuación funcional* $V_s^*(t) = sign(t)V_{-s}^*(t)$

(d)
$$\frac{\partial}{\partial s} V_s(t)|_{s=0} = -2\pi i e^{-2\pi t} E_1(4\pi|t|)$$
donde $E_1(t) = \int_1^\infty \frac{1}{x} e^{-xt} dx$, $t > 0$.

(e) $V_0(t) = -2\pi i e^{-2\pi t}$.

Demostración. La prueba se puede ver en [9]. ■

COROLARIO 3.16.

$$\mathrm{Tr}_N^{ND}(g_0^D)(z) = \sum_{m=0}^{\infty}\left(\sum_{0\le n\le \frac{m|D|}{N}} e_0(n,\tfrac{Ny}{|D|})e^{\frac{-2\pi Nny}{|D|}} r_{\mathscr{A}}(m|D|-nN)\right)e^{2\pi imz}.$$

Donde

$$e_0(n,\tfrac{Ny}{|D|})\; e^{\frac{-2\pi Nny}{|D|}} = \begin{cases} L(1,\varepsilon) - \frac{\varepsilon(N)\pi}{\sqrt{|D|}}L(0,\varepsilon) & si\ n=0 \\ \frac{-\varepsilon(N)2\pi}{\sqrt{|D|}}\sum\limits_{\substack{d>0\\ d|n}}\varepsilon(n,d) & si\ n\neq 0 \end{cases}$$

En particular los coeficientes no dependen de z y $\mathrm{Tr}_N^{ND}(g_0^D)$ es holomorfa.

DEMOSTRACIÓN. $V_0(0) = -2\pi i$, si sustituimos esto en 3.14 obtenemos el resultado de inmediato. ■

4. Ecuación funcional para $L_{\mathscr{A}}$

Queremos llegar a una ecuación funcional para $L_{\mathscr{A}}(f,s)$, para ello necesitaremos primero un lema que nos da una ecuación funcional para los coeficientes de Fourier de $\mathscr{E}_s$.

LEMA 3.17. *Los coeficientes de Fourier $e_s(n,y)$ satisfacen la siguiente ecuación*

$$e_s^*(n,y) := \pi^{-s}|D|^s\Gamma(s+1)e_s(n,y) = -\varepsilon(N)e_{-s}^*(n,y)$$

para $n\in\mathbb{Z}$ tal que existe un ideal entero $\mathfrak{a}\in\mathscr{A}$ con $l = N(\mathfrak{a})$ y $Nn+l\equiv 0 \pmod D$.

DEMOSTRACIÓN. Separemos en dos casos, primero consideremos $n=0$. Por el corolario 3.14

$$e_s(0,y) = L(2s+1,\varepsilon)(|D|y)^s - \frac{i\varepsilon(N)}{\sqrt{|D|}}L(2s,\varepsilon)V_s(0)(|D|y)^{-s}$$

La proposición 3.15 nos dice que $V_s(0) = -i\pi 2^{1-2s}\frac{\Gamma(2s)}{\Gamma(s)\Gamma(s+1)}$, sustituyendo esto en $e_s^*(0,y)$ obtenemos

$$e_s^*(0,y) = |D|^s\pi^{-s}L(2s+1,\varepsilon)\Gamma(s+1)(|D|y)^s - \varepsilon(N)\pi^{1-s}|D|^{s-\frac12}2^{1-2s}L(2s,\varepsilon)\frac{\Gamma(2s)}{\Gamma(s)}(|D|y)^{-s}$$

y por la Fórmula de duplicación de Legendre $\left(\Gamma(2s) = \frac{2^{2s-1}}{\sqrt{\pi}}\Gamma(s)\Gamma(s+\frac12)\right)$

$$e_s^*(0,y) = \left(\frac{|D|}{\pi}\right)^s L(2s+1,\varepsilon)\Gamma(s+1)(|D|y)^s - \varepsilon(N)\left(\frac{|D|}{\pi}\right)^{s-\frac12}L(2s,\varepsilon)\Gamma(s+\tfrac12)(|D|y)^{-s}.$$

D es un discriminante fundamental negativo primo, y por lo tanto la ecuación funcional para $L(s,\varepsilon)$ tiene la forma

$$\Lambda(s,\varepsilon) := -i|D|^{\frac{s}{2}}\pi^{\frac{-s-1}{2}}\Gamma\left(\frac{s+1}{2}\right)L(s,\varepsilon) = \Lambda(1-s,\varepsilon)$$

y como

$$e_s^*(0,y) = \frac{\pi}{\sqrt{|D|}}\Lambda(2s+1,\varepsilon)(|D|y)^s - \varepsilon(N)\frac{\pi}{\sqrt{|D|}}\Lambda(2s,\varepsilon)(|D|y)^{-s}$$

esto implica que $e_s^*(0,y)$ es invariante bajo el cambio $s\mapsto -s$.

Consideremos ahora $n \neq 0$. En este caso

$$e_s(n,y) = -\frac{i\varepsilon(N)}{\sqrt{|D|}} V_s(ny) \sum_{\substack{d|n \\ d>0}} \frac{\varepsilon(n,d)}{d^{2s}} (|D|y)^{-s} = -\frac{\pi i \varepsilon(N)}{|D|} V_s^*(ny) |n|^{s+1} y \sum_{\substack{d|n \\ d>0}} \frac{\varepsilon(n,d)}{d^{2s}}$$

en vista de la ecuación funcional para V_s^* esto es

$$e_s^*(n,y) = -\frac{\pi i \varepsilon(N)}{|D|} \operatorname{sign}(n) V_{-s}^*(ny) |n|^{s+1} y \sum_{\substack{d|n \\ d>0}} \frac{\varepsilon(n,d)}{d^{2s}}$$

y lo podemos reescribir como

$$e_s^*(n,y) = -\frac{\pi i \varepsilon(N)}{|D|} \operatorname{sign}(n) V_{-s}^*(ny) |n|^{1-s} y \sum_{\substack{d|n \\ d>0}} \varepsilon(n,d) \left(\frac{n}{d}\right)^{2s}$$

La ecuación funcional será inmediata si probamos la siguiente afirmación

$$\varepsilon(n, \tfrac{|n|}{d}) = -\varepsilon(N) \operatorname{sign}(n) \varepsilon(n,d)$$

la cual se sigue de observar que

$$\varepsilon(d)\varepsilon(\tfrac{|n|}{d}) = \varepsilon(|n|) = -\varepsilon(N) \operatorname{sign}(n) \varepsilon(-Nn) = \varepsilon(l) \tag{3.2}$$

Como l es norma de un ideal entero hay dos opciones, $\varepsilon(l) = 1$ o $\varepsilon(l) = 0$. En el primer caso la afirmación se sigue de forma inmediata y el segundo caso ocurre cuando $\varepsilon(n,d) = 0 \iff \gcd(d, \frac{n}{d}, D) > 1 \iff \varepsilon(n, \frac{|n|}{d}) = 0$. ■

Corolario 3.18.

$$L_{\mathscr{A}}^*(f,s) := (2\pi)^{-2s} N^s |D|^s \Gamma(s)^2 L_{\mathscr{A}}(f,s) = -\varepsilon(N) L_{\mathscr{A}}^*(f, 2-s)$$

Demostración.

$$\begin{aligned}
L_{\mathscr{A}}^*(f,s) &= (4\pi)^{-s} N^{s-1} \Gamma(s) L_{\mathscr{A}}(f,s) \Gamma(s) |D|^s \pi^{-s} \\
&= \pi^{-1}|D| \sum_{\substack{n\in\mathbb{Z} \\ l\geq 0 \\ Nn+l\equiv 0 \pmod D}} \Gamma(s)|D|^s \pi^{-s} e_{\bar{s}-1}(n, \tfrac{N}{|D|}y) r_{\mathscr{A}}(l) e^{\frac{-2\pi l y}{|D|}} e(\tfrac{Nn+l}{|D|}x) \\
&= -\varepsilon(N)\pi^{-1}|D| \sum_{\substack{n\in\mathbb{Z} \\ l\geq 0 \\ Nn+l\equiv 0 \pmod D}} e_{\bar{s}-1}^*(n, \tfrac{N}{|D|}y) r_{\mathscr{A}}(l) e^{\frac{-2\pi l y}{|D|}} e(\tfrac{Nn+l}{|D|}x) \\
&= -\varepsilon(N)\pi^{-1}|D| \sum_{\substack{n\in\mathbb{Z} \\ l\geq 0 \\ Nn+l\equiv 0 \pmod D}} \Gamma(s)|D|^s \pi^{-s} e_{1-\bar{s}}(n, \tfrac{N}{|D|}y) r_{\mathscr{A}}(l) e^{\frac{-2\pi l y}{|D|}} e(\tfrac{Nn+l}{|D|}x) \\
&= -\varepsilon(N) L_{\mathscr{A}}^*(f, 2-s)
\end{aligned}$$

■

Cuando el valor de ε es -1, tiene sentido estudiar qué ocurre en $s = 1$, en ese se tiene la siguiente fórmula.

PROPOSICIÓN 3.19. *Si $\varepsilon(N) = -1$ entonces existe $\tilde{\phi}_{\mathscr{A}} \in \tilde{M}_2(\Gamma_0(N))$ tal que*

$$L_{\mathscr{A}}(f,1) = \frac{8\pi^2}{\sqrt{|D|}}(f, \tilde{\phi}_{\mathscr{A}})_{\Gamma_0(N)} \ .$$

Pero nuestro caso de interés es $\varepsilon(N) = 1$, en ese caso la L-serie se anula en $s = 1$ y hay una fórmula similar a la anterior para su derivada.

PROPOSICIÓN 3.20. *Si $\varepsilon(N) = 1$ entonces existe $\tilde{\phi}_{\mathscr{A}} \in \tilde{M}_2(\Gamma_0(N))$ tal que*

$$L'_{\mathscr{A}}(f,1) = \frac{8\pi^2}{\sqrt{|D|}}(f, \tilde{\phi}_{\mathscr{A}})_{\Gamma_0(N)} \ .$$

Además $\tilde{\phi}_{\mathscr{A}} = \frac{\sqrt{|D|}}{2\pi}\frac{\partial}{\partial s}\tilde{\phi}_s|_{s=0}$ y tiene expansión de Fourier

$$\sum_{m=-\infty}^{\infty}\left[-\sum_{0<n\leq\frac{m|D|}{N}}\sigma'_{\mathscr{A}}(n)r_{\mathscr{A}}(m|D|-Nn) + \frac{\mathrm{h}}{u}r_{\mathscr{A}}(m)\left(\log y + A\right)\right.$$

$$\left. - \sum_{n=1}^{\infty}\sigma_{\mathscr{A}}(n)r_{\mathscr{A}}(m|D|+Nn)E_1\left(\frac{4\pi nNy}{|D|}\right)\right]e^{2\pi imz}$$

siendo

$$A = 1+\log N|D|-\log\pi+2\frac{L'}{L}(1,\varepsilon),\ \sigma_{\mathscr{A}}(n) = \sum_{\substack{d|n\\ d>0}}\varepsilon_{\mathscr{A}}(n,d),\ \sigma'_{\mathscr{A}} = \sum_{\substack{d|n\\ d>0}}\varepsilon_{\mathscr{A}}(n,d)\log\frac{n}{d^2}\ (n>0)$$

DEMOSTRACIÓN. Tenemos que calcular la derivada respecto de s de los coeficientes $e_s(n,y)$ y evaluarla en $s = 0$. Separemos en casos, según el signo de n.

Caso $n > 0$:
Cuando $n \neq 0$ la fórmula para $e_s(n,y)$ (que obtuvimos en el lema 3.17) es

$$e_s(n,y) = -\frac{i}{\sqrt{|D|}}V_s(ny)\sum_{\substack{d|n\\ d>0}}\frac{\varepsilon(n,d)}{d^{2s}}(|D|y)^{-s}.$$

Observemos que el límite de $\sum_{d|n}\frac{\varepsilon(n,d)}{d^{2s}}$ en $s = 0$ es 0, entonces el único término que no se anula de la derivada es

$$\frac{2i}{\sqrt{|D|}}V_0(ny)\sum_{d|n}\varepsilon(n,d)\log d$$

Finalmente la parte (e) de la proposición 3.15 nos da el valor de $V_0(ny)$ y obtenemos

$$\frac{\partial}{\partial s}e_s(n,y)\Big|_{s=0} = \frac{4\pi}{\sqrt{|D|}}\sigma'_{\mathscr{A}}(n)e^{-2\pi ny}.$$

Caso $n = 0$: Por definición de $e_s^*(n, y)$

$$\begin{aligned}\frac{\partial}{\partial s}e_s(0,y)\Big|_{s=0} &= \frac{\partial}{\partial s}\left(\left(\tfrac{\pi}{|D|}\right)^s e_s^*(0,y)\ \right)\Big|_{s=0}\\ &= \log\left(\frac{\pi}{|D|}\right)e_0^*(0,y) + \left(\frac{\pi}{|D|}\right)\frac{\partial}{\partial s}e_s^*(0,y)\Big|_{s=0}\end{aligned}$$

La ecuación funcional de $e_s^*(n, y)$ nos dice que $e_0^*(n, y) = 0$, por lo tanto solo debemos derivar la expresión

$$e_s^*(n,y) = \frac{\pi}{\sqrt{|D|}}\Lambda(2s+1,\varepsilon)(|D|y)^s - \Lambda(2s,\varepsilon)(|D|y)^{-s}$$

que obtuvimos en 3.17, por la ecuación funcional de $\Lambda(s, \varepsilon)$ esta expresión se anula en $s = 0$ y su derivada allí nos queda

$$\frac{\partial}{\partial s}e_s^*(0,y)\Big|_{s=0} = \frac{2\pi}{\sqrt{|D|}}\frac{\partial}{\partial s}\Lambda(2s+1,\varepsilon)(|D|y)^s\Big|_{s=0}$$

Podemos hacer este calculo usando la derivada logarítmica, como $f\frac{\partial}{\partial s}\log f = \frac{\partial f}{\partial s}$

$$\Lambda(1,\varepsilon)\frac{\partial}{\partial s}e_s^*(0,y) = \frac{2\pi}{\sqrt{|D|}}\frac{\partial}{\partial s}\log\left(-i|D|^{s+\frac{1}{2}}\pi^{-s-1}\Gamma\left(s+1\right)L(2s+1,\varepsilon)(|D|y)^s\right)$$

en s=0, y por lo tanto

$$\Lambda(1,\varepsilon)\frac{\partial}{\partial s}e_s^*(0,y)\Big|_{s=0} = 2\left(\log\left(\frac{|D|^2y}{\pi}\right)\frac{\Gamma'}{\Gamma}(1) + 2\frac{L'}{L}(1)\right).$$

Caso $n < 0$: En este caso $V_0(ny) = 0$ y por lo tanto

$$\frac{\partial}{\partial s}e_s(n,y) = \frac{2\pi}{\sqrt{|D|}}\sigma_{\mathscr{A}}(n)\frac{\partial}{\partial s}V_s(t)|_{s=0}.$$

Por 3.15 parte (d) esto es

$$\frac{\partial}{\partial s}e_s(n,y) = \frac{-\pi}{\sqrt{|D|}}\sigma_{\mathscr{A}}(n)E_1(4\pi|n|y)e^{-2\pi ny}.$$

La fórmula 3.1 para los coeficientes de Fourier de la traza nos permite escribir la derivada en 0 como

$$\frac{\partial}{\partial s}\operatorname{Tr}_N^{ND}(g_s^D)(z)\Big|_{s=0} = \sum_{m=0}^{\infty}\sum_{n\in\mathbb{Z}}\frac{\partial}{\partial s}\ e_s(n,\tfrac{Ny}{|D|})\Big|_{s=0}\ r_{\mathscr{A}}(m|D|-Nn)e^{-\frac{2\pi Ny}{|D|}}\ e^{-2\pi mz}$$

Y si separamos según el signo de n obtenemos

$$\begin{aligned}\sum_{m=0}^{\infty}\Bigg[\sum_{0<n\le\frac{m|D|}{N}}\frac{\partial}{\partial s}\ e_s(n,\tfrac{Ny}{|D|})\Big|_{s=0}\ r_{\mathscr{A}}(m|D|-Nn)e^{-\frac{2\pi Ny}{|D|}} + \frac{\partial}{\partial s}e_s(0,\tfrac{Ny}{|D|})\Big|_{s=0}\ r_{\mathscr{A}}(m|D|)e^{-\frac{2\pi Ny}{|D|}}\\ + \sum_{n=1}^{\infty}\frac{\partial}{\partial s}\ e_s(-n,\tfrac{Ny}{|D|})\Big|_{s=0}\ r_{\mathscr{A}}(m|D|+Nn)e^{-\frac{2\pi Ny}{|D|}}\Bigg]e^{-2\pi mz}.\end{aligned}$$

El resultado es inmediato sustituyendo las fórmulas obtenidas en cada caso y observando que $L(1,\varepsilon) = \frac{2\pi h}{w\sqrt{|D|}}$ y que $r_{\mathscr{A}}(m|D|) = r_{\mathscr{A}}(m)$. ■

Para hacer más explicita la fórmula tenemos que estudiar las funciones aritméticas $\sigma_{\mathscr{A}}$ y $\sigma'_{\mathscr{A}}$. Denotemos por $R(n)$ al número de ideales enteros de norma n y $\delta(n) = 2^s$ donde $s \in \{0, 1\}$ es la cantidad de factores primos de $\gcd(n, D)$. Concluimos la sección con la siguiente proposición:

PROPOSICIÓN 3.21. *Sea $n \in \mathbb{Z}$ tal que existe l norma de un ideal en $\mathscr{A}$ que satisface $Nn + l \equiv 0 \pmod{D}$. Si $\varepsilon(N) = 1$ entonces se cumplen*

(a) $\sigma_{\mathscr{A}}(n) = \delta(n)R(|n|)$ *para* $n < 0$.
(b) $\sigma'_{\mathscr{A}}(n) = \sum_{p|n} a_p(n) \log p$ *para* $n > 0$, *donde*

$$a_p(n) = \begin{cases} 0 & si\ \varepsilon(p) = 1 \\ (\operatorname{ord}_p(n) + 1)\delta(n)R\left(\frac{n}{p}\right) & si\ \varepsilon(p) = -1 \\ 2\operatorname{ord}_p(n)R\left(\frac{n}{p}\right) & si\ p = D \end{cases}$$

DEMOSTRACIÓN.

