Capítulo 5

Introducción a las formas modulares

5.1. Funciones elípticas y curvas elípticas

Hoy en día las curvas elípticas deben gran parte de su fama, más allá del recoleto círculo de profesionales, a su participación crucial en la prueba del último teorema de Fermat y también es destacable su relevancia en criptografía. Sin embargo estos temas tan aritméticos son muy novedosos; hace mucho tiempo lo realmente importante eran las funciones elípticas (sobre las que trabajaron Gauss, Jacobi, Abel, Riemann y otros muchos ilustres), y más atrás todavía, hubo alguna elipse que motivó al menos el nombre.

En la actualidad uno podría leer un tratado sobre curvas elípticas con apenas referencias marginales a las funciones elípticas y ni una sola elipse. En principio es bastante lógico, porque las curvas elípticas se han convertido en grandes estrellas de la teoría de números que las considera definidas en $\mathbb{Q}$, en cuerpos finitos o en cuerpos de números, mientras que las funciones elípticas tienen su hogar natural en $\mathbb{C}$, demasiado grande para los que cuentan con los dedos.

A pesar de ello, el lector novato puede encontrar interesante saber a grandes líneas la conexión entre estos temas, que es el propósito de esta sección.

Históricamente el ancestro de la saga elíptica fue la integral que se obtiene al hallar la longitud de arco de una elipse genérica $x^2/a^2 + y^2/b^2 = 1$, en la que aparece la raíz de un polinomio bicuadrático

$$\int \frac{a^3 - (a^2 - b^2)x^2/a}{\sqrt{(a^2 - x^2)(a^4 - (a^2 - b^2)x^2)}}\, dx.$$

En vano buscaremos en las tablas de integrales: no hay una fórmula "cerrada" general. Al mirar esa hipotética tabla o el libro para ingenieros del pasado (¿ahora usan ordenadores?) veremos que cuando se tienen funciones algebraicas con la raíz cuadrada de un polinomio de primer o segundo grado, hay métodos pero no más allá. Eso sí, con cambios de variable ingeniosos se pueden transformar integrales desconocidas en integrales desconocidas, no es un gran negocio pero permite clasificar nuestro desconocimiento al estudiar integrales con la raíz de un polinomio bicuadrático, y se habla de integrales elípticas de primera, segunda y tercera especie. Las que salen al calcular arcos de elipse

pertenecen a la segunda división, mientras que la división de honor la ocupan integrales de la forma[1]

$$\int \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} \tag{5.1}$$

con k un número real a pesar del nombre (no hay aritmética todavía). Con un cambio de variable $x = \sqrt{\lambda u + \mu}$ otra forma de escribir estas integrales es

$$\int \frac{dx}{\sqrt{x^3 + ax + b}}. \tag{5.2}$$

El caso de grado dos formalmente corresponde en (5.1) a $k = 0$ y $\int_0^t dx/\sqrt{1-x^2} = \operatorname{arc\,sen} t$ que es una función bastante fea (multivaluada), sin embargo su inversa es entera y tan bella como las suaves ondulaciones de un estanque. Jacobi demostró que algo similar ocurría con la función inversa de $\int_0^t dx/\sqrt{(1-x^2)(1-k^2x^2)}$, llamado a veces *seno de amplitud* $\operatorname{sn}(x;k)$, presenta oscilaciones periódicas y en grado mayor que las funciones trigonométricas de toda la vida, pues incluso son periódicas en el plano complejo. Es decir, existen dos números ω_1 y ω_2, uno real y otro complejo tales que $\operatorname{sn}(z;k) = \operatorname{sn}(z+\omega_1;k) = \operatorname{sn}(z+\omega_2;k)$. Por otra parte, $\operatorname{sn}(z;k)$ cumple unas "fórmulas de adición" que recuerdan vagamente a las que aprendimos de memoria en nuestros años mozos para $\operatorname{sen}(\alpha+\beta)$ y $\cos(\alpha+\beta)$ [Ma].

La doble periodicidad impide que $\operatorname{sn}(z;k)$ sea entera porque entonces sería también acotada y por tanto constante (teorema de Liouville), sin embargo tenemos todavía una flamante función meromorfa.

Las funciones meromorfas elementales que conocemos tienen a lo sumo un periodo, por ello se quedan cortas para que sus inversas produzcan fórmulas explícitas para (5.1) y (5.2) más allá de unos casos triviales. Por otro lado, técnicas de cálculo numérico, algunas notablemente desarrolladas por Gauss, permiten aproximarlas con gran precisión.

Con la fiebre calculadora ya calmada, pasamos a centrarnos en las delicias de estas "funciones maravillosas" (denominación tomada del título de [Ma]).

Definición: Se dice que una función meromorfa f es una *función elíptica* si es doblemente periódica, esto es, si existen $\omega_1, \omega_2 \in \mathbb{C}$ linealmente independientes sobre $\mathbb{R}$ tales que $f(z) = f(z+\omega_1) = f(z+\omega_2)$ para todo $z \in \mathbb{C}$.

Ovbiamente también se cumplirá $f(z) = f(z+m\omega_1+n\omega_2)$, recíprocamente para f no constante el conjunto $\{\lambda \ : \ f(z) = f(z+\lambda)\}$ es un retículo llamado *retículo de periodos*

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

Siempre que escribamos ω_1 y ω_2 daremos por supuesto que son generadores de Λ. Escribiremos también

$$\Lambda^* = \Lambda - \{0\}.$$

[1]Estas integrales se obtienen por ejemplo al tratar de resolver la ecuación del péndulo $x''(t) = \operatorname{sen}(2x(t))$. Multiplicando por x' e integrando, $(x')^2 = \text{cte} - \cos^2 x \Rightarrow t = \int dx/\sqrt{\text{cte} - \cos^2 x}$ que lleva a (5.1) con el cambio $u = \cos x$. Se podrían dar también ejemplos tomados de la teoría de la gravitación de Newton o de la relatividad general.

Una función elíptica puede considerarse por tanto como un elemento del cuerpo de funciones de la superficie de Riemann[2] $\mathbb{C}/\Lambda$, es decir, de un toro complejo. Aquí el cociente se hace de la manera obvia: $z_1 \sim z_2 \Leftrightarrow z_1 - z_2 \in \Lambda$. Denotaremos la clase de z con $[z]$.

