Trabajo monográfico

Curvas elípticas, formas modulares y el problema de los números congruentes

Gerónimo de León Ramírez

Orientador:

Dr. Gustavo Rama
Instituto de Matemática y Estadística Rafael Laguardia

Licenciatura en Matemática
Universidad de la República
Montevideo, Uruguay

Resumen

Las curvas elípticas y las formas modulares son unos de los objetos más estudiados en la teoría de números moderna, siendo las primeras un objeto también de la geometría algebraica y las segundas del análisis complejo. En esta monografía, nos introduciremos en el estudio de ambas, teniendo como leitmotiv el problema de los números congruentes, que contaremos enseguida. Daremos tres enunciados equivalentes en términos de curvas elípticas, L-series y formas modulares, de los cuales una implicancia depende de la conjetura de Birch y Swinnerton-Dyer, uno de los siete problemas del milenio del instituto Clay, que servirán como cadena para saber si un número es congruente.

Este trabajo se basa principalmente en el libro de Neal Koblitz *"Introduction to Elliptic Curves and Modular Forms"*[**Kob93**].

Agradecimientos

Este trabajo es el final de una aventura llena de experiencia, aprendizaje, estrés, levantadas temprano y acostadas tarde, jornadas de estudio, de juegos y de cervezas. Una aventura que, como dije en numerosas oportunidades, no hubiera podido hacer sin la ayuda y compañía de mucha gente. Intentaré recordarlos a todos, si me olvido de alguien, lo siento, es lo que hay.

Para empezar, a Gustavo, por orientarme este último año y pico y haberme propuesto el tema.

A Elena, Sofía, Taba y Fede, por habernos acompañado práctiamente toda la aventura, dentro y fuera de la matemática, desde Montevideo hasta Florianópolis, pasando por Valizas, con trucos, tragos, teoremas, llamados y gorros azules.

A Mel, por los febreros de diversión o de estudio, por la copañía en la joda, la cocina y los prácticos. A Rodri con sus diagramas, su emoción y su intensidad. A Pablo, Clara, Paula, Juan, Juan, Juan, Luciana, Nahuel, Santi, Alejo, Favio, Bellati. A Arya y a Sancho, por su presencia en los días más solitarios.

A todos los docentes con los que tuve el gusto de tener clase. En particular, a la Negra, por mostrarme que el álgebra es divertida y por estar siempre ahí, y al Gordo, por introducirme la amarga y enseñarme que siempre es un buen momento para hablar de matemática.

Al Agú y al Chiquito, por haber sido parte de mi aprendizaje.

Y por último, a mamá y a papá, por todo. Por haberme enseñado el mundo, por ayudarme a desfacer entuertos, por entrenarme para la vida y sus desafíos. Por enseñarme la brújula de la moral y por inculcarme el gusto por el saber. Por haberme dado todo el respeto y el amor que se puede pedir. Esta monografía se las dedico a ustedes, espero se enorgullezcan. Con un ranking a lo yankee porque esta vez lo merece: son las personas más importantes en mi vida, y lo serán siempre. Los amo.

Introducción

La matemática ha acompañado a la humanidad desde el comienzo de su historia, y la mayor influencia de la antigüedad la tenemos hoy desde la antigua Grecia. En esos lares y por aquellos tiempos, la matemática era vista casi únicamente en términos de la geometría euclideana, por lo que es entendible, aunque igualmente sorprendente, que el segundo libro con más ediciones publicadas (y uno de los más divulgados), después de la Biblia, sea *"Los elementos"*, de Euclides [**War21**, Página 73]. Los objetos más estudiados (o al menos es la sensación que me deja su influencia) fueron la circunferencia, con su constante π, y los triángulos rectángulos, con su famoso *Teorema de Pitágoras*.

Sobre éstos últimos, se han planteado y respondido muchas preguntas, siendo algunas tan difíciles que necesitaron siglos para obtener su respuesta. Una de éstas preguntas se la hicieron los antiguos griegos: ¿cuándo un número natural n es el área de un triángulo rectángulo con lados racionales? Un número con esa cualidad es un **número congruente**. Esta pregunta también se hicieron los árabes alrededor del siglo X, pero preferían trabajar con una equivalente: dado un n, ¿cuándo existe un racional x tal que $x, x+n$ y $x-n$ son los tres cuadrados de racionales? Esta será la primera proposición que veremos. Los matemáticos se preguntaron sobre estos números por muchísimos años. Euler, por ejemplo, fue el primero en mostrar que el 7 es un número congruente, y Fermat el primero en demostrar que el 1 no lo es. El problema que abordaremos será dar una manera simple de decidir cuándo un número natural n es congruente, que fue casi resuelto por Tunnell en 1983 mediante el siguiente teorema:

Teorema 1. *Sea n es un entero positivo libre de cuadrados. Si n es un número congruente, entonces:*

$$\begin{cases} \#\{x,y,z \in \mathbb{Z} : 2x^2+y^2+32z^2\} = \frac{1}{2}\#\{x,y,z \in \mathbb{Z} : n = 2x^2+y^2+8z^2\} \\ \textit{si } n \textit{ es impar;} \\ \#\{x,y,z \in \mathbb{Z} : 4x^2+y^2+32z^2\} = \frac{1}{2}\#\{x,y,z \in \mathbb{Z} : n = 4x^2+y^2+8z^2\} \\ \textit{si } n \textit{ es par.} \end{cases}$$

Si la conjetura débil de Birch y Swinnerton-Dyer es cierta para las curvas elípticas E_n, entonces el recíproco también es cierto, o sea, las igualdades de arriba implican que n es un número congruente.

El trabajo se divide en cuatro capítulos que funcionan de la siguiente forma: definimos un objeto, trabajamos con el mismo y al final, vemos cómo usarlo para

acercarnos a resolver el problema principal. En el primero introduciremos el problema y veremos curvas elípticas; en el segundo veremos las funciones L de Hasse-Weil y hablaremos sobre la conjetura de Birch y Swinnerton-Dyer; en el tercero veremos las formas modulares; y en el cuarto, con todo lo necesario ya definido, enunciaremos tres teoremas fuertes y veremos cómo se usan para terminar el problema.

Primero, a cada natural n le podemos asociar una curva $E_n : y^2 = x^3 - n^2x$, que resulta ser una curva elíptica sobre $\mathbb{Q}$. Una curva elíptica acepta estructura de grupo abeliano finitamente generado, y a la dimensión del subgrupo libre se le llama rango. El primer resultado al que llegamos es: que un número n sea es congruente equivale a que el rango de la curva elíptica E_n sea positivo.

Segundo, para una curva elíptica E_n, se define su correspondiente función compleja $L(E_n, s)$ como un producto infinito. El próximo gran resultado al que llegamos es a que esta función L se puede extender a una función meromorfa en todo el plano complejo. Luego, un teorema de Coates y Wiles nos dice que si la curva E_n tiene rango positivo, entonces $L(E_n, 1) = 0$, y si aceptamos la conjetura débil de Birch y Swinnerton-Dyer, que dice, en particular, que $L(E, 1) = 0$ si y sólo si el rango de la curva E es positivo, tenemos el recíproco. Esto, mediante la equivalencia mencionada anteriormente, nos acerca a lo que buscamos como solución del problema de los números congruentes.

Tercero y cuarto, están las formas modulares, que se pueden definir como funciones analíticas en el semiplano superior H holomorfas en el infinito que son invariantes bajo la acción de un subgrupo de $\mathrm{SL}_2(\mathbb{Z})$. Sobre estas, Shimura[**Shi73**] y Kohnen[**Koh80**], este último utilizando el teorema de Waldspurger[**Wal81a**][**Wal81b**], prueban que hay un isomorfismo entre las siguientes formas cuspidales:

$$S^+_{k/2}(\widetilde{\Gamma}_0(4)) \longrightarrow S_{k-1}(\Gamma),$$

Utilizando esto, Tunnell[**Tun83**] prueba que existe una forma modular f_1 con coeficientes relativamente sencillos de calcular para la cual $L(E_n, 1) = 0$ si y sólo si el coeficiente $n-$ésimo de f_1 es nulo. Juntando todo, tenemos lo que buscábamos (en la última página puede encontrar un esquema): una forma relativamente sencilla de saber si un número es congruente o no. El único paso que se necesitaría para que este problema de antaño se cierre, es que se pruebe la conjetura de Birch y Swinnerton-Dyer (o al menos, la conjetura débil), que al momento de escribir esta monografía es un problema abierto.

Índice general

Capítulo 1

De los números congruentes a las curvas elípticas

En este capítulo, definiremos lo que es un número congruente y probaremos algunas propiedades y equivalencias básicas de estos, veremos cómo asociarle cierta curva elíptica a cada natural n, definiremos y trabajaremos con curvas elípticas, usaremos retículos para probar que son un grupo abeliano y, al final, daremos una condición necesaria y suficiente para que un número sea congruente en términos de su curva elíptica asociada.

1. Números congruentes

Definición 1.1. Un número congruente es un $r \in \mathbb{Q}$ tal que existe un triángulo rectángulo de lados racionales con área r.

Ejemplo 1.1. El 6 es congruente ya que el triángulo de lados 3, 4 y 5 tiene área 6. Lo mismo para el 5, con triángulo de lados $(\frac{20}{3}, \frac{3}{2}, \frac{41}{6})$, y el 7, con triángulo $(\frac{24}{5}, \frac{35}{12}, \frac{337}{60})$.

Si r es un número congruente con triángulo asociado de lados X, Y, Z, existe $s \in \mathbb{Q}$ tal que $n = s^2 r$ es un natural libre de cuadrados. El área del triángulo sX, sY, sZ es n, por lo que podemos considerar sin pérdida de generalidad números congruentes naturales libres de cuadrados, que es lo que haremos de ahora en adelante.
Notar que en la definición de número congruente no pedimos que el triángulo sea único, de ahí que la siguiente proposición tiene sentido.

Proposición 1.1. *Sea n un entero positivo libre de cuadrados. Existe una correspondencia biyectiva entre los triángulos de lados racionales $X < Y < Z$ con área n y los números x tales que x, $x - n$ y $x + n$ son el cuadrado de un racional, y está dada por:*

$$X, Y, Z \longrightarrow x = \left(\frac{Z}{2}\right)^2, \tag{1.1}$$

$$x \longrightarrow X = \sqrt{x+n} - \sqrt{x-n},\ Y = \sqrt{x+n} + \sqrt{x-n},\ Z = 2\sqrt{x}.$$

Un número congruente es entonces un n para el que existe una solución racional al sistema

$$\begin{cases} X^2 + Y^2 = Z^2 \\ \frac{XY}{2} = n \end{cases} \tag{1.2}$$

que podemos, sumando y restando cuatro veces la segunda ecuación a la primera, relacionar en $(\frac{X\pm Y}{2})^2 = (\frac{Z}{2})^2 \pm n$. Si multiplicamos estas dos ecuaciones entre sí, obtenemos $(\frac{X^2-Y^2}{4})^2 = (\frac{Z}{2})^4 - n^2$, o sea que un n congruente nos da una solución racional a la ecuación $v^2 = u^4 - n^2$ siendo $v = \frac{X^2-Y^2}{2}$ y $u = \frac{Z}{2}$. Multiplicamos ahora por u^2 y obtenemos $(uv)^2 = u^6 - n^2u^2$. Si denotamos $x = u^2$ (notar que es el mismo x de la Prop. 1.1) e $y = uv$, tenemos que un número congruente n nos da una solución racional a la ecuación

$$y^2 = x^3 - n^2x. \tag{1.3}$$

El recíproco no es directamente cierto, o sea, si un punto (x, y) es solución a la ecuación, no quiere decir que la coordenada x venga de algún triángulo de área n ya que, para empezar, $x = u^2 = (\frac{Z^2}{4})$ tiene que ser el cuadrado de un racional. Segundo, el denominador de x debe ser par. Para ver esto, veamos que si el triángulo asociado a n es X, Y, Z, podemos multiplicar por algún racional s para que $X' = sX$, $Y' = sY$ y $Z' = sZ$ sean una terna de Pitagórica primitiva, esto es. una terna Pitagórica donde los lados son coprimos dos a dos. En dicha terna, uno de los catetos es par, el otro impar y por lo tanto Z' impar. [1] Como el área de X', Y', Z' es $s^2n = \frac{X'Y'}{2} \in \mathbb{Z}$ y n es libre de cuadrados, deducimos que $s \in \mathbb{Z}$ y por lo tanto $x = \left(\frac{Z}{2}\right)^2 = \left(\frac{Z'}{2s}\right)^2$ tiene denominador par.

Una tercera condición es que el numerador de x sea coprimo con n. Para ver esto, supongamos por absurdo que existe un primo $p > 2$ que divide tanto al numerador de x como a n, entonces divide al numerador de $x \pm n = \left(\frac{X\pm Y}{2}\right)^2$, [2] y por lo tanto al de $\frac{X\pm Y}{2}$. Si divide a estos dos términos, divide a su suma X y a su diferencia Y, y por lo tanto p^2 divide a $n = \frac{XY}{2}$, lo que es absurdo porque habíamos tomado n libre de cuadrados.

La siguiente proposición nos dice que estas tres condiciones no son sólo necesarias, si no suficientes.

PROPOSICIÓN 1.2. *Sea (x, y) de coordenadas racionales que es solución de la ecuación $y^2 = x^3 - n^2x$ tal que x satisface las tres condiciones:*

- *x es el cuadrado de un racional.*
- *El denominador de x es par.*
- *El numerador de x es coprimo con n.*

Entonces existe un triángulo rectángulo con lados racionales de área n correspondiente a x según la Prop. 1.1.

DEMOSTRACIÓN. Sea $u = \sqrt{x} \in \mathbb{Q}$, y sea $v = \frac{y}{u}$ con lo que $v^2 = \frac{y^2}{x} = x^2 - n^2$, o sea $v^2 + n^2 = x^2$. Sea t el denominador de u, que es par. El denominador de v^2 y de x^2 es el mismo ya que n^2 es un entero, y es t^4. Entonces, t^2v, t^2n y t^2x es una terna Pitagórica primitiva (ya que t^2x es el numerador de x, que es coprimo con n y con t). Por el lema 1.1 que veremos enseguida, existen entonces enteros a y b

[1] Si X' e Y' son ambos pares, tenemos que Z' es par. Si ambos son impares, $X'^2 \equiv Y'^2 \equiv 1$ (mód 4) y por lo tanto $Z'^2 \equiv 1 + 1 = 2$ (mód 4) que no puede ser si Z' es un entero.

[2] Usando 1.1 $\left(\frac{X\pm Y}{2}\right)^2 = \frac{X^2+Y^2\pm 2XY}{4} = \left(\frac{Z}{2}\right)^2 \pm n = x \pm n$.

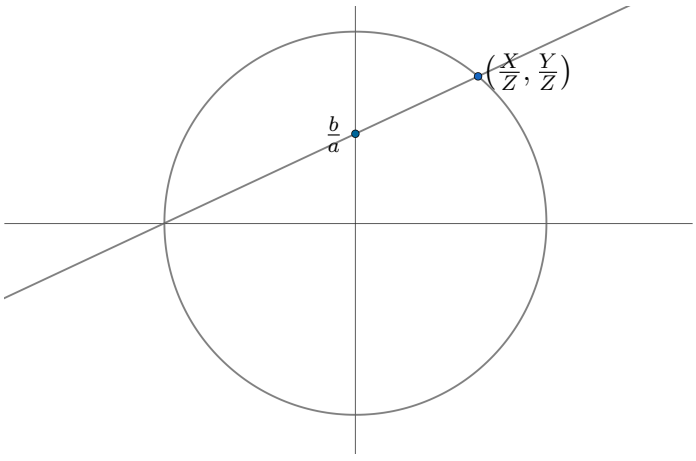
tales que $t^2n = 2ab$, $t^2v = a^2 - b^2$ y $t^2x = a^2 + b^2$. Entonces, el triángulo con lados $X = \frac{2a}{t}$, $Y = \frac{2b}{t}$ y $Z = 2u$ tiene área $\frac{2ab}{t^2} = n$ y es el correspondiente a x, ya que $x = u^2 = \left(\frac{Z}{2}\right)^2$. □

La ecuación 1.3 es un caso particular de lo que llamamos **curva elíptica**, pero antes de irnos por ese camino, veamos una aplicación de la Prop. 1.1 y de lo que hemos visto hasta ahora.

Ya vimos que algunos números, como el 6, son congruentes, pero también hay naturales que no son congruentes. El 1 es el primer ejemplo de esto, y la prueba nos da como corolario algo interesante. Necesitaremos primero el siguiente lema.

LEMA 1.1. *Sean $a > b$ enteros positivos con $\mathrm{mcd}(a, b) = 1$ y alguno de ellos par. Entonces la terna (X, Y, Z) con $X = a^2 - b^2$, $Y = 2ab$ y $Z = a^2 + b^2$ es una terna Pitagórica primitiva, y todas son de esta forma.*

DEMOSTRACIÓN. $X^2 + Y^2 = a^4 - 2a^2b^2 + b^4 + 4a^2b^2 = a^4 + 2a^2b^2 + b^4 = (a^2 + b^2) = Z^2$, por lo que es una terna Pitagórica, y si tuviéramos un primo p que dividiera a X y a Z, tendríamos primero que p es impar, y segundo que divide a la suma $Z + X = 2a^2$ y a la resta $Z - X = 2b^2$, y por lo tanto p dividiría a a y a b, lo que no puede pasar porque eran coprimos. Ahora, para ver que todas las ternas primitivas son de esta forma, tomemos una, (X, Y, Z), con Y par. Tenemos que $\left(\frac{X}{Z}\right)^2 + \left(\frac{Y}{Z}\right)^2 = 1$, por lo que el punto $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$ está en la circunsferencia unidad S^1. La recta que une este punto con el punto $(-1, 0)$ corta al eje y en algún punto con ordenada racional $\frac{b}{a} < 1$. Ahora, si pensamos esa recta en función de que pasa por los puntos (-1,0) y $(0, \frac{b}{a})$, tenemos que el otro punto de corte con S^1, que sabemos es $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$, tiene coordenadas $\left(\frac{a^2-b^2}{a^2+b^2}, \frac{2ab}{a^2+b^2}\right)$, por lo que $X = a^2 - b^2$, $Y = 2ab$ y $Z = a^2 + b^2$, y obviamente a y b tienen que ser coprimos y no ambos impares. □



Ahora si el 1 fuera un número congruente, tendríamos que existe un racional $x = \frac{r^2}{s^2}$ de la Prop. 1.1 tal que $\frac{r^2}{s^2} \pm 1 = \frac{r^2 \pm s^2}{s^2}$ son ambos cuadrados de racionales.

Como r y s son coprimos, tenemos que $r^2 \pm s^2$ y s^2 también son coprimos y entonces las fracciones $\frac{r^2 \pm s^2}{s^2}$ ya están reducidas, con lo que los numeradores son ambos enteros al cuadrado, ergo, lo es su producto, i.e., $r^4 - s^4 = u^2$, donde vemos que u es impar porque s es par. Por lo tanto, que el 1 sea congruente implica la existencia de una solución entera a la ecuación $x^4 - y^4 = v^2$ con v impar, y será x impar e y par por el mismo argumento de congruencia módulo 4 de antes. Veamos que la existencia de una tal solución es absurda usando el método de Fermat del *descenso infinito*, que consiste en suponer la existencia de una solución con un entero positivo a cierta ecuación y a partir de esta encontrar una solución estrictamente menor. Siguiendo inductivamente, tendríamos infinitas soluciones decreciendo estrictamente, pero esto es absurdo por el principio del buen orden de los números naturales.

Sea entonces la ecuación $x^4 - y^4 = v^2$, que la podemos tomar con los tres términos coprimos. Despejando tenemos $x^4 = v^2 + y^4$, que es una terna Pitagórica primitiva (v, y^2, x^2), con lo que usando el Lema tenemos:

$$\begin{aligned} v &= a^2 - b^2 \\ y^2 &= 2ab \\ x^2 &= a^2 + b^2. \end{aligned}$$

Supongamos que a es par y b impar (es casi análogo el otro caso). La segunda condición nos dice que $2ab = 4\frac{a}{2}b$ es un cuadrado, pero como a y b son coprimos, tenemos que $\frac{a}{2}$ y b son cuadrados, digamos $a = 2\alpha^2$, $b = \beta^2$. De la tercera condición obtenemos otra terna Pitagórica primitiva, a la que también le aplicamos el Lema y queda

$$\begin{aligned} b &= k^2 - l^2 \\ a &= 2kl \\ x &= k^2 + l^2. \end{aligned}$$

Repitiendo el mismo argumento, la segunda condición $a = 2\alpha^2 = 2kl$ nos deja $\alpha^2 = kl$, con lo que k y l son ambos cuadrados, digamos, $k = \kappa^2$ y $l = \lambda^2$. Sustituyendo en la primera de esta segunda tanda de ecuaciones tenemos:

$$\beta^2 = \kappa^4 - \lambda^4$$

donde $\kappa \leq k < x$, con lo que por el razonamiento del descenso llegamos a un absurdo y el número 1 no es congruente.

Esto mismo sirve para probar el *Último Teorema de Fermat*[3] para $n = 4$ y en consecuencia, cualquier múltiplo de 4, pues si tuviéramos una solución a la ecuación $x^4 + y^4 = z^4$, la tomamos coprima y sabemos que alguno, x ó y, es impar. Supongamos que es x, despejamos y tenemos

$$(x^2)^2 = z^4 - y^4,$$

[3]El Último Teorema de Fermat dice que si $n > 2$ es un entero, no existen soluciones enteras positivas a la ecuación $x^n + y^n = z^n$. Fue conjeturado por Pierre de Fermat en 1637 y demostrado por Andrew Wiles recién en 1995.

que, como acabamos de probar, es absurdo.
Para los casos en los que n no es múltiplo de 4, hay una prueba muy elegante, pero no entra en los márgenes (ni en ninguna parte) de esta humilde monografía.