(a) Sea $n < 0$, podemos escribir n como $D^k n_0$ con $D \nmid n_0$, por lo tanto los divisores de n tienen la forma $d = D^r d_0$ donde $0 \leq r \leq k$ y $d_0 \mid n_0$. Luego

$$\varepsilon(n, d) = \begin{cases} 0 & \text{si } 0 < r < k \\ \varepsilon(d_0) & \text{si } r = 0 \\ \varepsilon(-N\frac{n_0}{d_0}) & \text{si } r = k. \end{cases}$$

Observemos que $\varepsilon(-N\frac{n_0}{d_0}) = \varepsilon(N)\varepsilon(\frac{-n_0}{d_0}) = \varepsilon(d_0)$ pues por hipótesis $\varepsilon(N) = 1$ y $\varepsilon(-Nn) = \varepsilon(l)$ donde l es norma de un ideal en $\mathscr{A}$ (y por lo tanto no es inerte). Concluimos que

$$\sigma_{\mathscr{A}}(n) = (1 + \delta(n)) \sum_{\substack{d_0 | n_0 \\ d_0 > 0}} \varepsilon(d_0),$$

y la última suma es igual a $R(|n_0|)$: $R(k)$ es el coeficiente k-ésimo de la zeta de Dedekind ζ_K, que satisface la igualdad $\zeta_K = \zeta(s)L(s, \varepsilon)$ donde el coeficiente k-ésimo de la expresión de la derecha es $\sum_{m|k} \varepsilon(k)$. Finalmente observemos que $R(n_0)$ es igual a $R(n)$ ya que multiplicar por $\mathfrak{d}^k$ donde $\mathfrak{d}$ es un ideal de norma $-D$ da una correspondencia entre ideales de norma $|n_0|$ e ideales de norma $|n|$.

(b) En este caso $\varepsilon(n, d) = -\varepsilon(n, \frac{n}{d})$, como vimos en 3.2, luego (por hipótesis n no puede ser un cuadrado)

$$\sum_{\substack{d|n \\ d>0}} \varepsilon(n, d) = 0$$

y por lo tanto

$$\sigma'_{\mathscr{A}}(n) = -2 \sum_{\substack{d|n \\ d>0}} \varepsilon(n, d) \log(d)$$

que se puede reescribir como

$$\sigma'_{\mathscr{A}}(n) = -2 \sum_{\substack{d|n \\ d>0}} \varepsilon(n, d) \sum_{p|n} \operatorname{ord}_p(d) \log(p) = \sum_{p|n} a_p(n) \log(p)$$

$a_p(n) := -2\sum_{\substack{d|n\\ d>0}} \varepsilon(n,d)\,\mathrm{ord}_p(d)$. Sea $p \mid n$, podemos escribir n como $n = p^k n_1$ con $p \nmid n_p$, los divisores de n tienen la forma $d = p^r d_1$ donde $0 \le r \le k$ y $d_1 \mid n_1$. Como $\varepsilon(n,d)$ es multiplicativo en d podemos escribir a_p como

$$a_p(n) = -2\sum_{r=0}^{k} r\varepsilon(n,p^r) \sum_{\substack{d_1|n_1\\ d_1>0}} \varepsilon(n,d_1).$$

Ahora separemos en casos según el valor de $\varepsilon(p)$.

Si $\varepsilon(p) = 1$ entonces $\varepsilon(n,p^r) = \varepsilon(p^r) = 1$ para todo r y

$$\sigma_{\mathscr{A}}(n) = \sum_{r=0}^{k} \varepsilon(n,p^r) \sum_{\substack{d_1|n_1\\ d_1>0}} \varepsilon(n,d_1) = (k+1) \sum_{\substack{d_1|n_1\\ d_1>0}} \varepsilon(n,d_1)$$

pero ya vimos que $\sigma_{\mathscr{A}}(n) = 0$, lo cual implica que la última suma vale 0 y por lo tanto $a_p(n)$ también.

Si $p = D$, como en la parte (a) escribimos $n = D^k n_0$ con n_0 coprimo con D, vimos que $\varepsilon(n,d) = 0$ para cualquier divisor $d = D^r d_0$ con $0 < r < k$, entonces

$$\begin{aligned} a_p(n) &= -2\,\mathrm{ord}_p(n) \sum_{\substack{d_1|n_1\\ d_1>0}} \varepsilon(n, D^k d_1) \\ &= -2\,\mathrm{ord}_p(n) \sum_{\substack{d_1|n_1\\ d_1>0}} \varepsilon(n, \frac{n_1}{d_1}) \\ &= 2\,\mathrm{ord}_p(n) \sum_{\substack{d_1|n_1\\ d_1>0}} \varepsilon(d_1) \\ &= 2\,\mathrm{ord}_p(n) R\left(\frac{n}{p}\right) \end{aligned}$$

Si $\varepsilon(p) = -1$ entonces

$$\sigma_{\mathscr{A}}(n) = \sum_{r=0}^{k} \varepsilon(n,p^r) \sum_{\substack{d_1|n_1\\ d_1>0}} \varepsilon(n,d_1) = \sum_{r=0}^{k} (-1)^r \sum_{\substack{d_1|n_1\\ d_1>0}} \varepsilon(n,d_1)$$

sigue siendo 0, por lo tanto si k es par $\sum_{r=0}^{k} (-1)^r \neq 0$ y deducimos nuevamente que la última suma vale 0 y por lo tanto $a_p(n) = 0$. Si k es impar no podemos deducir lo mismo pero podemos observar que

$$\sum_{r=0}^{k} r\varepsilon(p^r) = \sum_{r=0}^{k} (-1)^r r = \frac{-k-1}{2},$$

luego $a_p(n) = (\mathrm{ord}_p(n)+1) \sum_{d_1|n_1} \varepsilon(n, d_1)$. Observemos que $\varepsilon(n, d_1) = \varepsilon(-n_1, d_1)$ pues si $\gcd(d_1, \frac{n_1}{d_1}, D) > 0$ ambos términos son 0, si $\gcd(d_1, D) = 1$ ambos términos son iguales a $\varepsilon(d_1)$ mientras que si $\gcd(d_1, \frac{n_1}{d_1}, D) = 1$ y $D \mid d_1$ tenemos que $\varepsilon(n, d_1) = \varepsilon(\frac{-Np^k n_1}{d_1}) = \varepsilon(\frac{-n_1}{d_1}) = \varepsilon(-n_1, d_1)$. Por la parte (a) concluimos que

$$a_p(n) = (\mathrm{ord}_p(n) + 1)\delta(n_1) R\left(\frac{n}{p^k}\right) = (\mathrm{ord}_p(n) + 1)\delta(n) R\left(\frac{n}{p}\right).$$

■

5. Proyección holomorfa

Hasta ahora tenemos una expresión para $L'_{\mathscr{A}}(f, 1)$ en términos del producto de Petersson $(f, \tilde{\phi}_{\mathscr{A}})$ donde $\tilde{\phi}_{\mathscr{A}}$ es una forma modular de peso 2 pero no holomorfa y buscamos una forma modular $\phi_{\mathscr{A}}$ de peso 2 *holomorfa* que preserve este producto, a la cual llamamos la *proyección holomorfa de* $\tilde{\phi}_{\mathscr{A}}$. Cuando $\tilde{\phi}_{\mathscr{A}}$ tiene peso par estrictamente mayor a 2, si escribimos su expansión de Fourier como $\tilde{\phi}_{\mathscr{A}}(z) = \sum_{-\infty}^{\infty} a_m(y) e^{2\pi i m z}$ la función

$$\phi_{\mathscr{A}}(z) = \sum_{m=1}^{\infty} \left(4\pi m \int_0^{\infty} a_m(y) e^{-4\pi m y}\, dy\right) e^{2\pi i m z}$$

satisface las propiedades que queremos. Sin embargo, en peso 2 esto no es cierto, pues los términos en $\tilde{\phi}_{\mathscr{A}}$ tienden a infinito con y en lugar de decaer con orden $O(y^{-\varepsilon})$ para algún $\varepsilon > 0$, condición necesaria para que la $\phi_{\mathscr{A}}$ anterior sea una forma modular holomorfa, esto mismo ocurre en las cúspides.

En las secciones anteriores el único requisito sobre N que usamos es $\varepsilon(N) = 1$, a partir de ahora vamos a agregar la condición N primo para simplificar las cuentas; aunque todos los resultados siguen valiendo sin esta nueva condición.

Cuando N es primo hay dos cúspides en $\Gamma_0(N)$ que se corresponden con el 0 y el ∞, la siguiente proposición nos da el comportamiento de $\tilde{\phi}_{\mathscr{A}}$ en estas cúspides.

Proposición 3.22. *Sea $\tilde{\phi}_{\mathscr{A}}$ la función definida en 3.20, su comportamiento en las cúspides viene determinado como sigue:*

$$\tilde{\phi}_{\mathscr{A}}(z) = A_\infty \log y + B_\infty + O(y^{-\varepsilon}) \quad y \to \infty \qquad (\varepsilon > 0).$$
$$\tilde{\phi}_{\mathscr{A}}|_2\alpha(z) = A_0 \log y + B_0 + O(y^{-\varepsilon}) \quad y \to \infty \qquad (\varepsilon > 0).$$

donde $\alpha = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ *lleva la cúspide* 0 *en* ∞ *y*

$$A_\infty = \frac{\mathrm{h}}{2}, \qquad B_\infty = \frac{\mathrm{h}}{2}\left(\log \frac{N\sqrt{|D|}}{\pi} - \gamma + 2\frac{L'}{L}(1, \varepsilon\right)$$
$$A_0 = \frac{\mathrm{h}}{2N}, \qquad B_0 = \frac{\mathrm{h}}{2N}\left(\log \frac{\sqrt{|D|}}{N\pi} - \gamma + 2\frac{L'}{L}(1, \varepsilon\right)$$

Demostración. El comportamiento en ∞ se deduce de la expansión de Fourier vista en 3.20 pues hay un sólo término que no tiene decrecimiento exponencial en infinito

y este es

$$\mathrm{h}\, r_{\mathscr{A}}(0)\left(\log\frac{N|D|y}{\pi}-\gamma+2\frac{L'}{L}(1,\varepsilon)\right)$$

y recordemos que $r_{\mathscr{A}}(0)=\frac{1}{2}$.

Por definición $\tilde{\phi}_{\mathscr{A}}=\frac{\sqrt{|D|}}{2\pi}\frac{\partial}{\partial s}\operatorname{Tr}_N^{ND}(g_s^D)|_{s=0}$ donde $g_s^D(z)=\theta_{\mathscr{A}}(z)E_s^D(Nz)$. Para estudiar el comportamiento en 0, consideremos la matriz α que intercambia el ∞ y 0. Como $\theta_{\mathscr{A}}$ y E_s^D son formas modulares de peso 1 para $\Gamma_0(N)$

$$(\operatorname{Tr}_N^{ND}(g_s^D|_2\alpha))(z)=\sum_{\gamma\in\Gamma_0(ND)\backslash\Gamma_0(N)\alpha}(g_s^D|_2\gamma)(z)$$

Ahora, observemos que si $\gamma=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in\Gamma_0(N)\alpha$, entonces $\gamma\alpha^{-1}=\begin{pmatrix}-b & a\\ -d & c\end{pmatrix}\in\Gamma_0(N)$ por lo que $N\mid d$ y $N\nmid c$. Consideremos $\gamma'=\begin{pmatrix}Na & b\\ c & \frac{d}{N}\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ y $z'=\frac{z}{N}$, entonces $cz'+\frac{d}{N}=\frac{cz+d}{N}$ y por lo tanto

$$\sum_{\gamma\in\Gamma_0(ND)\backslash\Gamma_0(N)\alpha}(g_s^D|_2\gamma)(z)=\sum_{\gamma\in\Gamma_0(ND)\backslash\Gamma_0(N)\alpha}(\theta_{\mathscr{A}}|_1\gamma)(z)\frac{1}{N}(E_s^D|_1\gamma')(z')$$

Las proposiciones 3.6 y 3.8 nos dicen que si $D\mid c$ entonces $\theta_A|_1\gamma(z)=\varepsilon(d)\theta_{\mathscr{A}}(z)$ y $E_s^D|_1\gamma'(z')=\varepsilon(d/N)E_s^D(z')$ y las proposiciones 3.7 y 3.9 nos dicen que en caso contrario

$$\theta_{\mathscr{A}}|_1(z)=\theta_A|_1\gamma=-\frac{i\varepsilon(c)}{\sqrt{|D|}}\theta_{\mathscr{A}}\left(\frac{z+c^*d}{|D|}\right)$$
$$E_s^D|_1\gamma'(z)=\varepsilon(c)|D|^{-s-1}E_s^1\left(\frac{z+cd/N}{|D|}\right)$$

por lo tanto

$$\theta_{\mathscr{A}}|_1\gamma(z)=\frac{1}{2}+O(e^{-y})$$
$$E_s^D|_1\gamma'(z')=\begin{cases}L(2s+1,\varepsilon)y'^s & \text{si } D\mid c\\ V_s(0)L(2s,\varepsilon)y'^{-s} & \text{si } D\nmid c\end{cases}$$

y finalmente

$$g_s^D|_2\gamma(z)\begin{cases}\frac{1}{2N}L(2s-1,\varepsilon)\left(\frac{y}{N}\right)^s & \text{si } D\mid c\\ \frac{-i|D|^{-\frac{3}{2}}}{2N}V_s(0)L(2s-1,\varepsilon)\left(\frac{y}{N}\right)^{-s} & \text{si } D\nmid c\end{cases}$$

Si ahora sumamos sobre un conjunto de representantes de $\Gamma_0(ND)\backslash\Gamma_0(N)$ sabemos que hay una sola clase con c divisible por D y $|D|$ clases con $(c,D)=1$, luego

$$\left(\tilde{\phi}_{\mathscr{A}}|_2\gamma\right)(z)=\frac{1}{2N}\left[L(2s+1,\varepsilon)\left(\frac{y}{N}\right)^s-\frac{iV_s(0)}{\sqrt{|D|}}L(2s,\varepsilon)\left(\frac{y}{N}\right)^{-s}\right]+O(e^{-y})$$

y el resultado es inmediato de derivar en 0 y sustituir $V_s(0)$. ■

El siguiente lema garantiza la existencia de constantes α_1 y α_N que aparecerán en la definición de $\phi_{\mathscr{A}}$, su demostración es sencilla y puede encontrarse en [9].