¿Cómo construir alguna función elíptica? Lo más sencillo es forzar la doble periodicidad sumando trasladados. A partir de un retículo de periodos Λ la función

$$f(z) = \sum_{\omega\in\Lambda} g(z+\omega)$$

es elíptica para cualquier g para la que la suma infinita tenga sentidoen el mundo de las funciones meromorfas. Digamos por ejemplo que g es una potencia. No es difícil probar que $\sum_{\omega\in\Lambda}(z+\omega)^{-k}$ converge si $k > 2$ y diverge si $k \leq 2$. En busca del ejemplo más sencillo modificaremos un poco ("renormalizaremos") el caso límite $k = 2$ para obligarlo a converger.

Definición: Dado un retículo de periodos Λ se llama *función $\wp$ de Weierstrass* asociada a Λ a la función elíptica

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

Nótese que las derivadas sucesivas de esta función producen los casos $k > 2$ ya libres de constantes de convergencia, por ejemplo. Por ejemplo

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

¿Parece poco haber construido dos funciones elípticas? Pues en realidad potencialmente en ella están incluidas todas.

Proposición 5.1.1 *Cualquier función elíptica f puede escribirse como*

$$f(z) = G\big(\wp(z)\big) + \wp'(z)H\big(\wp(z)\big)$$

donde G y H son funciones racionales (cocientes de polinomios).

Demostración: Por la identidad

$$f(z) = \frac{f(z)+f(-z)}{2} + \wp'(z)\frac{f(z)-f(-z)}{2\wp'(z)}$$

basta probar que toda función elíptica par g es una función racional de $\wp(z)$.

Sea el paralelogramo

$$R = \{\lambda\omega_1 + \mu\omega_2 \ : \ |\lambda|, |\mu| \leq 1/2\}.$$

[2]Una variedad de dimensión compleja uno con cambios de carta holomorfos.

Supondremos inicialmente que g no tiene ceros ni polos en el origen ni en la frontera γ de R. Por la doble periodicidad $\int_\gamma g'/g = 0$ (cada lado se anula con el opuesto). Lo que implica, por el principio del argumento [Ah], que hay tantos ceros como polos contando multiplicidades. Sean c y p un cero y un polo de g, entonces $g(z)\big(\wp(z)-\wp(p)\big)/\big(\wp(z)-\wp(c)\big)$ tiene menos ceros y menos polos que g en R, porque hemos cancelado los de c, $-c$, p y $-p$, y no hemos añadido ninguno nuevo ya que la función elíptica $\wp(z)-\text{cte}$ tiene exactamente un polo de orden 2 en R y por tanto sólo dos ceros.

Repitiendo el proceso se llega a una función elíptica entera y por tanto constante, esto es,

$$g(z) = C\prod_j \frac{\wp(z)-\wp(c_j)}{\wp(z)-\wp(p_j)}.$$

Si hubiera un polo o un cero en el origen, se puede eliminar multiplicando o dividiendo por potencias de $\wp$.

Los posibles ceros y polos que cayeran justamente en la frontera γ no causan problemas deformando ligeramente R (!?). □

La función $(\wp')^2$ es elíptica y par, por consiguiente, como se ha visto en la anterior demostración se puede escribir en términos de $\wp$. En vez de analizar el "algoritmo" allí aplicado, usaremos algo tan básico como el álgebra lineal:

Las partes principales de las cuatro funciones elípticas $\wp$, $\wp^2$, $\wp^3$ y $(\wp')^2$ son de la forma $P(z^{-1})$ con P un polinomio de grado a lo más 3 y $P(0)=0$. Tal espacio de polinomios tiene dimensión 3, entonces hay una combinación lineal no trivial que anula las partes principales y por consiguiente

$$\lambda_1\wp + \lambda_2\wp^2 + \lambda_3\wp^3 + \lambda_4(\wp')^2 = \text{cte}.$$

Los coeficientes se pueden hacer explícitos a partir del desarrollo de Laurent de $\wp$, digamos $z^{-2}+a_2z^2+a_4z^4+\dots$ obteniéndose

$$(\wp')^2 = 4\wp^3 - 20a_2\wp - 28a_4.$$

Podemos precisar fácilmente a_2 y a_4 a partir del retículo Λ usando la definición de $\wp$, siguiéndose $a_2 = 3\sum_{\omega\in\Lambda^*}\omega^{-4}$ y $a_4 = 5\sum_{\omega\in\Lambda^*}\omega^{-6}$. En resumidas cuentas, hemos probado:

Proposición 5.1.2 *La función $\wp$ verifica*

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

con $g_2 = 60\sum_{\omega\in\Lambda^*}\omega^{-4}$ *y* $g_3 = 140\sum_{\omega\in\Lambda^*}\omega^{-6}$.

Es fácil ver que ω_1, ω_2 y $(\omega_1+\omega_2)/2$ son ceros de $\wp'$ por tanto se puede escribir

$$4x^3 - g_2x - g_3 = 4\big(x-\wp(\omega_1/2)\big)\big(x-\wp(\omega_2/2)\big)\big(x-\wp((\omega_1+\omega_2)/2)\big),$$

en particular este polinomio tiene raíces simples (como habíamos visto en la demostración de la proposición anterior, $\wp(z)-\text{cte}$ tiene sólo dos ceros $\pm c$).

Desde el punto de vista de las superficies de Riemann lo que hemos hecho es hallar el cuerpo de funciones de $\mathbb{C}/\Lambda$ y probar que la ecuación algebraica de la superficie es $y^2 = 4x^3 - g_2x - g_3$, que no es singular por la ausencia de raíces dobles, y el cálculo de álgebra lineal es un caso muy sencillo del teorema de Riemann-Roch [Fa-Kr]. Con un poco más de lenguaje:

Proposición 5.1.3 *La aplicación*

$$\begin{aligned} \Phi: \ \mathbb{C}/\Lambda &\longrightarrow E \\ z &\mapsto \big(\wp(z), \wp'(z)\big) \end{aligned}$$

establece un isomorfismo holomorfo entre la superficie de Riemann $\mathbb{C}/\Lambda$ y la curva proyectiva $E:\ y^2 = 4x^3 - g_2x - g_3$, entendiendo que $\Phi([0])$ es el punto del infinito de E, de coordenadas proyectivas $(0:1:0)$.