2. Curvas elípticas

DEFINICIÓN 1.2. Sea $\mathbb{K}$ un cuerpo de característica distinta de 2 y $f \in \mathbb{K}[x]$ un polinomio de grado tres sin raíces múltiples (no necesariamente en $\mathbb{K}$). El conjunto de los puntos $(x, y) \in \mathbb{F} \times \mathbb{F}$ siendo $\mathbb{F}$ extensión de $\mathbb{K}$ que verifican

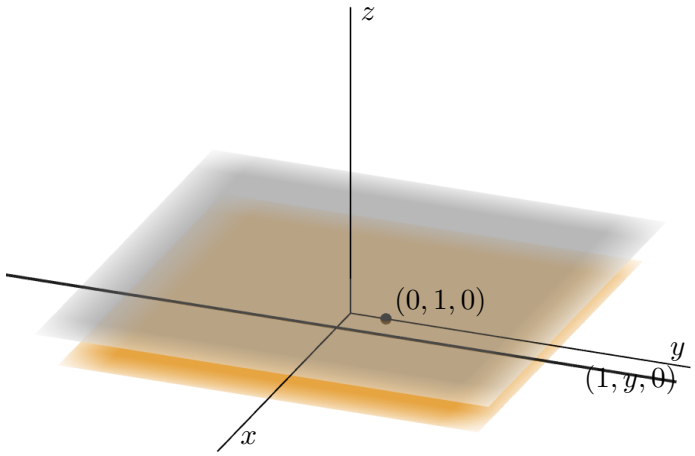
$$y^2 = f(x)$$

se denominan $\mathbb{F}$-puntos de la curva elíptica $y^2 = f(x)$.

Si consideramos $F(x, y) = y^2 - f(x)$ observar que nos interesa estudiar los puntos tales que $F(x, y) = 0$.

En realidad, cuando hablamos de una curva elíptica, nos referimos al conjunto anteriormente mencionado y a un "punto en el infinito", que es en algún sentido la completación de la curva. Para eso, tenemos que hablar del plano proyectivo.

Sea $\mathbb{K}$ un cuerpo cualquiera y $\mathbb{K}^{n+1}$ el espacio vectorial usual. El conjunto $\mathbb{P}^n_{\mathbb{K}}$, llamado *espacio proyectivo de dimensión* n se define como el conjunto de los subespacios de dimensión 1 de $\mathbb{K}^{n+1}$. Se lo puede ver como el conjunto cociente de $\frac{\mathbb{K}^{n+1}-\{0\}}{\sim}$ donde dos puntos están relacionados si son colineales. Nosotros trabajaremos sólo con la recta proyectiva $\mathbb{P}^1$ y el plano proyectivo $\mathbb{P}^2$.
Si $\mathbb{K} = \mathbb{R}$, podemos hacernos una idea de quién es $\mathbb{P}^2$ con un conjunto de representantes. Están los subespacios (rectas por el origen) que tienen coordenada $z \neq 0$. Para todos estos, podemos tomar el representante con $z = 1$ para cada recta, con lo que nos quedaría el plano xy pero con altura 1. Luego, están los subespacios con coordenada $z = 0$ y coordenada $x \neq 0$, para los que podemos tomar de representantes los puntos de la forma $(1, y, 0)$. Luego, nos queda sólo el subespacio con coordenadas $x = z = 0$, que tomamos como representante el punto $(0, 1, 0)$. De esta manera, $\mathbb{P}^2$ lo podemos ver como un plano, una recta y un punto como se ve en la siguiente figura (en naranja el plano xy, en gris claro el plano $z = 1$).

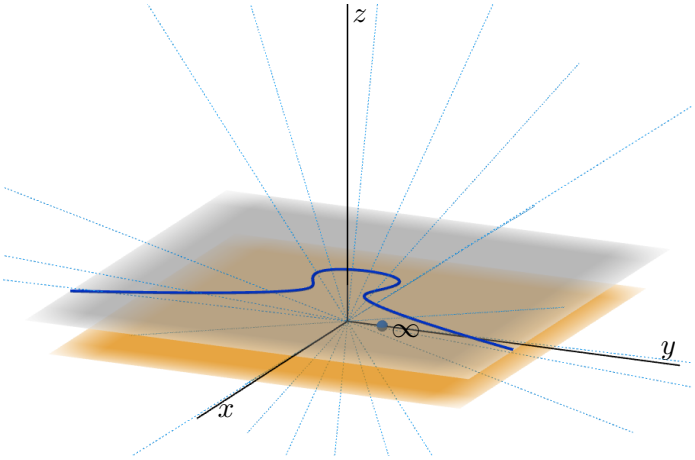


El *grado total* de un monomio de varias variables se define como la suma de los grados de todas sus variables (Ej: x^3yz^2 tiene grado total 6). Un polinomio se dice *homogéneo* si el grado total de todos sus monomios es el mismo.
Sea $F \in \mathbb{K}[x, y]$ un polinomio cualquiera. La *homogeneización* del polinomio F es el polinomio $\widetilde{F} \in \mathbb{K}[x, y, z]$ que se obtiene agregando la variable z a todos los monomios de F para que este sea homogéneo. O sea

$$\widetilde{F}(x, y, z) = z^n F(\frac{x}{z}, \frac{y}{z}) \tag{1.4}$$

siendo n el máximo de los grados totales de los monomios de F.
Notar que vale $\widetilde{F}(\lambda x, \lambda y, \lambda z) = \lambda^n \widetilde{F}(x, y, z)$ y por lo tanto, $\widetilde{F}(x, y, z) = 0 \iff$ $\widetilde{F}(\lambda x, \lambda y, \lambda z) = 0$ para todo $\lambda \in \mathbb{K}^*$. Esto último nos permite estudiar las raíces de $\widetilde{F}$ en el plano proyectivo.
Las raíces de $\widetilde{F}$ son entonces las que tienen coordenada $z \neq 0$ y las que son de la forma $(x, y, 0)$. Estas últimas las llamaremos "puntos en el infinito".

Volvamos ahora a nuestro polinomio $F(x, y) = y^2 - f(x) = y^2 - ax^3 - bx^2 - cx - d$. Si estudiamos los ceros de $\widetilde{F}$, aquellos que tienen coordenada $z \neq 0$ corresponden a los puntos en los cuales $\widetilde{F}(x, y, 1) = F(x, y) = 0$, o sea que coinciden con las raíces de F. Los otros ceros, los que tienen coordenada $z = 0$, deben ser $0 = ax^3$ y se tiene $x = 0$, por lo que los ceros de la recta en el infinito en $\mathbb{P}^2$ de $\widetilde{F}$ son únicamente el punto $(0, 1, 0)$. Este es el "punto en el infinito" al que nos referíamos de la curva elíptica. En la siguiente figura, podemos ver un sistema de representantes con $z = 1$ y el ∞ de la curva elíptica $zy^2 = x^3 - xz^2 + z^3$ en azul.



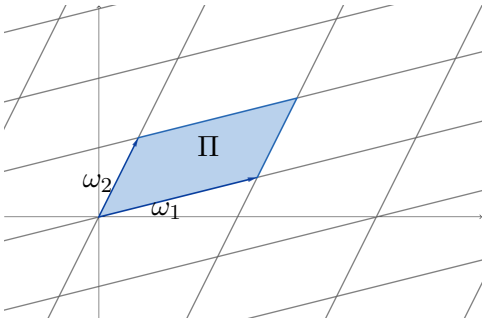
3. Retículos, toros y función de Weierstrass

DEFINICIÓN 1.3. Un retículo L es el conjunto en el plano complejo de las combinaciones lineales enteras de dos complejos linealmente independientes dados ω_1 y ω_2, no necesariamente únicos, i.e.:

$$L = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}. \tag{1.5}$$

El paralelogramo fundamental de ese retículo es:

$$\Pi = \{a\omega_1 + b\omega_2 : a, b \in [0, 1]\}. \tag{1.6}$$



OBSERVACIÓN 1.1. Como ω_1 y ω_2 son una base de $\mathbb{C}$ sobre $\mathbb{R}$, podemos escribir cualquier complejo z de forma casi única[4] como suma de un elemento del retículo y uno del paralelogramo fundamental, o sea

$$z = l + t,\ l \in L,\ t \in \Pi. \tag{1.7}$$

DEFINICIÓN 1.4. Una función meromorfa $f : \mathbb{C} \longrightarrow \mathbb{C}$ se dice **función elíptica** relativa a L si $f(z + l) = f(z)$ para todo $l \in L$. Al conjunto de funciones elípticas relativas al retículo L se lo denota $\mathscr{E}_L$.

[4]Si un z ya era parte del retículo, se puede escribir de diferentes formas, por ejemplo $\omega_1+0+0 = 0 + w_1 + 0$, donde en la primer forma el elemento del retículo es ω_1 y en la segunda es el 0.

Notar que es suficiente chequear la definición para ω_1 y ω_2, razón por la cual se le llama a f función de doble período.

Notar también que f queda definida por lo que vale en el paralelogramo fundamental Π, siendo que vale lo mismo en partes del borde. Podemos decir que f está definida entonces en el toro $\mathbb{C}/L$.

Las siguientes son algunas propiedades de las funciones elípticas que nos serán utiles.

PROPOSICIÓN 1.3. *Una función $f \in \mathscr{E}_L$ que no tiene polos en el paralelogramo fundamental Π es constante.*

DEMOSTRACIÓN. Como Π es compacto, tenemos que f está acotada en Π, pero lo que vale en Π es lo que vale en todo $\mathbb{C}$, por lo que f está acotada en todo $\mathbb{C}$. Por el teorema de Liouville, una función entera y acotada es constante. □

PROPOSICIÓN 1.4. *Sea $\alpha \in \mathbb{C}$ tal que f no tiene ceros ni polos en el borde γ de $\Pi + \alpha = \{z + \alpha : z \in \Pi\}$ (esto siempre es posible ya que f es meromorfa y sus ceros y polos son aislado). Entonces la suma de los residuos de f en $\Pi + \alpha$ es cero.*

DEMOSTRACIÓN. Por el teorema de los residuos, dicha suma es igual a

$$\frac{1}{2\pi i} \int_\gamma f(z)dz. \tag{1.8}$$

Pero f vale lo mismo en los lados opuestos de γ y está recorrida en el sentido opuesto, por lo que se cancelan y la integral da cero. □

PROPOSICIÓN 1.5. *Sea $f \in \mathscr{E}_L$ y sea α tal que f no tiene ceros ni polos en el borde de $\Pi + \alpha$. Entonces la suma de los órdenes de los ceros es igual a la suma de los órdenes de los polos de f en $\Pi + \alpha$.*

DEMOSTRACIÓN. Aplicamos la Prop. 1.4 a la derivada logarítmica de f $\frac{f'(z)}{f(z)}$, que también es elíptica relativa a L. Esta tiene un polo simple donde f tenía un cero o un polo, y el residuo es igual al orden del cero (o menos del orden el polo) de f en ese lugar[5]. Por lo tanto, la suma de los residuos es $\sum m_i - \sum n_j = 0$, donde $\{m_i\}$ son los órdenes de los distintos ceros y $\{n_j\}$ los órdenes de los distintos polos de f. □

Ahora, definiremos una función elíptica muy importante, que nos dará una nueva forma de estudiar a ciertas curvas elípticas.

DEFINICIÓN 1.5. Sea $L = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ un retículo. Definimos la función $\wp$ **de Weierstrass** relativa a L y la notamos $\wp(z, L)$, $\wp(z, \omega_1, \omega_2)$ o simplemente $\wp(z)$ si el retículo está implícito en el contexto como:

$$\wp(z) = \frac{1}{z^2} + \sum_{l \in L, l \neq 0} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right). \tag{1.9}$$

[5]Si $f(z) = c_m(z-a)^m + \ldots$, entonces $f'(z) = c_m m(z-a)^{m-1} + \ldots$ y entonces $\frac{f'(z)}{f(z)} = m(z-a)^{-1} + \ldots$

PROPOSICIÓN 1.6. *La suma definida en la función $\wp$ converge absoluta y uniformemente en cualquier compacto de $\mathbb{C} - L$.*

Observar que la derivada de $\wp(z)$ es

$$\wp'(z) = -2\sum_{l\in L}\frac{1}{(z-l)^3} \tag{1.10}$$

PROPOSICIÓN 1.7. *La función $\wp$ está en $\mathscr{E}_L$ y su único polo es un polo es un polo doble en los puntos del retículo.*

Sea $L = \{m\omega_1 + n\omega_2\}$ un retículo, definimos

$$G_k = G_k(L) := \sum_{l\in L^*} l^{-k} = \sum_{m,n\in\mathbb{Z},\text{no ambos cero}} \frac{1}{m\omega_1 + n\omega_2} \tag{1.11}$$

$$g_2 = g_2(L) := 60G_4; \qquad g_3 = g_3(L) := 140G_6. \tag{1.12}$$

PROPOSICIÓN 1.8. *El mapa que va del toro $\mathbb{C}/L$ en $\mathbb{P}^2_{\mathbb{C}}$ definido como*

$$z \mapsto (\wp(z), \wp'(z), 1), \ 0 \mapsto (0,1,0) \tag{1.13}$$

es una biyección entre el toro y la curva eliptica $y^2 = 4x^3 - g_2x - g_3$.

Esta correspondencia es fundamental para poder definir una estructura de grupo en la curva elíptica.

4. Ley de grupo

Como el toro tiene estructura de grupo abeliano (la de los complejos, que se porta bien con el cociente por ser abeliano), podemos inducir una suma en la curva $y^2 = 4x^3 - g_2x - g_3$ de modo que esta sea también un grupo abeliano con esa suma. Esto se puede hacer siempre que tengamos un conjunto en biyeción con una estructura algebraica cualquiera. Lo interesante en nuestro caso es que la suma inducida en la curva tiene una interpretación geométrica que nos permite operar en la curva sin conocer la biyección con el toro.

Para cada $z \in \mathbb{C}/L$, llamamos $P_z = (\wp(z), \wp'(z), 1)$" = "$(\wp(z), \wp'(z))$ y $P_0 = (0,1,0)$. Dados $P_{z_1} = (x_1, y_1)$ y $P_{z_2} = (x_2, y_2)$ nos interesa saber quién es $P_{z_1} + P_{z_2} = P_{z_1+z_2} = (x_3, y_3)$ sin tener que saber quiénes son z_1 y z_2. Empecemos por ver los casos más fáciles.

El neutro del grupo es claramente $(0,1,0)$. Supongamos que P_{z_1} y P_{z_2} tienen la misma coordenada x pero no son el mismo punto, o sea $x_1 = x_2$ e $y_1 = -y_2$ (recordar que son puntos de la curva elíptica). En este caso, tenemos que $\wp(z_1) = \wp(z_2)$, pero por las proposiciones 1.5 y 1.7, la función $\wp(z)$, y por lo tanto $\wp(z) - \wp(z_2)$, tiene dos ceros contados con multiplicidad en el toro; uno de ellos es claramente z_2, y el otro es $-z_2$ (ya que $\wp$ es par), por lo que no hay otra opción que $z_1 = -z_2$. Acabamos de probar:

PROPOSICIÓN 1.9. *El inverso de (x, y) en la curva es $(x, -y)$, su simétrico respecto al eje de las abscisas.*

Dados dos puntos P_1 y P_2 de la curva $y^2 = 4x^3 - g_2x - g_3$ distintos del neutro, llamamos $r = \overline{P_1P_2}$ a la recta que los une. Si $P_1 = P_2$ tomamos la recta tangente a la curva por el punto. Ya vimos que si r es vertical, $P_1 + P_2 = 0$. Si no lo es, podemos escribir r como $y = mx + b$. Un punto (x, y) vive en la curva elíptica y en la recta r sí y solo sí $(mx+b)^2 = f(x) = 4x^3 - g_2x - g_3$, o sea, si x es raiz de $f(x) - (mx+b)^2$. Ese polinomio tiene tres raíces que corresponden con los tres puntos de intersección teniendo la misma multiplicidad (si x e raíz doble o triple, la recta intersecta a la curva con multiplicidad dos o tres, respectivamente).
Notar que las rectas verticales también tienen tres puntos de intersección: P_1, P_2 y el punto en el infinito $(0, 1, 0)$. Esto es un caso particular, con $\widetilde{F} = y^2z - 4x^3 + g_2xz^2 + g_3z^3$ y $\widetilde{G} = y - mx - bz$ del siguiente:

Teorema de Bézout.[**Sha13**] Sean $\widetilde{F}(x, y, z)$ y $\widetilde{G}(x, y, z)$ polinomios homogéneos de grados m y n, respectivamente, sobre un cuerpo K algebraicamente cerrado y sin factores en común. Entonces las curvas $\widetilde{F} = 0$ y $\widetilde{G} = 0$ tienen mn puntos de intersección, contando multiplicidades.

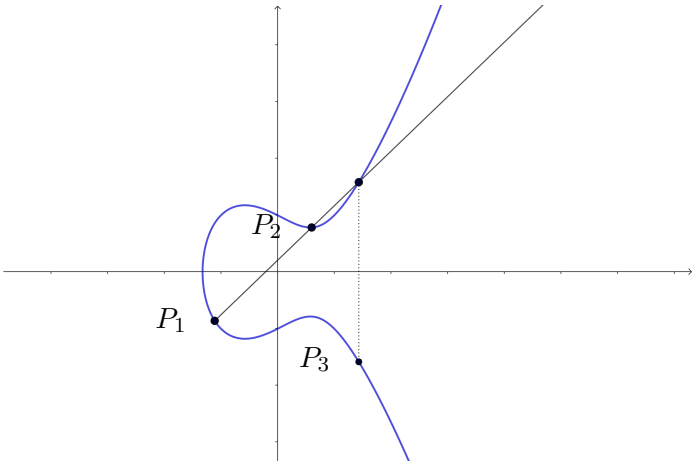
PROPOSICIÓN 1.10. *Si $P_1 + P_2 = P_3$ entonces $-P_3$, el simétrico respecto al eje x de P_3 en el plano xy es el tercer punto de intersección de la recta $r = \overline{P_1P_2}$.*

Para probar esto, necesitamos el siguiente lema, que no demostraremos.

LEMA 1.2. *Sean f una función elíptica sobre el retículo L, Π el paralelogramo fundamental de L y α tal que f no tiene ceros ni polos en el borde de $\Pi + \alpha$. Sean $\{a_i\}$ los ceros de f en $\Pi + \alpha$ contados con multiplicidad y $\{b_j\}$ los polos. Entonces $\sum a_i = \sum b_j$ en $\mathbb{C} - L$ (i.e. su resta vive en L).*

DEMOSTRACIÓN. Ya vimos el caso en el que alguno de los puntos es el $0 = (0, 1, 0)$ o en el que $P_1 = -P_2$, por lo que supongamos ahora que $l = \overline{P_1P_2}$ es de la forma $y = mx + b$.
Sean $P_1 = P_{z_1}$ y $P_2 = P_{z_2}$. Que un punto P_z esté en l quiere decir que $\wp'(z) = m\wp(z) + b$. La función $\wp'(z) - m\wp(z) - b$ tiene un polo de orden tres por la Prop. 1.7 y por la Prop. 1.5, tres ceros contados con multiplicidad en $\mathbb{C} - L$. Tanto z_1 como z_2 son ceros y el único polo es el 0, entonces por el Lema 1.2 tenemos que el tercer punto es $-(z_1 + z_2)$ (módulo L). Entonces, $P_{-(z_1+z_2)} = -P_{z_3}$.
Este argumento es correcto siempre y cuando los tres puntos hallados sean distintos. En otro caso, tenemos que ver que si una raíz es doble o triple de $\wp'(z) - m\wp(z) - b$, la intersección de la recta con la curva también tendrá multiplicidad dos o tres, respectivamente.
Sean z_1, z_2 y z_3 los ceros de $\wp'(z) - m\wp(z) - b$, contados con multiplicidad. Como estábamos suponiendo que r no era vertical, ninguno de los puntos es el opuesto del otro, por lo que los puntos $-z_1$, $-z_2$ y $-z_3$ son distintos a los de antes (o puede darse que algún punto sea cero, por lo que $z_k = -z_k$, pero esto no nos molesta). Estos puntos son los ceros de $\wp'(z) + m\wp(z) + b$ ya que $\wp$ es par y $\wp'$ es

impar (ver Def. 1.5). Por lo tanto, $\pm z_1$, $\pm z_2$ y $\pm z_3$ son los seis ceros del producto $\wp'(z)^2-(m\wp(z)+b)^2 = f(\wp(z))-(m\wp(z)+b)^2 = 4(\wp(z)-x_1)(\wp(z)-x_2)(\wp(z)-x_3)$, donde x_1, x_2 y x_3 son los ceros de $f(x)-(mx+b)^2$. Si, por ejemplo, $\wp(z_1)=x_1$, tenemos que la multiplicidad de x_1 depende sólo de cuántos de $\pm z_2$, $\pm z_3$ sean iguales a $\pm z_1$, pero esto es lo mismo que la cantidad de z_2, z_3 que sean iguales a z_1, o sea, la multiplicidad de una raíz de $f(x)-(mx+b)^2$, o sea, la multiplicidad de la intersección entre la recta r y la curva $y^2 = 4x^3 - g_2x - g_3$ es la misma que la multiplicidad de la raíz de la función elíptica $\wp'(z)+m\wp(z)+b$.
Esto concluye la demostración. □



La proposición anterior nos da entonces una forma geométrica de operar en la curva elíptica y sin necesidad de saber cuál es el punto correspondiente según la biyección de la Prop. 1.8. Para sumar dos puntos P_1 y P_2, trazamos la línea que los une (la tangente a la curva en caso de que sean el mismo punto), vemos el tercer punto de intersección con la curva y tomamos su opuesto (el simétrico respecto al eje x). Ese punto es P_1+P_2.
Podríamos haber definido la operación en la curva de esta forma desde un principio y haber probado que es un grupo. El paso más difícil yendo por ese camino es probar la asociatividad.
Una desventaja de nuestra prueba usando la función de Weierstrass es que, a priori, sólo sirve para curvas de la forma $y^2 = 4x^3 - g_2(L)x - g_3(L)$ y curvas que pueden ser llevadas a estas mediante un cambio de variables lineal (notar que los cambios de variables lineales preservan la estructura de grupo abeliano con la descripción geométrica). Más adelante veremos que cualquier curva elíptica sobre $\mathbb{C}$ se puede llevar a la forma de Weierstrass para algún retículo L.
Por otro lado, también podemos encontrar fórmulas explícitas para P_1+P_2 en función de x_1, y_1, x_2, y_2, y los coeficientes de $f(x)$, siendo $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ y, de nuevo, podríamos haber definido la operación del grupo a partir de estas fórmulas, siendo la parte más difícil de probar la asociatividad.
Hagamos esto suponiendo que las reglas de la suma geométrica valen para cualquier curva elíptica en $\mathbb{C}$, esto es, $y^2 = f(x) = ax^3+bx^2+cx+d$.

