REAL ACADEMIA DE CIENCIAS
EXACTAS, FÍSICAS Y NATURALES

Antecedentes y evolución de la teoría de la multiplicación compleja

DISCURSO
LEÍDO EN EL ACTO DE SU RECEPCIÓN
POR LA

EXCMA. SRA. D.ª PILAR BAYER ISANT

Y
CONTESTACIÓN
DEL

EXCMO. SR. D. MANUEL LÓPEZ PELLICER

EL DÍA 24 DE FEBRERO DE 2010

MADRID
Domicilio de la Academia
Valverde, 22
2010

ISBN: 978-84-87125-48-5
ISSN: 0214-9540
Depósito Legal: B-7931-2010

Impreso en Gráficas Rey. S.L.
Con financiación parcial del MICINN: MTM2006-04895

Índice general

DISCURSO DE LA EXCMA. SRA. D.ª PILAR BAYER ISANT

ANTECEDENTES Y EVOLUCIÓN DE LA TEORÍA DE LA MULTIPLICACIÓN COMPLEJA

Excmo. Sr. Presidente,

Excmo. Sr. Presidente de Honor,

Excmos. Srs. Académicos,

Excmas. Sras. Académicas,

Distinguido público

En primer lugar deseo expresar mi agradecimiento a la Real Academia de Ciencias Exactas, Físicas y Naturales por el honor que me confiere al nombrarme académica de número. Durante estos años como académica correspondiente, he podido apreciar en múltiples ocasiones la encomiable labor en favor de la ciencia que, desde ópticas diversas y con un cuidado exquisito, llevan a cabo sus ilustres miembros. Es por ello que me considero muy privilegiada por formar parte de esta corporación y que anhelo poder contribuir a las tareas que la Academia estime oportuno.

Como tema de mi discurso he elegido la teoría de la multiplicación compleja. Bajo esta denominación se conoce un capítulo de la aritmética que, siendo clásico, ha experimentado importantes transformaciones en las últimas décadas. Mi propósito es hacer una presentación histórica del mismo, poniendo de manifiesto su repercusión en la comprensión y resolución de determinados problemas diofánticos.

Capítulo 1

Problemas aritméticos

La teoría de cuerpos de clases proporciona una descripción de las extensiones abelianas de los cuerpos de números a partir de la aritmética del cuerpo base. Si bien se trata de una teoría profunda, cuya elaboración conllevó más de un siglo, sus resultados no son efectivos. La búsqueda de efectividad en la teoría de cuerpos de clases condujo al desarrollo paralelo de la teoría de la multiplicación compleja.

Como ilustración de los problemas que vamos a tratar, empecemos por considerar el ejemplo de las raíces complejas de la unidad. Las raíces de la unidad son las soluciones de las ecuaciones algebraicas $X^N - 1 = 0$, para $N \geq 1$. Se trata de enteros algebraicos cuyos polinomios irreducibles, los denominados polinomios ciclotómicos, se calculan recurrentemente.

Como es bien sabido, las raíces complejas N-ésimas de la unidad pueden identificarse con valores especiales de la función exponencial,

$$e^{iu} = \cos(u) + i \sin(u),$$

obtenidos al evaluar ésta en los puntos de división en N partes iguales del intervalo $[0, 2\pi)$. Escribiremos

$$P_N = \{\zeta_N^a : \ \zeta_N = e^{2\pi i/N}, \ 1 \leq a \leq N\}.$$

Dado un entero $N \geq 1$, denotemos por $\mathbb{Z}/N\mathbb{Z}$ el anillo de clases de restos módulo N y por $(\mathbb{Z}/N\mathbb{Z})^*$ su grupo multiplicativo, formado por las clases de enteros a que son primos con N. Al adjuntar al cuerpo de los números racionales $\mathbb{Q}$ las raíces N-ésimas de la unidad, P_N, se obtiene el denominado N-ésimo cuerpo ciclotómico $\mathbb{Q}(\zeta_N)$, cuyo grupo de Galois

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^*$$

es abeliano.

De este modo, para obtener algunos de los cuerpos de números más sencillos, observemos que hemos dividido la circunferencia unidad en N partes iguales, hemos utilizado una función transcendente y ha sido necesario normalizar el intervalo unidad mediante el uso de un número transcendente: π.

En la teoría de la multiplicación compleja se conjugan el álgebra, el análisis y la geometría para lograr una descripción explícita de las extensiones abelianas de los cuerpos de números. En una primera aproximación, esta teoría puede considerarse como una generalización de la trigonometría. Así como la trigonometría está íntimamente ligada a parametrizaciones analíticas de la circunferencia o, más generalmente, de la esfera, la multiplicación compleja se vale de parametrizaciones analíticas de curvas aritméticas o, más generalmente, de variedades aritméticas de dimensión superior (suficientemente simétricas).

Una importante fórmula, debida a C. F. Gauss, expresa las raíces cuadradas de los números primos impares como combinación lineal de raíces de la unidad. Más exactamente,

$$\sqrt{p^*} = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a, \quad p^* := (-1)^{\frac{p-1}{2}} p,$$

en donde $\left(\frac{a}{p}\right) = \pm 1$ denota el símbolo de Legendre. Puesto que $\mathbb{Q}(\sqrt{\pm 2}) \subseteq \mathbb{Q}(\zeta_8)$, se deduce que todas las extensiones cuadráticas del cuerpo racional son ciclotómicas. Es decir, para todo

cuerpo cuadrático $\mathbb{Q}(\sqrt{D})$, existe un entero $N > 1$ tal que

$$\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\zeta_N).$$

A finales del s. XIX, L. Kronecker y H. Weber descubrieron que todas las extensiones abelianas del cuerpo racional son ciclotómicas. En otras palabras, basta con que el grupo de Galois de un polinomio con coeficientes racionales sea conmutativo para que sus raíces sean expresables algebraicamente en función de raíces de la unidad.

En el inicio de su carrera matemática, Kronecker concibió la idea de generar todas las extensiones abelianas K de cuerpos cuadráticos imaginarios $\mathbb{Q}(\sqrt{-D})$, $D > 0$, mediante valores especiales de funciones meromorfas; concretamente, mediate puntos de división de funciones elípticas de módulos singulares.

El denominado *Sueño de Juventud* de Kronecker fue incorporado por D. Hilbert como Problema 12 de su célebre lista de 1900. En un enunciado un tanto impreciso, Hilbert se hizo eco de la afirmación de Kronecker (en aquel momento todavía no probada) sugiriendo encontrar funciones que desempeñaran para *cualquier cuerpo de números* el papel análogo al de la función exponencial, en el caso del cuerpo racional, o al de las funciones modulares elípticas, en el caso de los cuerpos cuadráticos imaginarios.

El estudio del sueño de juventud de Kronecker y del Problema 12 de Hilbert implicó el desarrollo de la teoría de la multiplicación compleja. A lo largo del siglo XX, esta teoría ha conocido formulaciones distintas, cada vez más amplias y sofisticadas. Nuestro propósito es hacer un recorrido histórico por la misma.

La obra de C. F. Gauss *Disquisitiones arithmeticæ*, publicada en latín en 1801, es el compendio de las investigaciones aritméticas realizadas por Gauss durante sus años de aprendizaje en la Universidad de Gotinga. Comprende el desarrollo de tres temas interrelacionados: la demostración de la ley de reciprocidad cuadrática, el estudio de las formas cuadráticas binarias enteras y el de las secciones del círculo. Los tres son básicos para la comprensión del tema que nos ocupa.

1.1. La ley de reciprocidad cuadrática

La ley de reciprocidad cuadrática es un resultado de aritmética modular que surge de manera natural en el tratamiento de las congruencias cuadráticas. Se trata de una ley de carácter global, de muy fácil comprobación numérica.

Dados dos números primos $p \neq q$, distintos de 2, la ley de reciprocidad cuadrática nos dice que el carácter cuadrático de p módulo q queda determinado por el de q módulo p; y que ambos coinciden salvo en el caso en que $p \equiv q \equiv 3$ (mód 4). La ley proporciona un primer aviso de que los números primos no se comportan de manera independiente los unos de los otros.

El descubrimiento de la ley de reciprocidad cuadrática se remonta (al menos) a L. Euler y a A. M. Legendre. Euler la demostró en algunos casos particulares. Legendre intentó su demostración en diversas ocasiones, pero siempre fue consciente de que sus razonamientos eran incompletos. Por ejemplo, Legendre usaba en sus razonamientos primos auxiliares sujetos a determinadas propiedades, cuya existencia podía comprobar pero que no sabía cómo demostrar:

> Remarque. Il serait peut-être nécessaire de démontrer rigoureusement une chose que nous avons supposée dans plusieurs endroits de cet article, savoir, qu'il y a une infinité de nombres premiers compris dans toute progression

> arithmétique, dont le premier terme et la raison sont premiers entr'eux [...] Cette proposition est assez difficile à demontrer, cependant on peut s'assurer qu'elle est vraie.
>
> A. M. Legendre [97].

La formulación más habitual de la ley de reciprocidad cuadrática es la dada mediante el símbolo de Legendre, definido por

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{si } p|a, \\ 1, & \text{si } p \nmid a \text{ y } X^2 = a \text{ tiene solución en } (\mathbb{Z}/p\mathbb{Z})^*, \\ -1, & \text{en los otros casos.} \end{cases}$$

Al utilizar el criterio de Euler para distinguir los cuadrados módulo un entero primo p, se tiene que

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}, \quad \text{para todo } a.$$

Por sus propiedades, podemos interpretar el símbolo de Legendre como un homomorfismo de grupos:

$$\left(\frac{-}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \{\pm 1\}.$$

La ley de reciprocidad cuadrática suele enunciarse con los denominados términos suplementarios, que proporcionan el carácter cuadrático de -1 y de 2 módulo un primo p cualquiera:

LEY DE RECIPROCIDAD CUADRÁTICA. Dados enteros primos p, q, distintos de 2, se satisface que

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

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

En las *Disquisitiones*, Gauss designa la ley de reciprocidad cuadrática con el nombre de teorema fundamental y de él proporciona dos demostraciones. La primera demostración se logra

después de un laborioso proceso de inducción. Para la segunda, Gauss utiliza resultados acerca del género de las formas cuadráticas binarias.

En años posteriores, Gauss proporcionó ocho demostraciones distintas de la ley de reciprocidad; seis de ellas fueron publicadas en vida de su autor; las otras dos se publicaron póstumamente. La obtención por parte de Gauss de distintas demostraciones de la ley de reciprocidad cuadrática obedecía a un propósito concreto: la investigación de la existencia de posibles leyes de reciprocidad de orden superior.

En la actualidad se tienen catalogadas cerca de 200 demostraciones de la ley de reciprocidad cuadrática, lo cual da una idea de su ubicuidad.

En la investigación de posibles leyes de reciprocidad más generales, Gauss se vio conducido a ampliar el anillo de los enteros adjuntando raíces de la unidad. Trabajó con $\mathbb{Z}[i] = \mathbb{Z}[\zeta_4]$, el llamado anillo de los enteros de Gauss, y con $\mathbb{Z}[\rho] = \mathbb{Z}[\zeta_3]$, denominado posteriormente el anillo de los enteros de Eisenstein.

1.2. Formas cuadráticas binarias

El núcleo central de las *Disquisitiones arithmeticæ* de Gauss está constituido por la sección quinta, dedicada al estudio de las formas binarias de segundo grado con coeficientes enteros. Gauss era conocedor de los resultados de P. de Fermat y de Euler sobre la caracterización de los enteros expresables como suma de dos cuadrados; o sea, de los enteros n para los cuales las ecuaciones $X^2+Y^2 = n$ poseen soluciones enteras. En la citada obra, Gauss emprende de una manera general el estudio de las ecuaciones

$$aX^2 + bXY + cY^2 = n,$$

en donde a, b, c, n son enteros arbitrarios. (Gauss supone que el término central, b, es siempre un número par.) Representamos

estas formas por (a, b, c) y denominaremos a $D := b^2 - 4ac$ su discriminante. El estudio de los dos cuadrados corresponde pues al caso de la forma $(1, 0, 1)$, de discriminante $D = -4$.

A lo largo de más de 300 páginas, Gauss elabora un estudio muy personal acerca de la caracterización de los enteros n representables por una forma dada (a, b, c) y la determinación, en tal caso, de sus representaciones.

Gauss empieza por clasificar las formas cuadráticas anteriores por medio de cambios de variable lineales con coeficientes enteros. En nuestro lenguaje actual, los cambios de variable obedecen a la acción del grupo modular (o especial lineal) $\mathbf{SL}(2, \mathbb{Z})$, en el caso de la denominada equivalencia propia, o a la del grupo lineal $\mathbf{GL}(2, \mathbb{Z})$, en el caso general. Con ello, D o $\pm D$ es un invariante de cada clase de formas.

En las consideraciones siguientes, nos centraremos en el caso de la equivalencia propia de formas y denotaremos por $H(D)$ el conjunto de las clases de formas de discriminante D. Denotaremos por $h(D) := \#H(D)$ el número de clases de formas de discriminante D.

Gauss procede a elegir representantes sencillos en cada clase de formas, a los que denomina formas reducidas. La reducción de formas es muy diferente según se trate de formas definidas o indefinidas. En los casos definidos ($a > 0, D < 0$; o bien $a < 0, D < 0$), cada clase de formas posee un único representante reducido. Una manera de elegir el representante es imponiendo que el cero de la ecuación $aX^2 + bX + c = 0$ con parte imaginaria positiva esté situado en el dominio $\mathcal{F}(\mathbf{SL}(2, \mathbb{Z}))$ de la figura 1.1. En el caso indefinido ($D > 0$), los representantes reducidos de una misma clase no son necesariamente únicos y constituyen un ciclo. En ambos casos, $h(D)$ es finito.

Puesto que la forma $(1, 0, 1)$ es la única forma reducida de discriminante -4, se tiene que $h(-4) = 1$.

A partir de las definiciones, resulta evidente que formas equi-

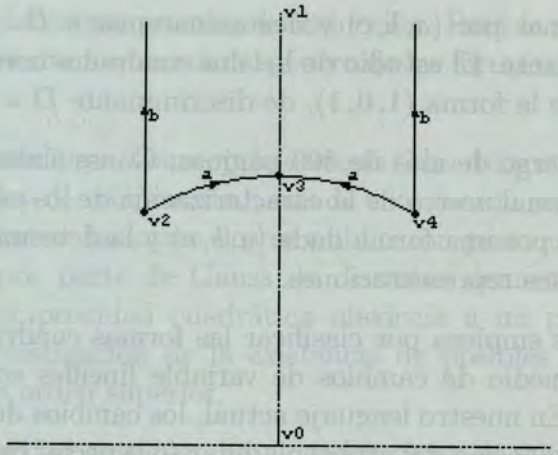

Figura 1.1: Dominio fundamental $\mathcal{F}(\mathbf{SL}(2,\mathbb{Z}))$

valentes representan los mismos números enteros. Gauss resuelve el problema de la representabilidad de enteros por formas del modo siguiente: dados un entero n y un discriminante D, Gauss obtiene un criterio que le permite decidir si n es representado por alguna de las clases de formas de discriminante D (a priori, no se sabe por cual). En particular, y puesto que $h(-4) = 1$, recupera teoremas de Fermat y de Euler acerca de la caracterización de los enteros expresables como suma de dos cuadrados.

A su vez, Gauss agrupa las clases de formas de un discriminante dado en órdenes y en géneros. [1] Los órdenes están formados por clases de formas del mismo discriminante que poseen el mismo máximo común divisor de sus coeficientes; cuando éste es igual a 1, las formas y el orden se denominan primitivos.

Un discriminante D se denomina fundamental si $D \equiv 1$ (mód 4) y D es libre de cuadrados, o bien si $D \equiv 0$ (mód 4), $D/4$ es libre de cuadrados y $D/4 \equiv 2, 3$ (mód 4). En este caso,

[1] Esta clasificación evoca la del naturalista Carl von Linné (1707-1778), que había aplicado las categorías aristotélicas a la clasificación de los seres vivos, distribuyéndolos en clases, órdenes, géneros y especies.

todas las formas de $H(D)$ son necesariamente primitivas.

La noción de género de formas surge en Gauss al observar que existen formas no equivalentes del mismo discriminante que representan los mismos números enteros. Ello le lleva a agrupar en géneros las clases de formas de $H(D)$ que representan los mismos enteros. Gauss consigue caracterizar los distintos géneros por medio de ciertos signos, denominados caracteres.

Gauss considera una composición de formas, que hace extensiva a una composición de clases, de órdenes y de géneros. Esta composición debe comportarse adecuadamente con respecto a la representabilidad de enteros y a su producto. En términos actuales, la composición de clases define en $H(D)$ una estructura de grupo abeliano, finito. El grupo cociente $H(D)/H(D)^2$ se corresponde con el grupo de géneros y los caracteres de Gauss son homomorfismos $\chi : H(D)/H(D)^2 \to \{\pm 1\}$.

En la misma sección quinta, Gauss inicia un estudio de las formas cuadráticas ternarias enteras con el fin de obtener información adicional sobre las formas cuadráticas binarias. Considera el problema de la representabilidad de formas cuadráticas binarias por ternarias como complementario al de la representabilidad de enteros por formas. En particular, al representar formas binarias por la ternaria especial $Y^2 - 2XZ$, Gauss consigue demostrar la existencia de géneros para exactamente la mitad de los caracteres totales asociados a un discriminante dado. Demuestra asimismo que todos los géneros de un orden dado contienen el mismo número de clases y calcula el número de clases ambiguas (elementos de orden dos) en $H(D)$. Si D es un discriminante fundamental, el número de géneros de $H(D)$ es igual a 2^{t-1}, siendo t el número de primos distintos que dividen a D; en particular, el número de clases $h(D)$ es siempre divisible por 2^{t-1}.

1.3. Las secciones del círculo

La sección séptima de las *Disquisitiones* está dedicada al estudio de las raíces de la unidad. A través de la determinación previa de los períodos de las ecuaciones ciclotómicas, Gauss caracteriza los polígonos regulares de N lados que pueden construirse con regla y compás, cerrando así un problema que permanecía abierto desde la matemática griega, tal y como él pone de manifiesto.

Gauss obtiene que la división de la circunferencia con regla y compás en N partes iguales es posible únicamente si la descomposición de N en factores primos es igual a una potencia de 2 por el producto de primos, dos a dos distintos, de la forma $F_r = 1 + 2^{2^r}$. Los primos de esta forma se denominan primos de Fermat; de ellos, únicamente se conocen cinco: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ y $F_4 = 65537$. La clave del resultado anterior se encuentra en la demostración de que, dado un primo p, las raíces $2^m p$-ésimas de la unidad, $m \geq 0$, son expresables mediante radicales cuadráticos si, y solamente si, p es un primo de Fermat. Por ejemplo,

$$\zeta_3 = \frac{1}{2}(-1 + i\sqrt{3}),$$

$$\zeta_4 = \sqrt{-1},$$

$$\zeta_5 = \frac{1}{4}(-1 + \sqrt{5}) + i\sqrt{\frac{5 + \sqrt{5}}{8}},$$

$$\zeta_6 = \frac{1}{2}(1 + i\sqrt{3}),$$

$$\frac{1}{2}(\zeta_{17} + \zeta_{17}^{-1}) = \cos\frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} +$$

$$\frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

En el tratamiento dado por Gauss a las secciones del círculo encontramos el primer ejemplo explícito de una correspondencia de Galois. Expresado en términos actuales, Gauss demuestra que el grupo de Galois del p-ésimo cuerpo ciclotómico $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, para p primo, es un grupo abeliano finito, isomorfo al grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$, del cual determina todos sus subgrupos. El cálculo de los períodos de las ecuaciones ciclotómicas le permite hacer explícitos los subcuerpos del cuerpo ciclotómico que son invariantes por la acción de los correspondientes subgrupos. Esta metodología estaba llamada a ejercer una enorme influencia en N. Abel y en E. Galois.

En la sección séptima del mismo tratado, Gauss formula un hermético comentario concerniente a que su teoría no sólo es válida para las funciones circulares seno y coseno, sino que también es aplicable a muchas otras funciones transcendentes como, por ejemplo, a las que dependen de cierta integral:

> Ceterum principia theoriae, quam exponere aggredimur, multo latius patent, quam hic extenduntur. Namque non-solum ad functiones circulares, sed pari successu ad multas alias functiones transscendentes applicari possunt, e. g. ad eas quae ab integrali $\int \frac{dx}{\sqrt{(1-x^4)}}$ pendent.
>
> C. F. Gauss [63].