Nota: La inyectividad se sigue porque, como hemos visto, definiendo R como en la demostración de la Proposición 5.1.1, $\wp(z) - \wp(z_1)$ sólo tiene como ceros z_1 y $-z_1$. La sobreyectividad se sigue porque ambas son superficies de Riemann compactas y Φ no es constante [Fa-Kr].

En el toro se puede sumar fácilmente, simplemente lo hacemos en $\mathbb{C}$ y tomamos módulo Λ, por ejemplo, si $\omega_1 = 1$, $\omega_2 = i$, entonces $[2 + \sqrt{2} + \pi i] + [17 - \sqrt{2} + ei] = [(\pi + e - 5)i]$. Se dice que $\mathbb{C}/\Lambda$ es una *variedad abeliana* porque sus puntos conforman un grupo abeliano. Entonces en E debe haber también una forma de sumar puntos.

Lema 5.1.4 *Si $u+v+w \in \Lambda$, esto es, si $[u]$, $[v]$ y $[w]$ suman cero en $\mathbb{C}/\Lambda$ entonces los puntos $\Phi(u)$, $\Phi(v)$ y $\Phi(w)$ están alineados.*

Demostración: Supondremos que $[u]$, $[v]$ y $[w]$ no son $[0]$, es decir, que $u, v, w \notin \Lambda$. Las tres imágenes están alineadas si y sólo si

$$\begin{vmatrix} \wp(u) & \wp'(u) & 1 \\ \wp(v) & \wp'(v) & 1 \\ \wp(w) & \wp'(w) & 1 \end{vmatrix} = 0.$$

Si $u + v + w \in \Lambda$ se puede reemplazar en este determinante w por $-u - v$ sin que varíe su valor. Sea $F(u)$ la función así obtenida (para v fijado). Es evidente que F es elíptica y no es difícil ver que F no tiene un polo en $u = 0$: multiplicando la segunda columna por $u/2$ y sumándosela a la primera se tiene

$$F(u) = \begin{vmatrix} \wp(u) - u\wp'(u)/2 & \wp'(u) & 1 \\ \wp(v) - u\wp'(v)/2 & \wp'(v) & 1 \\ \wp(-u-v) - u\wp'(-u-v)/2 & \wp'(-u-v) & 1 \end{vmatrix} = 0.$$

La segunda y la tercera filas coinciden hasta orden dos, por tanto no hay polo en $u = 0$.

De forma similar, por simetría, se deduce que no hay un polo en $u = -v$, entonces F es entera y elíptica, por tanto constante, además como $F(v) = 0$, debe ser idénticamente nula.

Si alguno de los elementos es [0] aparece el punto del infinito, pero el argumento no es diferente. Digamos por ejemplo $[v] = 0$ (el resto de los casos se reducen a éste), entonces la segunda fila del determinante inicial pasa a ser $(0, 1, 0)$. □

Se puede probar que el proceso se puede invertir asociando a cada curva no singular de la forma $E:\ y^2 = 4x^3 - \alpha x - \beta$ un toro $\mathbb{C}/\Lambda$ cuya imagen por Φ es E. El retículo Λ estará formado por los valores de $\int_\gamma \omega$ con ω la diferencial holomorfa dx/y y γ un lazo definido en (la superficie de Riemann que determina) E. Incluso tal retículo se puede calcular numéricamente con gran precisión [Kn] VI§9. Nótese que $\int \omega$ es como (5.2). Las "fórmulas de adición" antes mencionadas para este tipo de integrales corresponden a la suma en $\mathbb{C}/\Lambda$.

Simplemente para que las cosas sean más simples y se parezcan a las de los libros actuales, consideraremos $E:\ y^2 = x^3 + ax + b$ en lugar de $E:\ y^2 = 4x^3 - \alpha x - \beta$, tales curvas sólo difieren en un cambio lineal que por tanto no destruye la alineación de los puntos. La no singularidad de E equivale a que $x^3 + ax + b$ no tenga raíces dobles, o lo que es lo mismo, a que el determinante $4a^3 + 27b^2$ no sea nulo.

Proposición 5.1.5 *Sea $E:\ y^2 = x^3 + ax + b$ curva proyectiva sobre $\mathbb{C}$ no singular. Entonces se puede dotar a sus puntos de una ley de grupo $(E, +)$ de forma que el elemento neutro O es el punto del infinito, el elemento inverso de $P = (x, y)$ es $P = (x, -y)$ y si $P + Q = R$ entonces P, Q y $-R$ están alineados.*

Observación: Ciertamente uno podría definir directamente la ley de grupo en $E:\ y^2 = x^3 + ax + b$ con el simétrico del tercer punto de intersección de la recta secante, y demostrar que realmente es ley de grupo sin referencia a la función $\wp$ (como en los libros actuales) pero entonces la asociativa daría algún dolor de cabeza (cf. [Ca]).

Demostración: La ley de grupo viene heredada de la suma en $\mathbb{C}/\Lambda$, es decir,

$$P + Q = \Phi\big(\Phi^{-1}(P) + \Phi^{-1}(Q)\big)$$

y trivialmente comparte las propiedades de grupo abeliano con la suma usual.

Considerando $\Phi([0])$ y la paridad de $\wp$ es fácil deducir los elementos neutro y opuesto. Si $P + Q - R = 0$, por definición $\Phi^{-1}(P) + \Phi^{-1}(Q) + \Phi^{-1}(-R) = [0]$ y el lema anterior prueba que P, Q y $-R$ están alineados. □

Si dos raíces de un polinomio cúbico en $K[x]$ pertenecen a K, entonces la tercera raíz pertenece también a K. Esta sencilla observación prueba que la ley de grupo anterior tiene aplicaciones aritméticas. Desde el punto de vista de las ecuaciones diofánticas, las curvas de primer y segundo grado se pueden parametrizar si tienen un punto racional

(y esto se puede decidir algorítmicamente con el Teorema de Hasse-Minkowski [Bo-Sh], [Ca]), lo cual permite calcular fácilmente todos los puntos racionales[3]. La ley de grupo permite enfrentarse al caso de tercer grado.