Asumimos que P_1, P_2 son distintos del infinito y no son uno el opuesto del otro, por lo que la recta que los une (o la tangente si son el mismo punto) es de la forma $y = mx + \beta$, donde

$$\begin{aligned} m &= \frac{y_2 - y_1}{x_2 - x_1} \text{ si } P_1 \neq P_2 \\ m &= \frac{\partial y}{\partial x}|_{(x_1,y_1)} = \frac{f'(x_1)}{2y_1} \quad \text{si} \quad P_1 = P_2 \\ \beta &= y_1 - mx_1 \text{ en ambos casos} \end{aligned} \tag{1.14}$$

Entonces, x_3, la x-coordenada de la suma de los puntos es la tercera raíz del polinomio $f(x) - (mx + \beta)^2$. La suma de las raíces es igual al opuesto del coeficiente de x^2 del polinomio dividido por el coeficiente principal, i.e. $x_1 + x_2 + x_3 = -\frac{b-m^2}{a}$. Tenemos entonces

$$x_3 = -x_1 - x_2 - \frac{b}{a} + \frac{1}{a}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \quad \text{si} \quad P_1 \neq P_2; \tag{1.15}$$

$$x_3 = -2x_1 - \frac{b}{a} + \frac{1}{a}\left(\frac{f'(x_1)}{2y_1}\right)^2 \quad \text{si} \quad P_1 = P_2. \tag{1.16}$$

La $y-$coordenada, y_3 es el opuesto de $y = mx_3 + \beta$, i.e.

$$y_3 = -y_1 + m(x_1 - x_3), \tag{1.17}$$

donde x_3 está dado por 1.15 y 1.16, y m por 1.14.

5. Puntos de orden finito y volviendo a los números congruentes

Volvamos a nuestra ecuación especial $y^2 = x^3 - n^2x$, que de ahora en más llamaremos E_n. Los números congruente estaban relacionados con los $\mathbb{Q}$-puntos de esa curva, pero si $\mathbb{K}$ es un cuerpo cualquiera de característica $p \nmid 2n$, la misma ecuación es también una curva elíptica sobre $\mathbb{K}$. Notamos $E_n(\mathbb{K})$ a los $\mathbb{K}$-puntos de la curva elíptica E_n.

Para atacar el problema de los números congruentes, necesitamos pasar antes por una proposición que implica saber algo sobre cuerpos finitos.

Notamos $\mathbb{F}_q$ al cuerpo con q elementos donde q es potencia de algún primo $p = \text{char}(\mathbb{F}_q)$. Si tomamos $\mathbb{F}_q^\times$ los invertibles del cuerpo, estos forman un grupo con la multiplicación de orden $q - 1$. Los cuadrados son aquellos elementos y tales que existe $x \in \mathbb{F}_q^\times$ con $x^2 = y$, llamémosle momentáneamente C al conjunto con dichos elementos. Si $\text{char}(\mathbb{F}_q) \neq 2$, C es un subgrupo del grupo multiplicativo con índice dos, ya que:

- $\{x^2 : x \in \mathbb{F}_q^\times\} = C$.
- $x^2 = (-x)^2$ y como $\text{char}(\mathbb{F}_q) \neq 2$, $x \neq -x$, por lo que en el conjunto de arriba estoy nombrando al menos dos veces a cada elemento.
- Si $y \in C$, existen, cuando mucho, dos raíces del polinomio $X^2 - y$, por lo que el cardinal de C es exactamente $\frac{q-1}{2}$.

O sea $\mathbb{F}_q^\times = C \cup aC$, con a un no cuadrado, y deducimos:

PROPOSICIÓN 1.11. *El producto de un cuadrado con un no-cuadrado es un no-cuadrado, y el producto de dos no-cuadrados es un cuadrado.*

Ahora, veamos la siguiente proposición.

PROPOSICIÓN 1.12. *Sea $q = p^t$ con $p \nmid 2n$ y $q \equiv 3$ (mód 4). Hay exactamente $q+1$ $\mathbb{F}_q$-puntos en la curva elíptica $y^2 = x^3 - n^2x$.*

DEMOSTRACIÓN. Primero, hay 4 puntos conocidos: el punto en el infinito, $(0,0)$ y $(\pm n, 0)$. Contemos ahora los otros puntos (x,y), aquellos que tienen x distinto de 0 y $\pm n$. Hay $q-3$ posibles x, que los agrupamos en pares $\{x,-x\}$. Como la función $f(x) = x^3 - n^2x$ es impar, tenemos que $f(-x) = (-1)f(x)$ y como -1 no es un cuadrado en $\mathbb{F}_q$ (aquí usamos que $q \equiv 3$ (mód 4)), tenemos que uno sólo de $f(x),\ f(-x)$ es un cuadrado (aquí usamos la Obs. 1.11). Cualquiera sea el que sirve, nos da dos puntos $(x, \pm\sqrt{f(x)})$, $(-x, \pm\sqrt{f(-x)})$ que están en la curva elíptica. O sea, tenemos $\frac{q-3}{2}$ números x que nos sirven, cada uno aportando 2 puntos, más los 4 que contamos antes, totalizando $q+1$ $\mathbb{F}_q$-puntos como queríamos. □

A priori, como nos interesaba conocer $E_n(\mathbb{Q})$, uno se pregunta qué tiene que ver chorizo con bicicleta, o sea, por qué nos interesan los puntos de la curva sobre cuerpos finitos. Sin embargo, nos erá muy útil esta proposición para probar lo siguiente, que nos da una caracterización un poco más profunda de los números congruentes.

Como en cualquier grupo abeliano, en la curva elíptica podemos diferenciar entre los elementos de orden finito, conocidos como la parte de torsión, y los de orden infinito. Estudiando las cosas en el toro, vemos que un punto $P_z = (x,y)$ tiene orden finito si y sólo si existe un N tal que $Nz \in L$, que es lo mismo que decir que z es una combinación racional de ω_1 y ω_2. El **Teorema de Mordell**[**ST15**, Capítulo 5] nos dice que el grupo $E(\mathbb{Q})$ de los $\mathbb{Q}$-puntos de una curva elíptica E es un grupo abeliano finitamente generado, y el **Teorema de estructura de grupos abelianos finitamente generados**[**Jac85**, Capítulo 3.8] nos dice que el subgrupo de torsión es finito y que $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$, donde r es un entero no negativo que llamamos **rango** de la curva elíptica.

Sabemos que en $E_n(\mathbb{Q})$ tenemos cuatro puntos de orden menor o igual a 2: el infinito, $(0,0)$, $(n,0)$ y $(-n,0)$. La siguiente proposición nos dice que estos son los únicos puntos de torsión.

PROPOSICIÓN 1.13. *$\#E_n(\mathbb{Q})_{Tors} = 4$, o lo que es lo mismo por los puntos que ya conocemos, $E_n(\mathbb{Q})_{Tors} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, donde notamos $\mathbb{Z}_d = \mathbb{Z}/d\mathbb{Z}$.*

DEMOSTRACIÓN. La idea será construir un morfismo inyectivo de un subrgrupo fijo de $E_n(\mathbb{Q})_{Tors}$ en los $E_n(\mathbb{F}_p)$ para cada p primo y, partiendo de esto, llegar a una contradicción.
Comencemos por el mapa reducción módulo p de $\mathbb{P}^2_{\mathbb{Q}}$ en $\mathbb{P}^2_{\mathbb{F}_p}$. Recordar que los puntos de $\mathbb{P}^2_{\mathbb{Q}}$ son los subespacios de dimensión 1 de $\mathbb{Q}^3$. Para cada subespacio, puedo tomar un único representante $P = (x,y,z)$ (a menos del signo) con entradas enteras y

coprimas. Este punto, lo mando a $\overline{P} = (\overline{x}, \overline{y}, \overline{z})$, o sea la clase módulo p. Ningún punto va a parar al $(0,0,0)$ ya que no pueden ser las tres entradas x, y y z múltiplos de p a la vez. Recordar que si multiplico un punto de $\mathbb{P}^2_{\mathbb{F}_p}$ por un número coprimo con p, sigo teniendo el mismo punto, esto es muy importante.
Si un punto $P = (x, y, z)$ está en $E_n(\mathbb{Q})$, significa que cumple $y^2z = x^3 - n^2xz^2$ y por lo tanto también está en $E_n(\mathbb{F}_p)$ (las operaciones se preservan módulo p). Más aún, si P_1 y P_2 están en $E_n(\mathbb{Q})$, entonces $P_1 + P_2$ va a parar a $\overline{P_1} + \overline{P_2}$, pues las operacines de 1.15-1.17 preservan la clase módulo p. O sea, tenemos un morfismo de grupos de $E_n(\mathbb{Q})$ en $E_n(\mathbb{F}_p)$. Nos interesa saber cuándo este morfismo no es inyectivo, i.e., cuando dos puntos $P_1 = (x_1, y_1, z_1)$ y $P_2 = (x_2, y_2, z_2)$ en $\mathbb{P}^2_{\mathbb{Q}}$ distintos cumplen que $\overline{P_1} = \overline{P_2}$ en $\mathbb{P}^2_{\mathbb{F}_p}$.

Afirmación 1.1. $\overline{P_1} = \overline{P_2}$ si y sólo si el producto vectorial de $\mathbb{R}^3$ entre P_1 y P_2 es divisible por p, i.e., p divide a $y_1z_2 - y_2z_1$, $x_1z_2 - x_2z_1$ y $x_1y_2 - x_2y_1$.

Prueba de la afirmación. Para el directo, supongamos que $\overline{P_1} = \overline{P_2}$ y, sin pérdida de generalidad, podemos suponer que $p \nmid x_1$ (es análogo con las otras coordenadas), entonces, como $\overline{x_1} = \overline{x_2}$, $p \nmid x_2$. Entonces $(\overline{x_1x_2}, \overline{x_1y_2}, \overline{x_1z_2}) = \overline{P_2} = \overline{P_1} = (\overline{x_2x_1}, \overline{x_2y_1}, \overline{x_2z_1})$, o sea que las segundas y terceras coordenadas son iguales entre sí módulo p (las primeras es obvio), i.e., p divide a $\overline{x_1y_2} - \overline{x_2y_1}$ y a $\overline{x_2z_1} - \overline{x_1z_2}$. Nos falta ver que p divide a $\overline{y_1z_2} - \overline{y_2z_1}$. Si tanto y_1 como z_1 son múltiplos de p, entonces listo, y si alguno no lo es, procedemos de manera análoga a como hicimos con x_1.
Recíprocamente, supongamos que p divide al producto vectorial. Tenemos dos casos:

- $p \mid x_1$. Entonces p divide a x_2z_1 y a x_2y_1, y por lo tanto divide a x_2, porque de lo contrario debería diviri a y_1 y a z_1, pero los tomamos coprimos. Ya tenemos que son iguales las primeras coordenadas. Supongamos ahora que $p \nmid y_1$. Entonces $\overline{P_2} = (\overline{0}, \overline{y_1y_2}, \overline{y_1z_2}) = (\overline{0}, \overline{y_1y_2}, \overline{y_2z_1}) = (\overline{0}, \overline{y_2}, \overline{z_2}) = \overline{P_2}$ (aquí usamos el resto de las hipótesis del Lema).
- $p \nmid x_1$. Entonces tampoco divide a x_2 por el mismo argumento del caso anterior. Tenemos $\overline{P_1} = (\overline{x_2x_1}, \overline{x_2y_1}, \overline{x_2z_1}) = (\overline{x_2x_1}, \overline{x_1y_2}, \overline{x_1z_2}) = \overline{P_2}$.

Con esto queda probada la afirmación.
Ahora, sigamos con la Prop. 1.13. Supongamos por absurdo que hay más de cuatro puntos de torsión, entonces tenemos o bien algún elemento de orden impar, o todos los elementos de orden par y el grupo tiene tamaño $2^k \geq 8$. Entonces existe o bien un subgrupo $H < E_n(\mathbb{Q})_{tors}$ de orden impar o bien uno de orden 8. Veremos que cualquiera de los dos casos es absurdo.
Escribamos los puntos $P_i = (x_i, y_i, z_i) \in \mathbb{P}^2_{\mathbb{Q}}$ como veníamos haciendo (el representante con entradas enteras coprimas). Para cada par P_i, P_j, consideramos su producto vectorial $(y_iz_j - y_jz_i, x_iz_j - x_jz_i, x_iy_j - x_jy_i)$. Como los puntos son distintos en $\mathbb{P}^2_{\mathbb{Q}}$, no están alineados como vectores de $\mathbb{R}^3$ y por lo tanto su producto vectorial no es el vector nulo, así que podemos considerar n_{ij} el máximo común divisor de sus entradas. Por la afirmación, $\overline{P_i} = \overline{P_j}$ si y sólo si p divide a n_{ij}. Entonces, si tomamos un primo $p \nmid 2n$ más grande que todos los n_{ij}, esto no podrá pasar y tenemos que el mapa de la reducción módulo p de H en $E_n(\mathbb{F}_p)$ es un morfismo inyectivo, y esto va a pasar a partir de un primo para todos los siguientes. Pero esto nos dice que m,

el cardinal de H, divide al orden de $E_n(\mathbb{F}_p)$, y si consideramos sólo los primos $p \equiv 3$ (mód 4), todos aquellos que sean mayores que 2, que n y que los n_{ij}, por la Prop. 1.12, cumplen que $m \mid p+1$ i.e., $p \equiv -1$ (mód m), o sea que sólo una cantidad finita no lo cumplen. Veamos que esto contradice el Teorema de Dirichlet, que dice que si dos enteros a y b son coprimos, entonces existen infinitos primos p de la forma $p \equiv a$ (mód b).

- Si $m = 8$. Existen sólo finitos $p \equiv 3$ (mód 8).
- Si m es impar coprimo con 3. Existen sólo finitos primos $p \equiv 3$ (mód m) y $p \equiv 3$ (mód 4), o sea, por Teorema Chino de los Restos, $p \equiv 3$ (mód $4m$).
- Si m es impar y múltiplo de 3. Existen sólo finitos primos $p \equiv 1$ (mód 3) y $p \equiv 3$ (mód 4), o sea, por Teorema Chino de los Restos de nuevo, $p \equiv 7$ (mód 12).

En todos los casos, se contradice el Teorema de Dirichlet, por lo que fue absurdo suponer que hay más de cuatro elementos en $E_n(\mathbb{Q})_{tors}$, con lo que queda demostrada la Prop. 1.13. □

Esta proposición nos dice que no hay "puntos no obvios"de orden finito en $E_n(\mathbb{Q})$, que nos aproxima bastante a nuestra pregunta original: ¿Es n un número congruente? La siguiente proposición nos responderá esta interrogante (o nos acercará a lo que buscamos como respuesta definitiva).
Introduciremos la notación $p-$ádica para facilitar las cuentas.
Para un primo p, definimos la valuación $p-$ádica de un entero a como

$$v_p(a) := \text{máx}\{k : p^k \mid a\}, \tag{1.18}$$

y la extendemos a los racionales como:

$$v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b). \tag{1.19}$$

Es fácil ver que si tenemos dos racionales r, s, $v_p(rs) = v_p(r) + v_p(s)$ y que si $v_p(r) > v_p(s)$, entonces $v_p(r \pm s) = v_p(s)$.

PROPOSICIÓN 1.14. *Un natural libre de cuadrados n es un número congruente si y sólo si el rango r de $E_n(\mathbb{Q})$ es positivo, i.e. la curva $E_n(\mathbb{Q})$ tiene puntos de orden infinito.*

DEMOSTRACIÓN. Para el directo, supongamos que n es un número congruente. Al comienzo, por la proposición 1.1, vimos que un triángulo rectángulo de área n nos generaba una solución a la ecuación $E_n(\mathbb{Q})$ donde la coordenada x era el cuadrado de un racional positivo. Como la coordenada x de los puntos de orden finito es $0, \pm n$, y n lo venimos suponiendo libre de cuadrados, la solución a la ecuación que nos da ese triángulo debe ser una distinta, o sea, dar un punto de orden infinito.
Recíprocamente, supongamos que $P = (x, y)$ es un punto de orden infinito. Usemos la fórmula 1.16 para calcular la coordenada x de $2P$ y ver que esta cumple las tres

condiciones de la Prop. 1.2.

$$\begin{aligned} x_{2P} &= -2x + \left(\frac{f'(x)}{2y}\right)^2 \\ &= \frac{-2x(4y^2) + (3x^2 - n^2)^2}{(2y)^2} \\ &= \frac{-8x^4 + 8x^2n^2 + 9x^4 - 6x^2n^2 + n^4}{(2y)^2} \\ &= \frac{x^4 + 2x^2n^2 + n^4}{(2y)^2} = \left(\frac{x^2 + n^2}{2y}\right)^2. \end{aligned} \tag{1.20}$$

Por lo que x_{2P} es el cuadrado de un número racional.

Podemos escribir $x = \frac{a}{b}$ y la ecuación 1.20 queda:

$$x_{2P} = \frac{(a^2 + n^2b^2)^2}{4ab(a^2 - n^2b^2)} \tag{1.21}$$

Lo que queremos probar primero es $v_2((a^2 + n^2b^2)^2) < v_2(4ab(a^2 - n^2b^2))$. Si el primer término es cero (o sea, el numerador es impar), ya está listo. Si el numerador es par, tenemos dos casos:
Caso 1: Tanto a^2 como n^2b^2 son impares.

Entonces $a^2 \equiv n^2b^2 \equiv 1 \pmod 4$, por lo que su suma es 2 módulo 4, o sea, su valuación 2-ádica es 1.

$$v_2((a^2 + n^2b^2)^2) = 2v_2(a^2 + n^2b^2) = 2 < 2 + v_2(ab(a^2 - n^2b^2)) = v_2(4ab(a^2 - n^2b^2)).$$

Caso 2: Tanto a^2 como n^2b^2 son pares.

$a = 2a_0$, $n = 2n_0$ y b impar.

$$v_2((a^2 + n^2b^2)^2) = 2v_2(a^2 + n^2b^2) = 2v_2(4(a_0^2 + n_0^2b^2)) = 4 + 2v_2(a_0^2 + n_0^2b^2).$$

Como $n_0^2b^2$ es impar (n era libre de cuadrados), si a_0 es par, la última valuación es 0, y si a_0 es impar, por el mismo argumento del caso 1, esa valuación es 1.

$$v_2((a^2 + n^2b^2)^2) \leq 4 \text{ ó } 6.$$

Por otro lado, para el numerador, tenemos

$$v_2(4ab(a^2 - n^2b^2)) = v_2(4 \cdot 2 \cdot a_0 4(a_0^2 - n_0^2b^2)) = 5 + v_2(a_0(a_0^2 - n_0b^2)) \geq 6 \text{ ó } 7, \tag{1.22}$$

, en casos de que a_0 sea par o impar (ya que $a_0^2 - n_0^2b^2 \equiv 0 \pmod 4$) con lo que tenemos lo que buscábamos.

Nos falta ver que el numerador de x_{2P} es coprimo con n.
Sea p primo impar con $p \mid n$. Si $p \nmid a$, ya está listo, pues p no divide al numerador en la expresión 1.21. Si $p \mid a$, queremos probar que

$$v_p((a^2 + n^2b^2)^2) \leq v_p(4ab(a^2 - n^2b^2)) = v_p(a(a^2 - n^2b^2))$$

Escribimos $a = pa_0$ y $n = pn_0$. Como x_{2P} es el cuadrado de un racional, y el numerador en 1.21 es el cuadrado de un entero, el denominador también lo es, o sea que la valuación en cualquier primo es par. De la ecuación 1.21:
(1.23)
$v_p(4ba(a^2-n^2b^2)) = v_p(a(a^2-n^2b^2)) = v_p(pa_0p^2(a_0^2-n_0^2b^2)) = 3+v_p(a_0(a_0^2-n_0^2b^2))$,
se sigue que $p \mid a_0$ ó $p \mid (a_0^2 - n_0^2b^2)$, y no puede ser ambos a la vez.

Si $p \mid a_0$, tenemos:

$$v_p((a^2 + n^2b^2)^2) = v_p(p^4(a_0^2 + n_0^2b^2)^2) = 4$$
$$v_p(a(a^2 - n^2b^2)) = 3 + v_p(a_0(a_0^2 - n_0^2b^2)) \geq 4,$$

que es lo que queríamos probar.

Si $p \mid a_0^2 - n^2b^2$, entonces $a_0^2 \equiv n_0^2b^2 \not\equiv -n_0^2b^2$, pues p es impar, o sea, $p \nmid (a_0^2 + n^2b^2)$. Tenemos:

$$v_p((a^2 + n^2b^2)^2) = v_p(p^4(a_0^2 + n_0^2b^2)^2) = 4$$
$$v_p(4ba(a^2 - n^2b^2)) = 3 + v_p(a_0(a_0^2 - n_0^2b^2)) \geq 4,$$

que, de nuevo, es lo que queríamos probar. □

Capítulo 2

Funciones Z y L

Al final del capítulo pasado, trabajamos módulo p para obtener información sobre la curva $E_n : y^2 = x^3 - n^2x$ y el problema de los números congruentes. Vimos la curva E_n sobre el cuerpo finito $\mathbb{F}_p$ con $p \nmid 2n$ y llegamos a que resolver el problema de los números congruentes es equivalente a saber si el rango de E_n es positivo o no. Esto es bastante trabajoso. En general, calcular el rango de una curva elíptica es algo sumamente difícil, habiendo conjeturas muy importantes sobre ello (de las que hablaremos más adelante).

Para avanzar en nuestra pregunta, primero, daremos una fórmula para $\#E_n(\mathbb{F}_q)$ para cualquier potencia de primo q (lo habíamos resuelto para $q \equiv 3 \pmod 4$) y luego usaremos los números $N_r = N_{r,p} = \#E_n(\mathbb{F}_{p^r})$ para definir una función que es análoga a la famosa función zeta de Riemann. Luego, probaremos que esta función se puede extender a todo el plano complejo y de ahí, probaremos otra casi equivalencia a ser un número congruente.