LEMA 3.23. *El sistema de ecuaciones*

$$\begin{aligned}\alpha_1 + \alpha_N &= A\infty\\ \alpha_1 + \alpha_N \frac{1}{N^2} &= A_0\\ \beta_1 + \beta_N \log N &= B_\infty\\ \beta_1 + \beta_N \frac{1}{N^2} - \alpha_N \frac{\log(N)}{N^2} &= B_0\end{aligned}$$

tiene solución. Más aún,

$$\begin{aligned}\alpha_1 &= \frac{\mathrm{h}}{2N}\left(1+\frac{1}{N}\right)^{-1}\\ \beta_1 &= \alpha_1\left(\log\frac{\sqrt{|D|}}{N\pi} - \gamma + 2\frac{L'}{L}(1,\varepsilon) - 2\frac{\log N}{N^2-1}\right)\end{aligned}$$

TEOREMA 3.24. *Sea $\tilde{\phi}_{\mathscr{A}}$ como en el teorema 3.20 y α_1, β_1 como en el Lema anterior. Entonces existe una forma cuspidal holomorfa $\phi_{\mathscr{A}} = \sum_{m=1}^{\infty} a_m q^m \in S_2(\Gamma_0(N))$ tal que $(\phi_{\mathscr{A}}, f)_{\Gamma_0(N)} = (\tilde{\phi}_{\mathscr{A}}, f)_{\Gamma_0(N)}$ para toda $f \in S_2(\Gamma_0(N))$ y los coeficientes de Fourier para m tal que $N \nmid m$ están dados por*

$$\begin{aligned}a_m = \lim_{s\to 0}\left[4\pi m\int_0^\infty a_m(y)e^{-4\pi m y}y^s\,dy + 24\alpha_1\sigma_1(m)s^{-1}\right] + 24\beta_1\sigma_1(m) +\\ 48\alpha_1\left[\sigma_1'(m) - \sigma_1(m)\left(\log 2m + \frac{1}{2} + \frac{\zeta'}{\zeta}(2)\right)\right]\end{aligned}$$

donde $\sigma_1(m) = \sum_{d|m} d$ y $\sigma_1'(m) = \sum_{d|m} d\log d$

DEMOSTRACIÓN. Consideremos

$$E_{2,s}(z) = \sum_{\gamma\in\Gamma_\infty\backslash \mathrm{SL}_2(\mathbb{Z})} y^s|_2\gamma = \frac{1}{2}\sum_{\substack{(c,d)\in\mathbb{Z}^2\\ \gcd(c,d)=1}} \frac{1}{(cz+d)^2}\frac{y^s}{|cz+d|^{2s}}$$

Esta serie converge absolutamente para s con $\operatorname{Re} s > 2$ y admite continuación analítica al plano complejo, además define una serie de Eisenstein no holomorfa de peso 2 para $\mathrm{SL}_2(\mathbb{Z})$, como el producto interno está bien definido (converge) sigue siendo ortogonal a cualquier $f \in S_2(\Gamma_0(N))$. De igual manera que para E_s el orden de $E_{2,s}$ cuando $y\to\infty$ es $y^s + c(s)y^{-1-s} + O(e^{-y})$. A nosotros nos interesa tomar $s = 0$ pues allí

$$\begin{aligned}E(z) &:= E_{2,0}(z) = 1 + O\left(\frac{1}{y}\right) \quad y\to\infty\\ F(z) &:= \frac{\partial}{\partial s}E_{2,s}|_{s=0} = \log y + O\left(\frac{\log y}{y}\right) \quad y\to\infty\end{aligned}$$

La idea de la prueba es restarle a $\tilde{\phi}_{\mathscr{A}}$ algo de la forma $AF(z) + BE(z)$ para que quede crecimiento $O(e^{-y})$ en ∞, y luego lidiar con este crecimiento por separado.

$E(Nz) = E(z) = y^s + O(y^{-1-s})$ $(y \to \infty)$ ahora consideremos $\alpha = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ para intercambiar las cúspides 0 e ∞. Sea M un divisor de N (o sea, $M = 1$ o $M = N$) y $z' = \frac{z}{M}$, entonces $\alpha z' = M\alpha z$ y

$$\begin{aligned} E_{2,s}(Mz)|_2\alpha &= z^{-2}E_{2,s}\left(\frac{-M}{z}\right) \\ &= \frac{1}{(Mz')^2}E_{2,s}\left(\frac{-1}{z'}\right) \\ &= \frac{1}{M}E_{2,s}(z') = \frac{1}{M^{s+2}}y^s + O(y^{-1-s}) \end{aligned}$$

poniendo $s = 0$: $E(Mz)|_2\alpha = \frac{1}{M^2} + O\left(\frac{1}{y}\right)$ y derivando $F(Mz)|_2\alpha = \frac{1}{M^2}(\log \frac{y}{M}) + O\left(\frac{\log y}{y}\right)$ cuando $y \to \infty$. Teniendo entonces el comportamiento en las cúspides observamos que

$$\alpha_1 F(z) + \beta_1 E(z) + \alpha_N F(Nz) + \beta_N E(Nz) \tag{3.3}$$

tiene expansión

$$A_\infty \log y + B_\infty + O\left(\frac{\log y}{y}\right)$$

en ∞ y

$$A_0 \log y + B_0 + O\left(\frac{\log y}{y}\right)$$

en 0. Además, es una forma débilmente modular en el espacio de formas viejas de nivel 2. Entonces si tomamos $\tilde{\phi}^*_{\mathscr{A}} := \tilde{\phi}_{\mathscr{A}} - \alpha_1 F(z) + \beta_1 E(z) + \alpha_N F(Nz) + \beta_N E(Nz)$ obtenemos una forma modular que preserva el producto interno... pero tiene crecimiento $O(e^{-y})$ en lugar de ser holomorfa en las cúspides. Lo que hicimos hasta ahora fue reducir el problema al caso de crecimiento $O(e^{-y})$ en las cúspides, que es el caso $\alpha_1 = \alpha_N = \beta_1 = \beta_N = 0$, resta lidiar con este caso.

Para m coprimo con N consideremos la función

$$P_{m,s}(z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(N)} y^s e^{2\pi i m z}|_2\gamma = \sum_{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_\infty \backslash \Gamma_0(N)} \frac{1}{(cz+d)^2} \frac{y^s}{|cz+d|^{2s}} e^{2\pi i m \gamma z}$$

$P_{m,s}$ converge absolutamente en $\operatorname{Re} s > 0$ a una forma modular cuspidal de peso 2 para $\Gamma_0(N)$. Como $\tilde{\phi}^*_{\mathscr{A}} = \sum_{m=0}^{\infty} a^*_m(y) q^m = O(e^{-y})$ tenemos convergencia absoluta que nos permite intercambiar integral y suma y se puede ver que

$$\left(\tilde{\phi}^*_{\mathscr{A}}, P_{m,\bar{s}}\right)_{\Gamma_0(N)} = \int_{\Gamma_\infty \backslash \mathcal{H}} \tilde{\phi}^*_{\mathscr{A}}(z) e^{-2\pi i m \bar{z}} y^s \, dy = \int_0^\infty a^*_m(y) e^{-4\pi m y} y^s \, dy \, .$$

Como la función $\psi : S_2(\Gamma_0(N)) \to \mathbb{C}$, $\psi(f) = (\tilde{\phi}^*, f)$ es antilineal sabemos que existe una función holomorfa $\phi_{\mathscr{A}} = \sum_{m=0}^{\infty} b_m q^m$ tal que $(\tilde{\phi}^*_{\mathscr{A}}, f)_{\Gamma_0(N)} = (\phi_{\mathscr{A}}, f)_{\Gamma_0(N)}$, y podemos despejar sus coeficientes de Fourier:

$$(\phi_{\mathscr{A}}, P_{m,s})_{\Gamma_0(N)} = b_m \int_0^\infty e^{-4\pi m y} y^s \, dy = \frac{\Gamma(s+1)}{(4\pi m)^s} b_m$$

tomando límite $s \to 0$

$$b_m = 4\pi m \lim_{s\to 0}(\phi, P_{m,s})_{\Gamma_0(N)} = 4\pi m \lim_{s\to 0}\int_0^\infty a_m^*(y)e^{-4\pi m y}y^s\, dy$$

Si escribimos las expansiones $E(z) = \sum_{m=0}^{\infty} e(m,y)q^m$, $F(z) = \sum_{m=0}^{\infty} f(m,y)q^m$ por definición

$$a_m^*(y) = a_m(y) - \alpha_1 f(m,y) - \beta_1 e(m,y)$$

y para terminar la prueba hay que calcular $\int_0^\infty e(m,y)e^{-4\pi m y}y^s\, dy$ y $\int_0^\infty f(m,y)e^{-4\pi m y}y^s\, dy$ y tomar límite $s \to 0$. Los detalles se pueden ver en [9], se llega a

$$\begin{aligned}
\int_0^\infty e(m,y)e^{-4\pi m y}y^s\, dy &= \frac{-6}{\pi m}\sigma_1(m) + o(1).\\
\int_0^\infty f(m,y)e^{-4\pi m y}y^s\, dy &= \frac{-6}{\pi m}\sigma_1(m)s^{-1} - \frac{12}{\pi m}\sigma_1'(m) + \frac{12}{\pi m}\sigma_1(m)\left(\log 2m + \frac{1}{2} + \frac{\zeta'}{\zeta}(2)\right)\\
&\quad + o(1)
\end{aligned}$$

de donde se sigue el Teorema. ■

Finalmente solo resta calcular las integrales del teorema anterior y sustituir los α_1, β_1 del lema 3.23 para llegar al resultado principal de este capítulo.

TEOREMA 3.25. *Sean $D, \mathscr{A}, \mathrm{h}, \varepsilon$ como al principio del Capítulo y $\sigma_{\mathscr{A}}, \sigma'_{\mathscr{A}}$ los definidos en 3.20. Sea además N un primo distinto de D tal que $\varepsilon(N) = 1$. Entonces existe una forma modular $\tilde{\phi}_{\mathscr{A}}(z) = \sum_{m=1}^{\infty} a_{m,\mathscr{A}}q^m \in S_2(\Gamma_0(N))$ tal que para toda forma modular $f \in S_2(\Gamma_0(N))^{\mathrm{new}}$*

$$L_{\mathscr{A}}(f,1) = 0 \quad y \quad L'_{\mathscr{A}}(f,1) = \frac{8\pi^2}{\sqrt{|D|}}(f, \tilde{\phi}_{\mathscr{A}})_{\Gamma_0(N)}$$

y los coeficientes de Fourier para m coprimo con N están determinados por

$$\begin{aligned}
a_{m,\mathscr{A}} = &- \sum_{0<n\le \frac{m|D|}{N}} \sigma'_{\mathscr{A}}(n) r_{\mathscr{A}}(m|D| - nN)\\
&+ \lim_{s\to 1}\left[-2\sum_{n=1}^{\infty}\sigma_{\mathscr{A}}(n) r_{\mathscr{A}}(m|D| + nN)Q_{s-1}\left(1 + \frac{2nN}{m|D|} - \frac{\mathrm{h}\, k_N \sigma_1(m)}{s-1}\right)\right]\\
&+ \mathrm{h}\, k_N\left[\sigma_1(m)B + \sum_{d|m} d\log\frac{m}{d^2}\right] + \mathrm{h}\, r_{\mathscr{A}}(m)\left[A + \log\frac{|D|N}{4\pi^2 m}\right]
\end{aligned}$$

donde

$$\begin{aligned} A &= 2\frac{L'}{L}(1,\varepsilon) - 2\gamma \\ B &= \log\frac{N}{|D|} + 2\frac{\log N}{N-1} + 2 + 2\frac{\zeta'}{\zeta}(2) - 2\frac{L'}{L}(1,\varepsilon) \\ k_N &= \frac{-12}{N+1} \\ \sigma_1(m) &= \sum_{d|m} d \end{aligned}$$

y Q_{s-1} es la función de Legendre de segundo tipo.

Demostración. Para simplificar la notación escribamos

$$a_m = A_m \log y + B_m + \sum_{n=0}^{\infty} C_{m,n} E_1\left(\frac{4\pi n N y}{|D|}\right)$$

con

$$\begin{aligned} A_m &= h r_{\mathscr{A}}(m) \\ B_m &= A_m\left(\log\frac{N|D|}{\pi} - \gamma + 2\frac{L'}{L}(2,\varepsilon)\right) - \sum_{0<n\leq\frac{m|D|}{|N|}} \sigma'_{\mathscr{A}}(n) r_{\mathscr{A}}(m|D| - Nn) \\ C_{m,n} &= -\sigma_{\mathscr{A}}(m) r_{\mathscr{A}}(m|D| + Nn) \end{aligned}$$

Tenemos que calcular $\int_0^\infty a_m(y) e^{-4\pi m y} y^s\, dy$. Haciendo el cambio de variable $u = 4\pi m y$ y notando que $\Gamma'(s) = \int_0^\infty e^{-y} y^s \log y\, dy$ vemos que

$$\int_0^\infty (A_m \log y + B_m)\, e^{-4\pi m y}\, dy = \frac{\Gamma(s+1)}{(4\pi m)^{s+1}}\left(A_m \frac{\Gamma'}{\Gamma}(s+1) - A_m \log 4\pi m + B_m\right)$$

y tomando límite $s \to 0$

$$\lim_{s\to 0} \int_0^\infty (A_m \log y + B_m)\, e^{-4\pi m y}\, dy = \frac{-A_m\gamma - A_m \log 4\pi m + B_m}{4\pi m}$$

Por otra parte

$$\begin{aligned} \int_0^\infty E_1\left(\frac{4\pi n N y}{|D|}\right) e^{-4\pi m y} y^s\, ds &= \int_0^\infty \left(\int_1^\infty \frac{1}{x} e^{-\frac{4\pi n N y x}{|D|}} dx\right) e^{-4\pi m y} y^s\, dy \\ &= \frac{\Gamma(s+1)}{(4\pi m)^{s+1}} \int_1^\infty \left(1 + \frac{Nn}{m|D|}\right)\frac{dx}{x} \end{aligned}$$

y en $s = 0$ esto es igual a $\frac{1}{4\pi m}\log\left(1 + \frac{Nn}{m|D|}\right)$. Tomando límite cuando $n \to \infty$ obtenemos la identidad

$$\int_0^\infty E_1\left(\frac{4\pi n N y}{|D|}\right) e^{-4\pi m y} y^s ds = \frac{2\Gamma(2s+2)}{(4\pi m)^{s+1}\Gamma(s+2)} Q_s\left(1 + \frac{Nn}{m|D|}\right) + O(n^{-s-2})$$

Q_s es la función de Legendre de segundo tipo y es importante pues también nos aparecerá en el Capítulo siguiente, ahora solamente nos interesa su orden:

$$Q_0(1+2t) = \frac{1}{2}\log\left(1+\frac{1}{t}\right), \qquad Q_s(1+2t) = \frac{\Gamma(s+1)^2}{2\Gamma(2s+2)}[t^{-s-1}+O(t^{-s-2})] \quad (t\to\infty)$$

Ahora hay que tomar límite $s \to 0$ en

$$\sum_{n=0}^{\infty} C_{m,n}\int_0^{\infty} E_1\left(\frac{4\pi nNy}{|D|}\right)e^{-4\pi my}y^s\,dy = \frac{2\Gamma(2s+2)}{(4\pi m^{s+1}\Gamma(s+2))}\sum_{n=1}^{\infty} Q_s\left(1+\frac{Nn}{m|D|}\right)+o(1)$$

donde el $o(1)$ aparece porque $C_{m,n} = O(n^c)$. Con esto el resultado se sigue de sustituir estos límites en el Teorema anterior. ■

Capítulo 4

Alturas locales

A lo largo del capítulo N será un primo distinto de D tal que $\varepsilon(N) = 1$. Observemos que en particular N satisface la Hipótesis de Heegner por lo que existe un punto de Heegner $x = (E \xrightarrow{\phi} E')$ de discriminante D, es decir, ϕ es una isogenía de grado N y E, E' tienen multiplicación compleja por $\mathcal{O}_K$.

Buscamos calcular $\langle c, T_m d^\sigma \rangle$ donde $c = (x) - (\infty)$ y $d = (x) - (0)$ para lo que calcularemos las alturas locales primero, distinguiendo lugares arquimedianos de no arquimedianos.

1. Alturas arquimedianas

Al calcular las alturas hay un problema con el cual debemos lidiar, no podremos definir inicialmente el símbolo de altura para todo par de elementos en $\mathrm{Div}^0(X)$ sino para divisores con soporte disjunto, pues allí tenemos la descomposición como suma de alturas locales. El problema anterior hace que inicialmente no se pueda calcular $\langle c, T_m d^\sigma \rangle_v$ cuando $x \in \mathrm{Sop}(T_m d^\sigma)$. Veremos entonces como se calcula $\langle a, b \rangle_\infty$ usando funciones de Green cuando a y b tienen soporte disjunto, esta definición luego se extiende para contemplar todos los casos, eliminando el problema del soporte disjunto.