Definición: Una *curva elíptica* E sobre un cuerpo K es una curva proyectiva cúbica no singular sobre K con al menos un punto en este cuerpo.

En cuerpos normales y corrientes (por ejemplo en característica cero), es fácil ver que toda curva elíptica tras un cambio de variable se escribe como $y^2 = x^3 + ax + b$ con $4a^3 + 27b^2 \neq 0$, y en los casos patológicos donde no siempre puede hacerse (por ejemplo en $\mathbb{F}_2$) hay una expresión similar [Ca], [Si]. Por ello la ley de grupo se extiende a todas las curvas cúbicas no singulares.

Para los amigos de los formulones, unos cálculos consistentes en intersecar una recta y una cúbica, prueban que para una curva elíptica $E:\ y^2 = x^3 + ax + b$, se tienen las fórmulas:

$$P = (x_1, y_1), \qquad Q = (x_2, y_2), \qquad P + Q = (x, y)$$

con

$$x = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2, \qquad y = -\frac{y_1 - y_2}{x_1 - x_2}x - \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}$$

siempre que $x_1 \neq x_2$. Si $x_1 = x_2$ pero $P \neq Q$ debemos entender que el resultado es el punto del infinito y si $P = Q$, es el "límite" en E de la expresión anterior:

$$x = \left(\frac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1, \qquad y = -\frac{3x_1^2 + A}{2y_1}x - \frac{-x_1^3 + ax_1 + 2b}{2y_1}.$$

¿Y qué se sabe de la aritmética de las curva elípticas? Muchas cosas pero todavía hay grandes lagunas.

Se conoce que el grupo de puntos sobre $\mathbb{Q}$ de una curva elíptica está finitamente generado (teorema de Mordell), es decir, que a partir de algunas soluciones podemos generar todas a base de sumas. También se saben calcular los puntos de torsión: los puntos racionales que al ser operados consigo mismos vuelven a repetirse a la larga; pero se desconoce un algoritmo infalible desde el punto de vista teórico para calcular los puntos que no se repiten, los que dan lugar a infinitas soluciones, o saber si no existen.

Otro punto importante tiene que ver con las relaciones locales-globales. Por ejemplo, se cree que si en una curva elíptica hay "muchos" puntos módulo p para todo p, entonces debe contener infinitos puntos racionales (conjetura de Birch–Swinnerton-Dyer).

5.2. Formas modulares

Según hemos visto, las curvas elípticas se corresponden con los retículos. Una pregunta natural es si retículos diferentes pueden dar lugar a la misma curva salvo isomorfismos

[3]Por ejemplo $x^2 + y^2 = 1$ se parametriza como $x = (t^2 - 1)/(t^2 + 1)$, $y = 2t/(t^2 + 1)$ y eligiendo $t \in \mathbb{Q}$ se obtienen todas las soluciones racionales salvo $(1, 0)$.

(cambios de variable). Atacaremos primero el problema más básico, y realmente muy sencillo, consistente en decidir si dos retículos son iguales a partir de sus generadores.

Si Λ es el retículo (en $\mathbb{C}$) generado por $\{\omega_1, \omega_2\}$ y Λ' es el generado por $\{\eta_1, \eta_2\}$, entonces $\Lambda = \Lambda'$ si y sólo si hay un cambio de variable lineal con matriz entera e inversa entera que pase los generadores de uno a los del otro. Es decir

$$\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix} \begin{pmatrix}a & b\\ c & d\end{pmatrix} \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} \qquad \text{con} \quad ad - bc = \pm 1. \tag{5.3}$$

Si reordenamos los generadores de forma que tengan la misma orientación, por ejemplo $\angle\omega_1\omega_2,\ \angle\eta_1\eta_2 < \pi$, entonces $+1$ es la única posibilidad. La orientación elegida corresponde a exigir que $z_\Lambda = \omega_1/\omega_2$ y $z_{\Lambda'} = \eta_1/\eta_2$ estén en el semiplano superior

$$\mathbb{H} = \{x + iy \ : \ x \in \mathbb{R},\ y > 0\}.$$

Si dividimos las ecuaciones de la primera y la segunda coordenadas en (5.3) podemos escribir esta relación en términos de z_Λ y $z_{\Lambda'}$, y sólo perdemos la información de multiplicar ambas ecuaciones por una constante. Con un poco de lenguaje pero sin nada nuevo:

Lema 5.2.1 *Si $\Lambda = \Lambda'$ entonces*

$$z_{\Lambda'} = \gamma z_\Lambda \qquad \textit{con } \gamma = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in SL_2(\mathbb{Z})$$

donde se define $\gamma z = (az + b)/(cz + d)$. Además, si $z_\Lambda = z_{\Lambda'}$ entonces $\Lambda' = \mu\Lambda$ para algún $\mu \in \mathbb{C}$.

Nota: Recuérdese que $\mathrm{SL}_2(\mathbb{Z})$ es el grupo de matrices enteras con determinante uno. Sería más propio escribir $\gamma(z)$ en vez de γz, pero el uso ha privilegiado a esta última notación.

Es fácil ver que $\mathrm{SL}_2(\mathbb{Z})$ actúa "bien" en $\mathbb{H}$. Cada $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ define una biyección $\mathbb{H} \longrightarrow \mathbb{H}$ y la acción es propia y discontinua[4]. Un pequeño borrón en el historial de $\mathrm{SL}_2(\mathbb{Z})$ es que γ y $-\gamma$ actúan igual, por ello a veces se toma en consideración el grupo menos intuitivo $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$.

Los elementos de $\mathrm{SL}_2(\mathbb{Z})$ no envían un punto fijado a cualquier punto de $\mathbb{H}$ porque no todos los retículos son iguales. La relación es un poco más sutil.

Proposición 5.2.2 *Dado $z \in \mathbb{H}$ existe $\gamma \in SL_2(\mathbb{Z})$ tal que γz pertenece al* dominio fundamental

$$D = \{z \ : \ |\Re z| \le 1/2,\ |z| \ge 1\}.$$

De hecho z corresponde exactamente a un punto en D si se suprime la parte de la frontera en $\Re z < 0$.