1. Función zeta de congruencia

Definición 2.1. Dada una sucesión N_r de números reales, definimos su correspondiente **función zeta** como:

$$Z(t) := \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right) \in \mathbb{R}[[t]], \quad \text{donde} \quad \exp(u) := \sum_{k=0}^{\infty} \frac{u^k}{k!}.$$

Proposición 2.1. *Si $a, b \in \mathbb{C}$, la función* exp *cumple:*

$$\exp(a+b) = \exp(a)\exp(b),$$

de lo que sigue inmediatamente que si $N_r = A_r + B_r$ para todo r, y Z_N, Z_A y Z_B son las funciones zeta correspondientes entonces $Z_N = Z_A \cdot Z_B$

Demostración.

$$\begin{aligned}
\exp(a+b) &= \sum_{k=0}^{\infty} \frac{(a+b)^k}{k!} \\
&= \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{l=0}^{k} a^l b^{k-l} \frac{k!}{(k-l)!l!} \\
&= \sum_{k=0}^{\infty} \sum_{l=0}^{k} \frac{a^l b^{k-l}}{(k-l)!l!} \\
&= \sum_{i,j=1}^{\infty} \frac{a^i b^j}{i!j!} \\
&= \left(\sum_{i=0}^{\infty} \frac{a^i}{i!} \right) \left(\sum_{j=0}^{\infty} \frac{b^j}{j!} \right) \\
&= \exp(a) \exp(b)
\end{aligned}$$

□

Definición 2.2. Sea E una curva elíptica definida sobre el cuerpo finito $\mathbb{F}_q$. La **función zeta de la curva** E es la función zeta tomando como sucesión $N_r = \#E(\mathbb{F}_{p^r})$, o sea:

$$Z(E/\mathbb{F}_q; t) := \exp\left(\sum_{r=1}^{\infty} \#E(\mathbb{F}_{q^r}) \frac{t^r}{r} \right)$$

Es claro que $\#E(\mathbb{F}_{p^r})$ es finito para todo r pues el plano proyectivo $\mathbb{P}^2$ sobre el cuerpo finito $\mathbb{F}_{p^r}$ es un conjunto finito.

Observación 2.1. Esta definición se puede extender en a cualquier a cualquier variedad algebraica, ireducible o no, proyectiva o afín, sobre un cuerpo finito. Acá sólo nos interesa considerar el caso en que la variedad es una curva proyectiva lisa de género 1 donde la característica del cuerpo no es 2, i.e., una curva elíptica.

En general, calcular la función zeta de una curva elíptica es algo complicado, por lo que nosotros sólo nos concentraremos en el caso de la curva E_n.

2. Función Z de $\mathbf{E}_n$ y sumas de Gauss y Jacobi

Recordamos, como siempre, que E_n son los ceros proyectivos de la ecuación $zy^2 = x^3 - n^2xz^2$, la completación proyectiva de $y^2 = x^3 - n^2x$, que consiste en añadirle el"punto en el infinito"). E_n es una curva elíptica sobre cualquier cuerpo cuya característica no divida a $2n$. En particular, la hemos trabajado en $\mathbb{Q}$, $\mathbb{R}$ y en los cuerpos finitos $\mathbb{F}_p$ y $\mathbb{F}_q$, $q = p^r$. El propósito de esta sección es expresar $\#E_n(\mathbb{F}_q)$ en términos de *sumas de Jacobi*, que definiremos enseguida.

Primero, veamos cómo se relacionan los $\mathbb{F}_q-$puntos de las curvas E_n y E'_n : $u^2 = v^4 + 4n^2$. Como de costumbre, supondremos que $p \nmid 2n$. Si (u, v) está en $E'_n(\mathbb{F}_q)$, entonces el punto $(x, y) = (\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2))$ está en $E_n(\mathbb{F}_q) - \{(0, 0)\}$, pues $u + v^2 \neq 0$. Al revés, si (x, y) está en $E_n(\mathbb{F}_q) - \{(0, 0)\}$, entonces el punto $(u, v) = (2x - \frac{y^2}{x^2}, \frac{y}{x})$ está en E'_n. Más aún, estos mapas son inversos uno del otro, o sea que los puntos de $E_n - \{(0, 0)\}$ están en biyección con los puntos de E'_n. Sea N' la cantidad de $\mathbb{F}_q-$soluciones (u, v) de $u^2 = v^4+4n^2$. Entonces los puntos de nuestra curva elíptica E_n consisten en el $(0, 0)$, el punto en el infinito y los N' puntos correspondientes a los (u, v) de E'_n, o sea, $\#E_n(\mathbb{F}_q) = N' + 2$, por lo que sólo resta calcular N'. La ventaja de haber hecho todo este cuento es que la ecuación $u^2 = v^4 + 4n^2$ es lo que se conoce como *hipersuperficie diagonal*, i.e., los ceros de un polinomio f en $k[x_1, \ldots, x_m]$ (para cualquier cuerpo k) donde cada monomio incluye, a lo más, una variable y cada variable aparece, a lo más, en un monomio (otro ejemplo la curva de Fermat $x^d + y^d = 1$).

Lo que necesitaremos para determinar la cantidad de puntos de una hipersuperficie diagonal sobre un cuerpo finito son las sumas de Gauss y de Jacobi, que es lo que definiremos ahora.

Definición 2.3. Sea $\mathbb{F}_{q^m}/\mathbb{F}_q$ una extensión de cuerpos finitos. Se definen la **traza** y la **norma** de un elemento $a \in \mathbb{F}_{q^m}$ como $Tr(a) = a + a^q + a^{q^2} + \cdots + a^{q^{m-1}}$ y $N_o(a) = a \cdot a^q \cdot a^{q^2} \ldots a^{q^{m-1}} = a^{\frac{q^m-1}{q-1}}$.

Para más contenido sobre traza y norma en cuerpos finitos, ver [**LN08**, Cap. 2.3, pág. 50].

Observación 2.2. La norma N_o siempre pertenece a $\mathbb{F}_q$. Para ver esto, recordemos que el cuerpo $\mathbb{F}_q$ es el cuerpo de descomposición del polinomio $x^q - x$ sobre $\mathbb{F}_p$, así que basta chequear que $N_o(a)$ es raíz de ese polinomio para cualquier a. Si $a = 0$, es obvio, y si no, es lo mismo que chequear que es raíz de $x^{q-1} - 1$, que es cierto ya que a tiene orden divisor de $q^m - 1$ por vivir en $\mathbb{F}_{q^m}$. Además, es sobreyectiva en $\mathbb{F}_q$. Como $N_o(0) = 0$, es suficiente ver que es sobreyectiva de $\mathbb{F}^*_{q^m}$ en $\mathbb{F}^*_q$. Ahí, N_o es un morfismo de los grupos multiplicativos, y el núcleo son exacamente los elementos que son raíces del polinomio $f = x^{\frac{q^m-1}{q-1}} - 1$. En $\mathbb{F}_{q^m}$, ese polinomio escinde, por lo que el núcleo del morfismo N_o tiene cardinal $\frac{q^m-1}{q-1}$ y, por lo tanto, la imagen tiene cardinal $\frac{q^m-1}{\frac{q^m-1}{q-1}} = q - 1$, o sea, la imagen es todo $\mathbb{F}_q$.

Definición 2.4. Un **caracter aditivo** $\psi : \mathbb{F}_q \longrightarrow \mathbb{C}^*$ es un morfismo de grupos donde $\mathbb{F}_q$ es un grupo con la suma y $\mathbb{C}^*$ con el producto. Observar que como $\mathbb{F}_q$ es finito y todos los elementos tienen orden p, la imagen está dentro de las raíces $p-$ésimas de la unidad. De ahora en más, escribiremos $\psi(x) = \xi^{Tr(x)}$, donde $\xi = e^{\frac{2\pi i}{p}}$ y Tr es la traza de $\mathbb{F}_q$ en $\mathbb{F}_p$ (se puede ver que todos los caracteres aditivos son de esa forma). Un **caracter multiplicativo** $\chi : \mathbb{F}^*_q \longrightarrow \mathbb{C}^*$ es un morfismo de grupos donde ambos $\mathbb{F}^*_q$ y $\mathbb{C}^*$ son grupos con su producto.

Estas definiciones se pueden generalizar a cualquier anillo, aunque con propiedades menos buenas.

En lo que sigue, el caracter aditivo ψ será no trivial y estará fijo, en cambio, los caracteres multiplicativos irán variando. Definimos ahora la suma de Gauss de un caracter multiplicativo χ como:

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x),$$

donde convenimos por comodidad que $\chi(0) = 0$ para cualquier caracter, incluso el caracter trivial, y definimos también la suma de Jacobi de dos caracteres multiplicativos χ_1 y χ_2 como:

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1-x)$$

Las siguientes son algunas propiedades de las sumas de Gauss y Jacobi. No las vamos a probar acá. Para profundizar y ver una prueba de esto y varias prpoposiciones siguientes, ver [**LN08**, Teorema 5.12].

PROPOSICIÓN 2.2. *Denotamos χ_{triv} al caracter multiplicativo trivial, i.e. el que cumple que $\chi_{triv}(x) = 1$ para todo $x \neq 0$ y $\chi_{triv}(0) = 0$; χ, χ_1 y χ_2 caracteres multiplicativos no triviales; y $\overline{\chi}$ al caracter conjugado de χ, i.e., $\overline{\chi}(x) = \overline{\chi(x)} = \chi(x^{-1})$.*

1. $g(\chi_{triv}) = -1$;
2. $J(\chi_{triv}, \chi_{triv}) = q - 2$;
3. $J(\chi_{triv}, \chi) = -1$;
4. $J(\chi, \overline{\chi}) = -\chi(-1)$;
5. $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$;
6. $g(\chi) \cdot g(\overline{\chi}) = \chi(-1)q$;
7. $|g(\chi)| = \sqrt{q}$;
8. $J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}$;
9. $\sum_{x \in \mathbb{F}_q^*} \chi(x) = 0$.

Calculemos ahora la cantidad N' de puntos $(u, v) \in (\mathbb{F}_q)^2$ que verifican $u^2 = v^4 + 4n^2$. La clave es ver que, para cualquier $a \neq 0$ en $\mathbb{F}_q$ y cualquier $m \mid q-1$, se tiene que la cantidad de soluciones de $x^m = a$ está dada por:

$$\#\{x \in \mathbb{F}_q : x^m = a\} = \sum_{\chi : \chi^m = \chi_{\text{triv}}} \chi(a) \tag{2.1}$$

Esto se debe a que, como el conjunto de la derecha es no vacío debido a que $m \mid q-1$, tenemos $\chi(a) = \chi(x)^m = 1$ (aporta 1 a la suma). Fijada r una raíz primitiva de $\mathbb{F}_q$ y x_i una raíz m-ésima de a, para cada x del conjunto, podemos definir el caracter:

$$\chi_x(r) = x_i^{-1}x, \quad \chi_x^m(r) = a^{-1}a = 1.$$

Y es fácil ver, de la misma forma, que los caracteres que cumplen $\chi^m = \chi_{\text{triv}}$ son sólo esos, por lo que los tenemos todos y cada uno aporta 1.

Por la proposición 1.12 del capítulo 1, sabemos que $\#E_n(\mathbb{F}_q) = q+1$ si $q \equiv 3 \pmod 4$, así que calculemos sólo el caso en que $q \equiv 1 \pmod 4$.

Contamos por separado los pares (u,v) dependiendo de si alguna de las coordenadas es cero o no. Nos queda:

$$\begin{aligned} &N' = A + B + C, \quad \text{donde} \\ &A = \#\{u \in \mathbb{F}_q : u^2 = 4n^2\}; \\ &B = \#\{v \in \mathbb{F}_q : 0 = v^4 + 4n^2\}; \\ &C = \#\{(u,v) \in (\mathbb{F}_q^*)^2 : u^2 = v^4 + 4n^2\}. \end{aligned} \tag{2.2}$$

El primer término claramente es 2. Para el segundo, usamos la ecuación 2.1. Sea χ_4 un caracter de $\mathbb{F}_q^*$ que tenga orden 4, i.e. $\chi_4(g) = i$ para algún generador g de $\mathbb{F}_q^*$. Todos los caracteres de orden divisor de 4 son χ_4, $(\chi_4)^2$, $(\chi_4)^3 = \overline{\chi}_4$ y $(\chi_4)^4 = \chi_{\text{triv}}$. Usando que $-4n^2$ es un cuadrado (porque $q \equiv 1 \pmod 4$), nos queda:

$$\sum_{j=1}^{4} \chi_4^j(-4n^2) = 2\chi_4(-4n^2) + 2. \tag{2.3}$$

Ahora, calculemos el tercer término. Sea χ_2 el caracter no trivial de orden 2 (i.e. $\chi_2 = \chi_4^2$). Usando la ecuación 2.1 de nuevo, nos queda:

$$\sum_{\substack{a,b \in \mathbb{F}_q^* \\ a = b + 4n^2}} \#\{u^2 = a\} \cdot \#\{v^4 = b\} = \sum_{\substack{a \in \mathbb{F}_q^* \\ a - 4n^2 \neq 0}} \sum_{j=1}^{4} \sum_{k=1}^{2} \chi_2^k(a)\chi_4^j(a - 4n^2). \tag{2.4}$$

Notar que como $\chi_4(0) = 0$, podemos eliminar la condición de que $a - 4n^2 \neq 0$ en la suma final. Hacemos el cambio de variable $x = \frac{a}{4n^2}$ en la primera suma de la derecha. Nos queda, luego de cambiar el orden de las sumas:

$$\sum_{j=1}^{4} \sum_{k=1}^{2} \chi_4^j(-4n^2) \sum_{x \in \mathbb{F}_q^*} \chi_2^k(x)\chi_4^j(1-x) = \sum_{j=1}^{4} \sum_{k=1}^{2} \chi_4^j(-4n^2) J(\chi_2^j, \chi_4^j). \tag{2.5}$$

Finalmente, juntando las tres formas de escribir los términos de N', usando las propiedades 2, 3 y 4 mencionadas en 2.2, ya que $\chi_4^4 = \chi_2^2 = \chi_{\text{triv}}$ y que $\chi_4^2 = \chi_2 = \overline{\chi}_2$, nos queda:

(2.6)

$$\begin{aligned} N' &= 2 + 2 + 2\chi_4(-4n^2) + \sum_{j=1,3} \chi_4^j(-4n^2) J(\chi_2, \chi_4^j) + q - 2 + 3(-1) + 2\chi_4(-4n^2)(-1) \\ &= q - 1 + \chi_4(-4n^2)(J(\chi_2, \chi_4) + J(\chi_2, \overline{\chi}_4)). \end{aligned}$$

Es rutinario probar que $\chi_4(-4) = 1$, con lo que $\chi_4(-4n^2) = \chi_2(n)$, y si llamamos

$$\alpha = \alpha_{n,q} = -\chi_2(n) J(\chi_2, \chi_4), \tag{2.7}$$

concluímos que:

$$N_1 = \#E_n(\mathbb{F}_q) = N' + 2 = q + 1 - \alpha - \overline{\alpha}, \tag{2.8}$$

ya que $J(\chi_2, \overline{\chi}_4) = \overline{J(\chi_2, \chi_4)}$ y $\chi_2 = \overline{\chi}_2$.

Notar que $\alpha \in \mathbb{Z}[i]$, $\alpha = a + bi$. Usando la propiedad 8 de 2.2, tenemos:

$$\alpha = -\chi_2(n)\frac{g(\chi_2)g(\chi_4)}{g(\overline{\chi}_4)}, \tag{2.9}$$

y por lo tanto, usando la propiedad 7 de 2.2, tenemos:

$$|\alpha|^2 = a^2 + b^2 = q. \tag{2.10}$$

En cualquiera de los dos casos, $q = p \equiv 1 \pmod 4$ y $q = p^2, p \equiv 3 \pmod 4$, hay varias posibilidades para el α. En el primero, son 8 ($\pm a \pm bi$ y $\pm b \pm ai$) y en el segundo caso hay cuatro posibilidades ($\pm p \pm pi$). El siguiente lema nos ayudará a determinar cuál es en el teorema que probaremos.

LEMA 2.1. *Sea $q \equiv 1 \pmod 4$, y sean χ_2, χ_4 caracteres multiplicativos de $\mathbb{F}_q^*$ de órdenes 2 y 4, respectivamente. Entonces $1 + J(\chi_2, \chi_4)$ es divisible por $2 + 2i$ en el anillo $\mathbb{Z}[i]$.*

Ahora, tenemos todos los ingredientes necesarios para dar una fórmula explícita de $Z(E_n/\mathbb{F}_p; t)$.

TEOREMA 2.1. *Sea E_n la curva elíptica $y^2 = x^3 - n^2x$ sobre $\mathbb{F}_p$, con p primo y $p \nmid 2n$. Entonces:*

$$Z(E/\mathbb{F}_p; t) = \frac{1 - 2aT + pt^2}{(1-t)(1-pt)} = \frac{(1-\alpha t)(1-\overline{\alpha} t)}{(1-t)(1-pt)}, \tag{2.11}$$

donde $a = Re\alpha$, $\alpha = i\sqrt{p}$ si $p \equiv 3 \pmod 4$ y $\alpha \in \mathbb{Z}[i]$ es un elemento de norma p que es congruente a $\left(\frac{n}{p}\right)$[1] módulo $2 + 2i$ si $p \equiv 1 \pmod 4$.

DEMOSTRACIÓN. Para poder calcular $Z(E_n/\mathbb{F}_p; t)$, tenemos que hacer variar r y calcular $N_r = \#E_n(\mathbb{F}_{p^r})$ para los $p \equiv 1 \pmod 4$, y $N_{2r} = \#E_n(\mathbb{F}_{p^{2r}})$ para los $p \equiv 3 \pmod 4$ (pues ya sabemos que $N_r = p^r + 1$ si r impar en ese caso). Escribimos $q = p$ en el primer caso y $q = p^2$ en el segundo, así cuando variamos r por todos los enteros positivos, cubrimos todos los casos que queríamos.

Como r está variando y, por lo tanto, también el cuerpo $\mathbb{F}_{q^r}$, los caracteres que vamos a considerar también irán variando. Notamos $\chi_{2,1} = \chi_2$ al único caracter multiplicativo de orden 2 de $\mathbb{F}_q^*$ y $\chi_{4,1}$ a uno de los dos caracteres de orden 4. Componiendo χ_2 o χ_4 con la norma N_r de $\mathbb{F}_{q^r}/\mathbb{F}_q$, obtenemos caracteres multiplicativos de órdenes 2 y 4 de $\mathbb{F}_{q^m}$, que les llamamos $\chi_{2,r}$ y $\chi_{4,r}$. Para ver esto, sea g un generador del grupo cíclico $\mathbb{F}_q^*$ tal que $\chi_4(g) = i$ y sea g_r un generador del grupo cíclico $\mathbb{F}_{q^r}$ tal que $N_r(g_r) = g$ (esto por la observación 2.2). Con esto, tenemos que

[1]Dado un primo p y un entero cualquiera a, se define el símbolo de Legendre $\left(\frac{a}{p}\right)$ como 1 si a es un cuadrado módulo p (o sea, si existe $x \in \mathbb{Z}$ tal que $a \equiv x^2 \pmod p$), -1 si no lo es y 0 si $a \equiv 0 \pmod p$.

$\chi_{2,r}(g_r) = \chi_2(g) = 1$ y $\chi_{4,r}(g_r) = \chi_4(g) = i$, o sea que tienen órdenes 2 y 4, resectivamente.
Con esas definiciones y usando las igualdades 2.7 y 2.8, tenemos:

$$\begin{aligned} &\#E_n(\mathbb{F}_{q^r}) = q^r + 1 - \alpha_{n,q^r} - \overline{\alpha_{n,q^r}}, \\ &\text{donde} \quad \alpha_{n,q^r} = -\chi_{2,r}(n)\frac{g(\chi_{2,r})g(\chi_{4,r})}{g(\chi_{4,r})}. \end{aligned} \tag{2.12}$$

Ahora usamos una igualdad llamada relación de Hasse-Davenport[**LN08**, Teorema 5.14], que dice:

$$-g(\chi \circ N_r) = (-g(\chi))^r. \tag{2.13}$$

Si aplicamos esa igualdad al α_{n,q^r} que definimos recién, y usamos que $\chi_{2,r}(n) = \chi_2(n^r) = \chi_2(n)^r$ (ya que $n \in \mathbb{F}_p$ y entonces $n^q = n$), tenemos:

$$\alpha_{n,q^r} = \alpha_{n,q}^r. \tag{2.14}$$

Ahora, probemos el teorema mismo. Si $p \equiv 1 \pmod 4$, en la que por la cual $q = p$, $\chi_2(n)$ es el símbolo de Legendre $(\frac{n}{p})$. Usando 2.7 y el lema 2.1, tenemos que $\alpha = \alpha_{n,p}$ es un entero Gaussiano ($\mathbb{Z}[i]$) de norma p (por 2.10) que es congruente a $(\frac{n}{p})$ módulo $2 + 2i$. Ahora, usando 2.12 y 2.14, tenemos:

$$N_r = p^r + 1 - \alpha^r - \overline{\alpha}^r.$$

Ahora, usando las propiedades de la exponencial (2.1), tenemos:

$$Z(E_n/\mathbb{F}_p; t) = \frac{\exp(\sum \frac{t^r}{r})\exp(\sum \frac{(pt)^r}{r})}{\exp(\sum \frac{(\alpha t)^r}{r})\exp(\sum \frac{(\overline{\alpha} t)^r}{r})} = \frac{(1-\alpha t)(1-\overline{\alpha} t)}{(1-t)(1-pt)},$$

que era lo que buscábamos.