El símbolo de altura está caracterizado por los axiomas vistos en el Capítulo 2. En el caso arquimediano, diremos que el símbolo de altura para $X_{\mathbb{C}} := X_0(N)(\mathbb{C})$ es la única función definida en $\mathrm{Div}^0_{RP}(X_{\mathbb{C}})$ que satisface las siguientes propiedades

1. $\langle\ ,\ \rangle_v$ es biaditivo y simétrico.
2. Fijo a, el mapa $b \mapsto \langle a, b \rangle_v$ es continuo.
3. $\langle \sum_i m_i(x_i), \mathrm{div}(f) \rangle_v = \sum_i m_i \log |f(x_i)|^2$.

Proposición 4.1. *Sean $x_0, y_0 \in X(H_v)$ distintos. La función*

$$G(x, y) = \langle (x) - (x_0), (y) - (y_0) \rangle_v \tag{4.4}$$

está bien definida para $x \neq y,\ x \neq y_0,\ y \neq x_0\ y$

$$\langle a, b \rangle_v = \sum_{i,j} n_i m_j G(x_i, y_j) \tag{4.5}$$

si $a = \sum_i n_i(x_i)$ y $b = \sum_j m_j(y_j)$ tienen soporte disjunto.

Demostración. Los divisores son de grado 0 y disjuntos por lo que el símbolo está bien definido, además, como $\sum_i n_i = 0$ resulta que $\sum_i n_i(x_i) \in \mathrm{Div}^0(X_{\mathbb{C}})$ es el neutro y por

aditividad

$$\begin{aligned}\langle a,b\rangle_v &= \langle \sum_i n_i\left((x_i)-(x_0)\right), b\rangle_v \\ &= \sum_i n_i \langle (x_i)-(x_0), b\rangle_v \\ &= \sum_{i,j} n_i m_j \langle (x_i)-(x_0),(y_j)-(y_0)\rangle_v\end{aligned}$$

■

Es claro que fijo x, el mapa $y \mapsto G(x,y)$ es continuo en $X_{\mathbb{C}}$. Además, como el divisor $(y)-(y_0)$ es principal, digamos igual a $\operatorname{div}(f)$, $G(x,y) = \log|f(x)|^2 - \log|f(x_0)|^2$, como f es holomorfa satisface las ecuaciones de Cauchy-Riemann y esto resulta en que $\log|f(z)|$ es armónica en $X_{\mathbb{C}} \setminus \{x, x_0\}$. En x y x_0 hay dos singularidades logarítmicas de residuo 1 y -1 respectivamente, esto significa que $G(x,y) - \log|\rho_x(y)|^2$ es continua alrededor de $y = x$ y $G(x,y) + \log|\rho_{x_0}(y)|^2$ es continua alrededor de $y = x_0$, donde ρ representa a un uniformizador local, es decir, ρ es un mapa continuo de un entorno del punto a $\mathbb{C}$ tal que $\operatorname{ord}_\rho(x_0) = 0$. Recíprocamente, también es cierto que si una función posee las propiedades anteriores entonces el símbolo que define mediante (4.5) satisface los axiomas 1, 2 y 3.

Proposición 4.2. *Sea $G : X_{\mathbb{C}} \times X_{\mathbb{C}} \to \mathbb{R}$ una función simétrica tal que $G(x,\cdot)$ es continua y armónica en $X_{\mathbb{C}} \setminus \{x, x_0\}$ y tiene singularidades logarítmicas en x y x_0 con residuos 1 y -1 respectivamente.*

Entonces el símbolo definido como

$$\langle a,b\rangle_v := \sum_{i,j} n_i m_j G(x_i, y_j)$$

para $a = \sum_i n_i(x_i)$ y $b = \sum_j m_j(y_j)$ de soporte disjuntos satisface los axiomas 1. , 2. y 3.

Demostración. Chequeemos los axiomas.

1. Se cumple trivialmente.
2. Fijo $a = \sum_i n_i(x_i) \in \operatorname{Div}^0(X_{\mathbb{C}})$, sabemos que $\langle a,\cdot\rangle_v$ es continuo en el conjunto $\{b \in \operatorname{Div}^0(X_{\mathbb{C}}) : \operatorname{Sop}(b) \cap (\operatorname{Sop}(a) \cup \{x_0\}) = \emptyset\}$, nos hace falta ver que ocurre en x_0. Sea $b = m_0(x_0) + \sum_j m_j(y_j)$ donde $y_j \notin \operatorname{Sop}(a)$, entonces

$$\begin{aligned}\langle a,b\rangle_v &= \sum_i n_i G(x_i, x_0) \\ &= \sum_i n_i C \log|\rho(x_0)|^2 + \sum_{i,j} n_i m_j G(x_i, x_j) \\ &= \sum_{i,j} n_i m_j G(x_i, x_j)\end{aligned}$$

donde en la última igualdad usamos que a es de grado 0. Podemos entonces extender la definición de forma continua (en cada coordenada) para todo par de elementos con soporte disjunto.

3. Consideremos un divisor principal $\mathrm{div}(f)$. Fijo y tenemos que $x \mapsto G(x,y)$ es una función armónica excepto en y, y_0, donde tiene singularidades logarítmicas con residuo 1 y -1, resulta entonces que la función $x \mapsto \log|f(x)|^2 - \langle x-(x_0),(f)\rangle_\infty$ es armónica sin singularidades (ya vimos que en x_0 es evitable), por lo tanto es constante, luego

$$\langle \sum_i n_i x_i, (f)\rangle_v = \sum_i n_i \langle (x_i)-(x_0),(f)\rangle_v = \sum_i n_i(\log|f(x_i)|^2 + \mathrm{cte})$$
$$= \sum_i n_i \log|f(x_i)|^2.$$

■

Observemos que con las condiciones anteriores G queda determinada a menos de sumar una constante, pues por el mismo argumento usado en la proposición anterior, si tenemos dos funciones con esas propiedades su resta es una función armónica sin singularidades y por lo tanto es constante. Si establecemos la condición extra $G(x_0,y_0)=0$ para algún $y_0 \in X_{\mathbb{C}} \setminus \{x_0\}$ fijo, entonces la función que satisface esta condición y las de la proposición anterior es exactamente la definida en 4.4.

Hasta ahora sólo usamos que $X_{\mathbb{C}}$ es una superficie de Riemann compacta, recordemos que $X_{\mathbb{C}} = \Gamma_0(N)\setminus\mathcal{H} \cup \{\text{cúspides}\}$ y que nos interesa tomar $x_0=\infty$, $y_0=0$. Buscamos entonces una función $G : \mathcal{H}\times\mathcal{H} \to \mathbb{R}$ que sea invariante por la acción de $\Gamma_0(N)$, y armónica en cada coordenada, salvo por dos singularidades. Un uniformizador local para $z \in \mathcal{H}$ representando un elemento de $X_{\mathbb{C}} \setminus \{0,\infty\}$ es $\rho(z') = (z-z')^{e_z}(1+O(z-z'))$ donde e_z es el orden del estabilizador de z en $\Gamma_0(N)$ y para 0 e ∞ tomamos $e^{\frac{-2\pi i}{Nz}}$ y $e^{2\pi i z}$ respectivamente, teniendo esto en cuenta las condiciones para G se pueden reescribir como

C1. $G(\gamma z, \gamma' z') = G(z,z')\ \forall \gamma,\gamma' \in \Gamma_0(N)\ , \forall z,z' \in \mathcal{H}$.
C2. $G(z,z')$ es continua y armónica en $\{(z,z') : z \notin \Gamma_0(N)z'\}$.
C3. $G(z,z') = e_z \log|z-z'|^2 + O(1)$ cuando $z' \to z$.
C4. Fijo $z\in\mathcal{H}$, $G(z,\cdot)$ tiene el siguiente comportamiento en las cúspides
   a) $G(z,z') = 4\pi y' + O(1)$ cuando $z' = x'+iy' \to \infty$
   b) $G(z,z') = O(1)$ cuando $z' \to 0$.
   Y de forma análoga, fijo z'
   a) $G(z,z') = 4\pi y + O(1)$ cuando $z = x+iy \to 0$
   b) $G(z,z') = O(1)$ cuando $z \to \infty$.

Más una condición de simetría de la que hablaremos más adelante.

Una forma de obtener una tal G es promediando sobre $\Gamma_0(N)$ una función g invariante por $\mathrm{PSL}_2(\mathbb{Z})$. Más específicamente, si encontramos $g : \mathcal{H}\times\mathcal{H}\to\mathbb{R}$ que cumpla

c1. $g(\gamma z,\gamma z') = g(z,z')\ \forall \gamma \in \mathrm{PSL}_2(\mathbb{Z})\ z,z' \in \mathcal{H}$.
c2. Fijo z, $g(z,\cdot)$ y $g(\cdot,z)$ son continuas y armónicas en $\mathcal{H}\setminus\{z\}$.
c3. Cuando $z' \to z$, $g(z,z') = \log|z-z'|^2 + O(1)$.

entonces $G(z,z') = \sum\limits_{\gamma\in\Gamma_0(N)} g(z,\gamma z')$ cumple las condiciones C1-C4, siempre que esta suma sea convergente. Sobre este último punto se debe tener cuidado, un primer intento para

definir g puede ser considerar

$$g(z,z') = \log \frac{|z-z'|^2}{|\bar{z}-z'|^2}$$

pero su suma diverge. Una forma de lidiar con el problema de la convergencia es cambiar la condición $\Delta g = 0$ por la condición $\Delta g = \varepsilon g$ para $\varepsilon > 0$; si encontramos una g que cumpla esta nueva condición y cuya suma sobre $\Gamma_0(N)$ sea convergente, entonces al tomar límite $\varepsilon \to 0$ y restar las singularidades que surjan obtendremos la g que queremos.

El semiplano superior $\mathcal{H}$ viene equipado con la métrica dada por $dz = \frac{dxdy}{y^2}$, llamada métrica hiperbólica. Bajo esta métrica la distancia entre dos puntos es

$$d(z,z') = \log \frac{|z-\bar{z'}| + |z-z'|}{|z-\bar{z'}| - |z-z'|}$$

y expresado en términos del coseno hiperbólico

$$\cosh d(z,z') = 1 + \frac{|z-z'|^2}{2yy'}.$$

Las transformaciones de Möbius preservan esta distancia (más aún, estas son las únicas transformaciones que preservan la distancia y la orientación, ver [12] §2.3) por lo tanto una función $g : \mathcal{H} \times \mathcal{H} \to \mathbb{R}$ invariante bajo la acción de $\mathrm{PSL}_2(\mathbb{Z})$ sólo depende de la distancia hiperbólica entre z y z', en particular es simétrica.

El Laplaciano en $\mathcal{H}$ es $\Delta = y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$ y como $g(z,z')$ solo depende de la distancia hiperbólica, o lo que es lo mismo, del coseno hiperbólico de la distancia, podemos escribir $g(z,z') = Q(t)$, donde $t = 1 + \frac{|z-z'|}{2yy'}$ y la ecuación $\Delta g(z,\cdot) = \varepsilon g(z,\cdot)$ puede reescribirse como

$$(1-t^2)\frac{d^2}{dt^2}Q(t) - 2t\frac{d}{dt}Q(t) + \varepsilon Q(t) = 0,$$

esta es la ecuación diferencial de Legendre de índice $s-1$, donde $\varepsilon = s(s-1),\ s > 1$ y su solución es conocida:

Proposición 4.3. *La solución a*

$$(1-t^2)\frac{d^2}{dt^2}Q(t) - 2t\frac{d}{dt}Q(t) + s(s-1)Q(t) = 0$$

$t > 1, s > 0$ *es*

$$Q_{s-1}(t) = \int_0^\infty \left(1 + \sqrt{t^2-1}\cosh u\right)^{-s} du$$

Observemos que es la segunda vez que aparece esta función! En el Teorema principal del Capítulo anterior aparece $\lim_{s\to 0} Q_s(t)$.

Se deducen de la proposición anterior las siguientes fórmulas asintóticas.

Corolario 4.4.

- $Q_{s-1}(t) = -\frac{1}{2}\log(t-1) + O(1)$ *cuando* $t \to 1$.
- $Q_{s-1} = O(t^{-s})$ *cuando* $t \to \infty$.

El corolario anterior implica que

$$g_s(z,z'):= -2Q_{s-1}\left(1+\frac{|z-z'|^2}{2yy'}\right)$$

satisface los axiomas

c2'. $z \mapsto g_s(z,z')$ es continua y cumple la ecuación $\Delta g_s(z,\cdot) = s(s-1)g_s(z,\cdot)$.

y c3. Además, la suma

$$G_{N,s}(z,z') = \sum_{\gamma\in\Gamma_0(N)} g_s(z,\gamma z')$$

converge absolutamente para $s>1$. La función $G_{N,s}$ es conocida como el *resolvente* de $\Gamma_0(N)$ y satisface las siguientes propiedades:

Proposición 4.5 (Propiedades de $G_{N,s}$).

(a) $G_{N,s}$ *es* $\Gamma_0(N)$ *invariante en cada coordenada.*

(b) $\Delta_z G_{N,s}(z,z') = s(s-1)G_N(z,z')$.

(c) El mapa $s \mapsto G_{N,s}$ *es holomorfo para* $\operatorname{Re} s > 1$ *y se extiende a una función meromorfa alrededor de* $s=1$ *con un polo simple de residuo*

$$k_n = -\frac{12}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N)]} = -\frac{12}{N+1}.$$

(d) $G_{N,s}(z,z') = -\frac{4\pi}{2s-1}E_{N,s}(z')y^{1-s} + O(e^{-y}) \quad y\to\infty$
donde $E_{N,s}$ *es la serie de Eisenstein de peso* 0

$$E_{N,s}(z) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(N)} \operatorname{Im}(\gamma z)^s$$

Demostración. Los items (a) y (b) son inmediatos de lo anterior. La prueba de los ítems (c) y (d) se puede encontrar en [11]. Observemos que la igualdad $k_n = -\frac{12}{N+1}$ sólo vale cuando N es primo. ■

Para obtener una función armónica y holomorfa le restamos a $G_{N,s}$ una función invariante por $\Gamma_0(N)$ con un polo simple de residuo k_N en $s=1$ y que además sea solución de $\Delta f = s(s-1)f$. Resulta que la serie de Eisenstein $E_{N,s}$ cumple esto. La serie $-4\pi E_N(z,s)$ converge para $z\in\mathcal{H}$, $\operatorname{Re} s>1$ y se extiende de forma meromorfa en un entorno de $s=1$ con un polo de residuo k_N. Además $\Delta E_N(z,s) = s(s-1)E_N(z,s)$ y como mencionamos en el capítulo anterior, para N primo se tiene la siguiente identidad para $E_{N,s}$.

$$E_{N,s}(z) = (N^s - N^{-s})^{-1}\left(E_s\left(\frac{N}{d}z\right) - \frac{1}{N}E_s\left(Nz\right)\right) \tag{4.6}$$

donde $E_s = E_{1,s}$.

Finalmente podemos definir G, a menos de una constante a determinar.

Proposición 4.6.

$$G(z,z'):= \lim_{s\to 1}\left[G_{N,s}(z,z') + 4\pi E_{N,s}(z') + 4\pi E_{N,s}(\omega_N z) - \frac{k_N}{s-1}\right] + C$$

satisface C1-C4.

Demostración.

C1. Es claro pues $G_{N,s}(z,z')$ y $E_{N,s}(z)$ son $\Gamma_0(N)$-invariantes como funciones de z.

C2. También es claro pues, vistos como función de z, hay continuidad en $z \notin \Gamma_0(N)z'$, y allí

$$\Delta G(z,z') = \lim_{s\to 1}\left[s(s-1)G_{N,s}(z,z') - s(s-1)4\pi E_{N,s}(\omega_N z)\right] = k_N - k_N = 0.$$

C3. Por una parte $g_s(z,z') = -2Q(1+\frac{z-z'}{yy'})$, como $Q(t) = -\frac{1}{2}(\log t - 1) + O(1)$ cuando $t \to 1$ resulta que $g_s(z,z') = \log|z-z'|^2 + O(1)$. La suma sobre $\Gamma_0(N)$ puede dividirse en dos

$$\begin{aligned}\sum_{\gamma\in\Gamma_0(N)} g_s(z,\gamma z') &= \sum_{\gamma\in \mathrm{Stab(z)}} g_s(z,\gamma z') + \sum_{\gamma\notin \mathrm{Stab(z)}} g_s(z,\gamma z') \\ &= e_z \log|z-z'|^2 + O(1) + \sum_{\gamma\notin \mathrm{Stab(z)}} g_s(z,\gamma z')\end{aligned}$$

y con el mismo argumento con el que se prueba la convergencia de $G_{N,s}$ para $z' \notin \Gamma_0(N)z$ se prueba que la última suma converge.