[4]Que la acción sea discontinua significa que la órbita de un punto no tiene puntos límite (las imágenes de un punto caen en puntos aislados). Por poner más apellidos, $\mathrm{SL}_2(\mathbb{Z})$ es un grupo Fuchsiano de primera especie [Iw].

Demostración: El grupo $\mathrm{SL}_2(\mathbb{Z})$ está generado por las matrices $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ y $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ [Kn] Prop. 5.3, la primera corresponde a la traslación $z \mapsto z+1$ y la segunda a la inversión $z \mapsto -1/z$. A base de trasladar podemos enviar cualquier $z \in \mathbb{H}$ a $|\Re z| \leq 1/2$ y con una inversión podemos sacar fuera lo que está dentro del círculo unidad $|z| \leq 1$.

La traslación y la inversión pasan la frontera izquierda a la derecha de ahí la ambigüedad de estos puntos y hay que suprimir una de ellas para preservar la unicidad. □

Hay varias maneras de leer este resultado. Si consideramos el conjunto[5]

$$\mathbb{H}\backslash\mathrm{SL}_2(\mathbb{Z}) = \{\text{órbitas de } z \text{ en } \mathbb{H}\},$$

entonces hemos probado que $\mathbb{H}\backslash\mathrm{SL}_2(\mathbb{Z})$ es como D con las fronteras derecha e izquierda identificadas. Topológicamente es una esfera en la que un punto se ha llevado a infinito, si se emplea la métrica heredada de la natural[6] en $\mathbb{H}$.

Un isomorfismo de curvas elípticas $f : E \longrightarrow E'$ (pedimos que se conserve el punto del infinito, $f(O) = O$, lo cual es como decir que el isomorfismo también lo es de grupos) da lugar, a través de Φ^{-1}, a un isomorfismo holomorfo $F : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$. En particular F se puede extender a $\mathbb{C} \longrightarrow \mathbb{C}$ con $F(0) = 0$ y envía Λ en Λ'. Como las funciones holomorfas no singulares son conformes (conservan ángulos) es fácil deducir (!?) que F sólo puede ser un giro quizá combinado con una homotecia, es decir, $F(z) = \mu z$ y por tanto $\Lambda' = \mu\Lambda$. Con ello hemos resuelto el problema original.

Proposición 5.2.3 *Dos retículos $\Lambda, \Lambda' \subset \mathbb{C}$ corresponden a curvas elípticas isomorfas si y sólo si $z_\Lambda = z_{\Lambda'}$ están en la misma clase de $\mathbb{H}\backslash SL_2(\mathbb{Z})$, esto es, si $z_{\Lambda'} = \gamma z_\Lambda$ para algún $\gamma \in SL_2(\mathbb{Z})$.*

Si tuviéramos una función inyectiva $J : \mathbb{H}\backslash\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathbb{C}$ al "desenrollarla" a $\mathbb{H}$, definiendo $J(z) = J(\text{órbita de } z)$, se obtendría una función que satisface la relación modular[7]

$$J(z) = J(\gamma z) \qquad \forall \gamma \in \mathrm{SL}_2(\mathbb{Z}) \tag{5.4}$$

y la condición del resultado anterior equivaldría a $J(z_\Lambda) = J(z_{\Lambda'})$.

Por otro lado, dadas dos curvas elípticas $E : y^2 = x^3 + ax + b$, $E' : y^2 = x^3 + a'x + b'$, parece claro que no podemos hacer cambios de grado mayor o igual que uno para pasar de una a otra porque no serían invertibles, y entre los cambios lineales sólo aquellos

[5] Recuérdese de los cursos de teoría de grupos que la órbita de un elemento es la colección de imágenes por la acción de un grupo.

[6] La métrica de Poincaré en $\mathbb{H}$, $ds^2 = y^{-2}(dx^2+dy^2)$, es la métrica coherente con las transformaciones $\gamma \in \mathrm{SL}_2(\mathbb{R})$ porque éstas la dejan invariante (son isometrías). Con ella los puntos $-1/2+iy$ y $1/2+iy$ se acercan más cuanto mayor es y, de ahí que D sea como una esfera con un punto en el infinito y no una esfera con un círculo en el infinito como podría dictarnos nuestra visión euclídea.

[7] Este desafortunado nombre es una vetusta herencia de la teoría de funciones e integrales elípticas que deriva del nombre *módulo* que recibía la constante k de (5.1).

de la forma $y \mapsto \lambda^3 y$, $x \mapsto \lambda^2 x$ preservan la forma de la ecuación cúbica (con otros aparecería por ejemplo un término en x^2). Así pues la única posibilidad para que sean isomorfas es que $a' = \lambda^{-4}a$ y $b' = \lambda^{-6}b$. Entonces cualquier función $g = g(a,b)$ con $g(a,b) = g(\lambda^{-4}a, \lambda^{-6}b)$ será invariante en las curvas elípticas isomorfas y corresponderá a través de Φ^{-1} a una función que satisface (5.4). Hay muchas posibilidades, por ejemplo $g(a,b) = a^3/b^2$. Tomaremos sin embargo $g(a,b) = \text{cte}\ a^3/(4a^3 + 27b^2)$ que tiene la ventaja de que no produce nunca infinitos. Recuérdese que $y^2 = x^3 + ax + b$ se puede transformar en $y^2 = 4x^3 - g_2 x - g_3$ con g_2 y g_3 dependiendo del retículo como se indica en la Proposición 5.1.2.

Escribiendo como antes $z = \omega_1/\omega_2$ y revisando las cuentas, todo este galimatías se traduce en que una posibilidad para la función J que buscábamos es

$$J(z) = \frac{E_4^3(z)}{20E_4^3(z) - 49E_6^2(z)} \qquad \text{con} \qquad E_k(z) = \sum_{\substack{n,m=-\infty \\ n^2+m^2\neq 0}}^{\infty} \frac{1}{(nz+m)^k}.$$

Nótese que es muy fácil comprobar que $J(z) = J(z+1)$ y $J(z) = J(-1/z)$, consecuentemente (5.4) admite una prueba directa una vez que sabemos que $z \mapsto z+1$ y $z \mapsto -1/z$ generan la acción de $\mathrm{SL}_2(\mathbb{Z})$. La invariancia de J se deriva de que las funciones $E_k(z)$ satisfacen $E_k(z) = E_k(z+1)$ y $E_k(z) = z^{-2k}E_k(-1/z)$. Estas dos fórmulas se combinan en la expresión general

$$E_k(z) = j_\gamma^{-k}(z)E_k(\gamma z) \qquad \text{donde } j_\gamma(z) = cz + d \quad \text{para } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Es hora de dar alguna definición que justifique el título del capítulo.