La integral a la que Gauss hace referencia en la cita anterior surge del estudio de la rectificación de la lemniscata. Es probable que Gauss estuviera familiarizado con esta curva a través de la lectura de Euler. De hecho, a los 19 años, Gauss ya se había preguntado cómo, a partir de un arco de lemniscata de longitud s, se podía calcular la distancia del extremo del arco al origen de coordenadas $r = 0$. La respuesta a tal pregunta conduce al estudio de la función $r = \mathrm{sl}(s)$, definida por inversión de la integral

$$s(r) = \int_0^r \frac{d\rho}{\sqrt{1-\rho^4}}.$$

Gauss dio a esta función el nombre de seno lemniscático. A su vez, el seno lemniscático da lugar a un coseno lemniscático, definido por

$$\mathrm{cl}(s) = \mathrm{sl}(\varpi - s),$$

en donde ϖ es igual a la longitud de un semióvalo de la lemniscata; es decir

$$\varpi = \int_0^1 \frac{d\rho}{\sqrt{1-\rho^4}} \approx 1,31103.$$

Naturalmente, esta notación se introduce por analogía con las expresiones

$$s(r) = \int_0^r \frac{d\rho}{\sqrt{1-\rho^2}},$$

en las que

$$r = \sin(s), \quad \int_0^1 \frac{d\rho}{\sqrt{1-\rho^2}} = \frac{\pi}{2}.$$

Gauss conocía además la doble periodicidad del seno lemniscático:

$$\mathrm{sl}(s + 4\varpi) = \mathrm{sl}(s), \quad \mathrm{sl}(s + 4i\varpi) = \mathrm{sl}(s).$$

El hermético comentario de Gauss al que hemos aludido favoreció el descubrimiento de la doble periodicidad y estimuló el estudio de las funciones elípticas.

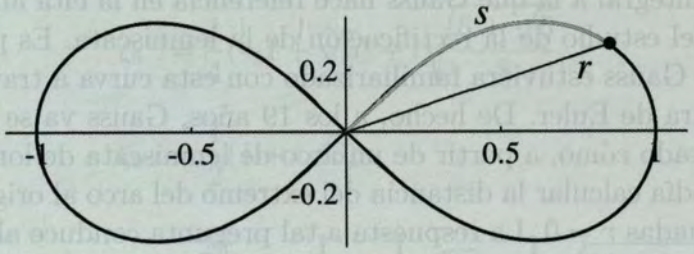

Figura 1.2: Arco de lemniscata como función del seno lemniscático

1.4. ¿Dividir o multiplicar?

Además de las mencionadas hasta aquí, las contribuciones de Gauss a la aritmética se difundieron en forma de artículos publicados, de notas en su diario, o bien como esbozos encontrados en sus papeles y publicados con carácter póstumo en el *Nachlass*. Nos limitaremos a comentar los avances que hizo Gauss en relación con el problema de la división de la lemniscata y en el tema de contar el número de soluciones de una ecuación de congruencias.

Si pensamos, por ejemplo, en la imposibilidad de la trisección del ángulo con regla y compás, vemos que ésta se debe al hecho siguiente. La igualdad

$$\cos(3u) = 4\cos^3(u) - 3\cos(u),$$

que se deduce de fórmulas elementales de la trigonometría, nos dice que, construido un ángulo tal que $\cos(v) = d$, el $\cos(v/3)$ será una raíz de la ecuación

$$4X^3 - 3X - d = 0.$$

En general, en la expresión de las raíces de esta ecuación intervendrán radicales cúbicos, por lo que el ángulo $v/3$ no será construible con regla y compás.

Como curiosidad, observemos que la ecuación de la trisección del ángulo se simplifica por reducción módulo 3:

$$\cos^3(u) \equiv \cos(3u) \pmod 3.$$

Vemos, pues, que el estudio del problema de la división de los ángulos u en N partes iguales nos conduce a la determinación de las funciones trigonométricas de sus múltiplos, Nu, requiriendo fórmulas que expresen las funciones trigonométricas de Nu en función de las de u.

En la entrada 62 (1797) de su Diario matemático (*Mathematisches Tagebuch*), Gauss escribió que la lemniscata es divisible

geométricamente en cinco partes. Cuando Gauss sugiere en las *Disquisitiones* el problema de la división de la lemniscata como análogo al de la división de la circunferencia, resulta evidente que está pensando en una parametrización analítica de esta curva. Por notas encontradas en sus papeles póstumos, se sabe que Gauss era conocedor de que el problema de la división por N de los arcos de lemniscata conduce a ecuaciones de grado N^2. En particular, Gauss estudió las ecuaciones de la división por 5 de la lemniscata de una manera sorprendente. Para dividir un arco de lemniscata en 5 partes iguales usó la igualdad

$$(2+i)(2-i) = 5,$$

dividiendo los arcos primero por $2+i$ y, a continuación, por $2-i$. Notemos que Gauss trabaja en el anillo $\mathbb{Z}[i]$ y descompone el 5 como producto de elementos primos de este anillo. Además, se sirve de que la lemniscata admite *multiplicaciones complejas* por $\mathbb{Z}[i]$. El estudio de la lemniscata y de los fenómenos de multiplicación compleja con ella relacionados fue emprendido por Abel, quien quedó fascinado por el intrigante comentario de Gauss en las *Disquisitiones* al que hemos aludido.

En la entrada 144 (1813) de su diario, Gauss apunta que, tras siete años del máximo esfuerzo (y precisamente el día en que nacía su hijo), ha descubierto los fundamentos de la teoría de los residuos bicuadráticos. Como veremos, esta teoría hace también referencia a propiedades de divisibilidad del anillo $\mathbb{Z}[i]$. Los problemas que surgieron en esta dirección fueron trabajados por F. Eisenstein.

No menos importante para el desarrollo del tema que nos concierne es la última entrada del diario de Gauss, 146 (1814), en la que su autor da cuenta de la observación de un importante hecho que conecta elegantemente la teoría de los residuos bicuadráticos con las funciones lemniscáticas. Gauss dice que si $a+bi$ es un número primo para el cual $a-1+bi$ es divisible por $2+2i$, entonces el número de soluciones de la congruencia

$$1 \equiv x^2 + y^2 + x^2y^2 \pmod{a+bi},$$

incluyendo las dadas por $x = \infty$, $y = \pm i$ e $y = \infty$, es igual a $(a-1)^2 + b^2$.

Bajo puntos de vista complementarios, la afirmación anterior sería trabajada por Eisenstein, Artin, Hasse, Deuring y Weil, entre otros, y se considera uno de los puntos de partida del estudio de las funciones zeta de las variedades algebraicas definidas sobre cuerpos finitos. Si denotamos por N_p el número de soluciones de la congruencia

$$1 \equiv x^2 + y^2 + x^2 y^2 \pmod{p},$$

y tenemos presente el resultado de Gauss, obtenemos que

$$|p + 1 - N_p| = |a^b + b^2 + 1 - (a-1)^2 - b^2| = |2a|,$$

lo cual, unido a la desigualdad evidente,

$$2|a| < 2\sqrt{a^2 + b^2} = 2\sqrt{p},$$

proporciona la desigualdad $|p + 1 - N_p| < 2\sqrt{p}$. Como veremos más adelante, éste es un caso particular de un teorema probado por H. Hasse en 1934.

A modo de resumen, podemos decir que las investigaciones de Gauss en aritmética marcaron el inicio de dos técnicas básicas para el conocimiento de los números enteros: el uso de números algebraicos, por un lado, y el uso de funciones especiales, por otro.

1.5. Cuerpos de números

Un cuerpo de números algebraicos es, por definición, un cuerpo K de característica cero que es a su vez un espacio vectorial de dimensión finita sobre el cuerpo $\mathbb{Q}$ de los números racionales. Los cuerpos de números más sencillos, aparte del propio cuerpo racional, son los cuerpos cuadráticos $\mathbb{Q}(\sqrt{D})$, que se obtienen al

adjuntar a $\mathbb{Q}$ la raíz cuadrada de un número racional no cuadrado, y los cuerpos ciclotómicos $\mathbb{Q}(\zeta_N)$, que se obtienen al adjuntar a $\mathbb{Q}$ las raíces N-ésimas de la unidad.

En general, el grado $n = [K : \mathbb{Q}]$ de un cuerpo de números es igual a r_1+2r_2, siendo r_1 el número de inmersiones reales $K \hookrightarrow \mathbb{R}$ y $r_2 : K \hookrightarrow \mathbb{C}$ el número de elementos de un sistema maximal de inmersiones complejas no reales y no conjugadas. Si $n = r_1$, el cuerpo K se denomina totalmente real; si $n = 2r_2$, se dice que K es un cuerpo totalmente imaginario. Avancemos que un cuerpo de números se denomina un cuerpo con multiplicación compleja, o de tipo MC, si es una extensión totalmente imaginaria de una extensión totalmente real. Por ejemplo, los cuerpos cuadráticos imaginarios $\mathbb{Q}(\sqrt{D})$, $D < 0$, y los cuerpos ciclotómicos $\mathbb{Q}(\zeta_N)$, $N > 1$, son de tipo MC.

Capítulo 2

Funciones elípticas y aritmética

2.1. Los orígenes

En sus intentos por rectificar la elipse, J. Wallis había obtenido en 1656 que si la elipse se parametriza en la forma

$$x = a\cos\theta, \quad y = b\sin\theta, \quad a > b,$$

la longitud de uno de sus arcos se computa por medio de la integral

$$\int_{s_0}^{s_1} ds = \int_{\theta_0}^{\theta_1} \sqrt{a^2\sin^2\theta + b^2\cos^2\theta}\, d\theta$$

$$= a\int_{\theta_0}^{\theta_1} \sqrt{1 - e^2\cos^2\theta}\, d\theta,$$

en donde $1 - b^2/a^2 = e^2$ es el cuadrado de su excentricidad. Sin embargo, no podía expresar esta integral con las funciones habituales de la época.

La curva lemniscata, que es un caso particular de los llamados

óvalos de Cassini, [1] puede describirse como el lugar de un punto del plano que se mueve manteniendo constante el producto de su distancia a dos puntos fijos dados de antemano. Su ecuación en coordenadas cartesianas es

$$(x^2 + y^2)^2 = a^2(x^2 - y^2);$$

y, en coordenadas polares, $r^2 = a^2 \cos(2s)$. Recibe su nombre de la palabra griega *lemniskos*, empleada para designar las cintas que pendían de las coronas.

Los matemáticos de la familia Bernoulli se dedicaron al estudio de la lemniscata. En 1694, Jacob Bernoulli había aludido a esta curva en su *Acta Eruditorum*. John Bernoulli intentó su rectificación, lo cual le condujo al estudio de la integral

$$s(r) = \int_0^r \frac{d\rho}{\sqrt{a^2 - \rho^4}}.$$

Notemos que

$$\varpi := \int_0^1 \frac{d\rho}{\sqrt{1 - \rho^4}} = 1 + \sum_{n=1}^{\infty} \frac{1 \cdot 3 \cdot 5 \ldots (2n-1)}{2^n \, n! \, (4n+1)}.$$

En 1751, y con motivo de haber sido nombrado miembro de la Academia de Berlín, el conde G. Fagnano sometió a aquella institución la obra titulada *Produzioni matematiche*, un tratado en dos volúmenes dedicado primordialmente al cálculo integral. Dos días antes de la Navidad de 1751, Euler recibió los dos volúmenes de Fagnano para su examen. Euler, que por aquel entonces poseía un gran número de responsabilidades en la academia, quedó especialmente intrigado por los resultados de Fagnano relativos a la adición de arcos de elipse y a la trisección de arcos de lemniscata.

[1] Estudiados por G. Cassini en 1680, en su tratamiento del movimiento relativo de la Tierra y el Sol.

Entre las numerosas fórmulas descubiertas por Fagnano, merece especial atención la siguiente. Si

$$z = \frac{(1+i)w}{\sqrt{1-w^4}},$$

entonces

$$\int_0^z \frac{dz}{\sqrt{1-z^4}} = (1+i)\int_0^w \frac{dw}{\sqrt{1-w^4}}.$$

Haciendo $w = \mathrm{sl}(s)$, la fórmula de Fagnano proporciona un primer ejemplo relativo a una multiplicación compleja, en tanto que permite expresar el seno lemniscático de $(1+i)s$ algebraicamente en función del seno lemniscático de s:

$$\mathrm{sl}\,((1+i)s) = \frac{(1+i)\,\mathrm{sl}\,(s)}{\sqrt{1-\mathrm{sl}^4(s)}}.$$

2.1.1. Integrales elípticas

C. G. J. Jacobi situó la fecha del nacimiento de las funciones elípticas en el 23 de diciembre de 1751, es decir, en el día en que Euler recibió la obra de Fagnano. En la sesión de la Academia del 27 de enero de 1752, celebrada al cabo de pocas semanas de haber recibido los trabajos de Fagnano, Euler expuso su trabajo sobre la comparación de los arcos de curva no rectificables. Euler demostró una serie de teoremas sobre arcos de elipse, de hipérbola y de lemniscata, cuyas coordenadas son la suma o la diferencia de una función algebraica; y sobre arcos que son múltiplos los unos de los otros. Euler afirmó, sin demostración, que la lemniscata puede ser dividida en k partes iguales (mediante el uso de la regla y del compás) si k es de la forma $2^n(1+2^m)$. Como veremos, esta afirmación de Euler no es del todo correcta. Posteriormente, Euler dedicaría a este tema numerosas publicaciones que se encuentran recogidas en diversos volúmenes de su *Opera Omnia* y de su *Opera postuma.* [2]

[2]Se ha señalado que el interés de Euler por los trabajos de Fagnano podría muy bien ser debido a que, en aquella época, Euler estaba inmerso

En la terminología clásica, una integral elíptica es una integral de la forma

$$\int_c^x R(t, P(t))dt,$$

en donde R es una función racional de dos variables, $P(t)$ es la raíz cuadrada de un polinomio de grado 3 o 4 sin raíces múltiples, y c, una constante.

Las investigaciones de Legendre sobre las integrales elípticas abarcaron un período de más de 40 años. Sus resultados sobre el tema aparecieron publicados en tres volúmenes bajo el nombre de *Exercices du Calcul Intégral* (1811, 1817, 1819); el tercer volumen contenía numerosas tablas. Legendre preparó una segunda edición bajo el nombre *Traité des Fonctions Elliptiques*, reorganizada respecto de la anterior y de nuevo en tres volúmenes (1821, 1826, 1830). [3] Legendre redujo las integrales elípticas a tres formas canónicas, llamadas de primera, de segunda y de

---

en el estudio de integrales relacionadas con problemas de elasticidad.

[3]Legendre aplicó las integrales elípticas al estudio de la rotación de la Tierra, a la determinación de la atracción ejercida por un elipsoide, y a la resolución de múltiples problemas de mecánica. En 1787, Legendre formó parte del equipo de científicos franceses que, juntamente con miembros del Real Observatorio de Greenwich, se encargarían de establecer la medida de la Tierra mediante una serie de triangulaciones efectuadas entre los Observatorios de París y de Greenwich. En 1791, Legendre formó parte del comité de la *Académie des Sciences* de París encargado de estandarizar el sistema de pesas y medidas. Este comité trabajó en la implantación del sistema métrico decimal y en las triangulaciones y observaciones astronómicas que condujeron al cálculo de la longitud de un grado de meridiano terrestre, cuyo objetivo principal era contrastar las diversas teorías propuestas acerca de la forma de la Tierra. En 1792, Legendre, Gaspard de Prony y Lazare Carnot lideraron un proyecto para la confección de extensas tablas logarítmicas y trigonométricas, calculadas entre 14 y 29 decimales; se dice que para su realización contaron con el concurso de unos 80 ayudantes. El proyecto fue acabado en 1801, pero las tablas no pudieron publicarse íntegramente debido a su enorme extensión. Debemos tener presente, además, que estos sucesos acaecían en los turbulentos años la Revolución Francesa (1789-1799).

tercera especie, respectivamente:

$$F(\varphi, k) = \int_0^{\varphi} \frac{d\theta}{\sqrt{1 - k^2 \sin^2 \theta}},$$

$$E(\varphi, k) = \int_0^{\varphi} \sqrt{1 - k^2 \sin^2 \theta}\, d\theta,$$

$$P(\varphi, k, n) = \int_0^{\varphi} \frac{d\theta}{\left(1 + n \sin^2 \theta\right) \sqrt{1 - k^2 \sin^2 \theta}}.$$

Según Legendre, φ es la amplitud de la integral; k, su módulo; y n, en el caso de la integral de tercera especie, su parámetro. Cuando la amplitud es igual a $\pi/2$, habla de integral completa.

El valor de la integral completa de primera especie fue obtenido por Gauss como resultado de sus investigaciones acerca de la media aritmético geométrica y de las series hipergeométricas:

$$K(k) = F\left(\frac{\pi}{2}, k\right) = \int_0^{\pi/2} \frac{1}{\sqrt{1 - k^2 \sin^2 \theta}}\, d\theta$$

$$= \frac{\pi}{2} \sum_{n=0}^{\infty} \left[\frac{(2n-1)!!}{(2n)!!}\right]^2 k^{2n}.$$

El valor de la integral completa de segunda especie se calcula de manera análoga:

$$E(k) = E\left(\frac{\pi}{2}, k\right) = \int_0^{\pi/2} \sqrt{1 - k^2 \sin^2 \theta}\, d\theta$$

$$= \frac{\pi}{2} \left(1 - \sum_{n=0}^{\infty} \left[\frac{(2n-1)!!}{(2n)!!}\right]^2 \frac{k^{2n}}{2n-1}\right),$$

en donde $0 < k < 1$.

La integral elíptica de primera especie aparece en el cálculo del período del péndulo. Legendre demostró que, como función

del módulo, esta integral satisface la ecuación diferencial de segundo orden:

$$k(k^2-1)\frac{d^2F}{dk^2}+(3k^2-1)\frac{dF}{dk}+kF=0.$$

La integral elíptica de segunda especie proporciona la longitud de un arco de elipse de excentricidad igual al módulo. A su vez, Euler conocía que dicha integral satisface la ecuación diferencial de segundo orden:

$$k(k^2-1)\frac{d^2E}{dk^2}+(k^2-1)\frac{dE}{dk}-kE=0.$$

Según Abel, la primera idea relativa a las funciones elípticas se debe a Euler, quien demostró que la ecuación diferencial de variables separadas

$$\frac{dx}{\sqrt{\alpha+\beta x+\gamma x^2+\delta x^3+\epsilon x^4}}=-\frac{dy}{\sqrt{\alpha+\beta y+\gamma y^2+\delta y^3+\epsilon y^4}}$$

podía ser integrada algebraicamente. En sus dos memorias sobre las funciones elípticas, de 1827 y 1828, Abel escribe las integrales elípticas de primera especie en la forma

$$\alpha=\int_0^x\frac{dx}{\sqrt{(1-c^2x^2)(1+e^2x^2)}}.$$

Por inversión de las mismas obtiene las funciones

$$\varphi(\alpha;c,e)=x,$$

a las que asocia dos funciones más de α:

$$f(\alpha;c)=\sqrt{1-c^2\varphi^2(\alpha)},\quad F(\alpha;e)=\sqrt{1+e^2\varphi^2(\alpha)}.$$

Demuestra que φ es una función doblemente periódica y que los valores de φ obtenidos por multiplicación y división por números enteros de los argumentos,

$$\varphi(N\alpha),\quad \varphi(\frac{\alpha}{N}),$$

se expresan algebraicamente en función de $\varphi(\alpha)$. Abel reduce la resolución de la ecuación de división $P_N = 0$, en principio de grado N^2, a la resolución de una ecuación de grado $N + 1$. Abel hace notar que esta ecuación no parece en general ser resoluble algebraicamente (es decir, por radicales, de acuerdo con la terminología actual). Sin embargo, prosigue, se puede resolver en muchos casos particulares, por ejemplo cuando $e = c$, $e = c\sqrt{3}$, $e = c(2 \pm \sqrt{3})$, etc.

Al estudiar el caso $e = c = 1$, Abel obtiene el notable resultado por el cual la lemniscata es divisible en N partes mediante la regla y el compás si N es el producto de una eventual potencia de 2 por primos distintos de Fermat. Es decir, Abel obtiene los mismos valores que en su día obtuvo Gauss para la división de la circunferencia.

En su estudio de las relaciones más generales entre un número arbitrario de funciones elípticas, Abel debe caracterizar los casos en que la ecuación diferencial de variables separadas puede ser integrada algebraicamente:

$$\frac{dy}{\sqrt{(1-y^2)(1+\mu y^2)}} = a\,\frac{dx}{\sqrt{(1-x^2)(1+\mu x^2)}}.$$

En el supuesto de que el multiplicador a sea un número real, descubre entonces que a debe ser un número racional. En el supuesto de que a sea imaginario no real, entonces a debe ser un irracional cuadrático $a = m + i\sqrt{n}$, $m, n \in \mathbb{Q}$, estando en este caso el módulo μ sujeto a restricciones.