C4. Fijemos z' para ver primero el comportamiento de $G(\,\cdot\,,z')$ en las cúspides. Por 4.5(d)

$$G_{N,s}(z,z') = -\frac{4\pi}{2s-1}E_{N,s}(z')y^{1-s} + O(e^{-y}) \quad (y\to\infty).$$

El comportamiento de $E_{N,s}$ es conocido y lo utilizamos en el Capítulo anterior

$$E_{N,s}(z) = y^s + \phi(s)y^{1-s} + O(e^{-y}) \quad (y\to\infty)$$

$\phi(s) = \frac{\Gamma(\frac{1}{2})\Gamma(s-\frac{1}{2})}{\Gamma(s)}\frac{\zeta(2s-1)}{\zeta(s)}y^{1-s}$. Cuando $z\to\infty$

$$\lim_{s\to1}\left[-\frac{4\pi}{2s-1}E_{N,s}(z')y^{1-s} + 4\pi E_{N,s}(z') + 4\pi E_{N,s}(\omega_N z) + \frac{k_N}{s-1}\right] + O(e^{-y}) + C =$$

$$\lim_{s\to1}\left[4\pi E_{N,s}(z')\left(1-\frac{y^{1-s}}{2s-1}\right) + 4\pi E_{N,s}(\omega_N z) + \frac{k_N}{s-1}\right] + O(e^{-y}) + C$$

Por una parte, como $4\pi E_{N,s}$ tiene un polo simple de residuo $-k_N$ en $s=1$ tenemos que

$$4\pi E_{N,s}(z) = -\frac{k_N}{s-1} + O(1)$$

y por otra parte, haciendo el desarrollo de Taylor de orden 2 en 1

$$\begin{aligned}1-\frac{y^{1-s}}{2s-1} &= 1 - \frac{1}{1-2t}e^{\log yt} \quad (t=1-s)\\ &= 1-\frac{1}{1-2t}\left(1+\log yt + \frac{1}{2}(\log y)^2t^2 + \frac{1}{6}(\log y)^3t^3\right) + O(t^2)\\ &= -(\log y+2)t + O(t^2)\end{aligned}$$

entonces el límite del primer término es $-k_N(\log y + 2)$. El segundo término es

$$\begin{aligned}
E_{N,s}(\omega_N z) &= (N^s - N^{-s})^{-1}\left(E_s\left(\frac{-1}{z}\right) - \frac{1}{N^s}E_s\left(\frac{-1}{Nz}\right)\right)\\
&= (N^s - N^{-s})^{-1}\sum_{d|n}\left(E_s(z) - \frac{1}{N^s}E_s(Nz)\right)\\
&= (N^s - N^{-s})^{-1}\left(y^s + \phi(s)y^{1-s} - y^s - \frac{(Ny)^{1-s}}{N^s}\phi(s) + O(e^{-y})\right)\\
&= N^{-s}\frac{1-N^{1-2s}}{1-N^{-2s}}\left(\phi(s)y^{1-s} + O(e^{-y})\right)
\end{aligned}$$

donde en la primera linea usamos la invariancia de E_s por $\mathrm{SL}_2(\mathbb{Z})$. Y entonces

$$\lim_{s\to 1}\left[E_s(\omega Nz) + \frac{k_N}{s-1}\right] = \lambda_N + k_N\log y + O(e^{-y})$$

donde

$$\begin{aligned}
\lambda_N &= \lim_{s\to 1}\left[N^{-s}\frac{1-N^{1-2s}}{1-N^{-2s}}\phi(s)y^{1-s} + \frac{k_N}{s-1}\right]\\
&= \lim_{s\to 1}\left[N^{-s}\frac{1-N^{1-2s}}{1-N^{-2s}}\frac{\Gamma(\frac{1}{2})\Gamma(s-\frac{1}{2})}{\Gamma(s)}\frac{\zeta(2s-1)}{\zeta(s)}y^{1-s} + \frac{1}{s-1}(s)\right]\\
&= \lim_{s\to 1}\left[N^{-s}\frac{1-N^{1-2s}}{1-N^{-2s}}\frac{\Gamma(\frac{1}{2})\Gamma(s-\frac{1}{2})}{\Gamma(s)}\frac{[(2s-2)^{-1} + \gamma + O(s-1)]}{\zeta(s)}y^{1-s} + \frac{k_N}{s-1}(s)\right]\\
&= k_N[\log N + 2\log 2 - 2\gamma + 2\frac{\zeta'}{\zeta}(2) - 2\frac{N\log N}{N^2-1}]
\end{aligned}$$

donde en la última desigualdad tomamos la derivada logarítmica para calcular los residuos y $\gamma = -\Gamma'(1)$ es la constante de Euler.

Tomando $y \to \infty$ vemos que la constante $C = \lambda_N - 2k_N$ hace que $G(z, z') \to 0$ cuando $z \to \infty$. Solo resta ver que $G(z, z') = 4\pi y + O(1) \quad (z \to 0)$. La matriz ω_N intercambia las cúspides 0 e ∞, por una parte tenemos

$$E_{N,s}(\omega_N z) = \mathrm{Im}(\omega_N z)^s + O(\mathrm{Im}(\omega_N z)^{1-s}) = \frac{\mathrm{Im}(z)^s}{N|z|^{2s}} + O(\mathrm{Im}(\omega_N z)^{1-s}) \quad (z \to 0)$$

Y por otra parte, como $G_{N,s}(z, z') = G_{N,s}(\omega_N z, \omega_N z')$ tenemos que

$$G_{N,s} = -\frac{4\pi}{2s-1}E_{N,s}(\omega_N z')(\mathrm{Im}\,\omega_N z)^{1-s} + O(e^{\mathrm{Im}\,\omega_N})$$

entonces $G(z, z') = 4\pi Y + \alpha\log Y + \beta + O(e^{-Y}) \quad (Y \to \infty)$ y como es una función armónica $\alpha = 0$. Esto culmina una parte de la prueba, resta ver el comportamiento en la otra variable, pero eso es inmediato por la propiedad $G_{N,s}(z, z') = G_{N,s}(\omega_N z, \omega_N z')$.

■

Corolario 4.7.

$$\langle (x)-(\infty),(x')-(0)\rangle_v = \lim_{s\to 1}\left[G_{N,s}(z,z') + 4\pi E_{N,s}(\omega_N z) + E_{N,s}(z') + \frac{k_N}{s-1}\right] - \lambda_N + 2k_N.$$

donde $z, z' \in \mathcal{H}$ son puntos en el semiplano superior representando x, x' respectivamente como en el capítulo 2.

Recordemos que a nosotros no nos interesa exactamente la expresión anterior sino $\langle (x)-(\infty), T_m((x')-(0))\rangle_v$, debemos ver entonces como actúa T_m en cada uno de los objetos anteriores como funciones de z'.

Como

$$G_{N,s}(z,z') = \sum_{\gamma\in\Gamma_0(N)} g_s(z,\gamma z')$$

y

$$T_m z' = \sum_{\substack{\gamma\in\Gamma_0(N)\backslash R_N \\ \det\gamma = m}} \gamma z'$$

$$G_{N,s}(z, T_m z') = \sum_{\substack{\gamma\in R_N/\pm 1 \\ \det\gamma = m}} g_s(z,\gamma z')$$

Como $E_{N,s}(\omega_N)$ y $\frac{k_N}{s-1}$ no dependen de z' allí la acción se reduce a multiplicar por $\#\{\gamma\in\Gamma_0(N)\backslash R_N : \det\gamma = m\} := \sigma_1(m) = \sum_{\substack{d|m \\ d>0}} d$. También se puede ver que

$$E_{N,s}(T_m z') = m^s \sum_{d|m} d^{1-2s} E_{N,s}(z').$$

Juntando los resultados anterior obtenemos la fórmula

(4.7)

$$\begin{aligned}\langle (x)-(\infty), T_m((x')-(0))\rangle_v &= \sigma_1(m)(2k_N - \lambda_N) \\ &+ \lim_{s\to 0}[G^m_{N,s}(z,z') + 4\pi\sigma_1(m)E_{N,s}(\omega_N z) + 4\pi m^s \sum_{d|m} d^{1-2s} E_{N,s}(z')]\end{aligned}$$

Ahora que tenemos una fórmula para la altura $\langle (x)-(\infty), T_m(x')-(0)\rangle_v$ tenemos que poder evaluarla en $x = x'$ un punto de Heegner, para eso recordemos que estos estaban en correspondencia con pares $(\mathscr{A}, \mathfrak{n})$ donde $\mathscr{A}\in Cl_K$ y $\mathfrak{n}$ es un ideal primitivo de norma N y a su vez con elementos que son raíces cuadráticas en el semiplano superior. También recordemos que en 1 vimos que el grupo de Galois actúa por multiplicación a derecha en $\mathscr{A}$: $(\mathscr{A},\mathfrak{n})^{\sigma_{\mathscr{B}}} = (\mathscr{A}\mathscr{B}^{-1}, \mathfrak{n})$, entonces solo nos interesa calcular

$$G^m_{N,s}(\tau_{\mathscr{A},\mathfrak{n}}, \tau_{\mathscr{A}\mathscr{B}^{-1},\mathfrak{n}})$$

donde $\tau_{\mathscr{A},\mathfrak{n}}\in\mathcal{H}$ está dado como en 2.3. Observemos que en particular el ideal primitivo $\mathfrak{n}$ es el mismo en ambos puntos.

Proposición 4.8.

Dadas dos clases de ideales $\mathscr{A}, \mathscr{B}\in Cl_K$ y un ideal primitivo $\mathfrak{n}\in\mathcal{O}$ existen exactamente un par de ideales $(\mathscr{A}_1, \mathscr{A}_2)$ tales que $\mathscr{A} = \mathscr{A}_1\mathscr{A}_2^{-1}$ y $\mathscr{A}_1\mathscr{A}_2[\mathfrak{n}]^{-1} = \mathscr{B}$.

Demostración. Aquí usaremos que D es un primo impar, ya que en ese caso hay un solo género en $\mathcal{O}_K$. Esto implica que el número de clases es impar y que el mapa elevar al cuadrado es un isomorfismo de grupos. En consecuencia, existe una única solución $\mathscr{A}_2^2 = \mathscr{A}^{-1}\mathscr{B}[\mathfrak{n}]$. ■

La proposición anterior nos permite definir

$$\gamma_{N,s}^m(\mathscr{A},\mathscr{B}) \coloneqq G_{N,s}^m(\tau_{\mathscr{A}_1,\mathfrak{n}}, \tau_{\mathscr{A}_2,\mathfrak{n}}).$$

Esta definición no depende de $\mathfrak{n}$, ya que, los únicos ideales de norma N son $\mathfrak{n}$ y su conjugado $\bar{\mathfrak{n}} = N\mathfrak{n}^{-1}$ e intercambiarlos corresponde a actuar por la involución canónica: $\omega_N((\mathscr{A}_1,\mathfrak{n})) = (\mathscr{A}_1[\mathfrak{n}]^{-1}), \bar{\mathfrak{n}})$ y $G_{N,s}$ es invariante por la acción de w_N. Lo único que hicimos fue reindexar los valores de $G_{N,s}^m(\tau_{\mathscr{A},\mathfrak{n}}, \tau_{\mathscr{A}\mathscr{B}^{-1},\mathfrak{n}})$, pero al hacerlo eliminamos la dependencia de $\mathfrak{n}$, lo cual será útil más adelante. El siguiente paso es probar la fórmula para $\gamma_{N,s}^m$:

Proposición 4.9.

$$\gamma_{N,s}^m(\mathscr{A},\mathscr{B}) = -2\sum_{n=1}^{\infty} \delta(n) r_{\mathscr{A}}(nN + m|D|) r_{\mathscr{B}}(n) Q_{s-1}\left(1 + \frac{2nN}{m|D|}\right)$$

donde $\delta(n) = 2$ *si* $D \mid n$ *y* 1 *si* $D \nmid n$.

Sumando sobre $\mathscr{B} \in Cl_K$ en la proposición anterior tenemos automáticamente el siguiente corolario

Corolario 4.10.

$$\gamma_{N,s}^m(\mathscr{A}) \coloneqq \sum_{\mathscr{B}\in Cl_K} \gamma_{N,s}^m(\mathscr{A},\mathscr{B}) = -2\sum_{n=1}^{\infty} \delta(n) r_{\mathscr{A}}(nN + m|D|) R(n) Q_{s-1}\left(1 + \frac{2nN}{m|D|}\right)$$

donde $R(n) = \sum_{\mathscr{B}\in Cl_K} r_{\mathscr{B}}(n)$.

Para probar 4.9 vamos a probar primero el siguiente lema, de aquí en más $\tau_{\mathscr{A},\mathfrak{n}}$ refiere al punto en el semiplano superior definido como en 2.3.

Lema 4.11. *Sean* $(\mathscr{A}_i,\mathfrak{n})$ $i = 1,2$ *dos puntos de Heegner y* $A_i x^2 + B_i x + C_i$ *el polinomio del que* $z_i = \tau_{\mathscr{A}_i,\mathfrak{n}}$ *es raíz. Sean también* $\mathfrak{a}_i \in \mathscr{A}_i$ *dos ideales enteros de norma* A_i *tales que* $\mathfrak{n} \mid \mathfrak{a}_i$. *Entonces, cuando* $r_{\mathscr{A}_1\mathscr{A}_2^{-1}} = 0$ *se satisface la igualdad*

$$G_{N,s}^m(\tau_{\mathscr{A}_1,\mathfrak{n}}, \tau_{\mathscr{A}_2,\mathfrak{n}}) = \sum_{n=1}^{\infty} \rho_{\mathscr{A}_1,\mathscr{A}_2}^m(n) Q_{s-1}\left(1 + \frac{2nN}{m|D|}\right)$$

donde

$$\rho_{\mathscr{A}_1,\mathscr{A}_2}^m(n) = \#\Big\{(\alpha,\beta) \in \bar{\mathfrak{a}}_1^{-1}\bar{\mathfrak{a}}_2^{-1} \times \mathfrak{a}_1^{-1}\mathfrak{a}_2^{-1}\mathfrak{n} \backslash \{\pm 1\} : A_1A_2\,\mathrm{N}(\alpha) = Nn + m|D|,$$
$$A_1A_2\,\mathrm{N}(\beta) = Nn, \mathfrak{d} \mid A_1A_2\alpha - A_1A_2\beta\}$$

Demostración.

Recordemos que $g_s(z_1,z_2) = -2Q_{s-1}\left(1+\frac{|z_1-z_2|^2}{2\operatorname{Im} z_1 \operatorname{Im} z_2}\right)$. Sea $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in R_N$.

$$\begin{aligned} g_s(\gamma z_1, z_2) &= -2Q_{s-1}\left(1+\frac{|\gamma z_1 - z_2|^2 |cz_1+d|^2}{\det\gamma \operatorname{Im} z_1 \operatorname{Im} z_2}\right) \\ &= -2Q_{s-1}\left(1+\frac{|az_1+b-z_2(cz_1+d)|^2}{\det\gamma \operatorname{Im} z_1 \operatorname{Im} z_2}\right) \\ &= -2Q_{s-1}\left(1+\frac{A_1A_2|az_1+b-z_2(cz_1+d)|^2}{\det\gamma D}\right) \\ &= -2Q_{s-1}\left(\frac{1+2Nn}{\det\gamma D}\right) \end{aligned}$$

donde $n{:=}\frac{A_1A_2(az_1+b-cz_1z_2-dz_2)}{N}$. Definamos ahora $\mathfrak{d} = \sqrt{D}\mathcal{O}_K$ $\alpha = az_1+b-cz_1\bar{z_2}-d\bar{z_1}$ y $\beta = az_1+b-cz_1z_2-dz_2$
Afirmación 1: $\alpha \in \mathfrak{a}_1\mathfrak{a}_2^{-1}$ y $\beta \in \mathfrak{a}_1\mathfrak{a}_2^{-1}\mathfrak{n}$.
Afirmación 2: $n = N^{-1}A_1A_2\,\mathrm{N}(\beta)$ es entero.
Afirmación 3: $l{:=}A_1A_2\,\mathrm{N}(\alpha)$ es entero.
Afirmación 4: $l - Nn = |D|\det\gamma$.
Afirmación 5: $\mathfrak{d} \mid A_1A_2\alpha - A_1A_2\beta$
La afirmación 1 se deduce de $z_i \in A_i\bar{\mathfrak{a}}_i = \mathfrak{a}_i^{-1}$ y $\mathfrak{n}\mathfrak{n}' = NO_K \mid c$. Las afirmaciones 2 y 3 son inmediatas de la primera. La afirmación 4 resulta de desarrollar $l - Nn = A_1A_2\det\left(\begin{smallmatrix}\alpha & \beta \\ \overline{\alpha} & \overline{\beta}\end{smallmatrix}\right)$. Y la 5 resulta de ver que $A_1A_2\alpha - A_1A_2\beta = A_1A_2[(\bar{z}_2-z_2)(c\tau_1+d)]$ y como entonces $A_2z_2 \in \mathcal{O}_K$ $\sqrt{D} \mid A_2\bar{z}_2 - A_2z_2$.