Definición: Se dice que una función holomorfa $f : \mathbb{H} \longrightarrow \mathbb{C}$ es una *función modular de peso* k si satisface

$$f(z) = j_\gamma^{-k}(z) f(\gamma z) \qquad \forall \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Se dice que una función modular es una *forma modular* si además es holomorfa en el infinito, $\lim_{y\to+\infty} f(x+iy) < \infty$. Si este límite es cero se dice que es una *forma parabólica* (o *cuspidal*).

Notación: Denotaremos con $\mathcal{M}_k$ el conjunto de formas modulares de peso k y con $\mathcal{S}_k$ las formas parabólicas de peso k.

Evidentemente $\mathcal{M}_k$ es un espacio vectorial sobre $\mathbb{C}$ y $\mathcal{S}_k$ es un subespacio suyo. Como γ y $-\gamma$ dan lugar a la misma acción sobre $\mathbb{H}$, estos espacios sólo pueden ser no triviales cuando k es par. No obstante hay generalizaciones de la definición anterior que cubren los casos $k \in \mathbb{R}$ (véase [Iw]). Así como una función modular de peso 0 corresponde a una función definida en $\mathbb{H}\backslash\mathrm{SL}_2(\mathbb{Z})$, una de peso 2 corresponde a una forma diferencial[8] y las de peso superior a diferenciales de orden superior. De alguna manera las formas parabólicas suplen a las diferenciales de soporte compacto que no existen en el mundo holomorfo. Todas ellas pueden verse como funciones homogéneas de cierto grado definidas en el

[8] La expresión $f(z)dz$ es invariante bajo $\mathrm{SL}_2(\mathbb{Z})$ si f es de peso 2 porque $d\gamma z = j_\gamma^{-2}(z)$.

espacio de retículos. Por ejemplo, si F es homogénea (de grado 0), la condición (5.3) para que no dependa de los generadores elegidos es $F(\omega_1, \omega_1) = F(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$ y equivale a que $J(z) = F(z, 1)$ verifique (5.4) con $z = \omega_1/\omega_2$ como antes.

Una forma modular f en particular es periódica de periodo uno y por tanto debe admitir un desarrollo de Fourier

$$f(z) = \sum_{m=0}^{\infty} a_m e(mz)$$

y $f \in \mathcal{S}_k$ cuando $a_0 = 0$.

Para las funciones E_k, llamadas *series de Eisenstein*, se puede obtener este desarrollo derivando el bien conocido desarrollo de la cotangente:

$$\pi i - 2\pi i \sum_{m=0}^{\infty} e(mz) = \pi \cot(\pi z) = \sum_{-\infty}^{\infty} \frac{1}{z+m}.$$

El resultado obtenido es

$$E_{2k}(z) = 2\zeta(2k) + 2\frac{(2\pi i)^k}{(2k-1)!} \sum_{m=1}^{\infty} \sigma_{2k-1}(m) e(mz)$$

donde $\sigma_{2k-1}(m) = \sum_{d|m} d^{2k-1}$.

Una de las propiedades básicas de los espacios vectoriales $\mathcal{M}_k$ y $\mathcal{S}_k$ es que tienen dimensión finita y además computable. La preuba de este hecho sólo requiere los rudimentos de variable compleja pero no la reproduciremos aquí (véase [Se]).

Proposición 5.2.4 *Para $k \geq 0$ par*

$$\dim \mathcal{M}_k = \begin{cases} [k/12] & si\ 12|k-2 \\ [k/12]+1 & si\ 12|k-2 \end{cases} \qquad \dim \mathcal{S}_k = \begin{cases} 0 & si\ k < 12 \\ \dim \mathcal{M}_{k-12} & si\ k \geq 12 \end{cases}$$

donde $[\cdot]$ indica la parte entera.

Esto permite demostrar algunas identidades asombrosas.

Por ejemplo, $\dim \mathcal{M}_8 = 1$ y como $E_4^2, E_8 \in \mathcal{M}_8$ deben ser proporcionales, comparando el primer coeficiente $2\zeta^2(4)E_8(z) = \zeta(8)E_4^2(z)$. Mirando una tabla o haciendo los cálculos, se cumple $\zeta(4) = \pi^4/90$ y $\zeta(8) = \pi^8/9450$ y el desarrollo de Fourier conduce a

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m).$$

Otro ejemplo tiene que ver con la primera forma parabólica, que aparece para el peso $k = 12$. Buscando la anulación del primer coeficiente de Fourier se tiene que la forma

modular $(2\zeta(6))^2E_4^3(z) - (2\zeta(4))^3E_6^2(z)$ está en $\mathcal{S}_{12}$. Por otra parte es posible probar, haciendo algunos pases mágicos con derivadas logarítmicas (véase [Se]), que

$$\Delta(z) = e(z)\prod_{m=1}^{\infty}(1-e(mz))^{24} \in \mathcal{S}_{12}$$

de donde se deduce la extraña igualdad (¿se podría probar de forma elemental y sencilla? quizá no)

$$\Delta(z) = \frac{675}{256\pi^{12}}\big(20E_4^3(z) - 49E_6^2(z)\big).$$

Todavía hay más misterios relativos a esta función. Si $\tau(n)$ es el n-ésimo coeficiente de Fourier de $\Delta(z)$ entonces z es una función multiplicativa. Esto fue conjeturado por S. Ramanujan, quien notó otras asombrosas propiedades como la fórmula $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ o la congruencia $\tau(n) \equiv \sigma_{11}(n)$ (691). Además la "función L" asociada a Δ

$$L(s,\Delta) = \sum_{n=1}^{\infty}\frac{\tau(n)}{n^s}$$

satisface una ecuación funcional sorprendentemente similar a la de la función ζ. Todas estas propiedades se encuadran y demuestran dentro de la teoría de formas modulares desarrollada por Hecke. Un asunto mucho más espinoso es el tamaño de los coeficientes de Fourier de una forma modular, en particular de $\Delta(z)$. Por ejemplo, la inocente conjetura de Ramanujan $|\tau(p)| < 2p^{11/2}$ debió esperar hasta el trabajo de P. Deligne que mereció la medalla Fields en los años 70. La sencilla distribución conjeturada para $p^{-11/2}\tau(p)$ cuando p varía (conjetura de Sato-Tate) es todavía un problema abierto.