2.1.2. Funciones theta de Jacobi

Poco tiempo después de la publicación del monumental tratado de Legendre sobre las integrales elípticas, Jacobi comunicaba a aquel sus resultados acerca de la multiplicación de estas integrales. Jacobi comparaba integrales elípticas asociadas tanto al mismo módulo como a módulos distintos. Transcribimos a con-

tinuación un fragmento de la primera carta escrita por Jacobi a Legendre. [4]

> Señor,
> Un joven geómetra se atreve a presentaros algunos descubrimientos realizados en la teoría de las funciones elípticas, a los cuales ha sido conducido por el asiduo estudio de vuestros bellos escritos. [...] se encuentra así el notable resultado por el cual *cada módulo dado forma parte de una infinidad de escalas de módulos en los que puede ser transformado mediante una sustitución algebraica y, de hecho, racional.*
>
> Dr. C. J. Jacobi, 5 de agosto de 1827 [81].

En una segunda carta, Jacobi informó a Legendre de los trabajos de Abel sobre el mismo tema:

> Señor,
> Después de mi última carta, han sido publicadas investigaciones de la mayor importancia sobre las funciones elípticas por parte de un joven geómetra, que puede que conozcáis personalmente. Se trata de la primera parte de una memoria del Sr. Abel, en Christiana, que me ha dicho haber estado en París hace dos o tres años, y que ha sido insertada en el número dos del segundo volumen del *Journal für die reine und angewandte Mathematik* (*Journal de Mathématiques pures et appliquées*), publicada en Berlín por el Sr. Crelle.
>
> Dr. C. J. Jacobi, 29 de noviembre de 1827 [81].

A continuación, Jacobi explica a Legendre los resultados de Abel utilizando su propia notación. En particular, describe una

[4] Debe tenerse en cuenta que los clásicos denominaban funciones elípticas a lo que nosotros llamamos integrales elípticas. Las funciones elípticas de la actualidad se obtienen por inversión de estas integrales.

serie de fórmulas de las que deduce la doble periodicidad. Por inversión de la integral elíptica de primera especie

$$(u \mid k)(\theta) = \int_0^\theta \frac{d\varphi}{\sqrt{1 - k^2 \sin^2 \varphi}},$$

define $(\theta \mid k) = \operatorname{am}(u \mid k)$, y demuestra la doble periodicidad de la función $\sin \operatorname{am}(u \mid k)$:

$$\sin \operatorname{am}(u + 4mK + 2m'iK' \mid k) = \sin \operatorname{am}(u \mid k),$$

siendo $K = K(k), K' = K'(k) = K(k'), k^2 + k'^2 = 1$.

Jacobi pone de manifiesto que las raíces de la ecuación de grado N^2 que proporciona la división de la integral elíptica u en N partes iguales son de la forma

$$\sin \operatorname{am}\left(\frac{u + 4mK + 2m'iK'}{N} \mid k\right), \quad 0 \leq m, m' \leq N - 1.$$

Jacobi comunica asimismo a Legendre que ciertas integrales elípticas admiten multiplicaciones por números complejos $a \pm bi$ de una cierta forma. Advierte que ello ocurre, por ejemplo, para todos los módulos que están ligados por una escala cualquiera con $k = \frac{1}{\sqrt{2}}$, y añade que es un tipo de multiplicación que no tiene análogo en el caso de los arcos del círculo.

Legendre, Jacobi y Abel, que estaban totalmente familiarizados con el tratado de Euler *Introductio in analysin infinitorum*, en el que se consideran las fórmulas de adición, de multiplicación y de división de las funciones circulares, se dieron cuenta enseguida de que estaban ante una nueva teoría que presentaba notables semejanzas, a la vez que notables diferencias, con la teoría de las funciones circulares. Así, mientras que $\sin(iu) = \sinh(u)$, $\cos(iu) = \cosh(u)$, se tiene que

$$\operatorname{sl}(iu) = i \operatorname{sl}(u), \quad \operatorname{cl}(iu) = 1/\operatorname{cl}(u).$$

Ch. Gudermann, uno de los primeros matemáticos que impartieron lecciones sobre funciones elípticas, simplificó algo la notación utilizada por Jacobi, introduciendo las funciones sn, cn, dn

(leídas *san, can, dan*), dadas por

$$\begin{aligned} \operatorname{sn}(u \mid k) &= \sin \operatorname{am}(u \mid k), \\ \operatorname{cn}(u \mid k) &= \cos \operatorname{am}(u \mid k), \\ \operatorname{dn}(u \mid k) &= \Delta \operatorname{am}(u \mid k) = \sqrt{1 - k^2 \sin^2 \operatorname{am}(u \mid k)}. \end{aligned}$$

En particular, se tiene que

$$(u \mid k) = \int_0^{\theta} \frac{d\varphi}{\sqrt{1 - k^2 \sin^2 \varphi}} = \int_0^{\operatorname{sn}(u|k)} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}.$$

Gudermann se había doctorado en 1841 en la Georg-August-Universität de Göttingen, bajo la dirección de Gauss, con una memoria de tesis titulada *Über die Entwicklung der Modularfunctionen.* A su vez, fue el director de tesis de K. Weierstrass.

Otra de las aportaciones de Jacobi, que no debemos omitir, es su expresión de las funciones elípticas como cocientes de funciones theta.

Las funciones theta habían sido ya utilizadas por matemáticos franceses. Por una parte, por J-B. Fourier, en su estudio de la ecuación del calor; por otra, en la tesis de L. Bachelier, publicada en 1900 y reconocida hoy como un antecedente de la matemática financiera.

Se define la función theta básica como

$$\theta(z, \tau) := \sum_{n \in \mathbb{Z}} e^{2\pi i n z + \pi i n^2 \tau},$$

en donde $z, \tau \in \mathbb{C}$ y $\Im(\tau) > 0$. Se trata de una función semiperiódica por cuanto que

$$\theta(z+1, \tau) = \theta(z, \tau), \qquad \theta(z+\tau, \tau) = e^{-\pi i \tau - 2\pi i z} \theta(z, \tau).$$

Las funciones theta de Jacobi con características son funciones analíticas en dos variables que se definen a partir de la función theta básica:

$$\theta_{a,b}(z, \tau) := e^{\pi i a^2 \tau + 2\pi i a(z+b)} \theta(z + b + a\tau, \tau), \quad a, b \in \mathbb{Q}.$$

Las funciones

$$\theta_1 = \theta_{\frac{1}{2},\frac{1}{2}}, \quad \theta_2 = \theta_{\frac{1}{2},0}, \quad \theta_3 = \theta_{0,0} = \theta, \quad \theta_4 = \theta_{0,\frac{1}{2}}$$

son las denominadas funciones theta de Jacobi. En particular se tiene que $\theta_3 = \theta$.

Al tener en cuenta los ceros y los polos de las funciones sn, cn, dn, Jacobi obtiene expresiones para las mismas en forma de cocientes de funciones theta:

$$\mathrm{sn}(u \mid k) = \frac{\theta_3(0)}{\theta_2(0)} \cdot \frac{\theta_1(z)}{\theta_4(z)}, \quad \mathrm{cn}(u \mid k) = \frac{\theta_4(0)}{\theta_2(0)} \cdot \frac{\theta_2(z)}{\theta_4(z)},$$

$$\mathrm{dn}(u \mid k) = \frac{\theta_4(0)}{\theta_3(0)} \cdot \frac{\theta_3(z)}{\theta_4(z)},$$

en donde

$$z = \frac{u}{\pi\theta_3^2(0)}, \quad k^2 = \frac{\theta_2^4(0)}{\theta_3^4(0)}, \quad \theta_i(z) = \theta_i(z, \tau),$$

para $\tau = iK'/K$, siendo $4K$, $2iK'$ los períodos de la función $\mathrm{sn}(u \mid k)$.

A lo largo del siglo XIX y buena parte del XX, las funciones theta de Jacobi y sus generalizaciones dieron lugar a una extensa literatura.

2.1.3. Cuerpos de funciones elípticas

Las funciones meromorfas doblemente periódicas pasaron a denominarse funciones elípticas. Sea $\Lambda = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$ un $\mathbb{Z}$-módulo libre de rango 2, $\lambda_i \in \mathbb{C}$; denotaremos por $\Lambda' = \Lambda \setminus \{(0,0)\}$. El conjunto de todas las funciones elípticas de retículo de períodos Λ constituye un cuerpo, que denotamos por $\mathbb{C}(\Lambda)$.

Weierstrass construyó la función elíptica que lleva su nombre como solución de la ecuación diferencial

$$\left(\frac{d\wp}{du}\right)^2 = 4\wp^3 - g_2\wp - g_3, \quad \Delta := g_2^3 - 27g_3^2 \neq 0,$$

con un polo en $u = 0$. Las funciones de Weierstrass:

$$\wp(u,\Lambda) = \frac{1}{u^2} + \sum_{\lambda\in\Lambda'} \left(\frac{1}{(u-\lambda)^2} - \frac{1}{\lambda^2} \right),$$

$$\wp'(u,\Lambda) = -2 \sum_{\lambda\in\Lambda} \frac{1}{(u-\lambda)^3}$$

proporcionan un sistema de generadores del cuerpo $\mathbb{C}(\Lambda)$.

Debido a que la función $\wp$ y su derivada $\wp'$ están ligadas por una relación algebraica, el grado de transcendencia del cuerpo $\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$ es igual a 1. Por tanto, las funciones de Weierstrass proporcionan una parametrización meromorfa de la curva elíptica de ecuación

$$E: \; Y^2 = 4X^3 - g_2 X - g_3, \quad \Delta \neq 0.$$

Los coeficientes g_2 y g_3 se obtienen a partir de las denominadas series de Eisenstein de pesos 4 y 6, respectivamente, al ser evaluadas en el retículo de períodos:

$$g_2(\Lambda) = 60 \sum_{\lambda\in\Lambda'} \lambda^{-4}, \quad g_3(\Lambda) = 140 \sum_{\lambda\in\Lambda'} \lambda^{-6}.$$

El problema clásico de la uniformización euclídea de las curvas elípticas consiste en saber si toda curva elíptica compleja

$$Y^2 = 4X^3 - AX - B, \quad A^3 - 27B^2 \neq 0, \quad A, B \in \mathbb{C}$$

admite una parametrización por funciones de Weierstrass. La respuesta es afirmativa y su demostración se obtiene a partir de las propiedades de la función modular j, de la cual hablaremos en capítulos posteriores.

Una vez parametrizada una curva elíptica por medio de las funciones de Weierstrass correspondientes, el método de la secante y de la tangente proporciona las fórmulas de adición y de

duplicación

$$\wp(u+v) = \frac{1}{4}\left(\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\right)^2 - \wp(u) - \wp(v), \quad u \neq v,$$

$$\wp(2u) = \frac{1}{4}\left(\frac{\wp''(u)}{\wp'(u)}\right)^2 - 2\wp(u).$$

En otras palabras, las funciones $\wp, \wp'$ de Weierstrass establecen un isomorfismo aditivo entre los puntos de un toro complejo con retículo de períodos $\Lambda = \langle \lambda_1, \lambda_2 \rangle$ y el grupo abeliano $E(\mathbb{C})$ de los puntos complejos de la curva elíptica correspondiente.

La función σ de Weierstrass se define por medio de un producto convergente que proporciona ceros simples en todos los puntos $\lambda \in \Lambda'$:

$$\sigma(u) = u \prod_{\lambda \in \Lambda'} \left(1 - \frac{u}{\lambda}\right) e^{\frac{u}{\lambda} + \frac{1}{2}(\frac{u}{\lambda})^2}.$$

Se satisface que

$$\wp(u) = -\frac{d^2(\log(\sigma(u)))}{du^2}.$$

El teorema de Abel proporciona una manera eficiente para construir funciones elípticas con ceros y polos dados de antemano. Dado un divisor $D = \sum_{j=1}^{r} m_j(u_j) - \sum_{j=1}^{s} n_j(v_j)$ en $\mathbb{C}/\Lambda$, la condición de Abel afirma que D es principal si, y solamente si, $\mathrm{gr}(D) = 0$ y

$$\sum_{j=1}^{r} m_j u_j \equiv \sum_{j=1}^{s} n_j v_j \quad (\text{mód } \Lambda).$$

En tal caso, D se puede representar en la forma $D = \sum_{j=1}^{n} a_j(u_j) - \sum_{j=1}^{n} b_j(v_j)$, $\sum_{j=1}^{n} a_j - \sum_{j=1}^{n} b_j = 0$, y basta tomar

$$\frac{\prod_{j=1}^{n} \sigma(u - a_j)}{\prod_{j=1}^{n} \sigma(u - b_j)}$$

para tener una función cuyo divisor es D. El teorema de Abel se generaliza a toda superficie de Riemann, sea cual sea su género.

En general, dada una curva elíptica E definida sobre un subcuerpo $K \subseteq \mathbb{C}$, su ley de adición determina que el conjunto $E(K)$ de sus puntos K-racionales tiene estructura de grupo abeliano. Los puntos de N-división de E, es decir, los puntos P que satisfacen $NP = 0_E$ son racionales sobre la clausura algebraica $\overline{K}$ de K. Su conjunto $E[N]$ es un subgrupo de $E(\overline{K})$ de N^2 elementos, isomorfo a $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

2.2. Problemas aritméticos

2.2.1. Leyes de reciprocidad superiores

Entre las primeras generalizaciones de la ley de reciprocidad cuadrática encontramos las leyes de reciprocidad cuártica y cúbica. La ley de reciprocidad cuártica (o bicuadrática) es debida al propio Gauss y es relativa al anillo $\mathbb{Z}[i]$ de los enteros de Gauss. La ley de reciprocidad cúbica es debida a Gauss, Jacobi y Eisenstein y se formula en el anillo $\mathbb{Z}[\rho]$ de los enteros de Eisenstein. Notemos que ambos anillos son de ideales principales y, en consecuencia, son dominios de factorización única.

Posteriormente, se descubrieron otras leyes de reciprocidad, por parte de Jacobi, Eisenstein, Dedekind, Kummer y Hilbert, entre otros. La búsqueda de una ley general de reciprocidad motivó una buena parte del desarrollo de la aritmética de los cuerpos de números.

En el caso de la ley de reciprocidad bicuadrática, dados enteros algebraicos primos $\pi, \lambda \in \mathbb{Z}[i]$, que no dividan a 2, se define el símbolo de residuos bicuadráticos $[\pi/\lambda]$ como la única unidad en $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ que satisface la congruencia superior

$$\left[\frac{\pi}{\lambda}\right] \equiv \pi^{(N\lambda-1)/4} \pmod{\lambda},$$

siendo $N(\lambda) := \#\mathbb{Z}[i]/\lambda\mathbb{Z}[i]$ la norma del elemento λ.

La ley de reciprocidad bicuadrática se expresa diciendo que, para cada par de elementos primos distintos $\pi, \lambda \in \mathbb{Z}[i]$ tales que $\pi \equiv \lambda \equiv 1 \pmod{(2+2i)}$, se satisface la igualdad

$$\left[\frac{\pi}{\lambda}\right] = (-1)^{\frac{N\pi-1}{4}\frac{N\lambda-1}{4}} \left[\frac{\lambda}{\pi}\right].$$

Como en el caso cuadrático, existen también leyes suplementarias para $\lambda = i$, $\lambda = 1+i$.

La ley de reciprocidad cúbica es parecida.

En relación con el tema de la multiplicación compleja, es importante destacar las demostraciones analíticas descubiertas por Jacobi y por Eisenstein de las leyes de reciprocidad conocidas en su día.

En el caso cuadrático, la demostración de Eisenstein se basa en la expresión del símbolo de Legendre mediante la función $\sin(2\pi u)$. Concretamente, si $A = \{\alpha \in \mathbb{Z} : 1 \leq \alpha \leq \frac{p-1}{2}\}$ denota la mitad de un sistema de representantes módulo un entero primo p, se tiene que

$$\left(\frac{q}{p}\right) = \prod_{\alpha \in A} \frac{\sin\left(\frac{2\pi}{p} q\alpha\right)}{\sin\left(\frac{2\pi}{p}\alpha\right)}.$$

En los casos bicuadrático y cúbico, las demostraciones analíticas de Eisenstein de las leyes de reciprocidad se basan en una expresión previa de los símbolos correspondientes por medio de funciones elípticas con multiplicación compleja, lo cual adelantemos que significa que sus retículos de períodos son ideales (posiblemente fraccionarios) de cuerpos cuadráticos imaginarios.

En el caso de los residuos bicuadráticos, Eisenstein utiliza la función seno lemniscático, de retículo de períodos $\mathbb{Z}[i]$:

$$\phi(u) := \mathrm{sl}((1-i)\varpi u),$$

que satisface

$$\phi(iu) = i\phi(u), \quad \phi(\mu u) = \varepsilon \prod_{\alpha \in A} \phi\left(z - \frac{\alpha}{\mu}\right),$$

para todo $\mu \in \mathbb{Z}[i]$, tal que $(2, \mu) = 1$ y ε es la raíz cuarta de la unidad tal que $\mu \equiv \varepsilon \pmod{(2-2i)}$. Con ello,

$$\left[\frac{\pi}{\lambda}\right] = \prod_{\alpha \in A} \frac{\phi(\pi\alpha/\lambda)}{\phi(\alpha/\lambda)},$$

en donde A denota $1/4$ de un sistema de representantes módulo λ. Los números algebraicos π, λ son enteros primos de Gauss que satisfacen las condiciones anteriormente impuestas. Las principales ideas que intervienen en la demostración de estos resultados son las mismas que se requieren para probar la afirmación que hace Gauss en la última entrada de su diario.

En la derivación de los resultados anteriores, es importante resaltar la relación algebraica que encuentra Eisenstein entre $\phi(\mu u)$ y $\phi(u)$. Escribamos $\mu = a + bi$; supongamos que $p = a^2 + b^2 = N(\mu)$ es un entero primo, congruente con 1 módulo 4. Valiéndose de las fórmulas de transformación asociadas a la ecuación diferencial

$$\frac{dy}{\sqrt{1-y^4}} = \mu \frac{dx}{\sqrt{1-x^4}},$$

Eisenstein obtiene que

$$\phi(\mu u) = \phi(u) \frac{\mu f + \phi(u)^{p-1}}{1 + \mu g},$$

en donde f, g son polinomios en $\phi(u)^4$ con coeficientes enteros algebraicos. El lector actual probablemente preferirá ver esta fórmula escrita en la forma

$$\varphi(u)^p \equiv \varphi(\mu u) \pmod{\mu},$$

en la que se vislumbra el cálculo explícito del automorfismo de Frobenius, propio de la teoría de la multiplicación compleja. Estos conceptos serían trabajados y extendidos, entre otros, por Kronecker, Hasse, Deuring, Weil, Eichler y Shimura.

En el caso de los residuos cúbicos, Eisenstein procede de una manera similar. Para ello utiliza una función elíptica ψ de retículo de períodos $\mathbb{Z}[\rho]$, $\rho = \zeta_3$, para la cual $\psi(\rho u) = \rho\psi(u)$.

Los teoremas de Eisenstein sobre los residuos bicuadráticos y los residuos cúbicos fueron generalizados por G. Herglotz en 1921. Empleando funciones elípticas con multiplicación compleja, Herglotz obtuvo leyes de reciprocidad para todos los cuerpos cuadráticos imaginarios. Herglotz, cuyo nombre hoy en día está prácticamente olvidado, fue el director de la tesis de E. Artin.

2.2.2. Puntos racionales de cúbicas

En 1901, H. Poincaré se ocupó de la determinación de la estructura del grupo de los puntos de coordenadas racionales de una curva elíptica definida sobre el cuerpo $\mathbb{Q}$ de los números racionales. Sus investigaciones dieron lugar a la denominada conjetura de Poincaré para curvas elípticas, según la cual, dada una curva elíptica E definida sobre $\mathbb{Q}$,

$$E: \quad Y^2 = X^3 + a_4X + a_6, \quad a_i \in \mathbb{Q},$$

el grupo abeliano $E(\mathbb{Q})$ es finitamente generado.

De hecho, en el trabajo mencionado, Poincaré no formula explícitamente ninguna conjetura. Se limita a constatar que

> Si les points d'arguments elliptiques α, α_1, α_2, ..., α_q sont rationnels, il en est de même de tous les points dont les arguments elliptiques sont compris dans la formule (1)
>
> $$\alpha + 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \cdots + p_q(\alpha_q - \alpha)$$

où n et les p sont entieres. On peut se proposer de choisir les arguments (2) $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_q$ de telle façon que la formule (1) comprenne tous les points rationnels de la cubique. Les $q+1$ points rationnels qui ont les arguments (2) forment alors ce que nous appellerons un *système de points rationnels fondamentaux.*

H. Poincaré [104]

Poincaré habla de un sistema de puntos racionales fundamentales, lo cual se traduce hoy en un sistema de generadores del grupo abeliano $E(\mathbb{Q})$.