Ahora, dados α y β en las condiciones de las afirmaciones anteriores podemos resolver un sistema y encontrar $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in R_N$ y la propiedad 4 nos dice que $\det\gamma = \frac{l-Nn}{|D|}$.

Entonces

$$G_{N,s}^m = -2\rho^m(n)Q_{s-1}\left(1+\frac{2Nn}{m|D|}\right)$$

donde

$$\rho^m(n) = \#\{(\alpha,\beta) : \text{ satisfaciendo Afirmaciones } 1-5\}.$$

■

Demostración de la proposición.
Solo tenemos que probar que $\rho^m(n) = \delta(n)r_{\mathscr{A}_1\mathscr{A}_2^{-1}}(Nn+m|D|)_{\mathscr{A}_1\mathscr{A}_2[\mathfrak{n}]^{-1}}(n)$.

Si $D \mid n$ entonces $\mathfrak{d} \mid A_1A_2\alpha$ y $\mathfrak{d} \mid A_1A_2\beta$ entonces

$$\begin{aligned} &\#\left\{(\alpha,\beta) \in \bar{\mathfrak{a}}_1^{-1}\bar{\mathfrak{a}}_2^{-1} \times \mathfrak{a}_1^{-1}\mathfrak{a}_2^{-1}\mathfrak{n} \backslash \{\pm 1\} : A_1A_2\,\mathrm{N}(\alpha) = Nn+m|D|, A_1A_2\,\mathrm{N}(\beta) = Nn\right\} \\ &= \frac{1}{2}\#\left\{\alpha \in \bar{\mathfrak{a}}_1^{-1}\bar{\mathfrak{a}}_2^{-1} : A_1A_2\,\mathrm{N}(\alpha) = Nn+m|D|\right\} \cdot \#\left\{\beta \in \bar{\mathfrak{a}}_1^{-1}\bar{\mathfrak{a}}_2^{-1}\mathfrak{n} : A_1A_2\,\mathrm{N}(\beta) = Nn\right\} \\ &= 2r_{\mathscr{A}_1\mathscr{A}_2^{-1}}(Nn+m|D|)r_{\mathscr{A}_1\mathscr{A}_2[\mathfrak{n}]^{-1}}(n) \end{aligned}$$

Mientras que si $D \nmid N$ el número se reduce a la mitad porque por cada (α, β) que satisface ambas condiciones el elemento $(\alpha, -\beta)$ también lo satisface y por reciprocidad la congruencia se da en exactamente uno de los dos pares. ■

Sumando sobre todas las clases de ideales obtenemos la fórmula

(4.8)
$$\gamma^m_{N,s}(\mathscr{A}) := \sum_{\mathscr{B}\in Cl_K} \gamma^m_{N,s}(\mathscr{A},\mathscr{B}) = -2\sum_{n\geq 0} \delta(n)R(n)r_{\mathscr{A}}(Nn+m|D|)Q_{s-1}\left(1+\frac{2nN}{m|D|}\right)$$

Finalmente podemos probar la fórmula principal de esta sección asumiendo $r_{\mathscr{A}}(m) = 0$.

Proposición 4.12. *Sea $x \in X_0(N)$ un punto de Heegner de discriminante D, $c = (x) - (\infty)$, $d = (x) - (0)$, $\sigma \in \mathrm{Gal}(H/K)$ asociado a una clase de ideales $\mathscr{A} \in Cl_K$. Sea $m \in \mathbb{N}$ coprimo con N y supongamos que $r_{\mathscr{A}}(m) = 0$ y $N \nmid m$. Entonces*

$$\sum_{v|\infty}\langle c, T_m d^\sigma\rangle_v = \lim_{s\to 1}\left[\gamma^m_{N,s}(\mathscr{A}) - \frac{\mathrm{h}\,\sigma_1(m)k_N}{s-1}\right] +$$
$$\mathrm{h}\,k_N\sigma_1(m)\left[\log\frac{N}{|D|} + \frac{2}{N^2-1}\log N + 2 + 2\frac{\zeta'}{\zeta}(2) - 2\frac{L'}{L}(1,\varepsilon) + \sum_{d|m} d\log\frac{m}{d^2}\right]$$

Demostración. Recordemos la correspondencia 2.4. Las h clases de ideales de Cl_K dan lugar a h lugares arquimedianos en H que son permutados por la acción de $\mathrm{Gal}(H/K) \simeq Cl_K$. Recordando que podemos eliminar la dependencia de $\mathfrak{n}$, el ideal de norma N, tenemos la igualdad

$$\sum_{v|\infty}\langle c, T_m d^\sigma\rangle_v = \sum_{\substack{\mathscr{A}_1,\mathscr{A}_2\in Cl_K\\ \mathscr{A}_1\mathscr{A}_2^{-1}=\mathscr{A}}} \langle(\tau_{\mathscr{A}_1,\mathfrak{n}}) - (\infty), T_m(\tau_{\mathscr{A}_2,\mathfrak{n}}) - (0)\rangle_v$$

Donde en la suma de la derecha $\mathfrak{n}$ es un ideal de norma N fijo (recordemos que N es un primo que descompone en K entonces sólo hay dos ideales de norma N en $\mathcal{O}_K$) y v es un lugar arquimediano cualquiera. La ecuación (4.7) nos da la expresión

(4.9)
$$\sum_{v|\infty}\langle c, T_m d^\sigma\rangle_v = \lim_{s\to 0}\left[\gamma^m_{N,s}(\mathscr{A}) + 4\pi\sigma_1(m)\sum_{\mathscr{A}_1\in Cl_K} E_{N,s}(\omega_N\tau_{\mathscr{A}_1,\mathfrak{n}}) + \right.$$
$$\left. 4\pi m^s\sum_{d|m} d^{1-2s}\sum_{\mathscr{A}_2\in Cl_K} E_{N,s}(\tau_{\mathscr{A}_2,\mathfrak{n}}) - \mathrm{h}\,\sigma_1(m)(\lambda_N - 2k_N)\right]$$

Ahora, por (4.6)

$$\sum_{\mathscr{A}\in Cl_K} E_{N,s}(\omega_N\tau_{\mathscr{A}_1,\mathfrak{n}})E_{N,s} = (N^s - N^{-s})^{-1}\sum_{\mathscr{A}\in Cl_K}\left[E_s\left(N\tau_{\mathscr{A},\mathfrak{n}}\right) - \frac{1}{N}E_s(\tau_{\mathscr{A},\mathfrak{n}})\right]$$

La identidad $\sum_{\mathscr{A}\in Cl_K} E_s(\tau_{\mathscr{A},\mathfrak{n}}) = 2^{-s}|D|^{-s}\zeta(2s)^{-1}\zeta_K(s)$ donde $\zeta_K(s) = \zeta(s)L(s,\varepsilon)$ (se puede ver en [1]) vale tomando cualquier $\tau_{\mathscr{A},\mathfrak{n}}$ en $\mathcal{H}$ correspondiente a una solución cuadrática de discriminante D con coeficiente A divisible por N, por lo tanto es invariante por multiplicar el punto por N.

Entonces también vale la igualdad $\sum_{\mathscr{A}\in Cl_K} E_s(N\tau_{\mathscr{A},\mathfrak{n}}) = 2^{-s}|D|^{-s}\zeta(2s)^{-1}\zeta_K(s)$

Sustituyendo estas igualdades en nuestra ecuación y usando la igualdad $L(1,\varepsilon) = \frac{\pi\,\mathrm{h}}{\sqrt{|D|}}$ y la factorización

$$\zeta_K(s) = \zeta(s)L(s,\varepsilon) = \left(\frac{1}{s-1} + \gamma + O(s-1)\right)\left(L(1,\varepsilon) + L'(1,\varepsilon(s-1) + O(s-1)^2)\right)$$

llegamos a la fórmula de la proposición. ■

Hasta ahora asumimos $r_{\mathscr{A}}(m) = 0$, la fórmula vale en general para m coprimo con N pero se debe extender la definición de la altura local que tenemos y por lo tanto modificar las definiciones de $G_{N,s}$ y G. En [9] se detalla el procedimiento para hacer esto, sumando la contribución de los términos con $r_{\mathscr{A}}(m) \neq 0$ se llega a la expresión

$$\begin{aligned}\sum_{v|\infty}\langle c, T_m d^\sigma\rangle_v = &+ \mathrm{h}\,k_N\left[\sigma_1(m)B + \sum_{j|m} j\log\frac{m}{j^2}\right] + \mathrm{h}\,r_{\mathscr{A}}(m)\left[A + \log\frac{|D|}{4\pi^2}\right]\\ &+ \lim_{s\to 1}\left[-2\sum_{n=1}^{\infty}\sigma_{\mathscr{A}}(n)r_{\mathscr{A}}(m|D| + nN)Q_{s-1}\left(1 + \frac{2nN}{m|D|} - \frac{\mathrm{h}\,k_N\sigma_1(m)}{s-1}\right)\right]\end{aligned} \tag{4.10}$$

donde $A = 2\frac{L'}{L}(1,\varepsilon) - 2\gamma$ y $B = \log\frac{N}{|D|} + 2\frac{\log N}{N-1} + 2 + 2\frac{\zeta'}{\zeta}(2) - 2\frac{L'}{L}(1,\varepsilon)$.

2. Alturas no arquimedianas

Hasta ahora hemos trabajado en la curva modular $Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}$ usando su interpretación como espacio de moduli donde sus puntos clasifican isogenias de grado N. Como ya vimos, $Y_0(N)$ admite una estructura como superficie de Riemann sobre $\mathbb{C}$ y agregando un conjunto finito de puntos, las cúspides, la podemos compactificar. Estos puntos que agregamos a la curva, que en nuestro caso son 2 pues N es primo, no tienen a priori una interpretación en términos de curvas elípticas.

Al reducir la curva módulo N comienzan a aparecer singularidades que el modelo anterior no ve, por lo que si queremos hacer un estudio local necesitamos un buen modelo sobre $\mathbb{Z}$ (y no sólo sobre $\mathbb{C}$). Para N primo este modelo fue propuesto por Deligne-Rapoport y hace uso de la Teoría de Esquemas, de hecho es un modelo más general para curvas elípticas sobre esquemas.

Una vez dado un modelo $\underline{X}$ para la curva modular se tienen dos elementos $\underline{x}, \underline{x}^\sigma$ que se corresponden con x y x^σ respectivamente; también se tiene un concepto de *intersección* o *producto de la intersección*: $(\underline{x}\cdot T_m\underline{x}^\sigma)$. Por la forma en que se define el modelo, para m coprimo con N es automática la fórmula

$$\langle c, T_m d^\sigma\rangle_v = -(\underline{x}\cdot T_m\underline{x}^\sigma)\log q$$

donde $q = \#\Lambda_v/\pi$ es el cardinal del cuerpo residual de Λ_v, el anillo de enteros de H_v. Cuando además $r_{\mathscr{A}}(m) = 0$ se tiene que $\underline{x}$ y $T_m\underline{x}^\sigma$ son disjuntos. En este caso, haciendo uso de la geometría algebraica y en particular de la *teoría de la intersección* se llega a la fórmula

$$(\underline{x}\cdot T_m\underline{x}^\sigma) = \frac{1}{2}\sum_{n=0}^{\infty}\#\,\mathrm{Hom}_{W_n}(\underline{x}, \underline{x}^\sigma)_{\deg m} \tag{4.11}$$

donde W es el cuerpo que se obtiene al completar la máxima extensión no ramificada de Λ_v y $W_n = \Lambda_v/\pi^n$. La suma anterior es finita, las isogenías de grado m en $\mathrm{Hom}_{W_n}(\underline{x}, \underline{x}^\sigma)$ se corresponden con elementos de orden m en una clase de ideales o en un orden maximal de un álgebra de cuaterniones, como mencionaremos más adelante.

Recordemos que nuestro punto de Heegner $x = (E \xrightarrow{\phi} E')$ en $X_0(N)$ tiene discriminante D y E, E' multiplicación compleja por $\mathcal{O}_K$. Vamos a denotar v a un lugar finito de H y H_v a su completado, Λ_v el anillo de enteros de H_v, p la característica del cuerpo residual y π un uniformizador. Con el fin de ilustrar los resultados supongamos de aquí en adelante que $r_{\mathscr{A}}(m) = 0$. Como en el capítulo anterior, las fórmulas se pueden generalizar para cualquier m coprimo con N.

Hay varias propiedades que naturalmente se cumplen en W, que observemos tiene característica 0, por ejemplo:

$$\mathrm{End}_W(\underline{x}) \simeq \mathrm{End}_W(\underline{x}^\sigma) \simeq \mathcal{O}_K, \qquad \mathrm{Hom}_W(\underline{x}, \underline{x}^{\sigma_{\mathscr{A}}}) \simeq \mathscr{A}$$

donde las isogenías de grado m se corresponden con ideales de norma m. Otra observación que podemos hacer es que en general

$$\mathrm{Hom}_W(\underline{x}, \underline{x}^\sigma) = \bigcap_{n \geq 1} \mathrm{Hom}_{W_n}(\underline{x}, \underline{x}^\sigma)$$

pero si p descompone en K se cumple además que todos estos espacios son iguales. Una consecuencia directa de esto es que si $r_{\mathscr{A}}(m) = 0$ y p descompone entonces $(\underline{x} \cdot T_m \underline{x}^\sigma) = 0$ porque no hay elementos de orden m en $\mathrm{Hom}_W(\underline{x}, \underline{x}^\sigma) = \mathrm{Hom}_{W_n}(\underline{x}, \underline{x}^\sigma)$ para todo $n \geq 1$. Esto nos da la siguiente proposición.

Proposición 4.13. *Si $N \nmid m$ y $r_{\mathscr{A}}(m) = 0$ entonces $(\underline{x} \cdot T_m \underline{x}^\sigma) = 0$.*

Los casos p inerte y p ramificado requieren más trabajo y se tratan aparte. Observemos que estos son los casos en que el primo racional al que divide v tiene un sólo primo de K en su factorización.

Teorema 4.14. *Sea v un lugar finito de H, digamos $v \mid p$ donde p es un primo racional. Entonces la curva reducida $\tilde{E} = E \pmod v$ es una curva elíptica sobre un cuerpo finito de característica p, y su reducción es supersingular si y sólo si p ramifica o es inerte.*

El Teorema anterior nos dice que si p ramifica o es inerte en K entonces el anillo de endomorfismos $\mathrm{End}_{W_1}(\underline{x})$ es isomorfo a un orden maximal R en el álgebra de cuaterniones $B = B_{p,\infty}$. Luego tenemos $\mathrm{End}_{W_1}(\underline{x}) \simeq R$ y $\mathrm{End}_W(\underline{x}) \simeq \mathcal{O}_K$. Vale de hecho la siguiente proposición más general:

Proposición 4.15.
Si $v \mid p$, donde p no descompone, entonces $\mathrm{End}_{W_n}(\underline{x}) \simeq \mathcal{O}_K + p^{n-1}R$.

Donde los casos anteriores corresponden a tomar $n = 1$ y $n \to \infty$.

Sea R el orden de arriba, entonces $R_p \coloneqq R \otimes \mathbb{Z}_p$ es un orden maximal en $B_p = B \otimes \mathbb{Q}_p$ y tenemos una inmersión $\mathcal{O}_K \hookrightarrow R$ que se extiende a $K \hookrightarrow B$. Entonces tenemos un generador del álgebra de cuaterniones B de la forma $\{1, i, j, ij\}$ donde $i^2 = D$, $j^2 \in \mathbb{Z}$ e $ij = -ji$; conjugar por i da lugar a una involución $a + bi + cj + dij \mapsto a + bi - (c + di)j$ que descompone B en dos subespacios propios $B = K \oplus Kj$. La norma de un elemento en

el álgebra es $\mathrm{N}(a+bi+cj+dij) = a^2 - Db^2 - j^2c^2 + j^2Dd^2$ y respeta esta descomposición. Entonces, para un elemento $\alpha + \beta j \in B$ podemos escribir $\mathrm{N}(\alpha+\beta j) = \mathrm{N}(\alpha) - j^2\,\mathrm{N}(\beta)$. Los elementos del anillo $\mathrm{End}_{W_n}(\underline{x})$ vienen caracterizados por $\mathrm{N}(\beta)$.