De las anteriores propiedades, la ecuación funcional es la más sencilla y nos ocuparemos de ella ahora. En la siguiente sección daremos los ingredientes para poder probar la multiplicatividad de los coeficientes.

Proposición 5.2.5 *Dada $f \in S_{2k}$ con $f(z) = \sum_{m=0}^{\infty} a_m e(mz)$, sea*

$$L(s,f) = \sum_{m=1}^{\infty}\frac{a_m}{m^s}.$$

Entonces $L(s,f)$ admite una extensión entera que verifica la ecuación funcional

$$(2\pi)^{-s}\Gamma(s)L(s,f) = (-1)^k(2\pi)^{s-2k}\Gamma(2k-s)L(2k-s,f).$$

Demostración: Por la definición de la función Γ y el desarrollo de Fourier de f, se tiene

$$(2\pi)^{-s}\Gamma(s)L(s,f) = \int_0^{\infty} f(it)t^{s-1}\,dt.$$

Esto prueba que $L(s,f)$ se extiende a una función entera. Por la relación modular $f(z) = z^{-2k}f(-1/z)$ se cumple $f(it) = (-1)^k t^{-2k}f(i/t)$ y sustituyendo en la integral y cambiando la variable $t \mapsto 1/u$ se deduce que el segundo miembro es invariante al reemplazar s por $2k-s$, salvo la multiplicación por $(-1)^k$. □

Una rica fuente de funciones y formas modulares son las funciones θ asociadas a formas cuadráticas. No se ajustan en general a la estricta definición dada aquí pero nos valdremos de un ejemplo para ilustrar la situación.

La función

$$\theta(z) = \sum_{m=-\infty}^{\infty} e(m^2 z/2),$$

por la periodicidad y la fórmula de sumación de Poisson, cumple

$$\theta(z) = \theta(z+2) \qquad \text{y} \qquad \theta(z) = (iz)^{-1/2}\theta(-1/z).$$

Es una forma modular de peso $1/2$ con dos salvedades frente a la definición de esta sección: En primer lugar el grupo que actúa no es todo $\mathrm{SL}_2(\mathbb{Z})$ pues no aparece $z \mapsto z+1$, y en segundo lugar, la relación modular está afectada por un "multiplicador" $i^{-1/2}$. Elevando a una potencia adecuada el multiplicador no será molesto. Por ejemplo, si estamos interesados en $r_8(m)$, el número de representaciones de m como suma de ocho cuadrtados,

$$\theta^8(z) = \sum_{m=0}^{\infty} r_8(m) e(mz/2)$$

y se tiene

$$\theta^8(z) = j_\gamma^{-4}(z)\theta(\gamma z) \qquad \text{para} \quad \gamma \in G$$

donde G es el grupo generado por $z \mapsto z+2$ y $z \mapsto -1/z$.

La teoría es paralela al caso de $\mathrm{SL}_2(\mathbb{Z})$ y por cuestiones de dimensión se puede deducir que $\theta^8(z)$ debe ser proporcional a una variante de la serie de Eisenstein y de ahí la fórmula cerrada

$$r_8(m) = 16(-1)^m m^3 \sum_{d|m} (-1)^{m/d} d^{-3}.$$

No hay fórmulas bonitas cuando la dimensión del espacio de formas modulares crece, pues entonces $\theta^{4k}(z)$ no se puede expresar sólo como suma de series de Eisenstein. Por ejemplo, el caso de 24 cuadrados lleva a considerar formas de peso $12 = 24 \cdot 1/2$ y el resultado final es una parte principal con sumas de divisores, que proviene de las series de Eisenstein, y otra menos influyente que contiene los coeficientes $\tau(n)$ de $\Delta(z)$, la "única" forma parabólica de peso 12. El método del círculo permite deducir el término principal sin necesidad de entrar en la teoría de formas modulares.

5.3. Operadores de Hecke

Se puede definir una función invariante en un retículo tomando otra y promediándola en retículos más finos que coinciden con el original tras aplicar una transformación lineal de determinante n. Elaborando esta idea en el contexto de las formas modulares [Kn], [Se], que a fin de cuentas son funciones homogéneas de retículos [Iw], se llega al concepto de operadores de Hecke.

Para definirlos se considera un conjunto Δ_n de representantes de los cogrupos a la derecha $\mathrm{SL}_2(\mathbb{Z})\backslash M_n$ con M_n las matrices de determinante n, o dicho de otra forma, se escoge Δ_n de manera que

$$M_n = \bigcup_{\alpha\in\Delta_n} \mathrm{SL}_2(\mathbb{Z})\alpha$$

sea una partición.

Proposición 5.3.1 *Para $n \in \mathbb{N}$ el* operador de Hecke *definido como*

$$T_n f = n^{k/2-1} \sum_{\alpha\in\Delta_n} j_\alpha^{-k}(z) f(\alpha z)$$

aplica $\mathcal{M}_k$ en $\mathcal{M}_k$ y $\mathcal{S}_k$ en $\mathcal{S}_k$.

La definición anterior se puede escribir de forma mucho más pedestre comprobando que un conjunto válido de representantes es (véase [Se], [Iw])

$$\Delta_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \ : \ ad = n,\ 0 \le b < d \right\}.$$

Es decir,

$$T_n f(z) = n^{k-1} \sum_{ad=n} \sum_{i=0}^{d-1} d^{-k} f\big(\frac{az+b}{d}\big).$$

Con esta fórmula simplificada en nuestras manos no es difícil dar una prueba directa de la proposición anterior y estudiar cómo actúa T_n sobre el desarrollo de Fourier de una forma modular.