Capítulo 3

Funciones abelianas

3.1. Los orígenes

Las integrales abelianas son la generalización natural de las integrales elípticas. El caso más sencillo corresponde al de las integrales hiperelípticas. Por inversión de las integrales hiperelípticas (en género 2) se obtienen las funciones hiperelípticas, que son periódicas con un retículo de períodos de dimensión 4. En general, por inversión de las integrales abelianas se obtienen las funciones abelianas, que son periódicas con un retículo de períodos de dimensión par $2g$. A su vez, estas funciones proporcionan parametrizaciones analíticas de ciertas variedades algebraicas: las variedades abelianas complejas de dimensión g, que están dotadas de una ley de adición algebraica y conmutativa. El caso $g = 1$ es el de las curvas elípticas.

3.1.1. Integrales hiperelípticas

Las integrales hiperelípticas clásicas son de la forma

$$\int \frac{R(x)}{\sqrt{P(x)}}\,dx,$$

en donde $R \in \mathbb{C}(x)$ es una función racional y $P \in \mathbb{C}[x]$ es un polinomio de grado menor o igual que 6. Asociadas a pares de diferenciales convenientes, las integrales hiperelípticas

$$u_1 := \int_{p_1}^{z_1} \omega_1 + \int_{p_2}^{z_2} \omega_1, \quad u_2 := \int_{p_1}^{z_1} \omega_2 + \int_{p_2}^{z_2} \omega_2$$

están definidas módulo un retículo de períodos de $\mathbb{C}^2$:

$$\Lambda = \langle \oint_{\alpha_1} \omega, \oint_{\alpha_2} \omega, \oint_{\beta_1} \omega, \oint_{\beta_2} \omega \rangle \simeq \mathbb{Z}^4, \quad \omega = (\omega_1, \omega_2).$$

El problema de inversión de estas integrales plantea expresar las funciones z_1, z_2 en función de las funciones (multiformes) u_1, u_2. Al hacerlo, se obtienen dos funciones analíticas en dos variables y cuatro períodos independientes

$$z_i = z_i(u_1, u_2) : \mathbb{C}^2/\Lambda \to \mathbb{C} \cup \{\infty\}, \quad i = 1, 2.$$

La inversión de integrales hiperelípticas fue estudiada por A. Göpel, K. Weierstrass y J. G. Rosenhain, entre otros.

3.1.2. Integrales abelianas

La forma general de una integral abeliana es

$$\int f(x, y)\, dx, \quad f(X, Y) \in \mathbb{C}(X, Y),$$

en donde las funciones x, y satisfacen una relación algebraica. Es decir, se supone que existe un polinomio irreducible y no constante $F(X, Y) \in \mathbb{C}[X, Y]$ tal que $F(x, y) = 0$.

La teoría de Riemann permite asociar al polinomio $F(X, Y)$ una superficie analítica compacta y g diferenciales holomorfas independientes:

$$\omega = (\omega_1, \ldots, \omega_g),$$

siendo g el género de la superficie topológica subyacente. Podemos ahora considerar las integrales abelianas,

$$(u_1, \ldots, u_g) \equiv (\sum_{k=1}^{g} \int_{p_k}^{z_k} \omega_1, \ldots, \sum_{k=1}^{g} \int_{p_k}^{z_k} \omega_g),$$

definidas módulo un retículo de períodos $\Lambda \simeq \mathbb{Z}^{2g}$ de $\mathbb{C}^g$.

Las funciones abelianas se obtienen al resolver el problema de la inversión de las integrales abelianas. De esta manera, se obtienen g funciones de g argumentos, Λ-periódicas:

$$z_i = z_i(u_1, \ldots, u_g): \quad \mathbb{C}^g/\Lambda \to \mathbb{C} \cup \{\infty\}, \quad 1 \leq i \leq g.$$

Denotemos por $\mathcal{C}$ la curva proyectiva y no singular con modelo afín $F(X, Y) = 0$. El toro complejo $\mathbb{C}^g/\Lambda$ es algebraico; es decir, podemos interpretarlo como el conjunto de los puntos complejos de una variedad algebraica no singular. Dicha variedad se representa por $J(\mathcal{C})$ y se denominada la variedad jacobiana de la curva $\mathcal{C}$,

$$\mathbb{C}^g/\Lambda \xrightarrow{\sim} J(\mathcal{C})(\mathbb{C}).$$

Por transporte de estructura, el conjunto $J(\mathcal{C})(\mathbb{C})$ de los puntos complejos de la jacobiana es un grupo abeliano. Fijado un punto p_0 de $\mathcal{C}$, la aplicación de Abel-Jacobi se define por

$$u: \mathcal{C} \to J(\mathcal{C}), \quad u(p) := \left(\int_{p_0}^{p} \omega_1, \ldots, \int_{p_0}^{p} \omega_g \right) \quad (\text{mód } \Lambda).$$

El teorema de Abel-Jacobi nos dice que, dados dos divisores efectivos D, E de $\mathcal{C}$, se satisface que $u(D) = u(E)$ si, y solamente si, D y E son linealmente equivalentes. Este resultado sirve de base para la definición de la variedad jacobiana de una curva sobre un cuerpo arbitrario (no necesariamente incluido en el cuerpo complejo), realizada de manera independiente de la teoría de funciones.

Los clásicos, empezando por B. Riemann e incluyendo a Poincaré, consideraron funciones theta asociadas a retículos, con la

idea de construir las posibles funciones periódicas asociadas al retículo como cocientes de tales funciones. Las funciones theta dependen de dos argumentos (u, Z). El módulo u es un vector de g coordenadas y Z es una matriz simétrica $g \times g$ de parte imaginaria definida positiva. El conjunto de estas matrices se designa por $\mathcal{H}_g$, y constituye el denominado espacio de Siegel en dimensión g. Se tiene que $\mathcal{H}_1 = \mathcal{H}$ es el semiplano de Poicaré, o semiplano superior complejo,

$$\mathcal{H} := \{z \in \mathbb{C} : \Im(z) > 0\}.$$

La función theta de Riemann se define como

$$\theta(u, Z) := \sum_{m \in \mathbb{Z}^g} \exp(\pi i({}^t m Z m + 2\,{}^t m(u))),$$

en donde $u \in \mathbb{C}^g$, $Z \in \mathcal{H}_g$.

En 1857, Riemann demostró que las funciones abelianas z_i anteriormente obtenidas son las soluciones de la ecuación

$$\Theta(z) := \theta\left(\int_{p_0}^{z} \omega - u - \kappa, Z\right) = 0.$$

En ella, $\langle 1_g, Z\rangle$ denota la normalización del retículo de períodos de la curva $\mathcal{C}$, obtenida previa elección de una base simpléctica de la homología respecto de la forma bilineal de intersección; y κ es el denominado vector de Riemann.

3.1.3. Funciones theta abelianas

Si partimos ahora de un retículo arbitrario Λ de $\mathbb{C}^g$, $g > 1$, lo más probable será que las únicas funciones Λ-periódicas sean las constantes. Sin embargo, este no es el caso cuando $g = 1$.

Una aportación notable en este contexto es el denominado teorema de Poincaré-Picard. En 1883, Poincaré y Picard, precisando resultados que eran ya familiares a Weierstrass, Riemann

y Hermite, demostraron que, dado un retículo Λ de $\mathbb{C}^n$, existen funciones de n variables, no constantes, y periódicas de retículo de períodos Λ si, y solamente si, Λ satisface las denominadas relaciones de Riemann respecto de una forma hermítica H positiva. En este caso, $\mathrm{Im}H$ es una forma alternada que toma valores enteros sobre la red. Si H es definida positiva, entonces el número de funciones independientes es máximo.

Supongamos que tenemos un retículo dotado de una forma de Riemann no degenerada. La obtención de una base simpléctica en el retículo permite la substitución del retículo original por uno normalizado: $\langle 1_g, Z\rangle$. Las funciones periódicas en cuestión se obtienen como cociente de funciones theta de dos variables con características:

$$\theta \begin{bmatrix} a \\ b \end{bmatrix}(u, Z) := \sum_{m \in a+\mathbb{Z}^n} \exp(\pi i({}^t mZm + 2{}^t m(u+b))),$$

${}^t a, {}^t b \in \mathbb{R}^g$, $u \in \mathbb{C}^g$. La variable u se denomina el argumento. La variable Z, que se denomina el módulo, es una matriz de $\mathcal{H}_g$. Las funciones theta con características proporcionan una generalitzación adecuada de las funciones theta de Jacobi, correspondientes al caso $g = 1$.

La funciones theta con características evaluadas en un Z fijo, $\theta \begin{bmatrix} a \\ b \end{bmatrix}(u, Z)$, proporcionan inmersiones proyectivas del toro complejo $\mathbb{C}^g/\Lambda$, que puede interpretarse de este modo como una variedad proyectiva. Esta variedad, que está provista de una ley de adición conmutativa, recibe el nombre de variedad abeliana.

Poincaré y Picard demostraron además que toda función periódica de retículo de períodos (Λ, H) es cociente de funciones theta abelianas; es decir, de funciones theta construidas a partir de retículos de períodos de integrales abelianas. No menos importante fue el estudio llevado a cabo por Poincaré sobre la reducción de integrales abelianas, que conduciría al concepto de isogenia entre variedades abelianas y al teorema de reducibilidad completa. Veamos como rezan parte de estos resultados en sus

propias palabras:

> Nous avons démontré [...] M. Picard et moi, qu'un système *quelconque* de fonctions abéliennes peut être déduit par réduction d'un système analogue, engendré par une courbe algébrique.
>
> H. Poincaré [103], t. IV, p. 315.

> J'ai donné moi-même, à ce sujet, un théorème, d'après lequel, quand il y a réduction, on peut, par une transformation d'ordre k, changer la fonction Θ à reduire en un produit de fonctions Θ, d'un moindre nombre de variables. L'entier k est alors le nombre caractéristique de la réduction.
>
> H. Poincaré [103], t. IV, p. 314.

Más adelante, estos teoremas de Poincaré se verían generalizados a variedades abelianas definidas sobre un cuerpo cualquiera y la teoría de funciones se vería reemplazada por el lenguaje de la teoría de haces.

3.2. Variedades abelianas

En 1921, S. Lefschetz daba la siguiente definición de variedad abeliana, en el marco de la teoría de funciones:

> An *Abelian* variety of genus p, V_p, is a variety whose non-homogeneous point coordinates are equal to $2p$-ply periodic meromorphic functions of p arguments $u_1, \ldots, u_p$, or whose homogeneous point coordinates are proportional to theta's of the same order and continuous characteristic. The variety is algebraic (Weierstrass) and of dimensionality p. When the periods are those of an algebraic curve of genus p, V_p is called a *Jacobi* variety.
>
> S. Lefschetz [96].

El functor $A \rightsquigarrow A(\mathbb{C})$ establece una equivalencia entre (la categoría de) las variedades abelianas complejas y (la categoría de) los toros complejos que admiten una forma de Riemann. Las variedades abelianas de dimensión 1 son las curvas elípticas.

En la segunda mitad del siglo XX el concepto de variedad abeliana experimentó una notable generalización pues fue extendido a cualquier cuerpo base. Ello significó que el estudio de las variedades abelianas tuvo que hacerse de manera independiente de la teoría de funciones. Por definición, dado un cuerpo K arbitrario, una variedad abeliana A/K es una variedad algebraica, proyectiva, definida sobre K que es, al mismo tiempo, un grupo algebraico; es decir, posee una ley de grupo definida sobre K por aplicaciones regulares. La ley de grupo en una variedad abeliana es necesariamente conmutativa y la variedad es no singular.

En el caso particular en que K sea un cuerpo de números y A una variedad abeliana definida sobre K, técnicas de reducción y de completación permiten obtener a partir de A variedades abelianas definidas sobre cuerpos finitos $\mathbb{F}_q$, sobre cuerpos $\mathfrak{p}$-ádicos $K_\mathfrak{p}$, sobre $\mathbb{R}$ o sobre $\mathbb{C}$.

Los homomorfismos entre variedades abelianas se definen por medio de aplicaciones regulares que son a su vez homomorfismos de grupos. Si A y B son variedades abelianas de la misma dimensión, existe un epimorfismo de A en B si, y solamente si, existe un epimorfismo de B en A. Cuando ello ocurre, se dice que A y B son isógenas; en tal caso se suele escribir $A \sim B$. El núcleo de una isogenia de A en B es un subgrupo finito, cuyo orden es igual al grado de separabilidad de la isogenia. Dada una variedad abeliana A, la multiplicación por un entero $N \geq 1$ es siempre una isogenia de A. Su núcleo, $A[N]$, está formado por los denominados puntos de N división de A.

La variedad producto de una variedad abeliana A por una variedad abeliana B es de nuevo una variedad abeliana cuya dimensión es igual a la suma de las dimensiones de A y de B. Una variedad se denomina simple si no es isógena a un producto de

variedades abelianas de dimensión menor. El teorema de reducibilidad completa (inspirado en los teoremas de reducción de integrales abelianas de Poincaré) afirma que toda variedad abeliana es isógena a un producto de variedades abelianas simples.

3.2.1. Variedades abelianas con MC

La teoría de la multiplicación compleja de variedades abelianas comprende como caso particular la teoría clásica de la multiplicación compleja de curvas elípticas. Para hablar de variedades abelianas con multiplicación compleja, debemos hacer unas consideraciones previas acerca de la estructura de las álgebras de endomorfismos de estos objetos.

Designemos por $\mathrm{End}(A)$ el anillo de todos los endomorfismos de una variedad abeliana A y por $\mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}(A) \otimes \mathbb{Q}$ su $\mathbb{Q}$-álgebra de endomorfismos.

Si A es una variedad abeliana simple y F es el centro de $\mathrm{End}_{\mathbb{Q}}(A)$, entonces F es un cuerpo de números totalmente real o bien es un cuerpo de números que es una extensión totalmente imaginaria de un cuerpo de números totalmente real, en cuyo caso, F es un cuerpo de tipo MC.

El teorema de reducibilidad completa permite deducir que la $\mathbb{Q}$-álgebra de endomorfismos de A descompone como una suma directa de álgebras de matrices sobre álgebras de división H_i de dimensión finita:

$$\mathrm{End}_{\mathbb{Q}}(A) \simeq \bigoplus_{i=1}^{s} M(n_i, H_i).$$

Las dimensiones $[H_i : \mathbb{Q}]$ están acotadas en términos de la dimensión de la variedad A. Las álgebras H_i son isomorfas o bien a un cuerpo de números totalmente real, o bien a un álgebra de cuaternios definida sobre un cuerpo de números totalmente real, o bien a un álgebra de división sobre un cuerpo de números con multiplicación compleja.

Las variedades abelianas con multiplicación compleja (MC) son las que poseen un álgebra de endomorfismos mayor. Más precisamente, una variedad abeliana simple $A/\mathbb{C}$ se dice que tiene multiplicación compleja cuando su álgebra de endomorfismos es un cuerpo F de grado $2\dim A$ sobre $\mathbb{Q}$; en tal caso, F es un cuerpo MC. El tipo MC de A se obtiene, por definición, por la acción de F en el espacio tangente en el cero de A y es equivalente a elegir un sistema maximal de inmersiones complejas no conjugadas de F en $\mathbb{C}$.

Si una variedad abeliana, no necesariamente simple, $A/\mathbb{C}$ es tal que $\mathrm{End}_{\mathbb{Q}}(A)$ posee un cuerpo F de dimensión $2\dim A$ sobre $\mathbb{Q}$, entonces A es isógena a un producto $B\times\cdots\times B$ de variedades simples y el conmutador de F en $\mathrm{End}_{\mathbb{Q}}(A)$ es el propio F.

Una variedad abeliana $A/\mathbb{C}$ se dice que tiene multiplicación compleja cuando cada uno de sus factores de isogenia simples posee multiplicación compleja; en tal caso, su álgebra de endomorfismos contiene un anillo conmutativo de dimensión $2\dim A$. Las jacobianas de las curvas de Fermat proporcionan ejemplos de variedades abelianas de dimensión superior con multiplicación compleja.

Las álgebras de endomorfismos de las curvas elípticas con multiplicación compleja son, por tanto, cuerpos cuadráticos imaginarios, y sus anillos de endomorfismos son órdenes de estos cuerpos.

Un importante teorema afirma que toda variedad abeliana $A/\mathbb{C}$ con multiplicación compleja posee un modelo definido sobre un cuerpo de números.

Capítulo 4

Funciones modulares elípticas

El semiplano superior complejo $\mathcal{H}$ dotado de la métrica hiperbólica proporciona un modelo del plano hiperbólico. En él opera el grupo proyectivo $\mathbf{PSL}(2,\mathbb{R})$ de acuerdo con las fórmulas

$$\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{SL}(2,\mathbb{R}), \quad z \in \mathcal{H}, \quad \gamma(z) := \frac{az+b}{cz+d},$$

constituyendo su grupo de automorfismos holomorfos.

Se denominan funciones modulares, o también funciones modulares elípticas, las funciones meromofas de $\mathcal{H}^* := \mathcal{H} \cup \mathbf{P}^1(\mathbb{Q})$ que son periódicas respecto de un subgrupo Γ del grupo modular $\mathbf{SL}(2,\mathbb{Z})$. Las funciones modulares elípticas difieren enormemente de las funciones elípticas, en tanto que las funciones elípticas son funciones periódicas respecto de subgrupos discretos de movimientos euclídeos y las funciones modulares elípticas lo son respecto de subgrupos discretos de movimientos hiperbólicos. Sin embargo, sin el estudio de las funciones modulares elípticas es imposible penetrar en el estudio de las funciones elípticas.

4.1. Los orígenes

Gauss hizo su descubrimiento particular de las funciones modulares a raíz de un estudio de la media aritmético-geométrica $\mathrm{MAG}(x, y)$ de dos números reales positivos, realizado en unos trabajos sobre perturbaciones seculares. Por medio de la fórmula

$$L = 4a \int_0^1 \frac{dt}{\sqrt{1-t^4}} = \frac{2\pi a}{\mathrm{MAG}(1, \sqrt{2})},$$

Gauss dió una aproximación de la medida L del arco de la lemniscata de parámetro a. En general, se tiene que

$$\mathrm{MAG}(x, y) = \frac{\pi}{4} \frac{x+y}{K\left(\left(\frac{x-y}{x+y}\right)^2\right)},$$

en donde $K(k)$ denota la integral completa de primera especie.

Otro de los orígenes del estudio de las funciones modulares (y, como veremos más adelante, de las formas modulares) se encuentra en la determinación de las fórmulas de transformación de las funciones theta con características.

4.1.1. Funciones modulares elípticas

Por integración de una ecuación diferencial de segundo orden de tipo fuchsiano, R. Dedekind construyó en 1877 una función especial, a la que denominó función valencia (*Valenz Funktion*), una normalización conveniente de la cual es la función modular elíptica j.

La función j es una función meromorfa en $\mathcal{H}^*$ con un único polo, que es simple y de residuo 1, situado en el infinito. Las relaciones satisfechas por esta función,

$$j(z+1) = j(z), \quad j(-1/z) = j(z),$$

ponen de manifesto su invariancia respecto del grupo modular:

$$j(\gamma(z)) = j(z), \quad \text{para todo } \gamma \in \mathbf{SL}(2,\mathbb{Z}).$$

En particular, la función j queda determinada por sus valores en un dominio fundamental $\mathcal{F}$ por la acción de $\mathbf{PSL}(2,\mathbb{Z})$ en $\mathcal{H}$. Como dominio fundamental podemos consider el usado por Gauss en su teoría de la reducción de las formas cuadráticas binarias definidas positivas (cf. figura 1.1).