Si $p \equiv 3 \pmod 4$, $q = p^2$, entonces $\chi_2(n) = 1$, pues todos los elementos de $\mathbb{F}_p$ son cuadrados en $\mathbb{F}_{p^2}$. Entonces, usando el lema 2.1 y la ecuación 2.10, tenemos que $\alpha_{n,q}$ es un entero Gaussiano de norma p que es congruente a 1 módulo $2 + 2i$. De los cuatro enteros Gaussianos de norma p ($i^k p$ con $k = 0, 1, 2, 3$), sólo $-p$ satisface la condición de congruencia. De nuevo, usando las ecuaciones 2.12 y 2.14, tenemos que para r par:

$$N_r = \#E_n(\mathbb{F}_{q^{r/2}}) = p^r + 1 - (-p)^{\frac{r}{2}} - (-p^{\frac{r}{2}}).$$

Como $N_r = p^r + 1$ cuando r es impar, tenemos que para cualquier r:

$$N_r = p^r + 1 - (i\sqrt{p})^r - (-i\sqrt{p})^r,$$

donde hacemos lo mismo que en el paso anterior y tenemos lo que buscábamos. □

3. Enteros de Gauss

Si consideramos el anillo de enteros guassianos $\mathbb{Z}[i]$, los ideales primos $\mathfrak{p}$ del anillo son de tres tipos: $\mathfrak{p} = (p)$ si $p \equiv 3 \pmod 4$, $\mathfrak{p} = (a + bi)$ si $a^2 + b^2 = p$, que eso ocurre para $p = 2$ y para los $p \equiv 1 \pmod 4$ (ya que un primo impar p es suma de dos cuadrados si y sólo si $p \equiv 1 \pmod 4$[**Ste09**][Teorema 5.7.1]). En este último caso, decimos que 2 ramifica y si p es impar, decimos que p escinde. El grado de un ideal

primo $\mathfrak{p}$, que se nota $\deg \mathfrak{p}$, se define como el grado es la extensión de cuerpos $\mathbb{Z}[i]/\mathfrak{p}$ (es un cuerpo ya que $\mathbb{Z}[i]$ es un dominio de ideales principales y por lo tanto $\mathfrak{p}$ es un ideal maximal) sobre $\mathbb{F}_p$; la misma es 2 en el primer caso y 1 si p escinde. No nos centraremos en el caso $p = 2$. De esta forma, podemos reescribir el último teorema como:

Proposición 2.3.

$$(1-t)(1-pt)Z(E_n/\mathbb{F}_p;t) = \prod_{p\in\mathfrak{p}}(1-(\alpha_{\mathfrak{p}}t)^{\deg\mathfrak{p}}), \tag{2.15}$$

donde el producto es sobre los (uno o dos) ideales primos $\mathfrak{p}$ *de* $\mathbb{Z}[i]$ *que contienen a* p *y* α *se define como* $\alpha_{\mathfrak{p}} = i\sqrt{p}$ *si* $\mathfrak{p} = (p)$*;* $\alpha_{\mathfrak{p}} = a + bi$ *si* p *escinde, donde* $a + bi$ *es el único generador de* $\mathfrak{p}$ *que es congruente a* $(\frac{n}{p})$ *módulo* $2 + 2i$*, y* $\alpha_{\mathfrak{p}} = 0$ *si* $2n \in \mathfrak{p}$.

Ahora, definiremos el mapa $\widetilde{\chi}_n$ en $\mathbb{Z}[i]$ que será multiplicativo y satisfará $\widetilde{\chi}_n(x) = \alpha_{\mathfrak{p}}^{\deg\mathfrak{p}}$ para cualquier generador x de $\mathfrak{p} = (x)$. Este mapa multiplicatido es de la forma $\widetilde{\chi}_n(x) = x\widetilde{\chi}'_n(x)$, donde $\widetilde{\chi}'_n(x)$ vale 0, ± 1 ó $\pm i$.
Primero, definimos $\widetilde{\chi}'_1(x) = 0$ si x tiene algún factor en común con $2n$. Luego, para $n = 1$ definimos $\widetilde{\chi}'_n(x) = i^j$ la única potencia de i tal que $i^j x \equiv 1 \pmod{2+2i}$ (estamos asumiendo x coprimo con 2). Finalmente, para los demás n y para $x \in \mathbb{Z}[i]$ coprimo con 2, definimos $\widetilde{\chi}'_n(x) = \widetilde{\chi}'_n(x)_1(\frac{n}{Nx})$, donde $Nx = x\overline{x}$, siendo N la norma de la extensión recién mencionada, es un entero positivo impar, y $(\frac{-}{m})$ es el símbolo de Legendre generalizado i.e. $(\frac{a}{m_1m_2}) = (\frac{a}{m_1})(\frac{a}{m_2})$. Resumiendo, tenemos:

$$\widetilde{\chi}_n(x) = x\widetilde{\chi}'_n(x); \qquad \widetilde{\chi}'_n(x) = \begin{cases} \widetilde{\chi}'_1(x)(\frac{n}{N_o x}) & \text{para } x \text{ coprimo con } 2n; \\ 0 & \text{en otro caso;} \end{cases} \tag{2.16}$$

para x en $\mathbb{Z}[i]$ coprimo con 2,

$$\widetilde{\chi}'_1(x) = i^k \quad \text{con } i^k x \equiv 1 \pmod{2+2i}. \tag{2.17}$$

Sobre esta función, se puede probar:

Proposición 2.4. *El mapa* $\widetilde{\chi}_n$ *es el único mapa multiplicativo de* $\mathbb{Z}[i]$ *que coincide con* $\alpha_{\mathfrak{p}}^{\deg\mathfrak{p}}$ *en cualquier generador del ideal primo* $\mathfrak{p}$.

Definición 2.5. Un caracter multiplicativo de un anillo R se dice primitivo para un ideal I si el caracter es no trivial para cualquier elemento invertible de R/J, donde J es cualquier ideal estrictamente más grande que I.

Proposición 2.5. *Sea* n' *un generador del ideal* $((2+2i)n)$ *cuando* n *es impar y del ideal* $(2n)$ *cuando* n *es par. El mapa* χ'_n *es un caracter multiplicativo primitivo para el ideal* (n')*. Además, si* ψ *es un caracter aditivo de* R/I *que es no trivial en cualquier* J/I *con* J *estrictamente más grande que* I*. Entonces, se cumple que:*

$$\sum_{x\in R/I} \chi'_n(x)\psi(ax) = \overline{\chi'_n}(a)g(\chi,\psi) \quad \forall a \in R/I,$$

donde g *es la suma de Gauss.*

PROPOSICIÓN 2.6.

$$g(\chi'_n) := \sum_{x\in\mathbb{Z}[i]/(n')} \chi'_n(x)e^{2\pi i \operatorname{Re}(x/n')} = \begin{cases} \left(\frac{-2}{n}\right) n', & n \text{ impar}; \\ \left(\frac{-1}{n_0}\right) n'i, & n = 2n_0 \text{ par}; \end{cases}$$

4. Función zeta de Riemann y función L de Hasse-Weil

En lo que sigue, definiremos varios objetos y enunciaremos algunas propiedades que no vamos a probar para centrarnos en demostrar el último teorema de esta sección, que nos permite relacionar las funciones zeta recién calculadas con el problema de los números congruentes.

DEFINICIÓN 2.6. Para los complejos s con $\operatorname{Re} s > 1$, definimos la función **zeta de Riemann** como:

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}}.$$

La idea de lo que sigue es construir una extensión analítica de la función ζ a todo el plano complejo salvo un punto, que es un polo.

DEFINICIÓN 2.7. La **transformada de Mellin** de una función real $f(t)$ se define para complejos s con $\Re s > 1$ como la integral:

$$M_f(s) := \int_0^{\infty} f(t)t^{s-1}dt.$$

DEFINICIÓN 2.8. La función gamma se define como la transformada de Mellin de e^{-t}, o sea:

$$\Gamma(s) = \int_0^{\infty} e^{-t}t^{s-1}dt.$$

Es fácil ver (resolviendo la integral usando partes) que satisface la siguiente ecuación funcional:

$$\Gamma(s+1) = s\Gamma(s),$$

la cual nos permite extender $\Gamma(s)$ a una función meromorfa en todo el plano complejo excepto por polos simples en $s = 0, -1, -2, \ldots$ (ya que $\Gamma(1) = 1$ y $\Gamma(s) = \frac{\Gamma(s+1)}{s}$).

DEFINICIÓN 2.9. Sea $\mathscr{L}$ el espacio de las funciones $f : \mathbb{R} \longrightarrow \mathbb{C}$ suaves i.e. infinitamente diferenciables que decrecen en el infinito con mayor velocidad que cualquier inversa polinomial i.e., $\lim_{x\longrightarrow\pm\infty} |x|^N f(x) = 0$, $\forall N \in \mathbb{N}$. La *transformada de Fourier* de una función $f \in \mathscr{L}$ es:

$$\hat{f}(y) := \int_{-\infty}^{\infty} e^{-2\pi ixy} f(x)dx.$$

Se puede probar sin dificultad que la integral converge para todo y y que $\hat{f} \in \mathscr{L}$.

Las siguientes son algunas propiedades de la transformada de Fourier:

1. Si $a \in \mathbb{R}$ y $g(x) = f(x+a)$, entonces $\hat{g}(y) = e^{2\pi iay}\hat{f}(y)$.
2. Si $a \in \mathbb{R}$ y $g(x) = e^{2\pi iay} f(x)$, entonces $\hat{g}(y) = \hat{f}(y-a)$.

3. Si $b > 0$ y $g(x) = f(bx)$, entonces $\hat{g}(y) = \frac{1}{b}\hat{f}(\frac{y}{b})$.

Se puede definir la transformada de Fourier de forma análoga para funciones $f : \mathbb{R}^m \longrightarrow \mathbb{C}$ y vamos a tener las mismas propiedades recién mencionadas (donde la integral es en todo $\mathbb{R}^m$). Lo mismo ocurre con las siguientes propiedades, que no demostraremos (incluyendo el teorema), pero se pueden ver en [**Kob93**][Cap. 2, sec. 4].

PROPOSICIÓN 2.7. *(Fórmula de suma de Poisson). Si $g \in \mathscr{L}$, entonces:*

$$\sum_{m=-\infty}^{\infty} g(m) = \sum_{m=-\infty}^{\infty} \hat{g}(m).$$

La versión, cuando $g : \mathbb{R}^m \longrightarrow \mathbb{C}$. es sumando a lo largo, ancho, profundo y lo que sea de las demás dimensiones de $\mathbb{Z}^m$, es decir:

$$\sum_{m\in\mathbb{Z}^m} g(m) = \sum_{m\in\mathbb{Z}^m} \hat{g}(m).$$

DEFINICIÓN 2.10. La *función theta* se define como:

$$\theta(t) := \sum_{m=-\infty}^{\infty} e^{-\pi t m^2} \quad \text{para} \quad t > 0.$$

PROPOSICIÓN 2.8. *La función theta satisface la ecuación funcional:*

$$\theta(t) = \frac{1}{\sqrt{t}}\theta\left(\tfrac{1}{t}\right).$$

TEOREMA 2.2. *La función zeta de Riemann $\zeta(s)$ definida en 2.6 para $\operatorname{Re} s > 1$ se extiende analíticamente a todo el plano complejo excepto por un polo simple en $s = 1$ con residuo 1. Además, si definimos:*

$$\Lambda(s) := \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

Entonces $\Lambda(s)$ es invariante al remplazar s por $1 - s$:

$$\Lambda(s) = \Lambda(1 - s),$$

y eso quiere decir que $\zeta(s)$ verifica la ecuación funcional:

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{(1-s)}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Únicamente mencionaremos que la idea de la prueba es considerar la transformada de Mellin de la función $\theta(t)$.

DEFINICIÓN 2.11. Sea $E_n : y^2 = x^3 - n^2x$ nuestra curva elíptica. Para $s \in \mathbb{C}$, definimos la función L **de Hasse-Weil** de la curva E_n como:

$$\begin{aligned} L(E_n, s) &:= \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E_n/\mathbb{F}_p : p^s)} \\ &= \prod_{p\nmid 2n} \frac{1}{1 - 2a_{E_n,p}p^{-s} + p^{1-2s}} \\ &= \prod_{2n\notin\mathfrak{p}} \frac{1}{1 - \alpha_{\mathfrak{p}}^{\deg \mathfrak{p}}(N\mathfrak{p})^{-s}}, \end{aligned}$$

donde $a_{E_n,p}$ es el a definido en el teorema 2.1, que depende de la curva y del primo en cuestión, y en la segunda ecuación, el producto es sobre todos los ideales primos de $\mathbb{Z}[i]$ para los cuales $p \in \mathfrak{p}$ y p es de buena reducción ($p \nmid 2n$). Recordar que estos ideales son de dos tipos: $\mathfrak{p} = (p)$ si $p \equiv 3 \pmod 4$ y $\deg \mathfrak{p} = 2$, $N\mathfrak{p} = p^2$; y $\mathfrak{p} = (a + bi)$, $a^2 + b^2 = p \equiv 1 \pmod 4$, $\deg \mathfrak{p} = 1$, $N\mathfrak{p} = p$. El valor de $\alpha_{\mathfrak{p}}$ y que las igualdades de arriba son ciertas se derivan de 2.3 y de la segunda igualdad en 2.6.

De la misma forma que para la función zeta de Riemann, podemos expandir el producto de Euler, escribir cada término como una serie geométrica y multiplicar todo. El resultado es:

$$L(E_n, s) = \sum_{m=1}^{\infty} b_m m^{-s}. \tag{2.18}$$

Usando la proposición 2.4, podemos reescribir la última igualdad de $L(E_n, s)$ en términos de la función $\widetilde{\chi}_n$:

$$L(E_n, s) = \prod_{\mathfrak{p}\nmid 2n} \left(1 - \frac{\widetilde{\chi}_n(\mathfrak{p})}{(N\mathfrak{p})^s}\right)^{-1}, \tag{2.19}$$

donde notamos $\widetilde{\chi}_n(\mathfrak{p})$ como $\widetilde{\chi}_n(x)$ para cualquier generador.

Ahora, expandimos este producto de la misma forma que se expande la función zeta de Riemann , y usando que todo ideal tiene una factorización única como producto de ideales primos (ya que $\mathbb{Z}[i]$ es un DIP) y que ambas, la norma N y $\widetilde{\chi}_n$ son multiplicativas, tenemos:

$$L(E_n, s) = \sum_{I} \widetilde{\chi}_n(I)(NI)^{-s}, \tag{2.20}$$

donde la suma es sobre todos los ideales no nulos de $\mathbb{Z}[i]$. Para relacionar esto con la expansión general que escribimos en 2.18, vemos que para obtener la serie en este último, juntamos todos los términos correspondientes a los ideales I con la misma norma, o sea:

$$b_m = \sum_{I, NI=m} \widetilde{\chi}_n(I). \tag{2.21}$$

Notar que, como $\widetilde{\chi}_n(I) = \widetilde{\chi}_1(I)(\frac{n}{NI})$, tenemos:

$$b_m = \left(\frac{n}{m}\right) \sum_{I, NI=m} \widetilde{\chi}_1(I) = \left(\frac{n}{m}\right) c_m, \tag{2.22}$$

donde los c_m son los b_m de la expansión 2.18 para $n = 1$. Entonces, si para un n fijo denotamos χ_n al mapa multiplicativo de $\mathbb{Z}$ dado por $m \longrightarrow (\frac{n}{m})$ (y ya notamos a χ'_n como un mapa multiplicativo de $\mathbb{Z}[i]$ en $\{0, \pm 1, \pm i\}$ de forma análoga a $\widetilde{\chi}'_n$) (para m coprimo con $2n$), tenemos:

$$L(E_n, s) = \sum_{m=1}^{\infty} \chi_n(m) c_m m^{-s}. \tag{2.23}$$

Por último, notamos que todo ideal no nulo tiene cuatro generadores posibles, ya que $\mathbb{Z}[i]$ tiene sólo cuatro invertibles (± 1, $\pm i$), y por lo tanto aparece cuatro veces si listamos elementos en vez de ideales. Entonces:

$$b_m = \frac{1}{4} \sum_{\substack{a+bi \\ a^2+b^2=m}} \widetilde{\chi}_n(a+bi),$$

y

$$\begin{aligned} L(E_n, s) &= \frac{1}{4} \sum_{x \in \mathbb{Z}[i]} \widetilde{\chi}_n(x)(Nx)^{-s} \\ &= \frac{1}{4} \sum_{a+bi \in \mathbb{Z}[i]} \frac{(a+bi)\chi'_n(a+bi)}{(a^2+b^2)^s}. \end{aligned} \tag{2.24}$$

El siguiente teorema es lo último que haremos en este capítulo y lo que necesitaremos para poder relacionar la función L de Hasse-Weil con el problema de los números congruentes.

Teorema 2.3. *La función L de Hasse-Weil $L(E_n, s)$ para la curva elíptica E_n, definida para los s con $\operatorname{Re} s > \frac{3}{2}$, se extiende analíticamente a una función holomorfa en todo $\mathbb{C}$. Además, sean:*

$$N = \begin{cases} 32n^2 & \text{si } n \text{ es impar;} \\ 16n^2 & \text{si } n \text{ es par,} \end{cases} \tag{2.25}$$

y

$$\Delta(s) := \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L(E_n, s). \tag{2.26}$$

Entonces $L(E_n, s)$ satisface la siguiente ecuación funcional:

$$\Delta(s) = \pm \Delta(2-s), \tag{2.27}$$

donde el signo es positivo si $n \equiv 1, 2, 3 \pmod 8$ y negativo si $n \equiv 5, 6, 7 \pmod 8$.

Demostración. Comenzaremos por expresar $L(E_n, s)$ escrita de la forma 2.24, en términos de la transformada de Mellin de una versión en dimensión dos de la función θ definida en 2.10.

Sea entonces $u = (u_1, u_2) \in \mathbb{R}^2$ con alguna coordenada no entera, y sea $t \in \mathbb{R}^+$. Sea $w = (1, i) \in \mathbb{C}^2$, con lo que expresaremos $m \cdot w = m_1 + m_2 i$ para $m \in \mathbb{Z}^2$. Definimos:

$$\begin{aligned} \theta_u(t) &= \sum_{m \in \mathbb{Z}^2} (m+u) \cdot w e^{-\pi t \|m+u\|^2}; \\ \theta^u(t) &= \sum_{m \in \mathbb{Z}^2} m \cdot w e^{2\pi i m \cdot u} e^{-\pi t \|m\|^2}. \end{aligned} \tag{2.28}$$

En función de u y t fijos, podemos encontrar una ecuación funcional para $\theta_u(t)$ usando la fórmula de la suma de Poisson pero variando en $\mathbb{Z}^2$. Tomamos la función $g : \mathbb{R}^2 \longrightarrow \mathbb{C}$ como:

$$g(x) = (x+u) \cdot w e^{-\pi t \|x+u\|^2}.$$

Lo que queremos entonces es encontrar la transformada de Fourier de la función $g(x)$ y, por lo tanto, el otro lado de la fórmula de Poisson. Para eso, llamamos $f(x) = e^{-\pi \|x\|^2}$, $g_1(x) = f(\sqrt{t}x)$, $g_2(x) = w \cdot \frac{\partial}{\partial x} g_1(x)$ y, por último, tenemos $g(x) = \frac{-1}{2\pi t} g_2(x+u)$. Con todo eso, tenemos, usando las propiedades en $\mathbb{R}^m$ de la definición de transformada de Fourier en 2.9:

$$\begin{aligned} \hat{f}(y) &= e^{-\pi \|y\|^2}; \\ \hat{g_1}(y) &= t^{-1} e^{-\pi/t \|y\|^2}; \\ \hat{g_2}(y) &= 2\pi i t^{-1} w \cdot y e^{-\pi \|y\|^2/t}; \\ \hat{g}(y) &= -i t^{-2} w \cdot y e^{2\pi i u \cdot y} e^{-\pi \|y\|^2/t}. \end{aligned}$$

Si ahora evaluamos $\hat{g}(m)$ en $m \in \mathbb{Z}^2$ y sumamos a lo largo y ancho de todo $\mathbb{Z}^2$, tenemos:

$$\theta_u(t) = \frac{-i}{t^2} \theta^u(\tfrac{1}{t}). \tag{2.29}$$

Consideramos ahora la transformada de Mellin de $\theta_u(t)$, $M_{\theta_u}(s) = \int_0^\infty t^{s-1} \theta_u(t) dt$, y veremos que esta se puede extender a una función entera, i.e. holomorfa en todo $\mathbb{C}$. Primero, si t está lejos del cero, el integrando está acotado por algo de la forma e^{-ct} pues $\|m+u\|^2$ está lejos del cero a lo largo de todo $m \in \mathbb{Z}^2$ porque $u \notin \mathbb{Z}^2$. Luego, si t está cerca del cero, usamos la ecuación funcional recién provista y acotar $\theta^u(\frac{1}{t})$ por algo de la forma e^{-ct}, usando que el único término en la definición de θ^u con $\|m\| = 0$ se anula porque $m \cdot w = 0$.

Si tomamos s con $\operatorname{Re} s > \frac{3}{2}$, podemos evaluar la transformada de Mellin término a término, obteniendo algo que se parece mucho a nuestra función L:

$$\begin{aligned} \int_0^\infty t^{s-1} \theta_u(t) dt &= \sum_{m \in \mathbb{Z}^2} (m+u) \cdot w \int_0^\infty t^{s-1} e^{-\pi t \|m+u\|^2} dt \\ &= \pi^{-s} \Gamma(s) \sum_{m \in \mathbb{Z}^2} \frac{(m+u) \cdot w}{\|m+u\|^{2s}}, \end{aligned} \tag{2.30}$$

usando que la transformada de Mellin de la función e^{-ct} para una constante $c > 0$ es:

$$\int_0^\infty e^{-ct} t^{s-1} dt = c^{-s}\Gamma(s).$$

Ahora, para $\operatorname{Re} s > \frac{3}{2}$ podemos reescribir $L(E_n, s)$ como una combinación lineal de esas sumas de variable u.

Suponemos ahora que n es impar. El caso n par es análogo y un poco más sencillo, usando que χ'_n depende módulo $2n$ en vez de $(2+2i)n$. Usando la igualdad en 2.24, como $\chi'_n(x)$ depende de x módulo $n' = (2+2)n$, con más razón, no varía si cambiamos x módulo $4n = 2(1-i)(2+2i)n$. Tenemos entonces:

$$\begin{aligned} L(E_n, s) &= \frac{1}{4} \sum_{0 \le a,b < 4n} \chi'_n(a+bi) \sum_{m \in \mathbb{Z}^2} \frac{a + bi + 4nm \cdot w}{\|(a,b) + 4nm\|^{2s}} \\ &= \frac{1}{4}(4n^{1-2s}) \sum_{a \le 0, b < 4n} \chi'_n(a+bi) \sum_{m \in \mathbb{Z}^2} \frac{(m + (\frac{a}{4n}, \frac{b}{4n})) \cdot w}{\|m + (\frac{a}{4n}, \frac{b}{4n})\|^{2s}}. \end{aligned} \tag{2.31}$$

Con esto y lo anterior, tenemos:

$$\pi^{-s}\Gamma(s)L(E_n, s) = \frac{1}{4}(4n)^{1-2s} \sum_{\substack{0 \le a,b < 4n \\ (a,b) \neq (0,0)}} \chi'_n(a+bi) \int_0^\infty t^{s-1}\theta_u(t)dt. \tag{2.32}$$

donde $u = (\frac{a}{4n}, \frac{b}{4n})$, y usaremos esa notación de ahora en adelante.