Proposición 5.3.2 *Sea $f(z) = \sum_{m=0}^{\infty} a_m e(mz) \in \mathcal{M}_k$, entonces*

$$T_n f(z) = \sum_{m=0}^{\infty} b_m e(mz) \qquad \textit{con} \qquad b_m = \sum_{d|(n,m)} d^{k-1} a_{nm/d^2}.$$

En particular, si $n = p$ es primo el coeficiente de Fourier m-ésimo de $T_n f(z)$ con $p \not| m$ es a_{pm}.

Empleando la proposición anterior o, mejor todavía, con la definición en términos de retículos [Kn] VIII.7, se deduce

Proposición 5.3.3 *Los operadores de Hecke verifican*

$$T_m T_n = \sum_{d|(n,m)} d^{k-1} T_{mn/d^2}.$$

En particular los operadores de Hecke conmutan y si $(n,m) = 1$ se tiene $T_m T_n = T_{mn}$.

Los operadores de Hecke son autoadjuntos con respecto al producto escalar de fromas modulares dado por

$$\langle f, g\rangle = \int_D f(z)\overline{g(z)}y^{k-2}\,dxdy$$

y por tanto se puede diagonalizar. Por simple álgebra lineal si tenemos endomorfismos diagonalizables y que conmutan, debe exisitr una base en la que todos ellos diagonalicen simultáneamente.

Definición: Se dice que $\mathcal{B} = \{f_1, f_2, \ldots, f_r\}$ es una *base de Hecke* de $\mathcal{M}_k$ o de $\mathcal{S}_k$ si cada $f \in \mathcal{B}$ cumple $T_n f(z) = \lambda_n f(z)$ para todo $n \in \mathbb{N}$ y ciertos λ_n (dependiendo de f).

El misterioso comportamiento de los coeficientes de la función $\Delta(z)$ está a punto de ser desvelado.

Proposición 5.3.4 *Sea $f(z) = \sum_{m=0}^{\infty} a_m e(mz)$ un elemento de una base de Hecke con $a_1 = 1$, entonces*

a) $a_n = \lambda_n$, el autovalor de f en T_n.

b) $a_n a_m = \sum_{d|(n,m)} d^{k-1} a_{nm/d^2}$.

Demostración: Por la Proposición 5.3.2 el coeficiente de $e(z)$ en el desarrollo de Fourier de $T_n f(z)$ es a_n y la relación $T_n f(z) = \Lambda_n f(z)$ termina la prueba de *a*).

Para *b*) basta aplicar *a*) junto con la Proposición 5.3.3. □

Corolario 5.3.5 *Sea $\tau(n)$ el n-ésimo coeficiente de $\Delta(z) = e(z)\prod_{m=1}^{\infty}(1-e(mz))^{24}$ entonces τ es una función multiplicativa que satisface $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ para p primo.*

Demostración: Como $\dim \mathcal{S}_{12} = 1$, $\mathcal{B} = \{\Delta(z)\}$ es una base de Hecke. Obviamente $\tau(1)1$ y se aplica la proposición. La conclusión buscada es consecuencia directa de *b*). □

Corolario 5.3.6 *La función $L(s, \Delta)$ admite el producto de Euler*

$$L(s,\Delta) = \prod_p \left(1 - \tau(p)p^{-s} + p^{11-2s}\right)^{-1}.$$

Demostración: Por ser τ multiplicativa

$$L(s,\Delta) = \prod_p \left(1 + \frac{\tau(p)}{p^s} + \frac{\tau(p^2)}{p^{2s}} + \frac{\tau(p^3)}{p^{3s}} + \ldots\right).$$

Multiplicando cada factor por $1 - \tau(p)p^{-s} + p^{11-2s}$ el coeficiente de p^{-rs}, $r \geq 2$ es $\tau(p^r) - \tau(p)\tau(p^{r-1}) + p^{11}\tau(p^{r-2}) = 0$ y de aquí (!?) cada uno de ellos es igual a $\left(1 - \tau(p)p^{-s} + p^{11-2s}\right)^{-1}$. □

En esta sección más que en otras es necesario mencionar que esto es sólo una mínima parte de una inmensa teoría que se esconde detrás. La conexión de las formas modulares con la aritmética se realiza fundamentalmente a través de los operadores de Hecke. Esta relación involucra ideas muy profundas. Por ejemplo, para peso $k = 2$ los operadores de Hecke se pueden "dualizar" para que actúen en la homología con coeficientes enteros en superficies de Riemann uniformizadas por ciertos subgrupos sencillos de $\mathrm{SL}_2(\mathbb{Z})$. Esto permite probar que los coeficientes de Fourier de las formas modulares de peso 2 de la base de Hecke correpsondiente a estos subgrupos, son números algebraicos. Si además son enteros, la teoría de M. Eichler y G. Shimura les asocia una curva elíptica sobre $\mathbb{Q}$ cuyo número de soluciones módulo p está relacionado con estos coeficientes. Las importantes contribuciones actuales, partiendo del trabajo de A. Wiles, han permitido ir en el sentido contrario asociando a las curvas elípticas sobre $\mathbb{Q}$ una forma modular, con algunas consecuencias bien conocidas.

Bibliografía

[Ah] L.V. Ahlfors. Análisis de variable compleja: Introducción a la teoría de funciones analíticas de una variable compleja. Aguilar, Madrid 1971.

[Bo-Sh] A.I. Borevich, I.R. Shafarevich. Number theory. Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London 1966.

[Ca] J.W.S. Cassels. Lectures on elliptic curves, London Mathematical Society Student Texts 24, Cambridge University Press, 1991.

[Fa-Kr] H.M. Farkas, I. Kra. Riemann surfaces. Graduate Texts in Mathematics, 71. Springer-Verlag, New York-Berlin, 1980.

[Iw] H. Iwaniec. Topics in classical automorphic forms. Graduate Studies in Mathematics, 17. American Mathematical Society, Providence, RI, 1997.

[Kn] A.W. Knapp. Elliptic curves. Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992.

[Ma] A.I. Markushevich. Curvas maravillosas. Números complejos y representaciones conformes. Funciones maravillosas. Lecciones populares de Matemáticas. Editorial Mir, 1977.

[Se] J.-P. Serre. A course in arithmetic. Graduate Texts in Mathematics, 7. Springer-Verlag, New York-Heidelberg, 1973.

[Si] J. Silverman, The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106. Springer-Verlag, 1986.