Salvo producto por una constante, esta función se conoce hoy como invariante j de Klein y constituye el primer ejemplo de una función modular. En un principio, las funciones modulares tenían por variable el módulo k de las integrales elípticas. A Klein se debe la introducción sistemática del invariante modular j. Interpretados como funciones sobre retículos, los invariantes j y k están ligados por una relación algebraica:

$$j(z) = 2^8 \frac{(k(z)^4 - k(z)^2 + 1)^3}{k(z)^4(k(z)^2 - 1)^2}, \quad z(k) = i\frac{K'(k)}{K(k)}, \quad z \in \mathcal{H}.$$

La función j establece un isomorfismo analítico

$$j : \mathbf{PSL}(2,\mathbb{Z})\backslash\mathcal{H}^* \xrightarrow{\sim} \mathbf{P}^1(\mathbb{C})$$

y es un generador del cuerpo de todas las funciones invariantes por el grupo modular $\mathbf{PSL}(2,\mathbb{Z})$; es decir, $\mathbb{C}(\mathbf{P}^1) = \mathbb{C}(j)$. En el entorno del infinito, j posee un desarrollo en serie de Fourier con coeficientes enteros:

$$\begin{aligned} j(q) &= \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 \\ &\quad + 20245856256q^4 + 333202640600q^5 + \mathrm{O}(q^6), \end{aligned}$$

siendo $q(z) := e^{2\pi i z}$, $z \in \mathcal{H}$.

En los textos actuales, la función j se define como

$$j(q(z)) = 1728\frac{g_2(z)^3}{\Delta(z)}, \quad z \in \mathcal{H}.$$

Para cada punto $z \in \mathcal{H}$, el valor $j(z)$ es un invariante de la clase de isomorfía de la curva elíptica de ecuación

$$Y^2 = 4X^3 - g_2(z)X - g_3(z).$$

La igualdad anterior, unida a las propiedades de la función j, permite demostrar que toda curva elíptica compleja es parametrizable analíticamente por medio de funciones elípticas. Ambas propiedades muestran que el cociente $\mathbf{PSL}(2,\mathbb{Z})\backslash\mathcal{H}^*$ es un espacio de módulos para las clases de isomorfía de las curvas elípticas $E/\mathbb{C}$.

En el mismo trabajo en que introduce la función j, Dedekind construye la función η que lleva su nombre:

$$\eta(z) = e^{2\pi iz/24} \prod_{n=1}^{\infty} (1 - e^{2\pi izn}).$$

Se trata de una raíz 24 del discriminante Δ:

$$\Delta(z) = (2\pi)^{12} \eta^{24}(z).$$

En la terminología actual, el comportamiento de esta función respecto de la acción del grupo modular se expresa diciendo que η es una forma modular de peso $1/2$.

4.1.2. Ecuaciones de transformación

Las denominadas ecuaciones de transformación de las funciones elípticas pueden considerarse como las análogas a las relaciones algebraicas existentes entre $\cos(Nz)$ y $\cos(z)$, bien conocidas por Euler. Su estudio dio origen a las ecuaciones modulares.

Jacobi y Abel se preocuparon de averiguar las condiciones bajo las cuales, dados dos módulos k, ℓ, existe una relación de la forma

$$\frac{dy}{\sqrt{(1-y^2)(1-\ell^2 y^2)}} = \frac{1}{M(k,\ell)} \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}$$

en la que el multiplicador $M(k,\ell)$ es una expresión algebraica de k y ℓ.

Jacobi demostró la existencia de una transformación de orden un entero cualquiera $m \geq 1$, proporcionando las fórmulas siguientes. Si $x = \mathrm{sn}(u \mid k)$ e $y = \mathrm{sn}(u/M \mid \ell)$, entonces existen polinomios U, V, primos entre si, tales que U es de grado m, V de grado $m-1$ e $y = U(x)/V(x)$. Explícitamente,

$$U(x) = \frac{x}{M}\prod_r \left(1 - \frac{x^2}{\mathrm{sn}^2(r\omega)}\right), \quad V(x) = \prod_r (1 - k^2x^2\mathrm{sn}^2(r\omega)),$$

$1 \leq r \leq (m-1)/2$, $\omega = 2(nK + in'K)/m$, siendo n, n' enteros primos con m; además,

$$\begin{aligned} M(k,\ell) &= (-1)^{(m-1)/2}\textstyle\prod_r \mathrm{sn}^2(K - r\omega)/\mathrm{sn}^2(r\omega), \\ \ell &= k^m \textstyle\prod_r \mathrm{sn}^4(K - r\omega). \end{aligned}$$

En particular, la multiplicación por N es una transformación de orden $m = N^2$ con $\ell = k$ y $M = 1/N$.

Formulado en el lenguaje actual, el problema que resuelve Jacobi equivale a encontrar fórmulas explícitas en función de $\mathrm{sn}(u \mid k)$ para todas las isogenias de un orden dado de una curva elíptica $E/\mathbb{C}$. Con ello estamos a un paso de la introducción de los operadores de Hecke.

De gran importancia en la teoría de las funciones elípticas son las ecuaciones modulares. Supongamos, para simplificar, que N es un entero primo. Por definición, las raíces de la ecuación modular de nivel N son los $(N+1)$ valores del módulo ℓ que son imagen del módulo k por las $(N+1)$ transformaciones de orden N. Los retículos respectivos vienen dados por:

$$\begin{aligned} \Lambda_0 &= \mathbb{Z}\frac{\omega_1}{N} \oplus \mathbb{Z}\omega_2, \\ \Lambda_r &= \mathbb{Z}\omega_1 \oplus \mathbb{Z}\left(\frac{\omega_2}{N} + r\frac{\omega_1}{N}\right), \quad 1 \leq r \leq N. \end{aligned}$$

Estas ecuaciones caracterizan la existencia de una relación algebraica de la forma

$$\frac{K'(\ell)}{K(\ell)} = N\frac{K'(k)}{K(k)},$$

entre las respectivas integrales completas de primera especie. Los primeros ejemplos, para $N = 3, 5, 7$, proporcionan las ecuaciones

$$\begin{aligned} u^4 - v^4 + 2uv(1 - u^2v^2) &= 0, \\ v^6 - u^6 + 5u^2v^2(v^2 - u^2) + 4uv(u^4v^4 - 1)) &= 0, \\ (1 - u^8)(1 - v^8) - (1 - uv)^8 &= 0, \end{aligned}$$

en donde $u^2 := \sqrt{k}$, $v^2 := \sqrt{\ell}$. Los multiplicadores respectivos son

$$M_3 = \frac{v}{v + 2u^3},$$

$$M_5 = \frac{v(1 - uv^3)}{v - u^5},$$

$$M_7 = \frac{v(1 - uv)(1 - uv + (uv)^2)}{v - u^7}.$$

Las dos primeras ecuaciones son debidas a Jacobi.

Con el uso sistemático del invariante modular j, promovido por Klein, en lugar del módulo k, introducido por Legendre, las denominadas ecuaciones modulares $\Phi_N(X, Y) = 0$ se convirtieron en una relación algebraica entre $j(z)$ y $j(z/N)$. Según la terminología actual, las ecuaciones anteriores definen las curvas modulares $X_0(N)$.

4.1.3. La ecuación de grado cinco

En 1799, P. Ruffini había publicado su *Teoria generale delle equazioni*, texto en que trataba la imposibilidad de la resolución por radicales de la ecuación general de grado mayor o igual que cinco. Como es bien sabido, estas investigaciones fueron reemprendidas por Abel y por Galois, introduciendo este último

el grupo de una ecuación y caracterizando su resolubilidad por radicales mediante la resolubilidad de su grupo de transformaciones; con ello, la ecuación general de grado mayor o igual que cinco resultó ser no resoluble por radicales.

Galois determinó el grupo del polinomio modular de nivel primo N, $\Phi_N(X, j)$, sobre el cuerpo $\mathbb{Q}(j, \zeta_N)$, resultando ser isomorfo al grupo $\mathbf{PSL}(2, \mathbb{F}_N)$, de orden $N(N^2-1)/2$. Por tratarse de un grupo simple y no abeliano cuando $N \geq 5$, su teoría le permitió concluir que las ecuaciones modulares para $N \geq 5$ no son resolubles por radicales.

Para $N = 5, 7, 11$, y sólo en estos casos, se tienen resolventes de Galois de grado N inferiores en 1 al grado de la ecuación modular. Los grupos de Galois de estas resolventes son de orden 60, 168 y 660, respectivamente. En 1859, Ch. Hermite abordó el problema del cálculo efectivo de las resolventes de la ecuación modular, obteniendo las resolventes de grado 5 y 7. De esta forma, Hermite llegó a una ecuación de grado cinco que, si bien no era resoluble por radicales, lo era mediante funciones modulares elípticas.

Para su estudio de la quíntica, Hermite partió de la substitución de E. W. von Tschirnhaus (de 1683), que elimina el término de grado $n-1$ en una ecuación cualquiera de grado n, y utilizó un resultado de G. B. Jerrard (de 1834) por el cual toda quíntica puede ser transformada en una quíntica en forma trinómica:

$$z^5 + az + b = 0.$$

En el método de Hermite para la resolución de la quíntica es fundamental el uso de funciones theta de Jacobi, así como el de la ecuación modular de grado 6, calculada por Jacobi.

A raíz de los trabajos de Hermite sobre la resolución de la quíntica, I. L. Fuchs y Hermite se pusieron en contacto. Los trabajos de Fuchs influyeron en C. Jordan, G. F. Frobenius y, especialmente, en Poincaré, que tuvo a Hermite como director de tesis.

En 1858, Kronecker y F. Brioschi hallaron asimismo otros métodos para la resolución de la quíntica mediante funciones modulares. A partir de 1878, las investigaciones de Hermite sobre la quíntica fueron proseguidas por Klein, siendo ésta una vía que condujo al estudio de las funciones automorfas.

4.1.4. Funciones automorfas

A partir de 1866, Fuchs emprendió el estudio de ecuaciones diferenciales ordinarias, lineales, homogéneas y con coeficientes variables:

$$\frac{d^n w}{dz^n} + p_1(z)\frac{d^{n-1}w}{dz^{n-1}} + \dots p_{n-1}(z)\frac{dw}{dz} + p_n(z)w = 0,$$

suponiendo que las funciones $p_i(z)$ son meromorfas en una región T simplemente conexa del plano complejo. De acuerdo con su maestro Weierstrass, Fuchs da el nombre de puntos singulares de la ecuación diferencial a los polos de las funciones p_i.

Supongamos que $z = 0$ es un punto singular de la ecuación diferencial. Fuchs considera un camino cerrado γ con base en un punto no singular $z_0 \in T$, dando una vuelta exactamente alrededor del origen. Siguiendo un procedimiento habitual en Riemann, estudia el comportamiento de un sistema fundamental de soluciones de la ecuación diferencial al ser prolongadas analíticamente a lo largo de γ. La transformación así obtenida, que se denomina de monodromía, da cuenta de este comportamiento. [1] A partir de la matriz de monodromía A asociada a un sistema fundamental de soluciones, obtiene la ecuación característica

$$\det(A - \sigma \mathrm{I}_n) = 0.$$

[1] La palabra *monodromía* deriva del sustantivo griego $\delta\rho o\mu o\varsigma$, que significa vuelta de paseo o carrera (recuérdese hipódromo, canódromo, etc.). Observemos que la transfromación de monodromía proporciona una representación lineal del grupo fundamental del espacio topológico que resulta de suprimir en T los puntos singulares de la ecuación diferencial.

Fuchs designa con el nombre de números característicos las raíces σ_i de la ecuación anterior. Considera asimismo números ρ_i dados por las igualdades $e^{2\pi i\rho_i} = \sigma_i$. A fin de obtener la forma general de las soluciones de la ecuación diferencial, debe distinguir dos casos. Si todas las raíces son simples, entonces existe un sistema fundamental de soluciones tales que:

$$w_i(z) = z^{\rho_i}\varphi_i(z), \quad 1 \leq i \leq n.$$

Si existen raíces múltiples, entonces en el sistema fundamental de soluciones aparecen logaritmos. Entre los puntos singulares, Fuchs distingue los denominados puntos singulares regulares de los irregulares. En el entorno de un punto singular regular, el crecimiento de las soluciones es dominado por una función algebraica. Las ecuaciones diferenciales anteriores en las cuales todos sus puntos singulares, incluido el infinito, son regulares pasaron a denominarse de tipo fuchsiano; en este caso la ecuación se integra por un método debido a Frobenius.

En 1880, Fuchs introdujo una nueva clase de funciones por medio de la resolución de un problema de inversión parecido al de Jacobi, pero partiendo de integrales de soluciones de ecuaciones diferenciales lineales con coeficientes funciones racionales. Limitándose al caso de orden 2, Fuchs considera la función $z(\zeta)$ que resulta de invertir el cociente $\zeta = f(z)/\varphi(z)$ de dos soluciones de la ecuación diferencial dada.

El 29 de mayo de 1880, Poincaré inició una correspondencia con Fuchs en la que le cuestionaba algunos de sus resultados. Poincaré quería caracterizar cuando el cociente

$$z = \frac{w_1(x)}{w_2(x)}$$

de dos soluciones independientes de una ecuación diferencial de segundo orden

$$\frac{d^2w}{dx^2} - Q(x)w = 0$$

definía, por inversión, una función meromorfa $x(z)$. Por este camino, Poincaré llegaría a su descubrimiento particular de las funciones modulares.

Considerando que las funciones periódicas en el plano euclídeo se agotan con las funciones elípticas —de acuerdo con un teorema debido a Kronecker—, Poincaré se dedicó a la búsqueda de funciones periódicas en el plano hiperbólico, considerando éste como un dominio mucho más idóneo para llevar a cabo sus investigaciones. Poincaré designó con el nombre de fuchsianas las funciones meromorfas en un disco, o equivalentemente en $\mathcal{H}$, con periodicidad dada por los elementos de un grupo fuchsiano: $f(\gamma(z)) = f(z)$, para todo $\gamma \in \Gamma$. La primera contribución de Poincaré al estudio de las funciones fuchsianas fue una nota enviada al *Comptes rendus de l'Académie des Sciences*, en 1881, en la que puede leerse:

> Le but que je me propose dans le travail que j'ai l'honneur de présenter à l'Académie, est de rechercher s'il n'existe pas des fonctions analytiques analogues aux fonctions elliptiques et permettant d'intégrer diverses équations différentielles linéaires à coefficients algébriques. Je suis arrivé à démontrer qu'il existe une classe très étendue de fonctions qui satisfont à ces conditions et auxquelles j'ai donné le nom de *fonctions fuchsiennes*, en honneur de M. Fuchs, dont les travaux m'ont servi très utilement dans ces recherches.
>
> Poincaré [103], t. II, p. 1.

En el transcurso de un año, Poincaré publicaría en dicha revista trece notas más sobre el mismo tema, recopilando finalmente los resultados obtenidos en dos memorias en *Acta mathematica*.

Para resolver el problema de la existencia de funciones fuchsianas no constantes respecto de un grupo fuchsiano Γ arbitrario, Poincaré imitó la idea de Jacobi de representar las funciones elípticas como un cociente de funciones theta, intentando expresar las funciones fuchsianas como cocientes de unas series

específicas a las que denominó thetafuchsianas. Según Poincaré, la expresión general de una serie thetafuchsiana es

$$\Theta(z) = \sum_{\gamma \in \Gamma} h(\gamma(z)) \left(\frac{d\gamma(z)}{dz} \right)^k, \quad k > 1,$$

en donde $h(z)$ denota una función racional arbitraria; k pasó a denominarse el peso de dicha función. Debido a que las series thetafuchsianas definen funciones quasiperiódicas:

$$\Theta(\gamma(z)) = \Theta(z) \left(\frac{d\gamma(z)}{dz} \right)^{-k}, \quad \text{para todo } \gamma \in \Gamma,$$

el cociente de dos funciones thetafuchsianas del mismo peso k y respecto del mismo grupo fuchsiano Γ es una función fuchsiana respecto de este grupo.

En analogía con las ecuaciones de transformación de las funciones elípticas, Poincaré investigó las posibles relaciones algebraicas entre dos funciones fuchsianas. Por medio de un salto cualitativo impresionante, identificó el motivo por el cual existe una relación algebraica entre una función fuchsiana y una transformada suya, siendo necesario y suficiente que los grupos de transformaciones respectivos compartan un subgrupo de índice finito:

> Pour qu'il y ait une relation algébrique entre une fonction fuchsienne $F(z)$ de groupe G et sa transformée $F(z \cdot S)$ par la substitution S, il faut et il suffit que les deux groupes G et $S^{-1}GS$ soient commensurables. [...] quand $F(z)$ se réduit à la fonction modulaire J, [...] nous savons qu'il y a une relation algébrique entre $F(z)$ et $F\left(\frac{z}{n}\right)$; c'est cette relation algébrique qui est bien connue sous le nom d'équation modulaire dans la théorie de la transformation des fonctions elliptiques.
>
> Poincaré [103], t. II, p. 508– 509.

Poincaré demuestra que toda función fuchsiana $x = x(z)$ permite integrar una ecuación diferencial con coeficientes algebraicos. Si

$$t_1 := \sqrt{\frac{dx}{dz}}, \quad t_2 := z\sqrt{\frac{dx}{dz}},$$

entonces t_1, t_2 satisfacen una ecuación diferencial

$$\frac{d^2t}{dx^2} = \varphi(x, y)t,$$

en la cual $\varphi(x, y)$ es una función racional.

Teniendo en cuenta que trabajos de Riemann, Schwarz, Dedekind y Klein sobre funciones Γ-periódicas eran previos al estudio de las funciones fuchsianas iniciado por Poincaré, y que Fuchs no tenía ninguna publicación específica sobre este tema, Klein propuso a Poincaré en repetidas ocasiones la substitución del nombre de *funciones fuchsianas* por el de *funciones automorfas*, a fin de eliminar de su designación cualquier referencia personal. Pero la recomendación de Klein cayó en saco roto por parte de Poincaré.

De acuerdo con Klein, hoy designamos como funciones automorfas las funciones que Poincaré denominó fuchsianas, y designamos con el nombre de formas automorfas las series que Poincaré denominó thetafuchsianas. Sin embargo, se sigue utilizando el adjetivo fuchsiano para designar a los grupos discretos de movimientos hiperbólicos que determinan la periodicidad de estas funciones. Cuando los grupos fuchsianos son subgrupos del grupo modular, las funciones y las formas automorfas asociadas reciben el calificativo de modulares.

4.2. Funciones modulares y aritmética

4.2.1. Módulos singulares

A Hermite le llamaron poderosamente la atención las propiedades de las funciones modulares.

> Se apreciará, hasta cierto punto, esta dificultad al observar que k y k' no existen como funciones de ω, a menos que se suponga esta variable imaginaria y de la forma $\omega = \alpha + i\beta$, β *estrictamente positivo*. Por tanto se trata en verdad de partes de funciones que, desde entonces, escapan a muchos de los métodos más habitualmente empleados. De este modo, no existe para k y k' un desarrollo según las potencias de ω, y si se toma $\omega = \omega_0 + h$ para poder usar la serie de Taylor, he aquí todavía las circunstancias particulares que concurrirán. Las cantidades k y k' se pueden determinar por medio de una ecuación numérica, para una infinidad de valores de ω tales que
>
> $$\omega_0 = \frac{A + \sqrt{-B}}{C},$$
>
> siendo A, B, C enteros y B, estrictamente positivo; pero, si el uso de estos valores iniciales, al hacer $\omega = \omega_0 + h$, proporciona un irracional simple como primer término de la serie, los términos siguientes serán necesariamente transcendentes. Así, por ejemplo, para $\omega_0 = i$, se tendrá que $k = \frac{1}{\sqrt{2}}$, $k' = \frac{1}{\sqrt{2}}$, y tomando $\omega = i + h$, la integral
>
> $$\int_0^1 \frac{dx}{\sqrt{1 - x^4}}$$
>
> será la que figurará en todos los coeficientes del desarrollo de k y k' según las potencias crecientes de h. Con ello se ve lo muy lejos que se está de las series que definen los

> transcendentes simples, en donde todos los coeficientes son siempre conmensurables.
>
> Ch. Hermite [75], T.II, p. 164.

Los argumentos especiales a los que alude Hermite son los ceros de las formas cuadráticas binarias cuyo estudio constituye el núcleo central de las *Disquisitiones* de Gauss. Con el tiempo, el conocer las propiedades de las funciones automorfas en tales puntos sería una parte esencial de la teoría de la multiplicación compleja. Los puntos en cuestión, situados en $\mathcal{H}$, se conocen con el nombre de puntos MC o de multiplicación compleja. (Se emplea asimismo el nombre de puntos de Heegner.)