Ahora, como la integral dentro de la suma (finita) es una función entera de s, ya que θ_u decrece exponencialmente, y también lo son $(4n^{1-2s})$ y $\frac{\pi^s}{\Gamma(s)}$, concluimos, despejando, que $L(E_n, s)$ tiene una continuación analítica a una función entera, probando la primera parte del teorema.

Para probar el resto, podemos usar la igualdad 2.29 y cambiar t por $\frac{1}{t}$ para obtener:

$$\int_0^\infty t^{s-1}\theta_u(t)dt = -i\int_0^\infty t^{s-3}\theta^u(\tfrac{1}{t})dt = -i\int_0^\infty t^{s-3}\theta^u(t)dt. \tag{2.33}$$

Si en la función entera de 2.31 consideramos sólo los s con $\Re 2 - s > \frac{3}{2}$ (i.e., $\operatorname{Re} s > \frac{1}{2}$), podemos ver la última integral como una suma infinita. Usando 4, la definición de la θ^u e intercambiando sumatoria con integral, tenemos:

$$\int_0^\infty t^{s-3}\theta^u(t)dt = \pi^{2-s}\Gamma(2-s) \sum_{m \in \mathbb{Z}^2} m \cdot w e^{2\pi i m \cdot (a,b)/4n} \|m\|^{-2(2-s)}.$$

Entonces, para los s con $\operatorname{Re} 2 - s > \frac{3}{2}$, el lado derecho de 2.31 queda:

$$-i(4n)^{1-2s}\pi^{s-2}\Gamma(2-s)\frac{1}{4} \sum_{m \in \mathbb{Z}^2} \frac{m \cdot w}{\|m\|^{2(2-s)}} S_m, \tag{2.34}$$

donde para $m \in \mathbb{Z}^2$, definimos:

$$S_m := \sum_{0 \le a,b < 4n} \chi'_n(a+bi) e^{\frac{2}{\pi} im \cdot (a,b)/4n}.$$

Para finalizar la prueba, veamos el siguiente lema y cómo usarlo:

LEMA 2.2. *Si $m_1 + m_2 i = m \cdot w$ no pertenece al ideal generado por $1+i$, entonces $S_m = 0$. Si, por el contrario, $m_1 + m_2 i = (1+i)x$ para algún $x \in \mathbb{Z}[i]$, entonces $S_m = 2\chi'_n(x) g(\chi'_n)$, donde g denota la suma de Gauss definida en la proposición 2.6.*

Si sustituímos $m \cdot 2 = m_1 + m_2 i = (1+i)x$ en la suma de arriba, el lema nos dice que:

$$\begin{aligned} \sum_{m \in \mathbb{Z}^2} \frac{m \cdot w}{\|m\|^{2(2-s)}} S_m &= \sum_{x \in \mathbb{Z}[i]} \frac{2(1+i)x}{\|(1+i)x\|^{2(2-s}} \chi'_n(x) g(\chi'_n) \\ &= (1+i) 2^{s-1} \left(\frac{-2}{n}\right) (2+2i) n \sum_{x \in \mathbb{Z}[i]} \widetilde{\chi}_n(x) (N_o x)^{-(2-s)} \end{aligned}$$

por la proposición 2.6, donde $N_o(x)$ es la norma de x definida en 2.2. La última suma es igual a $4L(E_n, 2-s)$ por 2.24. Juntando todo, tenemos que, si $\mathrm{Re}(2-s) > \frac{3}{2}$, el lado derecho en 2.32 es igual a:

$$\begin{aligned} &- i(4n^{1-2s}) \pi^{s-2} \Gamma(2-s)(1+i) 2^{s-1} \left(\frac{-2}{n}\right) (2+i) n L(E_n, s-s) \\ &= \left(\frac{-2}{n}\right) \pi^{s-2} \Gamma(2-s) (8n^2)^{1-s} L(E_n, 2-s). \end{aligned}$$

Por otro lado, si pasamos el término $\left(\frac{\sqrt{N}}{2}\right)^s$ para el lado derecho en la ecuación funcional, tenemos que lo que queremos probar es:

$$\begin{aligned} \pi^{-s} \Gamma(s) L(E_n, s) &= \left(\frac{-2}{n}\right) \left(\frac{\sqrt{N}}{2}\right)^{-s} (2\pi)^{s-2} \sqrt{N}^{2-s} \Gamma(2-s) L(E_n, 2-s) \\ &= \left(\frac{-2}{n}\right) \left(\frac{N}{4}\right)^{1-s} \pi^{s-2} \Gamma(2-s) L(E_n, 2-s), \end{aligned}$$

que es exactamente lo que vimos recién.
Ahora, probemos el lema:
Supongamos primero que $m_1 + m_2 i$ no es divisible por $1+i$. Esto es lo mismo que decir que m_1 y m_2 tienen distinta paridad (pues lo generado por $1+i$ son cosas de la forma $(x+yi)(1+i) = (x-y) + (x+y)i$, o sea, todos los enteros gaussianos con coordenadas de igual paridad). Por otro lado, como a y b van de 0 a $4n$ (sin ser $4n$), los elementos de la forma $a+bi$ recorren todas las clases módulo $(2+2i)n$ exactamente dos veces (ya que sumar o restar $2n+2ni$ ó $2n-2ni$ es estar en la misma clase). En ambos casos, $\chi'_n(a+bi)$ vale lo mismo por la proposición 2.5, pero veamos que sus términos exponenciales son iguales pero con signo opuesto. Para eso, tomemos $a+bi$ y $c+di$ dos elementos diferentes de esos, o sea, que sean congruentes

módulo $(2+2i)n$ pero no módulo $4n$. Tenemos que $a+bi-(c+di) \equiv (2+2i)n$ (mód $(4n)$), y por lo tanto:

$$\begin{aligned} e^{2\pi im\cdot(a,b)/4n}\left(e^{2\pi im\cdot(c,d)/4n}\right)^{-1} &= e^{2\pi im\cdot((a,b)-(c,d))/4n} \\ &= e^{2\pi im\cdot(2n,2n)/4n} \\ &= e^{\pi i m_1+m_2} \\ &= -1 \end{aligned}$$

porque m_1 y m_2 tienen diferente paridad. Esto prueba la primera parte.

Para la segunda, supongamos que $m_1+m_2i=(1+i)x$. Notar que $m\cdot(a,b) = m_1a+m_2b = \mathrm{Re}((m_1-m_2i)(a+bi)) = \mathrm{Re}((1-i)\overline{x}(a+bi))$ y entonces, el término exponencial en S_m es $\psi(\overline{x}(a+bi))$, donde:

$$\psi(x) := e^{2\pi i\,\mathrm{Re}(x/n')},$$

que es un caracter aditivo como el que se pide en 2.5. Como χ'_n es un caracter primitivo módulo $(2+2i)n$ (por 2.5), y la suma va recorriendo todos los elementos del cociente $\mathbb{Z}[i]/(n')$ dos veces, tenemos que:

$$\begin{aligned} S_m &= 2\sum_{a+bi\in\mathbb{Z}[i]/(2+2i)n} \chi'_n(a+bi)\psi(\overline{x}(a+bi)) \\ &= 2\overline{\chi'_n}(\overline{x})g(\chi'_n) = 2\chi'_n(x)g(\chi'_n), \end{aligned}$$

que es lo que queríamos probar. □

Ahora que tenemos el teorema, podemos relacionarlo con el problema de los números congruentes.

Decimos que una curva elíptica E tiene multiplicación compleja si el anillo $End(E)$ de los morfismos de grupos de E en sí misma contiene estrictamente a $\mathbb{Z}$. Se puede ver que nuestra curva tiene multiplicación compleja.

Conjetura 2.1. *(B. Birch y P. Swinnerton-Dyer, versión débil). Sea E una curva elíptica sobre $\mathbb{Q}$. Entonces el rango de $E(\mathbb{Q})$ es igual al orden del cero de $L(E,s)$ en $s=1$. En particular, $L(E,1)=0$ si y sólo si $E(\mathbb{Q})$ tiene rango positivo, i.e. tiene infinitos puntos racionales.*

Teorema 2.4. *(J. Coates y A. Wiles). Sea E una curva elíptica sobre $\mathbb{Q}$ con multiplicación compleja. Si E tiene infinitos $\mathbb{Q}-$puntos, entonces $L(E,1)=0$.*

Este teorema es bastante difícil y no lo demostraremos. Para una prueba, ver [**CW77**].
En nuestro caso, se puede ver que la curva E_n tiene multiplicación compleja, este teorema junto a la proposición 1.14 nos dice que si $L(E_n,1)\neq 0$ entonces n no es un número congruente, y si n es un número congruente, entonces $L(E_n,1)=0$. Recíprocamente, si la conjetura débil de Birch y Swinnerton-Dyer es cierta, entonces $L(E_n,1)=0$ implica que n es un número congruente. Finalizamos el capítulo con

la siguiente proposición, que nos da una forma de saber, con lo que tenemos hasta ahora, cuándo algunos números n libres de cuadrados son congruentes.

PROPOSICIÓN 2.9. *Si $n \equiv 5, 6$ ó 7 (mód 8), y vale la conjetura débil de Birch y Swinnerton-Dyer para la curva E_n, entonces n es un número congruente.*

DEMOSTRACIÓN. Por el teorema 2.3, tenemos que $\Lambda(s) = -\Lambda(2-s)$. Si ponemos $s = 1$, tenemos que $\Lambda(1) = -\Lambda(1)$, o sea que $\Lambda(1) = 0$. Pero, por la definición de Λ, esto sólo puede pasar si $L(E_n, 1) = 0$, y como la conjetura débil es cierta, esto implica que la curva elíptica tiene rango infinito, i.e., por la proposición 1.14 del capítulo 1, que n es un número congruente. □

Capítulo 3

Formas Modulares

En este capítulo, definiremos nuestro segundo objeto: las formas modulares. Primero, hablaremos de la base sobre la que éstas se paran: el grupo $\mathrm{SL}_2(\mathbb{Z})$; pasaremos a definir lo que es una forma modular de peso entero en un contexto general (subgrupos de congruencia) y sus operadores de Hecke; luego, generalizaremos la idea definiendo formas modulares de peso medio entero, hablaremos de sus respectivos operadores de Hecke y dejaremos todo listo para terminar el problema de los números congruentes en el capítulo final.

1. $\mathrm{SL}_2(\mathbb{Z})$ y subgrupos de congruencia

Para cualquier anillo conmutativo R con unidad, se define el *grupo general lineal* y se nota $\mathrm{GL}_2(R)$ al grupo de matrices $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con determinante en R^* (el subgrupo de los invertibles de R). El *subgrupo especial lineal* $\mathrm{SL}_2(R)$ es el subgrupo de $\mathrm{GL}_2(R)$ de matrices de determinante 1. En este capítulo, nos concentraremos en los casos $R = \mathbb{R}$, $R = \mathbb{Z}$ y $R = \mathbb{Z}/N\mathbb{Z}$ para un entero positivo N.

Sea $\widetilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ (i.e. el plano complejo con un punto, la recta proyectiva $\mathbb{P}^1_{\mathbb{C}}$, llamada la esfera de Riemann). Dado un elemento $g \in \mathrm{SL}_2(\mathbb{R})$ y un $z \in \mathbb{C}$, definimos

$$g \cdot z = \frac{az+d}{cz+d}; \qquad g \cdot \infty = \frac{a}{c} = \lim_{z \longrightarrow \infty} g \cdot z. \tag{3.1}$$

(Así tenemos $g \cdot \frac{-d}{c} = \infty$, y si $c = 0$, $g \cdot \infty = \infty$.)
El mapa $z \longrightarrow g \cdot z$ es una acción (a izquierda) del grupo $\mathrm{SL}_2(\mathbb{R})$, o sea: $g_1(\cdot g_2 \cdot z) = (g_1 g_2) \cdot z$ para todo $z \in \widetilde{\mathbb{C}}$. De ahora en más, para una lectura más cómoda, dejaremos de usar $\cdot$ para notar esta acción y pondremos directamente gz.

Notar que para $g = -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$, las fórmulas 3.1 nos da el mapa identidad, pero $\pm I$ son las únicas matrices que actúan trivialmente, por lo que el cociente $\mathrm{SL}_2(\mathbb{R})/\pm I$, a veces llamado $\mathrm{PSL}_2(\mathbb{R})$, actúa de forma fiel en $\widetilde{\mathbb{C}}$, i.e. la identidad es el único elemento que actúa trivialmente.

Sea $H \subset \mathbb{C}$ el semiplano superior, $H = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. Es importante notar que $\mathrm{SL}_2(\mathbb{R})$ preserva H, i.e. $\operatorname{Im} z > 0$ implica $\operatorname{Im} gz > 0$. Esto es porque

$$\operatorname{Im} \gamma z = \operatorname{Im} \frac{az+b}{cz+d} = \operatorname{Im} \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = |cz+d|^{-2} \operatorname{Im}(adz + bc\overline{z}).$$

pero $\operatorname{Im}(adz + bc\overline{z}) = (ad - bc)\operatorname{Im} z = \operatorname{Im} z$ porque $\det \gamma = 1$, entonces

$$\operatorname{Im} gz = |cz + d|^{-2} \operatorname{Im} z \quad \text{para} \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}). \tag{3.2}$$

Podemos considerar entonces la acción en H, que es lo que haremos de ahora en adelante. El subgrupo de $\mathrm{SL}_2(\mathbb{R})$ con entradas enteras es $\mathrm{SL}_2(\mathbb{Z})$, a veces notado Γ, es llamado el "grupo modular completo". Notamos $\overline{\Gamma} = \Gamma/\pm I$.

Sea N un entero positivo. Definimos:

(3.3)
$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod{N}, \quad b \equiv c \equiv 0 \pmod{N} \right\}.$$

Es llamado **subgrupo principal de congruencia de nivel** N. Es un subgrupo normal de Γ, ya que es el núcleo del morfismo que va de Γ en $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ reduciendo módulo N. O sea, $\Gamma(N)$ es el subgrupo de las matrices con entradas enteras y determinante 1 congruentes con I módulo N. Veremos más adelante que este es el análogo del semigrupo $1 + N\mathbb{Z}$, los enteros congruentes con 1 módulo N.

Notar que $\overline{\Gamma}(N) = \Gamma(N)/\pm I$, si $N > 2$, es $\overline{\Gamma}(N) = \Gamma(N)$, pues $-1 \not\equiv 1 \pmod{N}$) y por lo tanto $-I \notin \Gamma(N)$.

Un subgrupo de Γ es llamado *subgrupo de congruencia de nivel* N si contiene a $\Gamma(N)$ (o a $\overline{\Gamma}(N)$ si estamos en ese contexto). Notar que un subgrupo de congruencia de nivel N es también un subgrupo de congruencia de nivel N' si $N \mid N'$.

No todos los subgrupos de Γ son de congruencia, pero no nos importan los que no lo sean.

Definición 3.1. Los subgrupos de congruencia que más nos importarán son los siguientes:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}; \qquad \Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\};$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

donde $*$ indica que no hay condición de congruencia, o sea, puede ser cualquier entero.

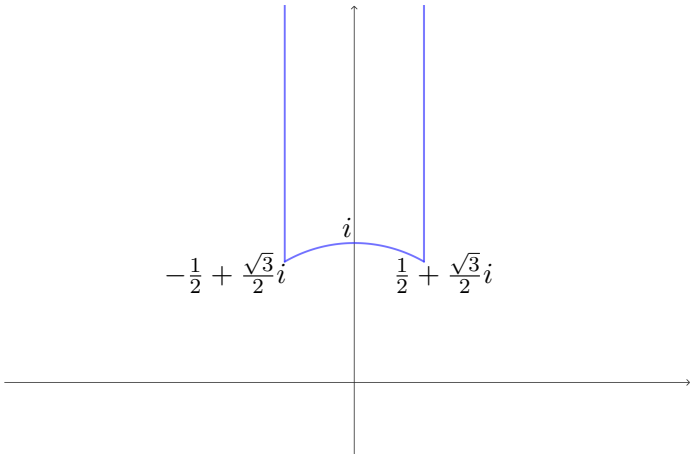
Cuando un grupo actúa sobre un conjunto, lo divide en clases de equivalencia, donde dos elementos son equivalentes si existe un elemento del grupo que lleva uno en el otro. En este caso, si G es un subgrupo de Γ, decimos que z_1 y z_2 son $G-$equivalentes si existe $g \in G$ tal que $gz_1 = z_2$.

Sea F un conjunto cerrado y conexo en H (usualmente también será simplemente conexo). Decimos que F es un *dominio fundamental* para el subgrupo G si todo

elemento de H es $G-$equivalente a alguno de F y no hay dos puntos en el interior de F que sean $G-$equivalentes. O sea, F contiene un conjunto de representantes de las clases que podrían repetirse sólo en el borde. El ejemplo más famoso de un dominio fundamental es:

$$F := \{z \in H : -\tfrac{1}{2} \leq \operatorname{Re} z \leq \tfrac{1}{2}, |z| \geq 1\}, \tag{3.4}$$

representado en la siguiente figura.



PROPOSICIÓN 3.1. *La región F definida en 3.4 es un dominio fundamental para Γ.*

Esta proposición la podemos dividir en las siguientes dos proposiciones más precisas.

PROPOSICIÓN 3.2. *Todo punto de H es $\Gamma-$equivalente a algún punto en F.*

PROPOSICIÓN 3.3. *Dos puntos z_1 y z_2 de F son $\Gamma-$equivalentes si y sólo si son iguales, Re $z_1 = \pm\frac{1}{2}$ y $z_2 = z_1 \pm 1$ ó z_1 está en el círculo unitario y $z_2 = -\frac{1}{z_1}$ (en particular, dos puntos distintos del interior no son equivalentes).*

Más precisamente, en la primera proposición probaremos que cualquier $z \in H$ es $\Gamma'-$equivalente a uno de F, donde Γ' es el subgrupo generado por los siguientes elementos S y T.

$$\begin{aligned} T &:= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : z \mapsto z+1; \\ S &:= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : z \mapsto -\tfrac{1}{z}. \end{aligned} \tag{3.5}$$

En realidad, estos dos elementos generan todo Γ; no es difícil probarlo por ejemplo, usando la *identidad de Bézout*[1], pero aprovecharemos la ocasión para probarlo usando que F es dominio fundamental.

[1]Si a y b son enteros y $d = \mathrm{mcd}(a,b)$, existen enteros x e y tales que $ax + by = d$. En particular, a y b son coprimos si y sólo si existen x e y tales que $ax + by = 1$.

DEMOSTRACIÓN. (3.2). Sea $z \in H$ cualquiera. Si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma'$, entonces $\operatorname{Im} \gamma z = \operatorname{Im} \frac{z}{|cz+d|^2}$ por la ecuación 3.2. Como c y d son enteros y no pueden ser ambos nulos, existe un γ tal que $|cz + d|$ es minimal (el retículo generado por z y 1 sin el 0 tiene un elemento de norma minimal), y para ese γ, tenemos entonces que $\operatorname{Im} \gamma z$ es maximal. Si cambiamos γ por $T^j\gamma$, c y d siguen siendo los mismos por lo que la maximalidad de $\operatorname{Im} \gamma \cdot z$ se mantiene, así que lo hacemos para un j conveniente que deje γz en la franja deseada. Si γz no estuviera en F, o sea, si $|\gamma z| < 1$, por 3.2 tenemos

$$\operatorname{Im} S(\gamma z) = \operatorname{Im} \frac{\gamma z}{|\gamma z|^2} > \operatorname{Im} \gamma z, \tag{3.6}$$

lo que contradice la elección de γ para que $\operatorname{Im} \gamma z$ sea maximal. Entonces existe $\gamma \in \Gamma$ tal que $\gamma z \in F$.

□

DEMOSTRACIÓN. (3.3). Sean z_1 y z_2 en F que son $\Gamma-$equivalentes. Suponemos sin pérdida de generalidad que $\operatorname{Im} z_2 \geq \operatorname{Im} z_1$. Sea $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ tal que $z_2 = \gamma z_1$. Como $\operatorname{Im} z_2 \geq \operatorname{Im} z_1$, por 3.2, tenemos $|cz_1 + d| \leq 1$. Como d es un real (de hecho, un entero), mirando la figura de F es fácil ver que esto sólo puede pasar si $|c| \leq 1$ y $|d| \leq 1$. Eso nos deja los siguientes cuatro casos:

I) $c = 0$ y $d = \pm 1$.
II) $c = \pm 1$, $d = 0$ y z_1 está en el círculo unitario.
III) $c = d = \pm 1$ y $z_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.
IV) $c = -d = \pm 1$ y $z_1 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$

En I), γ es una traslación $\pm T^a$ (el signo no importa ya que vimos que podemos pensar en $\mathrm{PSL}_2(\mathbb{Z})$), pero dicha traslación sólo puede llevar un elemento de F en otro si $a = 0$ y los puntos son iguales o si $a = \pm 1$ y los puntos están uno en el borde derecho de F y otro en el izquierdo.

En II) $\gamma = \pm \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} = \pm T^a S$ con $a = 0$ y z_1 y z_2 en el círculo unitario, simétricos entre ellos respecto al eje imaginario, o $a = \pm 1$ y $z_1 = z_2 =$ alguna de las puntitas de F.

En III), $\gamma = \pm \begin{pmatrix} a & a-1 \\ 1 & 1 \end{pmatrix} = \pm T^a \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, y eso actuando en $z_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ es $z_2 = T^a(-\frac{1}{z_1+1}) = T^a z_1$ donde $a = 0$ y $z_1 = z_2$ ó $z_1 + 1 = z_2$ y son las "puntitas"de F.

En IV), es casi lo mismo que en III) pero $\gamma = \pm \begin{pmatrix} a & 1-a \\ 1 & 1 \end{pmatrix} = \pm T^{-a} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, con lo que z_1 y z_2 o son el mismo punto o son las dos "puntitas"de F. □

PROPOSICIÓN 3.4. *El grupo* $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ *está generado por los elementos* S *y* T.