PROPOSICIÓN 4.16. *Si $v \mid p$ donde p no descompone, entonces*

1.

$$\mathrm{End}_{W_n}(\underline{x}) \simeq \begin{cases} \{\alpha+\beta j \in R:\ j^2\,\mathrm{N}(\beta) \equiv 0 \pmod{p^{2n-1}}\} & \text{si } p \text{ es inerte} \\ \{\alpha+\beta j \in R:\ j^2\,\mathrm{N}(\beta) \equiv 0 \pmod{p^{n-1}}\} & \text{si } p \text{ ramifica } (p = |D|) \end{cases}$$

2. $\mathrm{Hom}_{W_n}(\underline{x}, \underline{x}^\sigma) \simeq \mathrm{End}_{W_n}(\underline{x}) \cdot \mathfrak{a} \subseteq B$ *donde* $\mathfrak{a}$ *es cualquier elemento en la clase de ideales* $\mathscr{A}$*, asociada a* σ *vía el mapa de Artin. Además, si la isogenia* ϕ *se corresponde con* $b \in B$ *entonces* $\deg(\phi) = \frac{\mathrm{N}(b)}{\mathrm{N}(\mathfrak{a})}$.

COROLARIO 4.17. *Sea v un lugar finito dividiendo a p, un primo inerte. Si $N \nmid m$ y $r_{\mathscr{A}}(m) = 0$, entonces*

$$(\underline{x} \cdot T_m \underline{x}^\sigma) = \sum_{\substack{\alpha+\beta j \in R\mathfrak{a}/\pm 1 \\ \mathrm{N}(\alpha+\beta j) = m\,\mathrm{N}(a) \\ \beta \neq 0}} \frac{1}{2}\left[1 + \mathrm{ord}_p(j^2\,\mathrm{N}(\beta))\right]$$

DEMOSTRACIÓN. Por 4.11 y la proposición anterior

$$\begin{aligned}(\underline{x} \cdot T_m \underline{x}^\sigma) &= \frac{1}{2}\sum_{n=0}^{\infty} \#\,\mathrm{Hom}_{W_n}(\underline{x}, \underline{x}^\sigma)_{\deg m} \\ &= \frac{1}{2}\sum_{n=0}^{\infty} \#\{\alpha+\beta j \in R\mathfrak{a}:\ \mathrm{N}(\alpha+\beta j) = m\,\mathrm{N}(\mathfrak{a}),\ j^2\,\mathrm{N}(\beta) \equiv 0 \pmod{p^{2n-1}}\} \\ &= \sum_{\substack{\alpha+\beta j \in R\mathfrak{a}/\pm 1 \\ \mathrm{N}(\alpha+\beta j) = m\,\mathrm{N}(a) \\ \beta \neq 0}} \frac{1}{2}\left[1 + \mathrm{ord}_p(j^2\,\mathrm{N}(\beta)\right].\end{aligned}$$

■

De forma similar se tiene una fórmula para el caso ramificado.

COROLARIO 4.18. *Sea v un lugar finito dividiendo a p, un primo que ramifica. Si $N \nmid m$ y $r_{\mathscr{A}}(m) = 0$, entonces*

$$(\underline{x} \cdot T_m \underline{x}^\sigma) = \sum_{\substack{\alpha+\beta j \in R\mathfrak{a}/\pm 1 \\ \mathrm{N}(\alpha+\beta j) = m\,\mathrm{N}(a) \\ \beta \neq 0}} \mathrm{ord}_p(j^2\,\mathrm{N}(\beta))$$

Pero nosotros queremos una expresión que sólo dependa de K, y no del álgebra B, para esto hay que sumar sobre todos los lugares dividiendo a p y estudiar el álgebra de cuaterniones B.

PROPOSICIÓN 4.19. *Si p es inerte en K y $r_{\mathscr{A}}(m) = 0$ entonces*

$$\sum_{v \mid p} \langle \underline{x}, T_m \underline{x}^\sigma \rangle_v = -\left(\sum_{\substack{0 < n < \frac{m|D|}{N} \\ p \mid n}} \mathrm{ord}_p(pn) r_{\mathscr{A}}(m|D| - Nn)\delta(n) R(n/p) \right) \log p$$

DEMOSTRACIÓN. Comencemos considerando q un primo tal que $q \equiv -p \pmod D$, que existe por el Teorema de Dirichlet en progresiones aritméticas. Por su definición este primo descompone como $q = \mathfrak{q}\bar{\mathfrak{q}}$. El álgebra de cuaterniones $(D, -pq)_{\mathbb{Q}}$ ramifica en $\{p, \infty\}$ y podemos escribir $B = K \oplus Kj$, $j^2 = -pq$ de forma que ahora nuestra inmersión es la inclusión. Dado un orden R existe $\mathfrak{b} \in \mathcal{O}_K$ tal que $R\mathfrak{b} = \mathfrak{b}S$ en B, donde

$$S = \{\alpha + \beta j : \alpha \in \mathfrak{d}^{-1},\ \beta \in \mathfrak{d}^{-1}\mathfrak{q}^{-1}\mathfrak{n},\ \alpha \equiv \beta \pmod{\mathfrak{d}}\} \quad (\mathfrak{d} = \sqrt{D}\mathcal{O}_K)$$

(ver [5, p. 118]). La clase de dicho $\mathfrak{b}$ depende del v que tomamos. Supongamos que tenemos dos lugares $v' \neq v$ dividiendo al primo p, entonces $v' = v^{\sigma_{\mathscr{C}}}$ para alguna clase de ideales $\mathscr{C}$ y $[\mathfrak{b}_{v'}] = [\mathfrak{b}_v]\mathscr{C}$, por lo que cuando sumemos sobre todas las clases de ideales aparecerán las clases asociadas a cada $v \mid p$.
Si $\mathfrak{b}$ es tal que $R\mathfrak{b} = \mathfrak{b}S$ entonces

$$R\mathfrak{a} = \{\alpha + \beta j : \alpha \in \mathfrak{d}^{-1}\mathfrak{a}, \beta \in \mathfrak{d}^{-1}\mathfrak{q}^{-1}\mathfrak{n}\bar{\mathfrak{b}}\mathfrak{b}^{-1}\bar{\mathfrak{a}}, \alpha \equiv \beta \pmod{\mathfrak{d}}\}.$$

Supongamos que tenemos un elemento $\alpha + \beta j \in R\mathfrak{a}$ que aporta en la suma, es decir, $\mathrm{N}(\alpha) + pq(\mathrm{N}(\beta)) = m\,\mathrm{N}(\mathfrak{a})$ y $\beta \neq 0$. Si ahora definimos los ideales

$$\mathfrak{c} = (\alpha)\mathfrak{d}\mathfrak{a}^{-1} \in \mathscr{A}^{-1} \qquad \mathfrak{c}' = (\beta)\mathfrak{d}\mathfrak{q}\mathfrak{n}^{-1}\bar{\mathfrak{b}}^{-1}\mathfrak{b}\bar{\mathfrak{a}}^{-1} \in \mathscr{A}\mathscr{B}^2[\mathfrak{q}\mathfrak{n}^{-1}]$$

tenemos que

(4.12)

$$\mathrm{N}(\mathfrak{c}) + Np\,\mathrm{N}(\mathfrak{c}') = |D|\,\mathrm{N}(\alpha)\,\mathrm{N}(\mathfrak{a})^{-1} + Np|D|\,\mathrm{N}(\beta)qN^{-1}\,\mathrm{N}(\mathfrak{a})^{-1} = \mathrm{N}(\alpha) + pq\,\mathrm{N}(\beta) = m|D|.$$

Recíprocamente, si tenemos dos ideales $\mathfrak{c} \in \mathscr{A}^{-1}$ y $\mathfrak{c}' \in \mathscr{A}\mathscr{B}^2[\mathfrak{q}\mathfrak{n}^{-1}]$ que cumplen 4.12 entonces α y β quedan determinados a menos de signo y $\alpha + \beta j$ es un elemento de $R\mathfrak{a}$ si y solo si $\alpha \equiv \beta \pmod{\mathfrak{d}}$. La igualdad $\mathrm{N}(\alpha) + pq\,\mathrm{N}(\beta) = m\,\mathrm{N}(\mathfrak{a}) \in \mathcal{O}_K$ implica que $\alpha \equiv \beta \pmod{\mathfrak{d}}$ o $\alpha \equiv -\beta \pmod{\mathfrak{d}}$ (y no ocurren las dos porque $\mathrm{N}(\beta) \neq 0$).

En suma, hay una correspondencia 2 a 1 entre los pares de ideales $(\mathfrak{c}, \mathfrak{c}')$ como antes y los elementos de $R\mathfrak{a}$. Pero además, el elemento $b = \alpha + \beta j$ que determina siempre está en algún orden conjugado $R'\mathfrak{a}$ que corresponde a tomar otro $v \mid p$. La proposición se sigue de observar que si denotamos $n = \mathrm{N}(\mathfrak{c}')$ entonces $\mathrm{ord}_p(n) = \mathrm{ord}_p(pq\,\mathrm{N}(\beta))$ y $\mathrm{N}(\mathfrak{c}) = m|D| - nN$. ∎

Nuevamente, el caso ramificado se resuelve de forma similar.

PROPOSICIÓN 4.20. *Si p ramifica en K y $r_{\mathscr{A}}(m) = 0$ entonces*

$$\sum_{v|p} \langle \underline{x}, T_m \underline{x}^{\sigma} \rangle_v = -\Bigg(\sum_{\substack{0<n<\frac{m|D|}{N} \\ p|n}} \mathrm{ord}_p(pn) r_{\mathscr{A}}(m|D| - Nn)\delta(n)R(n/p) \Bigg) \log p$$

Como ya mencionamos, las pruebas para el caso $r_{\mathscr{A}}(m) = 0$ se pueden adaptar al caso general. Cuando $r_{\mathscr{A}}(m)$ es no nulo aparece un factor extra en $(\underline{x} \cdot T_m(\underline{x})^{\sigma})$ que en general viene dado por un término de la forma $\mathrm{C} \cdot r_{\mathscr{A}}(m)\,\mathrm{ord}_p(m)$.

La fórmula general nos la da el siguiente teorema.

TEOREMA 4.21. *Sea m coprimo con N.*

(a) Si p descompone en K entonces

$$\sum_{v|p} \langle \underline{x}, T_m \underline{x}^{\sigma} \rangle_v = -\,\mathrm{h}\, r_{\mathscr{A}}(m)\mathrm{ord}_p(m/N) \log p$$

(b) Si p es inerte en K entonces

$$\sum_{v|p}\langle \underline{x}, T_m\underline{x}^{\sigma}\rangle_v = \left(-\mathrm{h}\, r_{\mathscr{A}}(m)\,\mathrm{ord}_p(m) - \sum_{\substack{0<n<\frac{m|D|}{N}\\ p|n}} \mathrm{ord}_p(pn) r_{\mathscr{A}}(m|D|-Nn)\delta(n)R(n/p)\right)\log p$$

(c) Si p ramifica en K entonces

$$\sum_{v|p}\langle \underline{x}, T_m\underline{x}^{\sigma}\rangle_v = \left(-\mathrm{h}\, r_{\mathscr{A}}(m)\,\mathrm{ord}_p(m) - \sum_{\substack{0<n<\frac{m|D|}{N}\\ p|n}} \mathrm{ord}_p(n) r_{\mathscr{A}}(m|D|-Nn)\delta(n)R(n/p)\right)\log p$$

Y sumando sobre todos los lugares se llega a la fórmula central de esta sección:

$$\sum_{v \text{ finito}} \langle c, T_m d^{\sigma}\rangle_v = - \sum_{0<n\leq \frac{m|D|}{N}} \sigma'_{\mathscr{A}}(n) r_{\mathscr{A}}(m|D| - nN) + \mathrm{h}\, r_{\mathscr{A}}(m)\log\frac{N}{m} \tag{4.13}$$

Capítulo 5

La prueba del Teorema y aplicaciones

1. El resultado principal

Con los resultados obtenidos en los dos capítulos anteriores estamos en condiciones de ver la prueba al teorema principal. Comencemos recordando nuestras hipótesis.

- K es un cuerpo cuadrático imaginario de discriminante primo $D < -4$ y N es un primo distinto tal que $\varepsilon(N) = 1$.
- x es un punto de Heegner y $c = (x) - (\infty)$ en $J(H)$. Este elemento existe porque N satisface la Hipótesis de Heegner HH.
- f es una forma nueva de peso 2 para $\Gamma_0(N)$.
- $\mathscr{A}$ es una clase de ideales en $\mathcal{O}_K$ y $\sigma_{\mathscr{A}} \in \mathrm{Gal}(H/K)$ el elemento correspondiente vía el mapa de Artin.

Bajo estas hipótesis, tenemos el teorema de Gross–Zagier.

Teorema 5.1. *La serie*

$$g_{\mathscr{A}}(z) = \sum_{m \geq 0} \langle c, T_m c^{\sigma} \rangle q^m$$

es una forma modular cuspidal de peso 2 *para* $\Gamma_0(N)$ *y*

$$(f, g_{\mathscr{A}})_{\Gamma_0(N)} = \frac{\sqrt{D}}{8\pi} L'_{\mathscr{A}}(f, 1).$$

Demostración. La prueba se divide en dos partes.

$g_{\mathscr{A}} \in S_2(\Gamma_0(N))$:

Si J es una variedad abeliana cualquiera (variedad algebraica proyectiva con ley de grupo) y $T_O J$ el espacio tangente a J en el neutro O, tenemos una acción natural de $\mathrm{End}(J)$ en $T_O J$ que está dada por $\phi \cdot \omega = \omega \circ d_o \phi$. La acción anterior es fiel, lo que significa que el mapa que induce $\mathrm{End}_{\mathbb{Q}} J \to \mathrm{End}_{\mathbb{Q}} T_O J$ es inyectivo, esto ocurre porque si ϕ es una isogenía no trivial entonces es sobreyectiva, luego $d_0\phi$ también lo es y por lo tanto $\phi \cdot \omega = 0 \iff T_O J \subseteq \mathrm{Ker}\omega \iff \omega = 0$. Ahora, cuando J es el Jacobiano de la curva modular el espacio tangente se puede identificar con el espacio de formas cuspidales de peso 2 para $\Gamma_0(N)$ con coeficientes racionales en su expansión de Fourier, denotemos este espacio por S. Observemos que $S \otimes \mathbb{C} \simeq S_2(\Gamma_0(N))$.

El álgebra de Hecke $\mathbb{T}$ es la subalgebra de $\mathrm{End}_{\mathbb{Q}} J$ generada por los operadores de Hecke, de lo que mencionamos en el párrafo anterior se deduce que tenemos un mapa inyectivo

$$\mathbb{T} \hookrightarrow \mathrm{End}_{\mathbb{Q}} J \to \mathrm{End}_{\mathbb{Q}} S$$

lo que en particular implica que $\dim_{\mathbb{Q}} \mathbb{T} \leq d^2$ donde $d = \dim_{\mathbb{Q}} S = \dim_{\mathbb{C}} S_2(\Gamma_0(N))$. Denotemos por a_m al mapa que envía una forma modular en S a su m-ésimo coeficiente en la expansión de Fourier. Si componemos la acción de $\mathbb{T}$ en S con a_1 obtenemos un mapa bilineal $\beta : \mathbb{T} \times S \to \mathbb{Q}$ definido por $\beta(T, f) = a_1(Tf)$, si vemos que el mapa $f \mapsto \beta(\cdot, f)$ es un isomorfismo entre S y $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{T}, \mathbb{Q})$ entonces extendiendo escalares tendremos un isomorfismo entre $S_2(\Gamma_0(N))$ y $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{T}, \mathbb{C})$, lo cual en particular implica que existe $f \in S_2(\Gamma_0(N))$ tal que $\beta(\cdot, f)$ representa al mapa $T \mapsto \langle c, Tc^\sigma \rangle$, es decir,

$$a_m(f) = a_1(T_m f) = \langle c, T_m c^\sigma \rangle$$

como deseamos. Como β es un mapa bilineal y $\mathbb{T}, S$ son finito dimensionales sobre $\mathbb{Q}$ para ver que el mapa $f \mapsto \beta(\cdot, f)$ es un isomorfismo alcanza con chequear que $f \mapsto \beta(\cdot, f)$ y $T \mapsto \beta(T, \cdot)$ son mapas inyectivos.