La obra de H. Weber titulada *Lehrbuch der Algebra* es el último gran texto de álgebra que se publica en el siglo XIX. Sus dos primeros volúmenes vieron la luz en 1895 y 1896. El tercer volumen, y último, se publicó en 1908, pero se basa en un texto previo que Weber había publicado en 1891 bajo el título *Elliptische Funktionen und algebraische Zahlen.*

El libro de Weber contiene un capítulo entero dedicado al estudio de fenómenos de multiplicación compleja. En un principio, la multiplicación de funciones elípticas hacía referencia a expresar, dado un entero N, las funciones $\mathrm{sn}(Nu \mid k)$, $\mathrm{cn}(Nu \mid k)$, $\mathrm{dn}(Nu \mid k)$ como funciones racionales de $\mathrm{sn}(u \mid k), \mathrm{cn}(u \mid k)$, $\mathrm{dn}(u \mid k)$. Weber se pregunta si no habrá otro tipo de multiplicadores μ tales que las funciones $\mathrm{sn}(\mu u \mid k)$, $\mathrm{cn}(\mu u \mid k)$, $\mathrm{dn}(\mu u \mid k)$ posean los mismos períodos que las funciones de partida. Weber llega a la conclusión de que, si ello es así, el cociente $\tau = \omega_2/\omega_1$, situado en el semiplano superior complejo $\mathcal{H}$, debe ser un irracional cuadrático y el multiplicador μ un entero algebraico cuadrático, en sintonía con las conclusiones de Abel.

A partir de cocientes de funciones η de Dedekind, Weber construye las funciones modulares que llevan su nombre:

$$\mathfrak{f}(z) := e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{z+1}{2}\right)}{\eta(z)}, \quad \mathfrak{f}_1(z) := \frac{\eta\left(\frac{z}{2}\right)}{\eta(z)}, \quad \mathfrak{f}_2(z) := \sqrt{2}\frac{\eta(2z)}{\eta(z)}.$$

En el tercer volumen de su tratado, Weber utiliza una ecuación modular, debida a Schläfli, para evaluar estas funciones en ciertos irracionales cuadráticos, $\tau = \sqrt{-m}$, $m \in \mathbb{N}$. La ecuación modular de Schläfli se escribe como

$$\left(\frac{u}{v}\right)^3 + \left(\frac{v}{u}\right)^3 = 2\left(u^2v^2 - \frac{1}{u^2v^2}\right).$$

Los valores que obtiene resultan ser números algebraicos. A su vez, valores especiales de las funciones de Weber en irracionales cuadráticos son utilizados para el cálculo de valores especiales de la función j. Dado un irracional cuadrático $\tau \in \mathcal{H}$, Weber denomina módulos singulares a los valores $j(\tau)$ y se da cuenta de que los ceros en $\mathcal{H}$ de las formas quadráticas binarias enteras de discriminante D proporcionan módulos singulares que son enteros algebraicos de grado igual al número de clases $h(D)$.

4.2.2. La ecuación del icosaedro

En 1884, veinticinco años después de los trabajos de Brioschi y Kronecker sobre la ecuación de grado cinco, Klein emprendió su estudio particular de las ecuaciones de grado siete.

En el capítulo primero de sus *Lecciones sobre el icosaedro*, Klein determina los subgrupos finitos del grupo de las rotaciones $\mathbf{SO}(3)$ del espacio euclídeo $\mathbb{R}^3$, obteniendo los grupos de simetría de los cinco poliedros regulares inscritos en la esfera unidad S^2. Al proyectar la esfera S^2 en el plano complejo $\mathbf{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, los elementos de los grupos anteriores se representan por medio de homografías

$$z \mapsto \frac{az+b}{cz+d}, \quad z \in \mathbb{C} \cup \{\infty\},$$

que Klein determina explícitamente en cada caso.

Klein fija el icosaedro en la esfera de modo que la proyección estereográfica de sus doce vértices sean los puntos del plano

dados por

$$z = 0, \quad \infty, \quad \varepsilon^\nu(\varepsilon + \varepsilon^4), \quad \varepsilon^\nu(\varepsilon^2 + \varepsilon^3), \qquad 0 \leq \nu \leq 4,$$

siendo $\varepsilon = e^{2\pi i/5}$ una raíz quinta de la unidad. Con ello se obtiene una representación compleja del grupo de simetrías del icosaedro que conservan la orientación, isomorfo al grupo alternado A_5, en el grupo de proyectividades $\mathbf{PGL}(2, \mathbb{Q}(\varepsilon))$, definidas sobre el cuerpo ciclotómico $\mathbb{Q}(\varepsilon)$, de grado cuatro.

La proyección $q : \mathbf{P}^1 \to A_5\backslash\mathbf{P}^1$ es un morfismo de variedades algebraicas que realiza la recta proyectiva como un recubrimiento ramificado de grado 60 del cociente $A_5\backslash\mathbf{P}^1$, isomorfo de nuevo a $\mathbf{P}^1$. Klein fija un sistema de coordenadas de modo que los puntos de ramificación en el cociente sean $0, 1, \infty$ y que se correspondan con la proyección de los centros de las caras, con los puntos medios de las aristas y con los vértices del icosaedro, respectivamente. Con ello, puede determinar que la aplicación

$$q : \mathbf{P}^1 \to A_5\backslash\mathbf{P}^1, \quad z \mapsto u,$$

viene dada por

$$q(z) = \frac{H(z,1)^3}{1728 f(z,1)^5},$$

siendo

$$f = z_1 z_2 (z_1^{10} + 11 z_1^5 z_2^5 - z_2^{10}),$$

$$H = -(z_1^{20} + (z_2^{20}) + 228(z_1^{15} z_2^5 - z_1^5 z_2^{15}) - 494 z_1^{10} z_2^{10}.$$

Consideremos, además,

$$T = (z_1^{30} + z_2^{30}) + 522(z_1^{25} z_2^5 - z_1^5 z_2^{25}) - 10005(z_1^{20} z_2^{10} + z_1^{10} z_2^{20}).$$

La forma H se anula exactamente en los baricentros de las caras del icosaedro; la forma f en sus vértices y la forma T en los puntos medios de sus aristas. Las tres formas son invariantes por la acción de A_5 y entre ellas se satisface la relación

$$T^2 = -H^3 + 1728 f^5.$$

De este modo, la ecuación del icosaedro $q(z) = u$, de grado 60, se escribe como

$$((z^{20}+1)-228(z^{15}-z^5)+494z^{10})^3+1728uz^5(z^{10}+11z^5-1)^5 = 0.$$

Klein utiliza dos métodos para hallar las raíces de esta ecuación. En el primero se vale de resultados de 1873 debidos a Schwarz para expresar las raíces como cocientes de series hipergeométricas. Su segundo método se basa en el uso de integrales elípticas: primero resuelve la ecuación $J(\tau) = u$; y después la ecuación $z = J(5,\tau)$, en donde $J(\tau) = 1/1728 \cdot j(\tau)$ y $J(5,\tau)$ es el módulo principal de nivel cinco. El método funciona gracias a la existencia de un diagrama conmutativo

$$\begin{array}{ccccc} \mathcal{H} & \to & \Gamma(5)\backslash\mathcal{H} & \hookrightarrow & \mathbf{P}^1 \\ & \searrow & \downarrow & & \downarrow \\ & & \Gamma(1)\backslash\mathcal{H} & \hookrightarrow & A_5\backslash\mathbf{P}^1. \end{array}$$

en donde $\Gamma(5)$ es el grupo principal de congruencia de nivel cinco y $\Gamma(1) = \mathbf{SL}(2,\mathbb{Z})$, el grupo modular de nivel 1.

Una vez resuelta la ecuación del icosaedro, Klein procede a la resolución de la ecuación de grado cinco en forma cerrada. El camino todavía es largo, pues partiendo de un polinomio general de grado cinco debe proceder a la construcción de una resolvente Z, la cual le proporciona el elemento $U = q(Z)$ del cuerpo base general, así como cinco funciones racionales $X_i = X_i(Z)$. Por especialización de los coeficientes, obtiene u. Resolviendo la ecuación del icosaedro, obtiene z y, con ello, las cinco raíces $x_i = x_i(z)$ de la quíntica. En la construcción de Z desempeña un papel fundamental la teoría de invariantes, que Klein había aprendido de P. Gordan.

El resultado principal de Klein puede resumirse del modo siguiente: Sea $k \subseteq \mathbb{C}$ un subcuerpo de los números complejos tal que contenga el grupo μ_5 de las raíces quintas de la unidad. Sea $K|k$ una extensión de Galois tal que $\mathrm{Gal}(K|k) \simeq A_5$. Por adjunción a k de un radical cuadrático, existe un elemento $u \in k'$ tal que cada solución de la ecuación del icosaedro $q(z) = u$

genera la extensión $K'|k'$. Además, cada solución z de $q(z) = u$ determina un isomorfismo

$$\rho : \mathrm{Gal}(K|k) \to \mathbf{PGL}(2, k'), \quad \rho(\sigma) = \begin{bmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{bmatrix},$$

de manera que

$$\sigma^{-1}(z) = \rho(\sigma)(z) = \frac{a(\sigma)z + b(\sigma)}{c(\sigma)z + d(\sigma)}, \quad \text{para cada } \sigma \in \mathrm{Gal}(K'|k').$$

El método de Klein es sumamente elegante, en cuanto que relaciona el grupo de isometrías del icosaedro con la teoría de Galois y con las funciones modulares elípticas.

Desde un punto de vista histórico, los resultados anteriores son de gran importancia, por cuanto que presagian el papel que desempeñarían la modularidad y las representaciones de Galois en los años venideros.

4.2.3. El *Sueño de Juventud* de Kronecker

En un artículo publicado en 1853, Kronecker manifestó haber obtenido el notable resultado que las soluciones de cualquier ecuación polinómica con coeficientes enteros y grupo de Galois abeliano son expresables como funciones racionales de raíces de la unidad:

> [...] ergibt nämlich das bemerkenswerthe Resultat: 'dass die Wurzel jeder Abel'schen Gleichung mit ganzzahligen Coëffizienten als rationale Function von Wurzeln der Einheit dargestellt werden kann'.
>
> L. Kronecker [89].

La intuición de Kronecker resultó ser correcta. Sin embargo, el camino hasta obtener una primera demostración del hecho de

que toda extensión abeliana del cuerpo racional es ciclotómica fue laborioso. Tal afirmación se conoce hoy con el nombre de teorema de Kronecker-Weber. Weber logró diversas demostraciones del mismo, no exentas de críticas. En 1896, Hilbert dio la primera prueba aceptada, que incluyó en su *Zahlbericht* un año después.

Los intentos posteriores relativos a la generalización del teorema de Kronecker-Weber dieron lugar al nacimiento de la teoría de la multiplicación compleja. A partir de unos pocos ejemplos en los que se sabía que los valores de división $\mathrm{sl}(\varpi/4)$, $f(\varpi/4)$, $F(\varpi/4)$ generaban extensiones abelianas de $\mathbb{Q}(i)$, Kronecker afirmó que *todas* las extensiones abelianas de $\mathbb{Q}(i)$ deberían poder obtenerse adjuntando valores de división $\mathrm{sl}(\varpi/N)$, $N \in \mathbb{N}$. No contento con ello, pensó en una posibilidad semejante cuando el cuerpo base es un cuerpo cuadrático imaginario cualquiera.

En una carta dirigida a Dedekind, fechada el 15 de marzo de 1880, Kronecker (que a la sazón contaba 57 años de edad) le comunica su satisfacción porque cree haber culminado, después de una investigación reemprendida más a fondo en los últimos meses, la última de una serie de dificultades que aún quedaban pendientes relativas a su *Sueño de Juventud* más querido; a saber: la demostración de que las ecuaciones abelianas con coeficientes cuadráticos imaginarios se agotan con las ecuaciones de transformación de las funciones elípticas, del mismo modo que las ecuaciones abelianas con coeficientes enteros lo hacen con las ecuaciones de división del círculo:

> Meinen besten Dank für Ihre freundlichen Zeilen vom 12.c.! Ich glaube darin einen willkommenen Anlass finden zu sollen, Ihnen mitzutheilen, dass ich heute die letzte von vielen Schwierigkeiten besiegt zu haben glaube, die dem Abschlusse einer Untersuchung, mit der ich mich in den letzten Monaten wieder eingehender beschäftigt habe, noch entgegenstanden. Es handelt sich um meinen liebsten Jugentraum, nämlich um den Nachweis, dass die

> Abel'schen Gleichungen mit Quadratwurzeln rationaler Zahlen durch die Transformations Gleichungen elliptischer Functionen mit singulären Moduln grade so erschöpft werden, wie die ganzzahligen Abel'schen Gleichungen durch die Kreistheilungsgleichungen.
>
> L. Kronecker [91].

La interpretación de estas palabras no estuvo exenta de controversia. A decir verdad, en otro pasaje clave de 1877 en el que había aludido a su Sueño de Juventud, Kronecker nos habla de dos tipos de números algebraicos para generar las extensiones abelianas de los cuerpos cuadráticos imaginarios: los módulos singulares, correspondientes a valores especiales de funciones modulares elípticas, y los valores de división, dados por funciones elípticas con módulo singular valoradas en argumentos relacionados racionalmente con los períodos.

La afirmación de que toda extensión abeliana de un cuerpo cuadrático imaginario se genera mediante módulos singulares y valores de división de funciones elípticas de módulo singular es correcta. Su demostración constituye el teorema de completitud de la teoría de la multiplicación compleja en el caso cuadrático imaginario.

El mismo Kronecker no llegó a demostrar el teorema de completitud. Weber, tampoco, si bien hizo con respecto al mismo notables avances. En 1901, T. Takagi demostró la validez del teorema de completitud cuando el cuerpo base es el cuerpo $\mathbb{Q}(i)$ de los racionales de Gauss. Para ello utilizó las sencillas propiedades de divisibilidad del anillo de los enteros de Gauss y un conocimiento explícito de las ecuaciones de división de las funciones lemniscáticas.

Las primeras demostraciones del teorema de completitud se gestaron en una serie de artículos de R. Fueter, publicados entre 1905 y 1927, en los que hay multitud de afirmaciones incorrectas que el propio autor va corrigiendo en trabajos sucesivos. Takagi logró dar una demostración del teorema de completitud en 1920.

El desarrollo de la teoría de la multiplicación compleja en el caso cuadrático imaginario corrió paralelo con el descubrimiento de la teoría de cuerpos de clases. Después de la etapa inicial protagonizada por Fueter y Takagi, la teoría de la multiplicación compleja en el caso cuadrático imaginario alcanzó su formulación actual entre los años 1940-1950. En este período, Hasse y Deuring lograron expresar sus resultados en términos de las funciones L de las curvas elípticas dotadas de multiplicación compleja.

Capítulo 5

Funciones zeta de cuerpos de números

En lo sucesivo, denotaremos por $\overline{\mathbb{Q}}$ una clausura algebraica de $\mathbb{Q}$ contenida en $\mathbb{C}$.

5.1. Enteros algebraicos

Alrededor de 1840, y casi simultáneamente, Eisenstein, Dirichlet y Hermite habían llegado a la noción de elemento entero algebraico: un elemento $\alpha \in \overline{\mathbb{Q}}$ se dice que es un entero algebraico si es raíz de una ecuación de la forma

$$X^n + a_{n-1}X^{n-1} + \cdots + a_n = 0, \quad a_i \in \mathbb{Z}.$$

El conjunto $\mathcal{O}_K$ de los enteros algebraicos contenidos en un cuerpo de números K constituye un anillo; los ideales de este anillo y sus unidades se designan con el nombre de ideales y unidades, respectivamente, del cuerpo K. Los primeros ejemplos de anillos de enteros son el propio $\mathbb{Z}$, el anillo $\mathbb{Z}[\zeta_4]$ de los enteros de Gauss y el anillo $\mathbb{Z}[\zeta_3]$ de los enteros de Eisenstein.

Un primer paso para comprender la aritmética de los anillos

de enteros es la determinación del grupo multiplicativo $\mathcal{O}_K^*$ de las unidades (o elementos inversibles) de $\mathcal{O}_K$. Este grupo contiene el subgrupo $\mu(K)$ de las raíces de la unidad contenidas en K. Pero en K puede haber unidades de orden infinito, como es el caso de los cuerpos cuadráticos reales $\mathbb{Q}(\sqrt{D})$, $D > 0$, cuyas unidades se determinan mediante la resolución de la ecuación de Pell $X^2 - DY^2 = \pm 1$. En general, las unidades ε de un cuerpo de números K son los elementos de $\mathcal{O}_K$ que satisfacen la ecuación nórmica $N_{K|\mathbb{Q}}(\varepsilon) = \pm 1$, de grado $n = [K : \mathbb{Q}]$.

En 1844, Eisenstein obtuvo una descripción del grupo de las unidades de los cuerpos cúbicos. En su tesis de 1845, Kronecker estudió las unidades de los cuerpos ciclotómicos. Ambos resultados fueron generalizados en 1848 por Dirichlet a cualquier cuerpo de números mediante su teorema de estructura de las unidades.

El teorema de Dirichlet de las unidades afirma que el grupo multiplicativo $\mathcal{O}_K^*$ es un grupo abeliano finitamente generado, del cual determina su rango; su subgrupo de torsión es óbviamente $\mu(K)$. Por medio de la inmersión logarítmica de K^*, Dirichlet identifica el grupo grupo cociente $\mathcal{O}_K^*/\mu(K)$ con un retículo de un espacio euclídeo del que demuestra que es de dimensión $r := r_1 + r_2 - 1$, siendo $n = r_1 + 2r_2$ la descomposición del grado de K proporcionada por el número r_1 de sus inmersiones reales y el número $2r_2$ de sus inmersiones complejas no reales. El punto clave para la determinación de r se encuentra en el hecho de que un determinante, R_K, formado con logaritmos de cierto sistema de unidades, es no nulo; R_K se denomina el regulador del cuerpo K. De este modo, Dirichlet demuestra la existencia de unidades fundamentales $\varepsilon_i \in \mathcal{O}_K^*$ tales que toda unidad ε de $\mathcal{O}_K$ se escribe de manera única en la forma

$$\varepsilon = \zeta \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}, \quad \zeta \in \mu(K),\ n_i \in \mathbb{Z}.$$

El paso siguiente en el estudio aritmético de los cuerpos de números fue la construcción por E. Kummer de su teoría de los números ideales para los anillos de enteros $\mathbb{Z}[\zeta_N]$ de los cuerpos ciclotómicos $\mathbb{Q}(\zeta_N)$. Kummer fue llevado al estudio de la divisi-

bildad en $\mathbb{Z}[\zeta_N]$ a raíz de sus investigaciones sobre a la ecuación de Fermat $X^N + Y^N = Z^N$. Los conceptos más importantes elaborados por Kummer son, aparte de su definición de números ideales, el estudio de las unidades ciclotómicas; la división de los números primos en regulares y en irregulares; la caracterización de éstos en términos de números de Bernoulli; el estudio de las leyes de reciprocidad de los cuerpos ciclotómicos, así como su demostración del teorema de Fermat para todos los exponentes primos regulares, además de sus múltiples aportaciones al caso irregular. Sin embargo, y a pesar de que sus investigaciones se extendieron a lo largo de toda su vida, Kummer no pudo demostrar haber establecido la veracidad del teorema de Fermat para una infinidad de exponentes primos. Todavía hoy se desconoce si el número de primos regulares es infinito; sin embargo, se ha demostrado que el número de primos irregulares es infinito.

La teoría de la divisibilidad creada por Kummer en los cuerpos ciclotómicos fue extendida por Dedekind y por Kronecker a cualquier cuerpo de números. Dedekind demostró que todo ideal no nulo del anillo de enteros $\mathcal{O}_K$ de un cuerpo de números descompone de manera única como producto de un número finito de ideales primos de este anillo. Los ideales primos $(0) \neq \mathfrak{p} \subseteq \mathcal{O}_K$ son maximales, por lo que los anillos de clases residuales $\mathcal{O}_K/\mathfrak{p}$ son cuerpos. Puesto que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo finitamente generado, dichos cuerpos residuales son finitos. Con la introducción de la noción de ideal fraccionario de K, el conjunto de todos los ideales (enteros y fraccionarios) se organiza como un grupo multiplicativo, I_K, que posee como subgrupo el grupo P_K formado por los ideales fraccionarios principales. Por un teorema debido a Minkowski, el grupo de clases de ideales $\mathrm{Cl}_K := I_K/P_K$ es un grupo abeliano finito; su número de elementos h_K es el denominado número de clases de K. El entero h_K mide lo lejos que está $\mathcal{O}_K$ de ser un dominio de ideales principales.

Un entero primo p se dice que ramifica en K cuando en la descomposición del ideal $p\mathcal{O}_K$ aparecen factores múltiples. El discriminante del cuerpo K es un ideal de $\mathbb{Z}$ divisible únicamen-

te por los ideales primos ramificados (afectados de exponentes convenientes).

Cuando el cuerpo K es cuadrático de discriminante D, el grupo de clases de ideales de K recupera el grupo de clases de formas cuadráticas binarias de discriminante fundamental D.

En el caso de los cuerpos ciclotómicos, los primos regulares en el sentido de Kummer son aquellos para los cuales p no divide al número de clases $h_{\mathbb{Q}(\zeta_p)}$.