DEMOSTRACIÓN. Sea Γ' el subgrupo generado por los elementos recién mencionados, y sea z un elemento cualquiera en el interior de F (el que se te cante, elegilo sin miedo). Sea ahora un $g \in \Gamma$ y consiederemos $gz \in H$. Por la Prop. 3.2, existe un $\gamma \in \Gamma'$ tal que $\gamma(gz) \in F$. Pero como z está en el interior de F, por la Prop.

3.3, $(\gamma g)z = z$ y por lo tanto, $\gamma g = \pm I \in \Gamma'$ y $g = \pm\gamma^{-1} \in \Gamma'$, terminando la demostración. □

Recordemos que en el primer capítulo también teníamos un dominio fundamental, el paralelogramo $\Pi \subset \mathbb{C}$, donde el grupo era el retículo L y la acción era $g \cdot z = g + z$. En ese caso, nos convenía identificar los puntos que eran $L-$equivalentes y el paralelogramo de convertía en el toro $\mathbb{C}/L$ y obteníamos un isomorfismo entre este y la curva elíptica $y^2 = 4x^3 - g_2x^2 - g_3$. También nos era conveniente agregar un "punto en el infinito". Haremos ambas cosas en este caso también.

DEFINICIÓN 3.2. Sea $\overline{H} := H \cup \{\infty\} \cup \mathbb{Q}$, o sea, el semiplano superior, los racionales que están en el eje real y el infinito (que lo podemos pensar como el límite de cualquier complejo con norma tendiendo a infinito, como yi con $y \mapsto \infty$). Los puntos nuevos $\mathbb{Q}$ e ∞ los llamamos *cúspides*.

Es fácil ver que Γ permuta las cúspides transitivamente, o sea, ∞ y los racionales están en la misma clase de equivalencia según Γ. Extendemos la topología de H a $\overline{H}$ de la siguiente manera: consideramos el mapa de H en el disco unidad pinchado dado por:

$$z \mapsto q = e^{2\pi i z}$$

y lo extendemos a $\overline{H}$ mandando ∞ en 0. La topología de $\overline{H}$ es la que hace a dicho mapa continuo. Notar que una base de entornos de ∞ en $\overline{H}$ es la pre-imagen de los discos abiertos de centro 0 y radio menor a 1, o sea, los conjuntos $N_C = \{z \in \mathbb{C} : \Im z > C\} \cup \{\infty\}$ para todo $C > 0$. El cambio de variable de z a $q = e^{2\pi i z}$ es muy importante para definir lo que es una forma modular, ya que diremos que una función es meromorfa en infinito si se puede escribir como serie de potencias de q con finitos términos negativos, o sea, que la expansión de Fourier sea de la forma:

$$f(z) = \sum_{n=-l}^{\infty} a_n q^n, \quad l \in \mathbb{N}. \tag{3.7}$$

Decimos que es holomorfa en infinito si $a_n = 0$ para todo $n < 0$ y que se anula en infinito si $a_0 = 0$.
Por último, una base de entornos de las cúspides $\frac{a}{b} \in \overline{H}$ estará dada por extender a y c a una matriz $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ y considerar αN_C, o sea, trasladar N_C por la acción de α. Nos queda que una base de entornos de $\frac{a}{c}$ son las bolas abiertas tangentes a $\frac{a}{c}$ con el punto racional abajo.

2. Formas modulares

DEFINICIÓN 3.3. Sean $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, $f(z) : \overline{H} \longrightarrow \mathbb{C} \cup \{\infty\}$ y k un entero. Definimos una acción (a derecha) de $\mathrm{SL}_2(\mathbb{Z})$ en las funciones f como la mencionada, y de peso introducimos su notación, como:

$$f|[\gamma]_k(z) := (cz + d)^{-k} f(\gamma z). \tag{3.8}$$

Este es el ingrediente principal para definir formas modulares.

DEFINICIÓN 3.4. Sea $f(z)$ una función meromorfa en H, sea $\Gamma' < \Gamma = \mathrm{SL}_2(\mathbb{Z})$ un subgrupo de congruencia de nivel N, o sea, $\Gamma(N) < \Gamma'$ y sea $k \in \mathbb{Z}$. Decimos que f es una función modular de peso k para el subgrupo Γ' si:

$$f|[\gamma]_k = f \quad \text{para todo} \quad \gamma \in \Gamma', \tag{3.9}$$

y, para todo $\gamma_0 \in \Gamma = \mathrm{SL}_2(\mathbb{Z})$, la función $f|[\gamma_0]_k$ sea meromorfa en el infinito y que su desarrollo de Fourier sea de la forma:

$$f|[\gamma_0]_k(z) = \sum_{n=-l}^{\infty} a_n q_N^n \quad l \in \mathbb{N}, \quad q_N = e^{\frac{2\pi i z}{N}}. \tag{3.10}$$

Notar que la diferencia está en que las potencias son q_N y no q.

Si la función f es además holomorfa en H y el infinito (i.e. $a_n = 0$ para todo $n < 0$), $f(z)$ es llamada"forma modular de peso k para el subgrupo Γ'". Al conjunto de dichas funciones lo notamos $\mathrm{M}_k(\Gamma')$. Si, aún más, la función se anula en el infinito (i.e. $a_0 = 0$) $f(z)$ es llamada "forma cuspidal de peso k para Γ'", y al conjunto de esas funciones lo notamos $\mathrm{S}_k(\Gamma')$. Por último, a la expansión 3.7 de una función modular $f(z)$ le llamamos "$q-$expansión".

OBSERVACIÓN 3.1. 1. La condición 3.9, cuando consideramos todo el grupo Γ, es equivalente a que la relación valga para T y S, los generadores de Γ, que lo podemos traducir en:

$$f(z) = f(z+1) \tag{3.11}$$

$$f(-\tfrac{1}{z}) = (-z)^k f(z) = z^k f(z) \text{ porque } k \text{ es par.} \tag{3.12}$$

2. Si k es impar, no hay funciones modulares para $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ no nulas de peso k; se puede ver fácilmente tomando $\gamma = -I$ en 3.9.
3. Las condiciones se preservan por suma y producto por escalares, o sea, los conjuntos de las funciones modulares, $\mathrm{M}_k(\Gamma')$ y $\mathrm{S}_k(\Gamma')$ son espacios vectoriales sobre los complejos. Por otro lado, si multiplicamos dos funciones modulares (o formas, o cuspidales) de pesos k_1 y k_2, nos da una forma de peso $k_1 + k_2$, y la inversa (con el producto punto a punto) de una función modular de peso k es una función modular de peso $-k$, por lo que las funciones modulares de cualquier peso son un cuerpo.

Un primer ejemplo de una función modular para $\mathrm{SL}_2(\mathbb{Z})$ son las Series de Einsestein, que se definen, para cualquer entero par $k > 2$, como

$$G_k(z) := \sum_{m,n \in \mathbb{Z}} \frac{1}{(mz+n)^k}, \tag{3.13}$$

donde la suma es sobre los enteros no ambos nulos. Notar que si tomamos L_z el retículo generado por el 1 y por z en $\mathbb{C}$, entonces $G_k(z) = G_k(L_z)$, que definimos en el capítulo 1 (ecuación 1.20). Como k es al menos 4, la suma es absolutamente convergente y uniformemente en cualquier compacto de H.

Otro ejemplo, que nos será útil más adelante, es la función $(\Theta(z))^2 \in \mathrm{M}_1(\Gamma_1(4))$, definida por:

$$\Theta(z) := \sum_{n\in\mathbb{Z}} e^{2\pi i z n^2} = \sum_{n\in\mathbb{Z}} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \dots \tag{3.14}$$

Si Γ'' es un subgrupo normal de Γ' y χ es un caracter para Γ'/Γ'', i.e.; un morfismo de grupos $\chi : \Gamma'/\Gamma'' \longrightarrow \mathbb{C}^*$, podemos considerar unas ciertas formas modulares para el grupo Γ'' pero no necesariamente para Γ' que serán necesarias para entender los teoremas finales. Definimos entonces:

$$M_k(\Gamma', \chi) := \left\{ f \in M_k(\Gamma'') : f|[\gamma^{-1}]_k = \chi(\gamma) f \quad \text{para todo } \gamma \in \Gamma' \right\}.$$

Si en el caso anterior consideramos, para un N, los subgrupos $\Gamma_1(N)$ y $\Gamma_0(N)$, ya que el primero es normal en el segundo, y un caracter χ en el cociente $\Gamma_0(N)/\Gamma_1(N) \equiv \mathbb{Z}/N\mathbb{Z}$, utilizamos la notación:

$$M_k(N, \chi) := \left\{ f \in M_k(\Gamma_1(N)) : f|[\gamma]_k = \chi(d) f \text{ para todo } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\}.$$

De manera análoga, podemos hablar de $S_k(N, \chi) := M_k(N, \chi) \cap S_k(\Gamma_1(N))$.

3. Operadores de Hecke

Nos concentraremos ahora en los subgrupos de congruencia más importantes, definidos en 3.1: Γ, $\Gamma_1(N)$, $\Gamma_0(N)$ y $\Gamma(N)$. Notar que si tomamos $N = 1$, todos los recién mencionados son iguales.

Definición 3.5. Un "punto modular" de Γ' se refiere a lo siguiente, dependiendo del contexto:

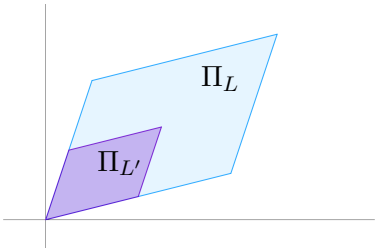
1. si $\Gamma' = \Gamma$, un retículo $L \subset \mathbb{C}$, que notamos e_L;
2. si $\Gamma' = \Gamma_1(N)$, un par (L, t) donde L es un retículo y $t \in \mathbb{C}/L$ es un punto de orden N, que notamos $e_{L,t}$;
3. si $\Gamma' = \Gamma_0(N)$, un par (L, S) donde L es un retículo y $S \subset \mathbb{C}/L$ es un subgrupo cíclico de orden N, que notamos $e_{L,S}$;
4. si $\Gamma' = \Gamma(N)$, una terna (L, t_1, t_2) donde L es un retículo, $t_1, t_2 \in \mathbb{C}/L$ son tales que todo $t \in \frac{1}{N}L/L$ es de la forma $t = mt_1 + nt_2$, o sea, $\{t_1, t_2\}$ es una base (como combinación lineal entera) de los puntos de orden N, que notamos e_{L,t_1,t_2}.

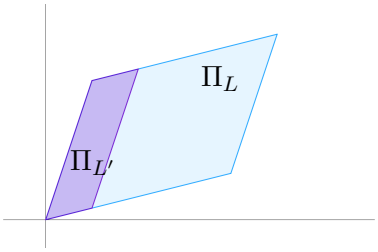
Sea $\mathscr{L}$ el $\mathbb{Q}-$espacio vectorial de las sumas formales finitas de puntos modulares sobre $\Gamma' = \Gamma_1(N)$, i.e., $\mathscr{L} = \bigoplus \mathbb{Q}(L, t)$, donde la suma es sobre todos los retículos L y todos los puntos t de orden N.

DEFINICIÓN 3.6. Sea n un entero positivo. Definimos el operador de Hecke asociado a n como el mapa $\mathbb{Q}-$lineal $T_n : \mathscr{L} \longrightarrow \mathscr{L}$ definido en la base canónica de $\mathscr{L}$ por:

$$T_n(e_{L,t}) = \frac{1}{n} \sum e_{L',t},$$

donde la suma es sobre todos los retículos L' que contienen a L de índice n tales que $e_{L',t}$ es un punto modular. Aquí, si $t \in \mathbb{C}/L$, también estará en $\mathbb{C}/L'$ via proyectar (ya que L' es más grande (más fino) que L). En la siguientes imágenes, dos ejemplos de retículos $L < L'$ (en realidad, sólo sus paralelogramos fundamentales Π_L y $\Pi_{L'}$) de índice 4.





L'/L es un subgrupo de $\mathbb{C}/L$ de orden n.

Notar que la suma recién definida es finita, ya que los retículos L' tienen que estar contenidos en $\frac{1}{n}L = \{\frac{1}{n}l : l \in L\}$, o sea, los retículos L' con paralelogramo fundamental Π' que entre n veces en el paralelogramo fundamental de L, Π, son finitos (no hay muchas formas de hacer entrar n Π's en Π). O sea, cada L' en la suma corresponde a un subgrupo de orden n de $\frac{1}{n}L/L \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Notar que $T_1 = Id$.

Luego, para cualquier entero positivo n coprimo con N, definimos otro mapa lineal:

$$T_{n,n} : \mathscr{L} \longrightarrow \mathscr{L}, \quad T_{n,n}(e_{L,t}) := \frac{1}{n^2} e_{\left(\frac{1}{n}\right)L,t}. \tag{3.15}$$

Notar que tiene sentido ya que t tiene orden N por ser N y n coprimos.

Para estos mapas, es fácil ver que vale la conmutatividad de la composición:

$$T_{n_1,n_1}T_{n_2,n_2} = T_{n_1n_2,n_1n_2} = T_{n_2,n_2}T_{n_1,n_1}; \quad T_{n,n}T_m = T_mT_{n,n}.$$

La conmutatividad sólo para los T_n también vale en ciertos casos, y es lo que veremos ahora.

PROPOSICIÓN 3.5. *1) Si mcd$(m,n) = 1$, entonces $T_{mn} = T_mT_n$; en particular, T_n conmuta con T_m.*
2) Si p es un primo que divide a N, entonces $T_{p^l} = T_p^l$.
3) Si p es un primo que no divide a N, entonces, para $l \geq 2$:

$$T_{p^l} = T_{p^{l-1}}T_p - pT_{p^{l-2}}T_{p,p}.$$

Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ es la descomposición en factores primos de n, entonces $T_n = T_{p_1^{\alpha_1}} \dots T_{p_r^{\alpha_r}}$, y cada uno los puedo descomponer usando las partes 2 y 3 de la proposición 3.5. Esto quiere decir que los $T_{n,n}$ para n coprimo con N y los T_m con m cualquiera, generan un álgebra conmutativa $\mathscr{H}$ de operadores de $\mathscr{L}$ en $\mathscr{L}$.

DEFINICIÓN 3.7. Sean $\Gamma' < \Gamma$ un subgrupo de congruencia, F' un dominio fundamental para Γ' y $f, g \in \mathrm{M}_k(\Gamma')$, siendo alguna de las dos una forma cuspidal. Se define el siguiente producto interno:

$$< f, g >:= \frac{1}{[\Gamma : \Gamma']} \int_{F'} f(z)\overline{g(z)}y^{k-2}dxdy.$$

PROPOSICIÓN 3.6. *Sean n y N enteros coprimos y χ un caracter multiplicativo módulo N. Sea c_n cualquiera de las dos raíces cuadradas de $\overline{\chi}(n)$. Entonces el operador de Hecke c_nT_n es autoadjunto respecto al producto interno definido en 3.7, i.e.; $< c_nT_nf, g >=< f, c_nT_ng >$.*

PROPOSICIÓN 3.7. *Sea N un entero positivo y χ un caracter multiplicativo módulo N. Existe una base de $S_k(N,\chi)$ como $\mathbb{C}-$espacio vectorial formada por formas modulares que son vectores propios para todos los T_n con mcd$(n,N) = 1$.*

DEMOSTRACIÓN. Para empezar, aclaramos que los espacios de formas modulares son de dimensión finita. Esta afirmación no la probaremos, pues escapa de nuestro interés la prueba.
Para cada n con $\mathrm{mcd}(n,N) = 1$ y cada subespacio $S \subset S_k(N,\chi)$ invariante por T_n, como c_nT_n es autoadjunto y S tiene dimensión finita, el teorema de descomposición espectral nos dice que existe una base (el teorema nos dice, aún más, que esta base es ortonormal, pero no nos importa) de S formada por vectores propios de c_nT_n. Luego, cualquier subespacio propio de T_n es invariante bajo los otros $T_{n'}$. Para ver esto, como tanto n como n' son coprimos con N, por la proposición 3.5, los operadores T_n y $T_{n'}$ conmutan. Sea entonces f un vector propio de T_n, o sea, $T_nf = \lambda f$. Queremos ver que $T_{n'}f$ es un vector propio para el mismo λ de T_n. En efecto, tenemos:

$$T_n(T_{n'}f) = T_{n'}(T_nf) = T_{n'}\lambda f = \lambda T_{n'}f.$$

La demostración sigue así: primero, ordenamos todos los operadores T_n con n coprimo a N. El espacio $S_k(N,\chi)$ se escribe como suma directa de subespacios propios

para el primer T_n, o sea:

$$S_k(N,\chi) = S_1 \oplus \cdots \oplus S_r, \quad S_i \text{ subespacio propio de } T_n.$$

Luego, como los S_i son invariantes bajo T_n' para el siguiente operador, podemos escribir este como suma de subespacios propios:

$$S_i = S_{i,1} \oplus \cdots \oplus S_{i,l_i}$$

$$S_k(N,\chi) = (S_{1,1} \oplus \cdots \oplus S_{i,l_1}) \oplus \cdots \oplus (S_{r,1} \oplus \cdots \oplus S_{r,l_r}).$$

Seguimos de esta forma y como $S_k(N,\chi)$ tiene dimensión finita, pueden pasar dos cosas: eventualmente llegamos a una descomposición en subespacios de dimensión uno, con lo que habremos llegado a la base que buscábamos (ya que estos subespacios serán invariantes bajo todos los T_n siguiente, o sea, propios), o en algún paso dejamos de achicar los subespacios. Si esto pasa es porque los subespacios propios de un operador son iguales a los de todos los siguientes, con lo que una base de este nos sirve. En ambos casos, la proposición queda demostrada. □

4. Formas modulares de peso medio entero

Sea k un entero positivo impar. El objetivo de esta sección es definir formas modulares de peso $\frac{k}{2}$.

Consideramos, para un complejo, la raíz con argumento en $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right]$. Así, la función $\sqrt{z}$ es holomorfa en $\mathbb{C} - (-\infty, 0]$.

Observación 3.2. La función $\sqrt{z}$ lleva reales positivos en reales positivos, el semiplano superior en el primer cuadrante y el semiplano inferior en el cuarto cuadrante.

Notamos $z^{\frac{k}{2}} = \sqrt{z}^k$.

Cuando tenemos una regla del tipo $f(\gamma z) = (cz+d)^k f(z)$, al término $(cz+d)^k$ se le llama factor automorfo, que depende de γ y de z. O sea, un factor automorfo para una función no nula f es una función $J(\gamma, z)$ con la propiedad $f(\gamma z) = J(\gamma, z) f(z)$ para γ en algún grupo de matrices y z en H. Como la función f verifica:

$$\frac{f(\gamma\beta z)}{f(z)} = \frac{f(\gamma\beta z)}{f(\beta z)} \cdot \frac{f(\beta z)}{f(z)},$$

se tiene que un factor automorfo verifica:

$$J(\gamma\beta, z) = J(\gamma, z) J(\beta, z). \tag{3.16}$$

Si quisiéramos definir las formas modulares de peso $\frac{k}{2}$ para k impar de la misma forma que antes: una función holomorfa que verifica $f(\gamma z) = (cz+d)^{\frac{k}{2}} f(z)$, $J(\gamma, z) = (cz+d)^{\frac{k}{2}}$ no es un factor automorfo ya que no siempre verifica la igualdad recién mencionada. En efecto, sea $N > 2$ y consideramos en el subgrupo de congruencia

$\Gamma(N)$ las matrices $\alpha = \begin{pmatrix} 1+N & N \\ -N & 1-N \end{pmatrix}$ y $\beta = \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$. La condición 3.16 nos dice que debería valer:

$$\sqrt{(N^2-2N)z+1-N}^k = \left(\sqrt{-Nz+1-N}\sqrt{-Nz+1}\right)^k. \tag{3.17}$$

Sin tener en cuenta los k, tenemos que el cuadrado de la izquierda y el de la derecha son iguales, así que sus raíces, o son iguales, o difieren en un signo. Veamos que difieren en un signo y, por lo tanto, al elevarlos a k impar, seguirán difiriendo en un signo, no cumpliendo así la igualdad 3.16. El discriminante de la izquierda está el el semiplano superior ya que z lo está y $(N^2-2N)¿0$ y el $1+N$ sólo lo mueve horizontalmente, por lo que la raíz está en el primer cuadrante por la observación 3.2, y los discriminantes de la derecha están ambos en el semiplano inferior, por lo que sus raíces están en el cuarto cuadrante. El producto de dos números que están en el cuarto cuadrante siempre estará en el semiplano inferior, por lo que estos números nunca podrán ser iguales y deberán diferir en un signo.

Lo que tenemos que hacer para definir las formas de peso medio entero es forzar la condición 3.16, definiendo el factor automorfo como $J(\gamma, z) = j(\gamma, z)^k$ en vez de $(cz+d)^k$, donde j está dada por:

$$j(\gamma, z) := \frac{\Theta(\gamma z)}{\Theta(z)} \quad \text{para } \gamma \in \Gamma_0(4), \tag{3.18}$$

donde Θ está definida en la fórmula 3.14. La razón de considerar sólo $\Gamma_0(4)$ es porque la función j se suele definir de otra forma y se puede probar que verifica ser igual al cociente de las Θ. Así que, de ahora en adelante, para las formas modulares de peso medio entero trabajaremos siempre dentro del subgrupo de congruencia $\Gamma_0(4)$.

Además de ser invariante por esa acción, igual que en el caso entero, le tenemos que pedir ser "meromorfa" en las cúspides, que es lo que pasaremos a definir ahora.