- Si $\beta(T, f) = 0$ para todo $T \in \mathbb{T}$ entonces en particular $a_m(f) = a_1(T_m(f)) = 0$ para todo $m \geq 0$, lo que implica que $f = 0$.
- Si $\beta(T, f) = 0$ para toda $f \in S$ entonces $\beta(T, T_m f) = 0$ para toda $f \in S$, $m \geq 0$. Luego $a_1(TT_m f) = a_1(T_m T f) = a_m T f = 0$ y por lo tanto $T = 0$.

Prueba de la fórmula

Para simplificar la notación volvamos a usar las siguientes constantes

$$\begin{aligned} A &= 2\frac{L'}{L}(1, \varepsilon) - 2\gamma \\ B &= \log \frac{N}{|D|} + 2\frac{\log N}{N-1} + 2 + 2\frac{\zeta'}{\zeta}(2) - 2\frac{L'}{L}(1, \varepsilon) \\ k_N &= \frac{-12}{N+1} \end{aligned}$$

Observemos que k_N coincide con el definido como el residuo del resolvente que apareció en el capítulo 3 sección 1 donde obtuvimos la igualdad

$$\begin{aligned} \sum_{v|\infty} \langle c, T_m d^\sigma \rangle_v = \lim_{s \to 1} \left[-2 \sum_{n=1}^{\infty} \sigma_{\mathscr{A}}(n) r_{\mathscr{A}}(m|D| + nN) Q_{s-1} \left(1 + \frac{2nN}{m|D|} - \frac{\mathrm{h}\, k_N \sigma_1(m)}{s-1} \right) \right] \\ + \mathrm{h}\, k_N \left[\sigma_1(m) B + \sum_{j|m} j \log \frac{m}{j^2} \right] + \mathrm{h}\, r_{\mathscr{A}}(m) \left[A + \log \frac{|D|}{4\pi^2} \right] \end{aligned}$$

para m coprimo con N. En la sección 2 del mismo capítulo obtuvimos la igualdad

$$\sum_{v \text{ finito}} \langle c, T_m d^\sigma \rangle_v = - \sum_{0 < n \leq \frac{m|D|}{N}} \sigma'_{\mathscr{A}}(n) r_{\mathscr{A}}(m|D| - nN) + \mathrm{h}\, r_{\mathscr{A}}(m) \log \frac{N}{m}$$

Y sumando ambas fórmulas obtenemos una para la altura global

$$\begin{aligned}\sum_v \langle c, T_m d^\sigma\rangle = &- \sum_{0<n\leq \frac{m|D|}{N}} \sigma'_{\mathscr{A}}(n) r_{\mathscr{A}}(m|D| - nN) \\ &+ \lim_{s\to 1}\left[-2\sum_{n=1}^{\infty}\sigma_{\mathscr{A}}(n) r_{\mathscr{A}}(m|D|+nN) Q_{s-1}\left(1+\frac{2nN}{m|D|} - \frac{\mathrm{h}\, k_N \sigma_1(m)}{s-1}\right)\right] \\ &+ \mathrm{h}\, k_N \left[\sigma_1(m) B + \sum_{j|m} j \log\frac{m}{j^2}\right] + \mathrm{h}\, r_{\mathscr{A}}(m)\left[A + \log\frac{|D|N}{4\pi^2 m}\right]\end{aligned}$$

que coincide con el coeficiente de Fourier $a_{m,\mathscr{A}}$ hallado en 3.25! Entonces los coeficientes de Fourier de $g_{\mathscr{A}}$ y $\phi_{\mathscr{A}}$ coinciden excepto cuando $\gcd(m, N) > 1$, pero esto implica que ambas formas difieren por una forma vieja en $\Gamma_0(N)$ y esto no afecta el producto de Petersson pues por definición las formas viejas son ortogonales a f. Observemos que obtuvimos la altura global $\langle c, T_m d^\sigma\rangle_v$ y no $\langle c, T_m c^\sigma\rangle_v$, pero estas coinciden por el teorema de Manin-Drinfeld, que establece que la diferencia entre dos cúspides de la curva modular tiene orden finito en el Jacobiano y en consecuencia altura 0. ■

Sumando sobre todas las posibles clases de ideales $\mathscr{A}$ en $\mathcal{O}_K$ obtenemos la fórmula para $L'(f, 1)$

Teorema 5.2.

$$L'(f,1) = \frac{8\pi^2}{\sqrt{|D|}}(f,f)_{\Gamma_0(N)}$$

Demostración. Consideremos la traza de c, $\tilde{c} := \sum_{\mathscr{A}\in Cl_K} c^{\sigma_{\mathscr{A}}}$, entonces

$$\langle \tilde{c}, T_m \tilde{c}\rangle = \mathrm{h} \sum_{\mathscr{A}\in Cl_K} \langle c, T_m c^{\sigma_{\mathscr{A}}}\rangle$$

y por lo tanto

$$L'(f,1) = \frac{8\pi^2}{\sqrt{|D|}}(f, \sum_{\mathscr{A}\in Cl_K} g_{\mathscr{A}})_{\Gamma_0(N)}$$

donde

$$\sum_{\mathscr{A}\in Cl_K} g_{\mathscr{A}} = \frac{1}{\mathrm{h}} \sum_{m\geq 1} \langle \tilde{c}, T_m \tilde{c}\rangle q^m.$$

La primera parte en la prueba del Teorema previo nos dice que si tomamos una base ortonormal $\{f_1 = f, \ldots, f_n\}$ de $S_2(\Gamma_0(N))$ entonces nuestro $\tilde{c}$ se descompone como $\tilde{c} = \sum_{i=1}^{n} \tilde{c}_i$, donde $T_m(\tilde{c}_i) = a_m(f_i)\tilde{c}_i$ (basicamente nos dice que tenemos $\tilde{c}_i$ asociados a las formas nuevas f_i que son autovectores de T_m con el mismo valor propio $a_m(f_i)$). Luego

$$L'(f,1) = \frac{8\pi^2}{\sqrt{|D|}}\left(f, \frac{1}{\mathrm{h}}\sum_{m\geq 1}\langle \tilde{c}, T_m\tilde{c}\rangle q^m\right)_{\Gamma_0(N)} = \frac{8\pi^2}{\sqrt{|D|}}\left(f, \frac{1}{\mathrm{h}}\sum_{i,j\leq n}\langle \tilde{c}_i, \tilde{c}_j\rangle f_j\right)_{\Gamma_0(N)}$$

Como la base es ortonormal $(f_1, f_j) = 0$ si $j \neq 1$, por lo que

$$L'(f,1) = \frac{8\pi^2}{\mathrm{h}\sqrt{|D|}}\left(f, \sum_{i\leq n}\langle \tilde{c}_i, \tilde{c}_1\rangle f_1\right)_{\Gamma_0(N)}$$

Los $\tilde{c}_i$ son vectores propios de T_m para todo m y como las f_i son distintas difieren en al menos un coeficiente: $a_n(f_1) \neq a_n(f_i)$, lo que se traduce en que $\tilde{c}_1$ y $\tilde{c}_j$ son ortogonales por pertenecer a espacios propios distintos para el operador T_n. Concluimos que

$$L'(f,1) = \frac{8\pi^2}{\mathrm{h}\sqrt{|D|}} h(\tilde{c}_1)\,(f,f)_{\Gamma_0(N)}\,.$$

■

Esto concluye la prueba del Teorema, ahora es natural preguntarnos sobre generalizaciones de este resultado.

2. Generalizaciones

El Teorema fue probado con más generalidad que la aquí presentada. Las hipótesis originales son: D un discriminante fundamental y N tal que $\varepsilon(p) = 1$ para todo $p \mid N$, la última hipótesis implica la Hipótesis de Heegner (existe un ideal primitivo de norma N) que es requerida para la existencia de Puntos de Heegner de discriminante D en $X_0(N)$. Podríamos preguntarnos que pasa si $\varepsilon(N) = 1$ pero existe algún $p \mid N$ con $\varepsilon(N) \neq 1$; en este caso también hay una fórmula que relaciona puntos de Heegner con la derivada de la L-serie pero dichos puntos de Heegner son puntos en una curva de Shimura.

Es importante resaltar que el lado analítico de la prueba, que involucra las L-series de Rankin, no asume ninguna condición sobre N más que ser coprimo con D. Cuando $\varepsilon(N) = -1$ la L-serie no se anula en $s = 1$ y su valor allí también admite una interpretación algebraica como la altura de cierto punto especial en una curva asociada a un álgebra de cuaterniones sobre $\mathbb{Q}$; este resultado fue establecido por Gross en [8] y una presentación sobre el mismo puede verse en [18]. Cuando $\varepsilon(N) = 1$ se obtiene la fórmula que vimos, que no requiere ninguna otra suposición sobre N.

El caso $N = 1$ merece mencionarse aparte, no hay curvas elípticas de conductor 1 entonces la fórmula es trivial, además la curva modular $X_0(N)$ tiene género 0 y por lo tanto su Jacobiano y la altura global son triviales siempre; sin embargo tiene sentido estudiar las alturas locales arquimedianas y no arquimedianas con las mismas técnicas que antes y ver sus relaciones; esto da lugar a expresiones analíticas y algebraicas involucrando los puntos cuadráticos en el semiplano superior. En particular, en su artículo [10] Gross y Zagier dan dos pruebas diferentes para encontrar la factorización de enteros del tipo $N_{\mathbb{Q}}(j(\tau_1) - (\tau_2))$, luego en 2002 hallaron una fórmula relacionando la traza de estos puntos con los coeficientes de una forma modular de peso $\frac{3}{2}$.

3. BSD

La Conjetura Birch-Swinnerton-Dyer ($\sim$ 1960) predice que el rango algebraico y analítico de una curva elíptica E definida sobre un cuerpo de números K coincide con su

rango algebraico, más aún, predice la siguiente fórmula

$$\frac{L^r(E)}{r!} = \frac{\#Ш\omega_1 R_E \prod_{p|N} c_p}{\#(E_{\text{tor}})^2}$$

donde $r = \text{ord}_{s=1} L_E$, E_{tor} son los puntos de torsión de la curva sobre K, $\#Ш$ es el orden del grupo de Shafarevich-Tate, ω_1 es el período real de la curva, R_E es el regulador que se define a partir de la altura de una base de puntos racionales y los c_p son ciertos enteros llamados números de Tamawaga. Observemos que en particular la conjetura implica que el Ш es finito! Cuando $r_{\text{an}} = 1$ la fórmula de Gross–Zagier da la desigualdad $r_{\text{alg}}(E) \geq r_{\text{an}}(E)$ para curvas elípticas sobre $\mathbb{Q}$, Kolyvagin (1989) luego mostró que el rango debe ser exactamente uno, estos resultados juntos prueban BSD para rango analítico igual a 1.

4. El problema del número de clases

> Dear Dick,
>
> Wonderful news. Does this mean that in particular you can show $L' = 0$ when it ought to (thus fulfilling Dorian Goldfeld's requirements?).
>
> Will send O/P when Xmas recedes — at the moment all offices, not to mention the mail system, are inert.
>
> Yours,
> Bryan

Carta de Birch a Gross, 27 de diciembre de 1982.

El problema de encontrar un algoritmo *efectivo* que determine todos los cuerpos cuadráticos imaginarios con un número de clases dado se conoce como el Problema del número de clases de Gauss. En el año 1935 Siegel probó el siguiente Teorema:

Teorema 5.3. *(Siegel) Sea $d < 0$ un discriminante fundamental. Para todo $\varepsilon > 0$ existe $c > 0$ tal que*

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

Y este fue mejorado por Tatuzawa en 1951:

Teorema 5.4 (Tatuzawa). *Sea $0 < \varepsilon < \frac{1}{11.2}$, si $|d| > e^{\frac{1}{\varepsilon}}$ entonces*

$$\text{h}(d) > \frac{0.655\ \omega}{2\pi}|d|^{\frac{1}{2}-\varepsilon}$$

excepto, a lo sumo, para un discriminante d.

Pero la constante en el Teorema de Siegel no se puede calcular de forma efectiva y la posible excepción de un discriminante en el Teorema de Tatuzawa hace que el problema de la efectividad siga estando. En 1976 Dorian Goldfeld prueba el siguiente Teorema

TEOREMA 5.5 (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*

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

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

y resuelve el Problema del número de clases, a menos de encontrar una curva elíptica que tenga un cero de orden al menos 3 en $s = 1$. Finalmente, con el Teorema de Gross y Zagier se demuestra que la curva $E : -139y^2 = x^3 + 4x^2 - 48x + 80$ de conductor $37 \cdot (139)^2$ cumple este requisito. Pero la cota que se obtiene usando esta curva en el Teorema de Goldfeld no es lo suficientemente buena. Por ejemplo, para $\mathrm{h}(-d) \leq 100$ se obtiene $d \leq \exp 26880000$, y en la práctica esta cota no ha permitido listar los cuerpos cuadráticos imaginarios con número de clases mayor a 7. Watkins modificó las técnicas empleadas para dar esta cota y probó que $d \leq 2^{162}$ para $\mathrm{h}(-d) \leq 100$, lo cual le permitió completar la clasificación de cuerpos cuadráticos imaginarios con número de clases $\mathrm{h} \leq 100$.

Bibliografía

[1] Carolina Chiesa. *El problema del número de clases de Gauss: la solución de Goldfeld-Oesterlé*. https://hdl.handle.net/20.500.12008/39904. 2023.

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

[3] Henri Darmon y Shou-Wu Zhang. *Heegner Points and Rankin L-Series*. Cambridge University Press, 2010. ISBN: 9780511756375. URL: https://doi.org/10.1017/CBO9780511756375.

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

[5] M. Eichler. *Lectures on Modular Correspondences*. Tata Institute of Fundamental Research, Bombay, 1957, pág. 118.

[6] Camilo Gallardo. *El Teorema de Mazur*. https://www.cmat.edu.uy/biblioteca/monografias-y-tesis/tesis-de-maestria. 2024.

[7] B. Gross. «Heegner Points on X0(N)». En: *Rankin, R.A. (ed): Modular forms* (1986), págs. 87-106.

[8] B. Gross. «Heights and the special values of L-series». En: *Conference Proceedings of the CMS* 7 (1986), págs. 225-320.

[9] B. Gross y D. Zagier. «Heegner points and derivatives of L-series.» En: *Inventiones mathematicae* 84 (1986), págs. 225-320. URL: http://eudml.org/doc/143341.

[10] B.H. Gross y D. Zagier. «On singular moduli.» En: *Journal für die reine und angewandte Mathematik* 355 (1984), págs. 191-220. URL: http://eudml.org/doc/152694.

[11] Dennis A. Hejhal. *The Selberg Trace Formula for PSL (2,R)*. Springer, 1983, págs. 29-42. ISBN: 978-3-540-40914-4. DOI: https://doi.org/10.1007/BFb0061302.

[12] Jürgen Jost. *Compact Riemann Surfaces: An Introduction to Contemporary Mathematics*. Springer-Verlag, ene. de 2006. ISBN: 978-3-540-33065-3. DOI: 10.1007/978-3-540-33067-7.

[13] The LMFDB Collaboration. *The L-functions and modular forms database*. https://www.lmfdb.org. [Online; accessed 26 March 2025]. 2025.

[14] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994. ISBN: 9780387943251.

[15] Joseph H. Silverman y John T. Tate. *Rational Points on Elliptic Curves*. 2nd. Springer Publishing Company, Incorporated, 2015. ISBN: 331918587X.

[16] Vijay Srinivasan. *Notes for Gross–Zagier seminar*. https://math.mit.edu/ vijayrs/GZ/. 2022.

[17] Gonzalo Tornaría. *Notas para AGRA II: Formas modulares cuaterniónicas*. https://webusers.imj-prg.fr/ harald.helfgott/agraweb/notes-es.html. 2015.

[18] Soledad Villar. *La fórmula de Gross sobre alturas y valores especiales de L-series*. https://hdl.handle.net/20.500.12008/5467. 2012.

[19] John Voight. *Quaternion Algebras*. Springer, ene. de 2021. ISBN: 978-3-030-56692-0. DOI: 10.1007/978-3-030-56694-4.

[20] D. Zagier. «Modular points, modular curves, modular surfaces and modular forms». En: *Arbeitstagung Bonn 1984*. Ed. por Friedrich Hirzebruch, Joachim Schwermer y Silke Suter. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, págs. 225-248. ISBN: 978-3-540-39298-9.

[21] D. Zagier, W. Kohnen y B. Gross. «Heegner Points and Derivatives of L-Series. II.» En: *Mathematische Annalen* 278 (1987), págs. 497-562. URL: http://eudml.org/doc/164302.