5.1.1. Funciones zeta de Dedekind

Una herramienta fundamental para el estudio de los números primos es la función zeta de Riemann:

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1-\frac{1}{p^s}}, \quad \Re(s) > 1.$$

Por ser $\mathbb{Z}$ un dominio de factorización única, en la descomposición de esta función en producto de Euler aparecen todos los números primos exactamente una vez.

La teoría de ideales en los anillos de Dedekind permite asociar a todo cuerpo de números una función zeta, siguiendo el modelo establecido por Euler y por Riemann. La función zeta de Dedekind de un cuerpo de números K se define según

$$\zeta(K,s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}}, \quad \Re(s) > 1.$$

En ella, el sumatorio se extiende a todos los ideales $\mathfrak{a}$ no nulos de $\mathcal{O}_K$ y $N(\mathfrak{a}) = \#\mathcal{O}_K/\mathfrak{a}$ denota la norma del ideal $\mathfrak{a}$. Puesto que la serie anterior es uniformemente convergente en los compactos de $\Re(s) > 1$, la función zeta es holomorfa en este semiplano. La descomposición de los ideales no nulos de $\mathcal{O}_K$ como producto de un número finito de ideales primos, y de manera única, se traduce

en la expresión de la función ζ como producto de Euler en el que aparecen todos los ideales primos no nulos de $\mathcal{O}_K$ exactamente una vez. De la descomposición en forma de producto de Euler se deduce que $\zeta(K, s)$ no se anula para $\Re(s) > 1$.

Un carácter de Dirichlet χ módulo un entero $N \geq 1$ es un homomorfismo de grupos

$$\chi : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{C}^*.$$

A todo carácter de Dirichlet χ se le puede asociar una función L definida por

$$L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \Re(s) > 1.$$

El símbolo de Legendre puede interpretarse como un carácter de Dirichlet. Dado un discriminante fundamental D, definamos

$$\chi_D(p) := \left(\frac{D}{p}\right) \quad \text{si } p \neq 2 \text{ es un entero primo,}$$

$$\chi_D(2) := \begin{cases} 0, & \text{si } D \equiv 0 \pmod 4, \\ 1, & \text{si } D \equiv 1 \pmod 8, \\ -1, & \text{si } D \equiv 5 \pmod 8, \end{cases}$$

$$\chi_D(p_1^{n_1} \cdots p_s^{n_s}) := \chi_D(p_1)^{n_1} \cdots \chi_D(p_s)^{n_s}.$$

Además,

$$\chi_D(-1) := \begin{cases} 1 & \text{si } D > 0, \\ -1 & \text{si } D < 0. \end{cases}$$

La ley de reciprocidad cuadrática implica que χ_D es un carácter de Dirichlet módulo $|D|$.

Si K es un cuerpo cuadrático de discriminante D, se satisface que

$$\zeta(K, s) = \zeta(s) L(\chi_D, s),$$

proporcionando esta descomposición una interpretación analítica de la ley de reciprocidad cuadrática. El carácter χ_D suele designarse como carácter de Kronecker del cuerpo cuadrático.

Más generalmente, avancemos que las leyes de reciprocidad propias de las extensiones abelianas $K|\mathbb{Q}$ permiten descomponer la función zeta de Dedekind $\zeta(K,s)$ como producto de n funciones $L(\chi,s)$, siendo $n=[K:\mathbb{Q}]$.

5.1.2. El teorema de la progresión aritmética

Euler, Legendre y Gauss eran conscientes de que toda progresión aritmética $\{a+tN : t \geq 0\}$, en la que $\mathrm{mcd}(a,N)=1$, debía contener infinitos números primos. La demostración de este hecho, conocido como teorema de la progresión aritmética, es debida a Dirichlet.

Dado un discriminante fundamental D, mediante un uso adecuado del cálculo integral, Dirichlet determinó el valor de la función $L(\chi_D,s)$ en $s=1$. Para ello hizo uso de la teoría de la reducción de las formas cuadráticas binarias, debida a Gauss. Su resultado constituye la denominada fórmula analítica del número de clases en el caso cuadrático:

$$h(D)=\begin{cases} \dfrac{w\sqrt{|D|}}{2\pi}L(\chi_D,1), & \text{si } D<0, \\ \dfrac{\sqrt{D}}{\log\varepsilon_0}L(\chi_D,1), & \text{si } D>0. \end{cases}$$

En ella, w denota el número de raíces de la unidad contenidas en el cuerpo cuadrático imaginario y ε_0, la unidad fundamental del cuerpo cuadrático real.

En particular, de la fórmula analítica para el número de clases se deduce que

$$L(\chi_D,1)\neq 0, \quad \text{para todo } D.$$

A partir de este hecho, Dirichlet demostró que el conjunto de primos contenidos en una progresión aritmética de módulo N posee una densidad en el conjunto de todos los números primos igual a $1/\varphi(N)$, siendo $\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^*$. Es decir, los números primos que no dividen a N se reparten por igual entre las $\varphi(N)$ clases de restos del grupo multiplicativo $(\mathbb{Z}/N\mathbb{Z})^*$; en particular, cada clase contiene infinitos primos.

5.1.3. Fórmula analítica del número de clases

La función $\zeta(K, s)$ de Dedekind asociada a un cuerpo de números admite una prolongación analítica una función meromorfa del plano complejo; una vez completada con factores Γ adecuados, satisface una ecuación funcional; y posee un único polo, que es simple, en $s = 1$. En el caso de la función zeta de Riemann ($K = \mathbb{Q}$), la demostración de estos hechos es debida al propio Riemann. En el caso general, la demostración es debida a E. Hecke. La demostración de Hecke se basa en expresar la función zeta como una trasformada integral de funciones theta. La ecuación funcional de las funciones theta permite la obtención de la prolongación analítica de $\zeta(K, s)$.

El método de Hecke se extiende a las funciones $L(\chi, s)$ de Dirichlet y a las funciones $L(\psi, s)$ de Hecke, asociadas a caracteres más generales y de las que hablaremos más adelante.

Los cálculos de Dirichlet relativos a la fórmula analítica del número de clases de los cuerpos cuadráticos fueron generalizados por Hecke a cualquier cuerpo de números, obteniendo la celebrada fórmula analítica del número de clases de ideales. Mediante un cálculo de integrales múltiples, se obtiene que

$$\lim_{s\to 1}(s-1)\zeta(K,s) = \frac{2^{r_1}(2\pi)^{r_2}\, h_K\, R_K}{w_K\sqrt{|D_K|}}.$$

En ella, r_1 y $2r_2$ denotan el número de inmersiones reales y el número de inmersiones complejas no reales de K, respectivamente; h_K es el orden del grupo de clases de ideales K; R_K es el

regulador del cuerpo K (que mide el volumen de un paralelepípedo fundamental del grupo de las unidades); w_K es el número de raíces de la unidad contenidas en K; y $|D_K|$ es el valor absoluto del discriminante de K (que mide el volumen de un paralelepípedo fundamental del anillo de enteros).

La fórmula analítica del número de clases se considera una de las maravillas de la aritmética. En particular, en el caso $K = \mathbb{Q}$, el hecho de que el polo en $s = 1$ de la función zeta de Riemann sea de residuo 1,

$$\lim_{s \to 1}(s-1)\zeta(s) = 1,$$

sintetiza los hechos aritméticos siguientes: $\mathbb{Z}$ es un dominio de ideales principales ($h = 1$) que posee dos raíces de la unidad ($w = 2$) y ninguna unidad de orden infinito ($R = 1$); ningún ideal de $\mathbb{Z}$ es ramificado ($D = 1$); $\mathbb{Q}$ posee una única inmersión en $\mathbb{R}$ ($r_1 = 1$) y ninguna inmersión compleja no real ($r_2 = 0$).

5.2. La teoría de cuerpos de clases

La teoría de cuerpos de clases se encarga del estudio y de la clasificación de las extensiones abelianas de los cuerpos de números; es decir, de aquellas cuyo grupo de Galois es abeliano.

Entre los años 1896 y 1900 apareció una serie de trabajos de Hilbert en los que profundizaba en importantes conceptos, familiares a Kronecker y a Weber. Estas publicaciones de Hilbert contienen, por una parte, el estudio de los grupos de ramificación superior en las extensiones de Galois de los cuerpos de números y, por otra, la importante noción de cuerpo de clases. El llamado cuerpo de clases de Hilbert H de un cuerpo de números K es su extensión abeliana no ramificada maximal. Entre sus propiedades, destaquemos la existencia de un isomorfismo

$$I_K/P_K \simeq \mathrm{Gal}(H/K).$$

En particular, el grado del cuerpo de clases de Hilbert $[H : K]$ coincide con el número de clases h_K del cuerpo base. Otro hecho

a destacar de H es el teorema de los ideales principales, por el cual todos los ideales de K se convierten en principales al ser extendidos a H.

En el período comprendido entre 1900 y 1920, Takagi creó una teoría para las extensiones abelianas de los cuerpos de números en la cual, mediante grupos de clases generalizadas de ideales, identificaba todas las extensiones abelianas de cualquier cuerpo de números. Sin embargo su teoría adolecía de la falta de una ley de reciprocidad general.

Dado un cuerpo de números K y una métrica $|\ |_v$ del mismo, denotaremos por K_v el cuerpo completado de K en v. Si la métrica es no arquimediana, designaremos por $\mathcal{O}_v$ el anillo de enteros de K_v, que se obtiene por completación de $\mathcal{O}_K$. El anillo de adeles $\mathbb{A}_K$ es, por definición, el anillo que se obtiene como producto topológico restringido de los cuerpos K_v con respecto de los anillos $\mathcal{O}_v$, estando definidas las operaciones de suma y producto componente a componente. El grupo multiplicativo $\mathbb{I}_K := \mathbb{A}_K^*$ se denomina el grupo de las ideles de K. El anillo $\mathcal{O}_v$ es compacto, lo cual implica que K_v y $\mathbb{A}_K$ son localmente compactos. Esta construcción, genuina de C. Chevalley, permite integrar principios de carácter local-global en el tratamiento de problemas aritméticos.

5.2.1. El teorema de densidad de Chebotarev

El teorema de densidad de Chebotarev generaliza de una forma sorprendente el teorema de la progresión aritmética de Dirichlet. Se trata de un resultado que había sido conjeturado por Frobenius en 1880, en una carta dirigida a L. Stickelberger y a Dedekind. La primera demostración por G. Chebotarev fue publicada en ruso, en 1923; en 1925 apareció una versión en alemán.

El teorema de densidad de Chebotarev se suele demostrar hoy como un corolario de los teoremas de la teoría de cuerpos

de clases. Sin embargo, la primera demostración de Chebotarev no hacía uso de esta teoría sino que se basaba en un proceso de reducciones sucesivas a extensiones ciclotómicas en las que imitaba la demostración del teorema de la progresión aritmética de Dirichlet.

Consideremos un polinomio irreducible $f(X) \in \mathbb{Z}[X]$, de grado n; sea K su cuerpo de descomposición sobre $\mathbb{Q}$ y sea $G = \mathrm{Gal}(K|\mathbb{Q})$ su grupo de Galois. La acción de G sobre las raíces de f proporciona una representación de G como subgrupo del grupo simétrico S_n. Denotemos por $D(f)$ el discriminante de f. Para cada primo $p \nmid D(f)$, la descomposición de $f(X)$ en el anillo de polinomios $\mathbb{F}_p[X]$ (con coeficientes en el cuerpo finito $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$) carece de factores múltiples; con ello, si

$$f(X) = p_1(X) \cdots p_g(X), \quad p_i(X) \in \mathbb{F}_p[X],$$

es la descomposición de $f(X)$ en factores irreducibles, la suma de los grados n_i de los polinomios $p_i(X)$ debe ser igual a n. Escritos los grados en orden creciente, diremos que $(n_1, \ldots, n_g)$ es el tipo de la descomposición de f en p.

El teorema descubierto y probado por Frobenius afirma que, dado $f(X)$, los primos p para los cuales la reducción de $f(X)$ presenta un tipo de descomposición $(n_1, \ldots, n_g)$ poseen una densidad en el conjunto de todos los primos y que ésta es igual a $1/\#G$ veces el número de elementos $\sigma \in G$ para los cuales $\sigma \in S_n$ descompone como producto de ciclos disjuntos de longitudes $n_1, \cdots, n_g$. Este teorema no fue publicado por Frobenius hasta 1896, dos años después de que Dedekind hubiera dado a conocer su teoría de ideales.

Para entender la generalización que supone el teorema de densidad de Chebotarev frente al teorema de la progresión aritmética de Dirichlet, deben tenerse en cuenta dos hechos. Primero, que el grupo multiplicativo de las clases de restos $(\mathbb{Z}/N\mathbb{Z})^*$ es isomorfo al grupo de Galois del N-ésimo cuerpo ciclotómico $\mathbb{Q}(\zeta_N)$. Y, segundo, que el isomorfismo entre el grupo multiplicativo anterior y el grupo de Galois se obtiene al asignar a cada en-

tero m primo con N el automorfismo definido por $\sigma_m(\zeta_N) := \zeta_N^m$. Cuando $m = p$ es primo, $\sigma_p =: \mathrm{Frob}(\mathbb{Q}(\zeta_N)|\mathbb{Q}, p)$ es el denominado automorfismo de Frobenius.

Para toda extensión de Galois de cuerpos de números $L|K$, de grado n, la teoría de la ramificación de Hilbert asocia a cada ideal primo no nulo $\mathfrak{p} \subseteq \mathcal{O}_K$, que no divida al discriminante $D(L|K)$, el elemento de Frobenius $\mathrm{Frob}(L|K, \mathfrak{p})$. El elemento de Frobenius es una clase de conjugación de automorfismos $\sigma_{\mathfrak{P}}$ del grupo de Galois $G = \mathrm{Gal}(L|K)$. Los automorfismos $\sigma_{\mathfrak{P}}$ se caracterizan por

$$\sigma_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}, \quad \text{para todo } x \in \mathcal{O}_L.$$

Naturalmente, cuando la extensión $L|K$ es abeliana, las clases de conjugación en G son unitarias, por lo que el elemento de Frobenius es un automorfismo del grupo de Galois. En todos los casos, los elementos de Frobenius dan cuenta de la descomposición del ideal primo $\mathfrak{p}$ en producto de ideales primos del anillo de enteros $\mathcal{O}_L$: si esta descomposición es

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_{g_\mathfrak{p}},$$

entonces el grado residual en $\mathfrak{p}$, $f_\mathfrak{p} := n/g_\mathfrak{p}$, coincide con el orden de los elementos en la clase de conjugación $\mathrm{Frob}_\mathfrak{p}$. Así, $f_\mathfrak{p}$ es el menor entero positivo que satisface

$$\sigma_{\mathfrak{P}}^{f_\mathfrak{p}}(x) = x, \quad \text{para todo } x \in L, \ \mathfrak{P}|\mathfrak{p}.$$

Para asignar a cada ideal primo no ramificado $\mathfrak{p}$ su elemento de Frobenius, $\mathrm{Frob}(L|K, \mathfrak{p}) = [\sigma_{\mathfrak{P}}]$, debemos repartir el conjunto infinito de los ideales primos de K no ramificados en el conjunto finito de las clases de conjugación de $\mathrm{Gal}(L|K)$. Pues bien, el teorema de densidad de Chebotarev afirma que el reparto es proporcional: todas las clases de conjugación van a contener infinitos elementos y, además, las clases de conjugación con más elementos tendrán una densidad más alta de ideales primos. Concretamente, el teorema afirma que, para cada clase de conjugación C del

grupo de Galois $\mathrm{Gal}(L|K)$, la densidad, en el conjunto de todos los ideales primos de $\mathcal{O}_K$, de los ideales $\mathfrak{p}$ para los cuales $\mathrm{Frob}(L|K,\mathfrak{p}) = C$ es igual a $\#C/\#G$.

El teorema de densidad de Chebotarev es un resultado técnico que interviene en la obtención de numerosos resultados aritméticos. Las ideas básicas subyacentes en su demostración contribuyeron notablemente al avance de la teoría de cuerpos de clases.

5.2.2. Funciones L de Hecke

Las series L de Hecke están asociadas a caracteres de Hecke, que se definen sobre grupos de ideales de los anillos de enteros de los cuerpos de números.

Sea $\mathfrak{m} \subseteq \mathcal{O}_K$ un ideal entero de un cuerpo de números K, de grado n. Un carácter de Hecke módulo $\mathfrak{m}$ es un homomorfismo continuo

$$\chi : I_K^{\mathfrak{m}} \to S^1 = \{z \in \mathbb{C} : |z| = 1\},$$

en donde $I_K^{\mathfrak{m}}$ denota el grupo multiplicativo de los ideales fraccionario primos con $\mathfrak{m}$. El módulo de definición más pequeño se denomina el conductor del carácter.

A todo carácter de Hecke se le asocia una serie L definida por

$$L(\chi, s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s}}, \quad \Re(s) > 1.$$

El sumatorio se extiende a todos los ideales enteros no nulos y el producto a todos los ideales primos no nulos de $\mathcal{O}_K$. Entendemos que $\chi(\mathfrak{a}) = 0$ cuando $\mathfrak{a}$ y $\mathfrak{m}$ no sean coprimos. A fin de que las series L de Hecke admitan una prolongación analítica y satisfagan una ecuación funcional, es necesario imponer restricciones adicionales a los caracteres. Al imponer ciertas condiciones sobre

los lugares del infinito se obtienen los caracteres de Hecke de tipo $A_0 = (p, q)$. En tal caso, existen dos homomorfismos continuos

$$\chi_{\mathrm{f}} : (\mathcal{O}/\mathfrak{m})^* \to S^1, \quad \chi_\infty : \mathbb{R}^* \to S^1,$$

tales que

$$\chi((a)) = \chi_{\mathrm{f}}(a)\chi_\infty(a),$$

para todo $a \in \mathcal{O}_K$, $(a) \in I_K^{\mathfrak{m}}$ y de forma que

$$\chi_\infty(x) = N(x^p|x|^{-p+iq}).$$

Un carácter de Dirichlet módulo $\mathfrak{m}$ es un homomorfismo del grupo radial de clases de ideales módulo $\mathfrak{m}$ en la circunferencia unidad:

$$\chi : \mathrm{Cl}_K(\mathfrak{m}) := I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \to S^1.$$

Todo carácter de Dirichlet módulo $\mathfrak{m}$ da lugar a un carácter de Hecke $\chi : I_K^{\mathfrak{m}} \to S^1$ tal que $\chi(P_K^{\mathfrak{m}}) = 1$. Se trata de un carácter de Hecke de tipo $A_0 = (p, 0)$, ya que satisface una igualdad de la forma

$$\chi((a)) = \chi_{\mathrm{f}}((a))N(a^p|a|^{-p}),$$

para un cierto carácter χ_{f} de $(\mathcal{O}/\mathfrak{m})^*$. De hecho, los caracteres de Dirichlet módulo $\mathfrak{m}$ son, exactamente, los caracteres de Hecke módulo $\mathfrak{m}$ de tipo $A_0 = (p, 0)$. Los caracteres del grupo de las clases de ideales Cl_K son los caracteres de Hecke de tipo A_0 y $\mathfrak{m} = (1)$, para los cuales $\chi_\infty = 1$.

Dados un carácter de Hecke χ de tipo A_0, primitivo de módulo $\mathfrak{m}$, y una clase de ideales $A \in I_K/P_K$, se define la serie L parcial relativa a la clase A según

$$L(A, \chi, s) := \sum_{\mathfrak{a} \in A} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}, \quad \text{para } \Re(s) > 1.$$

La serie L asociada a χ descompone entonces en una suma finita de series L parciales

$$L(\chi, s) = \sum_A L(A, \chi, s),$$

donde A recorre el conjunto de las clases de ideales de K.

Conviene ahora que completemos las series L mediante factores de Euler en el infinito. Se define la serie L de Hecke completa

$$\Lambda(A, \chi, s) = (|D_K| N(\mathfrak{m}))^{s/2} L_\infty(\chi, s) L(A, \chi, s),$$

en donde

$$\begin{aligned} L_\infty(\chi, s) &= L_{\mathbb{R}}^{r_1} L_{\mathbb{C}}^{r_2}, \\ L_{\mathbb{R}}(s) &= \pi^{-s/2} \Gamma(s/2), \\ L_{\mathbb{C}}(s) &= 2(2\pi)^{-s} \Gamma(s). \end{aligned}$$

Entonces,

(i) La serie $\Lambda(A, \chi, s)$ admite una prolongación analítica a todo $\mathbb{C}$ y satisface la ecuación funcional

$$\Lambda(A, \chi, s) = W(\chi) \Lambda(A', \overline{\chi}, 1 - s),$$

donde $AA' = [\mathfrak{m} D_K]$ y $W(\chi)$ es una suma de Gauss normalizada para la cual $|W(\chi)| = 1$.