Definición 3.8. Sea Γ' un subgrupo de $\Gamma_0(4)$. Definimos el conjunto de pares:

$$\widetilde{\Gamma}' := \{(\gamma, j(\gamma, z)) : \gamma \in \Gamma'\}. \tag{3.19}$$

Notamos $\widetilde{\gamma} = (\gamma, j(\gamma, z))$ a los elementos de $\widetilde{\Gamma}'$, y para estos, definimos también una acción en las funciones holomorfas en H para todo entero k:

$$f(z)|[\widetilde{\gamma}]_{k/2} := f(\gamma z) j(\gamma, z)^{-k}. \tag{3.20}$$

Sea $\Gamma' < \Gamma_0(4)$ subgrupo de congruencia de índice finito. Para la cúspide ∞, como Γ' tiene índice finito en $\Gamma_0(4)$, también lo tiene en Γ, entonces, la intersección con Γ_∞,

$$\Gamma_\infty = \left\{ \pm \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} : j \in \mathbb{Z} \right\},$$

es de la forma:

$$\Gamma' \cap \Gamma_\infty = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^j : j \in \mathbb{Z} \right\},$$

para algún h entero mayor que 1, o bien sólo los positivos o sólo los negativos si $-I \notin \Gamma'$. Como la acción por $|[\widetilde{-I}]_{k/2}$ es trivial, en ambos casos ($-I$ está o no en Γ') tenemos que $f(z) = f(z+h) = f(\gamma z)$, donde γ es $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$, por lo que f tiene una expansión en términos de $q_h = e^{2\pi i z/h}$. De la misma forma que en caso entero, decimos que f es **meromorfa** si tiene finitos términos negativos en esa expansión, **holomorfa** si no tiene ninguno y **cuspidal** si sólo tiene términos positivos.

Para una cúspide $s \in \mathbb{Q}$, sea $\alpha \in \Gamma$ tal que $s = \alpha\infty$ (esto por lo mencionado enseguida de la definición 3.2). Supongamos que f es una función en el plano superior invariante bajo la acción de $|[\widetilde{\gamma}]_{k/2}$ para cualquier $\widetilde{\gamma} \in \widetilde{\Gamma}'$ y sea $g = f|[\widetilde{\alpha}]_{k/2}$. Se puede probar que g verifica lo siguiente:

$$g(z) = t^{-k} g(z+h), \quad t = 1, i, -1, -i. \tag{3.21}$$

Podemos escribir $t^- k = e^{-2\pi i r}$ con $r = 0, \frac{1}{4}, \frac{1}{2}$ ó $\frac{3}{4}$. Entonces, $e^{-2\pi i r z/h} g(z)$ es invariante bajo $z \mapsto z + h$. En efecto:

$$e^{-2\pi i r z/h} g(z) = e^{-2\pi i r z/h} e^{-2\pi i r} g(z+h) = e^{-2\pi i r (z+h)/h} g(z+h).$$

Entonces, tenemos que $e^{-2\pi i r z/h} g(z)$ tiene un desarrollo de Fourier en términos de q_h^n, $q_h = e^{2\pi i z/h}$,i.e., $e^{-2\pi i r z/h} g(z) \sum a_n q_h^n$. Tenemos entonces:

$$g(z) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i z (n+r)/h}.$$

Decimos que f es **meromorfa** en la cúspide s si $a_n \neq 0$ sólo para finitos términos con $n < 0$, **holomorfa** si $a_n = 0$ para todo $n < 0$. Si f es holomorfa, definimos $f(s) := \lim_{z \longrightarrow i\infty} g(z)$. En este caso, $f(s) = 0$ si $r \neq 0$ y $f(s) = a_0$ si $r = 0$. Se puede ver también que esta definición no depende de la clase de equivalencia de s según Γ'.

Resumimos entonces:

Definición 3.9. Sea k un entero impar y un subgrupo de congruencia $\Gamma' < \Gamma_0(4)$ de índice finito. Dada la acción a derecha por un elemento $\gamma \in \Gamma'$ como:

$$f|[\gamma]_{k/2}(z) = j(\gamma, z)^{-k} f(\gamma z),$$

una función modular de peso $\frac{k}{2}$ para el subgrupo Γ' es una función $f : \overline{H} \longrightarrow \mathbb{C}$ meromorfa (en H y en las cúspides, en el sentido definido anteriormente) que verifica:

$$f|[\gamma]_{k/2} = f \quad \text{para todo } \gamma \in \Gamma'.$$

Igual que antes, decimos que es una forma modular si es holomorfa en todos lados y cuspidal y se anula en las cúspides.

Definición 3.10. Sea ahora un entero positivo N múltiplo de 4, o sea que $\Gamma_0(N) < \Gamma_0(4)$. Sea χ un caracter del grupo multiplicativo $(\mathbb{Z}/N\mathbb{Z})^*$. Definimos el siguiente subespacio de $M_{k/2}(\widetilde{\Gamma}'_1(N))$:

$$M_{k/2}(\widetilde{\Gamma}'_0(N), \chi) := \{f : f|[\widetilde{\gamma}]_{k/2} = \chi(d) f\}.$$

y defimos las cuspidales, $S_{k/2}(\widetilde{\Gamma}'_0(N), \chi) = S_{k/2}(\widetilde{\Gamma}'_1(N)) \cap M_{k/2}(\widetilde{\Gamma}'_0(N), \chi)$.

5. Operadores de Hecke para formas de peso medio entero

La definición de operadores de Hecke para formas modulares de peso medio entero es también más complicada que en el caso entero. Primero, veamos otra forma de construir los operadores de Hecke para las formas de peso entero y generalicemos esta idea.

Sea n un entero positivo y $f \in \mathrm{M}_k(\Gamma)$. Sea Δ^n el conjunto de las matrices 2×2 con entradas enteras y determinante n. Se define, para un $\alpha \in \Delta^n$, la coclase doble $\Gamma\alpha\Gamma = \{\gamma_1\alpha\gamma_2 : \gamma_1, \gamma_2 \in \Gamma \subset \Delta^n$. Esta definición se puede extender a un grupo cualquiera con dos subgrupos, y es fácil ver que las coclases dobles parten al grupo en clases de equivalencia, de forma análoga a las coclases simples. Se puede probar, en este caso, que la cantidad de coclases es finita, o sea que existen un r y un s tal que:

$$\begin{aligned} \Gamma\alpha\Gamma &= \bigcup_{i=1}^{r} \Gamma\alpha\gamma_i; \\ \Delta^n &= \bigcup_{j=1}^{s} \Gamma\alpha_j\Gamma. \end{aligned} \tag{3.22}$$

Definimos una nueva acción en las formas modulares como:

$$f|[\Gamma\alpha\Gamma]_k := \sum_{i=1}^{r} f|[\alpha\gamma_i], \tag{3.23}$$

y en base a eso, definimos el operador T_n como:

$$T_n f = n^{k/2-1} \sum_{j=1}^{s} f|[\Gamma\alpha_j\Gamma]_k. \tag{3.24}$$

Se puede probar que esta definición coincide con 3.6.

De la misma forma, podemos definirlo para el subgrupo de congruencia $\Gamma_1(N)$, siendo Δ^n las matrices 2×2 de determinante n que son congruente a $\begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix}$ módulo N. Para una $f \in \mathrm{M}_k(\Gamma_1(N))$, se define:

$$T_n f := n^{k/2-1} \sum f|[\Gamma_1(N)\alpha\Gamma_1(N)]_k, \tag{3.25}$$

donde la suma es sobre todas las coclases dobles de $\Gamma_1(N)$ en Δ^n, que, de nuevo, se puede probar que son finitas.

Para el caso de las formas de peso medio entero, lo definimos de forma parecida pero tomando $\widetilde{\Gamma}_0(4)$. Sea $\xi_n = \left(\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}, \sqrt[4]{n} \right)$ un par definido de forma muy parecida a los $\widetilde{\gamma}$, y consideramos la coclase doble $\widetilde{\Gamma}_1(4)\xi\widetilde{\Gamma}_1(4)$, donde el producto es punto a punto (porque los elementos son pares de dos entradas). Definimos la acción

en f como:

$$f|[\widetilde{\Gamma}_1(4)\xi\widetilde{\Gamma}_1(4)]_{k/2} := \sum_j f|[\xi_n\widetilde{\gamma_j}]_{k/2}, \tag{3.26}$$

donde la acción por el elemento $\xi_n\widetilde{\gamma}$ está dada de la misma forma que en la acción 3.20, solo que el factor automorfo en este caso (por el producto punto a punto) es $\sqrt[4]{n}j(\gamma, z)$. O sea:

$$f(z)|[\xi_n\widetilde{\gamma}]_{k/2} = f(a\gamma_j z)(\sqrt[4]{n}j(\gamma, z))^{-k}, \tag{3.27}$$

donde la suma es sobre las distintas coclases dobles de $\widetilde{\Gamma}_1(4)\xi\widetilde{\Gamma}_1(4)$. También se puede probar lo siguiente:

PROPOSICIÓN 3.8. *Si n es un entero positivo coprimo con N que no es un cuadrado perfecto, entonces $f(z)|[\xi_n\widetilde{\gamma}]_{k/2} = 0$.*

Esta proposición nos dice que sólo tiene sentido definir los operadores de Hecke para cuadrados perfectos, e igual que antes (proposición 3.5), podemos probar que conmutan cuando son coprimos y se descomponen según primo cuadrado, o sea, es suficiente definir:

$$T_{p^2}f := p^{k/2-2}f|[\widetilde{\Gamma}_1(N)\chi_{p^2}\widetilde{\Gamma}_1(N)]_{k/2}, \quad \text{donde } \chi_{p^2} = \left(\begin{pmatrix}1 & 0\\ 0 & p^2\end{pmatrix}, \sqrt{p}\right). \tag{3.28}$$

Nos interesa obtener una obtener una base de vectores propios como en el caso entero, y eso es lo que enunciaremos en el próximo capítulo.

Capítulo 4

Teoremas de Shimura, Waldspurger, Tunnell y meollo del asunto

En este último capítulo, enunciaremos dos teoremas muy fuertes y veremos como estos, junto a la conjetura de Birch y Swinnerton-Dyer, nos ayudan a terminar el problema de los números congruentes.

TEOREMA 4.1 ([**Shi73**]). *Sean $k \geq 3$ un entero impar, N un natural múltiplo de 4, χ un caracter del grupo multiplicativo $(\mathbb{Z}/N\mathbb{Z})^*$ y, usando la notación $q = e^{2\pi iz}$ $f(z) = \sum_{n=1}^{\infty} a_n q^n \in S_{k/2}(\widetilde{\Gamma}_0(N), \chi)$ una forma cuspidal que es vector propio del operador T_{p^2} para todo primo p con respectivo valor propio λ_p. Sea g la función:*

$$g(z) = \sum_{n=1}^{\infty} b_n q^n,$$

donde los b_n son los coeficientes de:

$$\sum_{n=1}^{\infty} b_n n^{-s} = \prod_{p \ primo} \frac{1}{1 - \lambda_p p^{-s} + \chi(p)^2 p^{k-2-2s}}.$$

Entonces $g \in M_{k-1}(N', \chi^2)$ para algún entero N' divisible por el conductor[1] *de χ^2. Además, si $k \geq 5$, g es una forma cuspidal. Notamos* $\text{Shimura}(f) = g$.

En el contexto de la teoría de representaciones, el teorema de Waldspurger [**Wal81a**][**Wal81b**] nos dice cuánto es el valor de $L(E, 1)$ para ciertos casos. El enunciado del teorema escapa de los contenidos e intereses de este trabajo (y por lo que tengo entendido, tampoco entraría en el margen de ninguna página), pero este fue usado para los siguientes resultados (tanto el de Kohnen como los de Tunnell). Cuando $N = 4$, Kohnen [**Koh80**, pág. 249-256] prueba que la correspondencia es un isomorfismo:

$$S^+_{k/2}(\widetilde{\Gamma}_0(4)) \longrightarrow S_{k-1}(\Gamma), \tag{4.1}$$

donde

$$S^+_{k/2}(\widetilde{\Gamma}_0(4)) := \left\{ f = \sum a_n q^n \in S_{k/2}(\widetilde{\Gamma}_0(4)) : a_n = 0 \text{ si } (-1)^{\frac{k-1}{2}} n \equiv 2, 3 \pmod 4 \right\}.$$

Bajo este isomorfismo, Tunnel prueba los siguientes:

[1] Para no sobrecargar de información la definición de conductor se puede ver en [**Kob93**, pág. 67]

TEOREMA 4.2 ([**Tun83**]). *Sean* $L(E_1,s)=\sum b_m m^{-s}$ *y* $g(z)=\sum b_m q^m$. *Existen una constante* $\beta\neq 0$, *una forma* $f=\sum a_m q^m\in S_{3/2}(\widetilde{\Gamma}_0(128))$ *y una forma* $f'=\sum a'_m q^m\in S_{3/2}(\widetilde{\Gamma}_0(128),\chi_2)$, *donde* χ_2 *es el caracter no trivial de orden 2 de* $(\mathbb{Z}/128\mathbb{Z})^*$, *tales que* $\text{Shimura}(f)=\text{Shimura}(f')=g=\sum b_m q^m$, *y:*

$$L(E_n,1)=\begin{cases}\frac{\beta}{4\sqrt{n}}a_n^2 & \text{para } n \text{ impar;}\\ \frac{\beta}{2\sqrt{n}}a'^2_{n/2} & \text{para } n \text{ par.}\end{cases}$$

En particular, $L(E_n,1)=0$ *si y sólo si* $a_n=0$ *para* n *impar y* $a'_{n/2}=0$ *para* n *par.*

PROPOSICIÓN 4.1 ([**Tun83**]). *Si definimos:*

$$f_1(z)=(\Theta(z)-\Theta(4z))(\Theta(32z)-\tfrac{1}{2}\Theta(8z)),$$

entonces las funciones:

$$f_1(z)\Theta(2z),\ f_1(z)\Theta(8z)\in S_{3/2}(\widetilde{\Gamma}_0(128)),$$
$$f_1(z)\Theta(4z)\quad y\quad f_1(z)\Theta(16z)\in S_{3/2}(\widetilde{\Gamma}_0(128),\chi_2),$$

donde Θ *está definida en la ecuación 3.14, son un conjunto maximal linealmente independiente de vectores propios para los operadores* T_{p^2} *para todos los primos* p *tales que sus imágenes por la correspondencia de Shimura coinciden entre ellas y con la función* $g(z)\in S(\Gamma_0(32))$ *correspondiente a* $L(E_1,s)$.

En particular, Tunnell nos dice que podemos tomar $f(z)=f_1(z)\Theta(2z)$ y $f'(z)=f_1(z)\Theta(4z)$, o sea:

$$\begin{aligned}f(z)&=(\Theta(z)-\Theta(4z))(\Theta(32z)-\tfrac{1}{2}\Theta(8z))\Theta(2z)\\ f'(z)&=(\Theta(z)-\Theta(4z))(\Theta(32z)-\tfrac{1}{2}\Theta(8z))\Theta(4z).\end{aligned}\tag{4.2}$$

Como n es libre de cuadrados, notar que en el teorema 4.2 sólo nos interesa saber cuándo los coeficientes impares de f y f' son cero, y como multiplicar $\Theta(4z)(\Theta(32z)-\frac{1}{2}\Theta(8z))\Theta(2z)$ nos da coeficientes pares, pues todos son z multiplicado por algo par y eso pasa a que la q-expansión tenga sólo términos elevados a una potencia par, los coeficientes que nos interesan son los impares de:

$$\Theta(z)(\Theta(32z)-\tfrac{1}{2}\Theta(8z))\Theta(2z)=\sum_{a,b,c\in\mathbb{Z}}q^{a^2+32b^2+2c^2}-\tfrac{1}{2}\sum_{a,b,c\in\mathbb{Z}}q^{a^2+8b^2+2c^2}\tag{4.3}$$

para f (caso n impar) y:

$$\Theta(z)(\Theta(32z)-\tfrac{1}{2}\Theta(8z))\Theta(4z)=\sum_{a,b,c\in\mathbb{Z}}q^{a^2+32b^2+4c^2}-\tfrac{1}{2}\sum_{a,b,c\in\mathbb{Z}}q^{a^2+8b^2+4c^2}\tag{4.4}$$

para f' (caso n par).

Recordar que nos interesaba saber cuándo estos coeficientes eran o no nulos. Notar que, si n es impar, el coeficiente de q^n es claramente 0 si $n\equiv 5$ ó $7\pmod 8$, ya que ninguno de los exponentes en las dos sumas para el caso de f puede ser de esa forma, y si n es par, el coeficiente de $q^{n/2}$ es claramente cero si $\frac{n}{2}\equiv 3$ ó $7\pmod 8$, o sea, si $n\equiv 6\pmod 8$, por el mismo argumento, pero esto no nos dice nada nuevo, ya que el teorema de Tunnell nos dice que $L(E_n,1)=0$ en esos casos, pero ya lo

habíamos probado en la proposición 2.9 del capítulo 2.

Como nos interesa saber cuándo esos coeficientes son cero, juntando esa información con todo lo que venimos haciendo hasta ahora, obtenemos la siguiente versión del teorema de Tunnell.

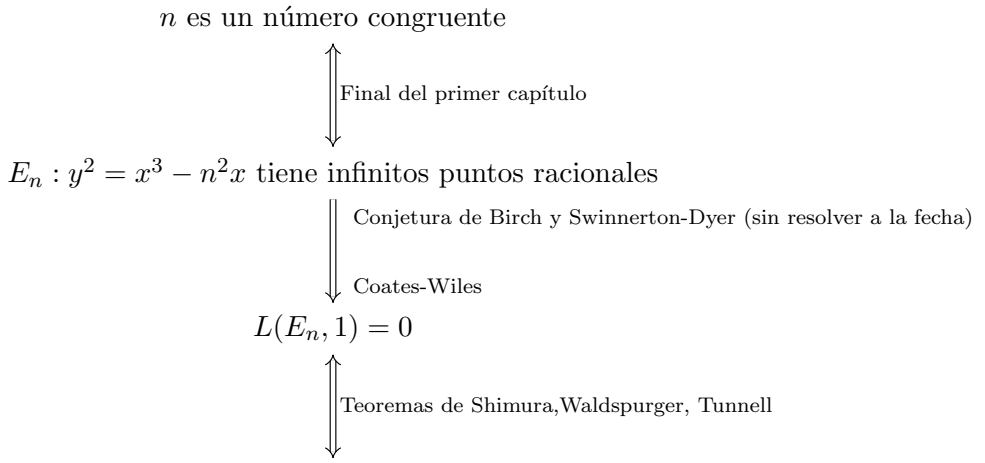
TEOREMA 4.3 ([**Tun83**]). *Sea n es un entero positivo libre de cuadrados. Si n es un número congruente, entonces:*

$$\begin{cases} \#\{x,y,z \in \mathbb{Z} : n = 2x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x,y,z \in \mathbb{Z} : n = 2x^2 + y^2 + 8z^2\} \\ \textit{si } n \textit{ es impar;} \\ \#\{x,y,z \in \mathbb{Z} : n = 4x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x,y,z \in \mathbb{Z} : n = 4x^2 + y^2 + 8z^2\} \\ \textit{si } n \textit{ es par.} \end{cases}$$

Si la conjetura débil de Birch y Swinnerton-Dyer es cierta para las curvas elípticas E_n, entonces el recíproco también es cierto, o sea, las igualdades de arriba implican que n es un número congruente.

Sabemos que el 5, el 6 y el 7 son números congruentes, por lo que deberían verificar las igualdades. En efecto, tenemos que ambos conjuntos son vacíos, pues z debe ser necesariamente 0, si x fuera 0, no habría solución ya que ninguno es un cuadrado y no habría un y posible, si x fuera 1 lo mismo, y si x fuera mayor o igual que 2 ya nos pasaríamos, así que las igualdades se cumplen trivialmente. Esta misma cuenta la podemos hacer para los casos en que n es congruente con $5, 6$ y $7 \pmod 8$, ya que ambos conjuntos son vacíos. Por ejemplo, para $n \equiv 5 \pmod 8$, tendríamos que no hay solución a la ecuación $5 \equiv 2x^2 + y^2 \pmod 8$ (omitimos el último término porque módulo 8 siempre será 0), ya que, si el x fuera par, $2x^2$ es múltiplo de 8 y tendríamos que $y^2 \equiv 5 \pmod 8$, pero el único cuadrado impar módulo 8 es el 1, y si el x fuera impar, tendríamos que $2 + y^2 \equiv 5 \pmod 8$, o sea que $y^2 \equiv 3 \pmod 8$, lo cual tampoco puede ser. La misma cuenta funciona para los casos 6 y 7, o sea que si n es congruente con $5, 6$ ó 7 módulo 8, y vale la conjetura débil de Birch y Swinnerton-Dyer, entonces n es congruente. Esto en realidad ya lo habíamos probado al final del capítulo 2, en la proposición 2.9.

El cierre se puede concluir en la siguiente imagen, donde la implicancia hacia arriba de la segunda flecha es cierta si vale la conjetura débil de Birch y Swinnerton-Dyer.



Bibliografía

[CW77] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39:223–251, 1977.

[Jac85] Nathan Jacobson. Basic algebra I. 2nd ed. New York: W. H. Freeman and Company. XVIII, 499 p. £ 19.95 (1985)., 1985.

[Kob93] Neal Koblitz. *Introduction to elliptic curves and modular forms.*, volume 97 of *Grad. Texts Math.* New York: Springer-Verlag, 2. ed. edition, 1993.

[Koh80] Winfried Kohnen. Modular forms of half-integral weight on $\Gamma_0(4)$. *Math. Ann.*, 248:249–266, 1980.

[LN08] Rudolf Lidl and Harald Niederreiter. *Finite fields.*, volume 20 of *Encycl. Math. Appl.* Cambridge: Cambridge University Press, paperback reprint of the hardback 2nd edition 1996 edition, 2008.

[Sha13] Igor R. Shafarevich. *Basic algebraic geometry 1. Varieties in projective space. Translated from the Russian by Miles Reid.* Berlin: Springer, 3rd ed. edition, 2013.

[Shi73] Goro Shimura. On modular forms of half integral weight. *Ann. Math. (2)*, 97:440–481, 1973.

[ST15] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves.* Undergraduate Texts Math. Cham: Springer, 2nd ed. edition, 2015.

[Ste09] William Stein. *Elementary number theory. Primes, congruences, and secrets. A computational approach.* Undergraduate Texts Math. New York, NY: Springer, 2009.

[Tun83] J. B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72:323–334, 1983.

[Wal81a] J. L. Waldspurger. Correspondance de Shimura. Theorie des nombres, Semin. Delange-Pisot-Poitou, Paris 1979-80, Prog. Math. 12, 357-369 (1981)., 1981.

[Wal81b] J.-L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl. (9)*, 60:375–484, 1981.

[War21] Benjamin Wardhaugh. *Encounters with Euclid. How an ancient Greek geometry text shaped the world.* Princeton, NJ: Princeton University Press, 2021.