(ii) La función $\Lambda(A, \chi, s)$ es meromorfa y posee como singularidades, a lo sumo, un polo simple en $s = \mathrm{Tr}(-p + iq)/n$, $s = 1 + \mathrm{Tr}(p + iq)/n$.

(iii) Si $\mathfrak{m} \neq 1$ o bien $p \neq 0$, entonces la función $\Lambda(A, \chi, s)$ es entera.

Como corolario se obtiene que la serie $\Lambda(\chi, s)$ admite una prolongación holomorfa en

$$\mathbb{C} \setminus \{\mathrm{Tr}(-p + iq)/n, 1 + \mathrm{Tr}(p + iq)/n\}$$

y satisface la ecuación funcional

$$\Lambda(\chi, s) = W(\chi) \Lambda(\overline{\chi}, 1 - s).$$

Si $\mathfrak{m} \neq 1$ o bien $p \neq 0$, la serie de Hecke $\Lambda(\chi, s)$ admite una prolongación analítica a una función entera.

5.2.3. La ley de reciprocidad de Artin

En el Problema 9 de su lista de 1900, Hilbert planteó la formulación de una ley de reciprocidad general que fuera válida para cualquier cuerpo de números. Hilbert pensaba que la respuesta podía obtenerse a través del uso de su símbolo de residuos nórmicos.

En 1923, y en base a trabajos de Furtwängler, Takagi y Hasse, E. Artin descubrió un teorema que incluía como casos especiales todas las leyes de reciprocidad conocidas hasta aquella fecha. De hecho, y tal como él mismo explica, no pudo probar su resultado hasta tres años después, a partir de ideas utilizadas por Chebotarev en la demostración del teorema de densidad.

Para comprender la formulación de la ley de reciprocidad de Artin, debemos considerar nuevamente el automorfismo de Frobenius. En todo anillo conmutativo R de característica un número primo p, la aplicación elevar a la potencia p-ésima es un homomorfismo de anillos:

$$R \to R, \quad a \mapsto a^p.$$

Muchas leyes de la teoría de números se hacen patentes mediante formulaciones alternativas de la aplicación de Frobenius. Por ejemplo, el pequeño teorema de Fermat puede enunciarse diciendo que el automorfismo de Frobenius en las clases de restos $\mathbb{Z}/p\mathbb{Z}$ es la identidad:

$$a^p \equiv a \pmod{p}.$$

Por medio del homomorfismo de Frobenius, los símbolos de Legendre, Eisenstein, Hilbert encuentran su generalización en el denominado símbolo de Artin. Dada una extensión de Galois $L|K$ de cuerpos de números, el símbolo de Artin asocia a cada ideal primo $\mathfrak{p}$ de K la clase de conjugación en $\mathrm{Gal}(L|K)$ de los elementos de Frobenius: $\left(\dfrac{L|K}{\mathfrak{p}}\right) := \mathrm{Frob}(L|K, \mathfrak{p})$.

Si $L|K$ es una extensión abeliana de cuerpos de números, la

ley de reciprocidad de Artin establece un isomorfismo entre el grupo generalizado de clases de ideales de K asociado a L (en el sentido de Takagi) y el grupo de Galois $\mathrm{Gal}(L|K)$. En particular, si H es el cuerpo de clases de Hilbert de K, la ley de reciprocidad de Artin establece un isomorfismo

$$\mathrm{Cl}_K := I_K/P_K \to \mathrm{Gal}(H|K), \quad [\mathfrak{p}] \mapsto \left(\frac{H|K}{\mathfrak{p}}\right),$$

entre el grupo multiplicativo Cl_K de las clases de ideales de K y el grupo de Galois $G = G(H|K)$. Ante la presencia de ramificación, la misma ley de reciprocidad proporciona isomorfismos de la forma

$$\mathrm{Cl}_K^{\mathfrak{m}} := I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \simeq \mathrm{Gal}(K^{\mathfrak{m}}|K),$$

siendo $K^{\mathfrak{m}}$ el denominado cuerpo de clases radial módulo $\mathfrak{m}$.

En el caso $K = \mathbb{Q}$, el cuerpo de clases radial módulo un entero m es el cuerpo ciclotómico $\mathbb{Q}(\zeta_m)$. El teorema de Kronecker-Weber se generaliza al probar que, para todo cuerpo de números K, los cuerpos de clases radiales $K^{\mathfrak{m}}$ forman un sistema cofinal en el conjunto de las extensiones abelianas de K. Por definición el conductor de una extensión abeliana $L|K$ es el menor módulo $\mathfrak{m}$ de K tal que $K \subseteq L \subseteq K^{\mathfrak{m}}$.

Cuando el cuerpo base contiene las raíces ℓ-ésimas de la unidad y $L = K(\sqrt[\ell]{\alpha})$, el símbolo de Frobenius $\mathrm{Frob}(L|K, \mathfrak{p})$ es esencialmente el símbolo de residuos nórmico $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell$. La ley de reciprocidad de Artin implica que este símbolo depende únicamente de la clase de $\mathfrak{p}$. Al hacer explícita esta dependencia en casos particulares, se recuperan la ley de reciprocidad cuadrática, las leyes de reciprocidad de Eisenstein, de Herglotz, de Kummer y la fórmula del producto de Hilbert para los símbolos de residuos nórmicos.

Por tanto, la ley de reciprocidad de Artin proporciona una respuesta al Problema 9 de Hilbert que abarca todas las extensiones abelianas de los cuerpos de números. Hoy suele formularse a través de los grupos de clases de ideles (en el sentido de Chevalley) $\mathbb{C}_K$ de un cuerpo de números K. Dada una extensión de

cuerpos de números $L|K$, la ley de reciprocidad de Artin establece un isomorfismo

$$\mathbb{C}_K/N_{L|K}(\mathbb{C}_L) \simeq \mathrm{Gal}(L|K)^{\mathrm{ab}},$$

siendo $N_{L|K}$ la norma y G^{ab} el grupo abelianizado de un grupo G. La demostración suele hacerse por vía cohomológica, empleando los grupos de cohomología galoisiana de Tate de las clases de ideles. La ley de reciprocidad de Artin resulta de un isomorfismo de periodicidad

$$\hat{H}^i(\mathrm{Gal}(L|K), C_L) \simeq \hat{H}^{i+2}(\mathrm{Gal}(L|K), \mathbb{Z}),$$

el cual es consecuencia de que el sistema $(\mathrm{Gal}(\overline{K}|K), \mathrm{ind}\lim C_L)$ constituye una formación de clases en el sentido de Artin-Tate.

Otras demostraciones de dicha ley se logran por via analítica, y se basan en el empleo de funciones L. Tanto las demostraciones cohomológicas como las analíticas pueden deducir las leyes globales de leyes análogas probadas previamente en el caso local, es decir para los cuerpos $\mathfrak{p}$-ádicos $K_{\mathfrak{p}}$ que se obtienen por completación de los cuerpos de números en sus métricas arquimedianas y no arquimedianas. El uso de los grupos de ideles y de clases de ideles de Chevalley pone de relieve los principios locales-globales de la teoría de cuerpos de clases.

A pesar de sus casi cien años de existencia y de su carácter básico (pues está presente en la demostración de cualquier resultado aritmético de cierta profundidad) la teoría de cuerpos de clases sigue siendo una teoría difícil de asimilar y la exposición de sus demostraciones (con independencia del método que se siga) es siempre laboriosa.

5.2.4. Series L de Artin

Las series L de Artin son un objeto de una gran riqueza. Artin llegó al descubrimiento de la ley de reciprocidad a través de la introducción de estas funciones. A su vez, en la naturaleza de las

funciones L se encuentra una de las claves para una posible generalización no abeliana de la teoría de cuerpos de clases. Como el lector apreciará, las series L de Artin son una generalización muy imaginativa de las series $L(\chi, s)$ usadas por Dirichlet en su demostración del teorema de la progresión aritmética.

Sean $L|K$ una extensión finita y de Galois de cuerpos de números, V un $\mathbb{C}$-espacio vectorial de dimensión n y

$$\rho : G = \mathrm{Gal}(L|K) \to \mathrm{Aut}(V) \simeq \mathbf{GL}(n, \mathbb{C})$$

una representación lineal compleja de su grupo de Galois. Denotamos por

$$\chi_\rho : G \to \mathbb{C}, \quad \chi_\rho(\sigma) := \mathrm{Tr}\, \rho(\sigma),$$

el carácter de la representación ρ. Para cada ideal primo $\mathfrak{p}$ de K, sea $\mathfrak{P}|\mathfrak{p}$ un ideal primo de L. Denotemos por $I_\mathfrak{P}$ el grupo de inercia en $\mathfrak{P}$, según la teoría de la ramificación de Hilbert, y sea $V^{I_\mathfrak{P}}$ el subespacio de V fijo por la inercia. La serie L de Artin asociada a la representación ρ del grupo de Galois $\mathrm{Gal}(L|K)$ se define por el producto de Euler

$$L(\rho, s) := \prod_\mathfrak{p} \frac{1}{\det(1 - \rho(\varphi_\mathfrak{P}) N(\mathfrak{p})^{-s}; V^{I_\mathfrak{P}})}, \quad \text{para } \Re(s) > 1,$$

en donde $\varphi_\mathfrak{P} = \mathrm{Frob}(L|K, \mathfrak{P})$ en los ideales primos no ramificados.

La serie L de Artin asociada al carácter trivial $\mathbf{1}$ coincide con la función zeta de Dedekind del cuerpo K. Por un teorema debido a R. Brauer, relativo a la inducción de caracteres en grupos finitos, las series L de Artin se expresan como cocientes de productos de funciones L asociadas a caracteres de Hecke, por lo que se extienden a funciones meromorfas del plano y satisfacen una ecuación funcional. A la vista de este resultado, se impone completar las series L de Artin con factores gamma.

La denominada conjetura de Artin en este contexto se expresa diciendo que, para toda representación de Galois irreducible

$$\rho : \mathrm{Gal}(L|K) \to \mathbf{GL}(n, \mathbb{C}),$$

tal que $\chi_\rho \neq \mathbf{1}$, la serie de Artin $L(\rho, s)$ admite una prolongación analítica a una función entera.

En dimensión 1, la conjetura de Artin es cierta. Su validez es consecuencia de la ley de reciprocidad de Artin, pues ésta nos permite expresar toda función L de Artin abeliana como un producto de funciones L asociadas a caracteres de Hecke finitos: las representaciones irreducibles del grupo de Galois de una extensión abeliana se leen en las representaciones irreducibles de los correspondientes grupos de clases de ideales.

Aparte del caso abeliano, el carácter holomorfo de las funciones de Artin se ha podido demostrar en muy pocos casos. En los últimos años ha habido avances notables en la demostración de la conjetura de Artin en el caso de representaciones de Galois de dimensión 2, que han sido suficientes para la demostración del teorema de Fermat (por ejemplo, los teoremas de Langlands y de Tunnell para representaciones de Galois de dimensión 2 y de tipo tetraédrico u octaédrico).

La principal dificultad para la demostración de la conjetura de Artin estriba en tener suficientes funciones que permitan expresar $L(\rho, s)$ como una transformada integral. Como veremos al final de esta exposición, el Programa de Langlands predice donde deben encontrarse los correspondientes núcleos integrales.

Otra propiedad importante de las funciones L de Artin es que permiten factorizar las funciones zeta de Dedekind de los cuerpos de números. A partir de la descomposición del carácter r_G de la representación regular de $G = \mathrm{Gal}(L|K)$ como suma de caracteres irreducibles,

$$r_G = \sum_\chi \chi(1)\chi,$$

se obtiene que, para toda extensión de Galois $L|K$ de cuerpos de números, se satisface que

$$\zeta(L, s) = \zeta(K, s) \prod_{\chi \neq \mathbf{1}} L(\rho_\chi, s)^{\chi(1)},$$

en donde el producto se extiende a todas las representaciones irreducibles de $\mathrm{Gal}(L|K)$ no triviales.

Digamos para terminar esta sección que el uso de las funciones L de Artin permite una demostración cómoda del teorema de densidad de Chebotarev.

Capítulo 6

Problemas aritméticos

6.1. Series L de curvas elípticas

El estudio de los cuerpos de funciones elípticas sobre $\mathbb{C}$ derivó en el de las curvas elípticas complejas y, posteriormente, en el de las curvas elípticas definidas sobre un cuerpo arbitrario. Dado un cuerpo k, una curva elíptica E/k es una curva proyectiva, definida sobre k, regular, de género 1 y dotada de un punto k-racional, al menos. Su cuerpo de funciones tiene a k por cuerpo de constantes. Toda curva de estas características posee un modelo plano dado por una ecuación de Weierstrass $F(X,Y) = 0$, siendo

$$F(X,Y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6,\ a_i \in k.$$

La forma diferencial asociada es $\omega = dX/F_Y = -dY/F_X$. Se trata de una forma diferencial de primera especie que no se anula en ningún punto.

6.1.1. El teorema de Mordell

La conjetura de Poincaré, según la cual el grupo $E(\mathbb{Q})$ de puntos racionales de una curva elíptica $E/\mathbb{Q}$ es finitamente ge-

nerado, fue demostrada por Mordell en el año 1922. La demostración del teorema de Mordell se inicia probando la finitud del grupo cociente $E(\mathbb{Q})/2E(\mathbb{Q})$, necesaria para la generación finita del grupo $E(\mathbb{Q})$. La prueba depende de un método de descenso, que utiliza la noción de altura de los puntos de $E(\mathbb{Q})$. Estas alturas miden el número de dígitos necesarios para escribir las coordenadas de los puntos racionales $P = (x, y)$ de la curva.

Por el teorema de estructura de los grupos abelianos finitamente generados, $E(\mathbb{Q})$ posee una parte libre y una parte de torsión:

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}.$$

Por definición, el entero $r = \operatorname{rg} E(\mathbb{Q}) \geq 0$ es el rango aritmético de la curva elíptica. Se desconoce si r puede tender a infinito. Como comentaremos más adelante, el grupo de torsión de las curvas elípticas $E/\mathbb{Q}$ está mucho más controlado que su rango.

6.1.2. El teorema de Hasse

Artin, en su tesis de 1920, y Deuring, en la suya de 1931, se dedicaron el estudio aritmético de cuerpos de funciones algebraicas de una variable. Deuring intentó extender la teoría de la ramificación de Hilbert a estos cuerpos. Artin conjeturó el análogo de la hipótesis de Riemann para cuerpos de funciones elípticas sobre cuerpos de constantes finitos. Mientras que la hipótesis de Riemann hace referencia a las leyes que rigen la distribución de los números primos, en el caso de curvas elípticas sobre cuerpos finitos, la conjetura de Artin es equivalente a la obtención de cotas uniformes para el número de divisores primos de grado uno en tales curvas.

La denominada hipótesis de Riemann para cuerpos de funciones elípticas definidos sobre cuerpos de constantes finitos fue probada por Hasse en 1934 para curvas que se obtienen por reducción de curvas elípticas con multiplicación compleja y, en 1936, para curvas elípticas generales.

Hasse considera un cuerpo $K_0 = k_0(x, y)$ de funciones algebraicas de una variable, de característica un número primo p, de género 1, definido sobre un cuerpo de constantes finito k_0 de $q = p^f$ elementos. La función zeta asociada al mismo

$$L(s) := 1 - \frac{(q + 1 - N_1)}{q^s} + \frac{q}{q^{2s}}$$

da cuenta del número N_1 de divisores de primer grado de K_0. Mediante el cambio de variable $z = q^s$, se obtiene que

$$z^2 L(s) = P(z) = z^2 - (q + 1 - N_1)z + q.$$

El teorema de Riemann-Roch permite afirmar que

$$h = L(0) = P(1) = N_1,$$

siendo h el número de clases de divisores de grado cero de K_0.

Hasse considera el endomorfismo de K_0 definido por

$$\pi : (x, y) \mapsto (x^q, y^q);$$

y demuestra que satisface una ecuación cuadrática de la forma

$$Q(\pi) = \pi^2 - \ell\pi + q, \quad \ell^2 \leq 4q.$$

El resultado final se obtiene a partir de la igualdad de los polinomios $P(z) = Q(z)$, la cual proporciona la desigualdad:

$$(q + 1 - N_1)^2 \leq 4q.$$

6.1.3. La conjetura de Hasse-Weil

Siguiendo el modelo proporcionado por la función zeta de Riemann en el estudio de los números primos, Hasse asoció a toda curva elíptica $E/\mathbb{Q}$ una serie

$$L(E/\mathbb{Q}, s) := \prod_p \frac{1}{1 - a_p(E)p^{-s} + \psi(p)p^{1-2s}}, \quad \Re(s) > 3/2,$$

en donde

$$a_p := p + 1 - \#\widetilde{E}(\mathbb{F}_p),$$

y ψ es el carácter trivial módulo un cierto entero N_E. La serie L contiene información aritmética de E, ya que en su definición intervienen los números de puntos de las reducciones $\widetilde{E}$ en los diferentes primos. Puesto que, por el teorema de Hasse, se satisface que $|a_p| < 2p^{1/2}$, el producto infinito converge absolutamente y uniformemente sobre los compactos situados en el semiplano $\Re(s) > 3/2$. Por tanto, $L(E, s)$ define una función holomorfa y sin ceros en el semiplano mencionado.

Como en el caso de la función zeta de Riemann, la función L debe completarse con factores proporcionados por la función Γ de Euler:

$$\Lambda(E/\mathbb{Q}, s) := N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E/\mathbb{Q}, s), \quad \Re(s) > 3/2.$$

La constante N_E se determina por medio de los símbolos de Kodaira de las fibras de mala reducción de la curva, y se denomina el conductor aritmético de E.

En el año 1967, y por analogía con la función zeta de Riemann, Hasse y Weil conjeturaron que la función $\Lambda(E/\mathbb{Q}, s)$ debía admitir una prolongación analítica a una función entera y satisfacer una ecuación funcional de la forma

$$\Lambda(E/\mathbb{Q}, 2 - s) = \mathrm{w}(E)\Lambda(E/\mathbb{Q}, s), \quad s \in \mathbb{C}, \quad \mathrm{w}(E) = \pm 1.$$

Debido a esta simetría, la región $0 \leq \Re(s) \leq 2$ se denomina la banda crítica y $\Re(s) = 1$, la recta crítica de la función L.

La conjetura de Hasse-Weil fue demostrada por Deuring en el caso de las curvas elípticas con multiplicación compleja. Posteriormente se vería que la conjetura es cierta para todas las curvas elípticas $E/\mathbb{Q}$ parametrizables analíticamente por funciones modulares.

Uno de los artículos más importantes de Deuring es el publicado en 1941 sobre el tipo de anillos de multiplicadores de los

cuerpos de funciones elípticas. A raíz de una segunda demostración de la hipótesis de Riemann para cuerpos de funciones elípticas, Hasse había probado en 1936 que la clase de isomorfía del álgebra de multiplicadores $\mathrm{End}(E/k) \otimes \mathbb{Q}$ de una curva elíptica puede ser de tres tipos: (i) el cuerpo $\mathbb{Q}$ de los números racionales; (ii) un cuerpo cuadrático imaginario; (iii) un álgebra de cuaternios definida. Este último tipo sólo puede presentarse cuando el cuerpo de constantes es de característica positiva (lo cual explica que esta estructura no se halle presente en los trabajos de Abel sobre multiplicadores de diferenciales elípticas de primera especie). En su trabajo, Deuring va mucho más allá y determina la estructura del anillo $R = \mathrm{End}(E/k)$. Ésta puede ser: (i) el anillo $\mathbb{Z}$ de los números enteros; (ii) un orden en un cuerpo cuadrático imaginario de conductor primo con la característica p del cuerpo de funciones elípticas, siendo además p un ideal que descompone completamente en el cuerpo cuadrático de las multiplicaciones; (iii) un orden maximal en el álgebra de cuaternios sobre $\mathbb{Q}$ de discriminante igual a $p\infty$. Además, en los casos (ii), (iii) el invariante j de E es absolutamente algebraico; es decir, algebraico sobre el cuerpo primo de k. En el caso (iii) tiene además grado ≤ 2. La presencia del tipo (iii) está condicionada asimismo a que $k(E)$ carezca de clases de divisores de orden p, en cuyo caso la curva elíptica se denomina supersingular.

Para la demostración de los resultados anteriores, Deuring debió proceder al traslado de resultados conocidos en característica cero a característica positiva. Paulatinamente, se presentaron fenómenos ligados a la buena reducción de las curvas elípticas, pudiendo ser ésta ordinaria o supersingular, según se tenga la presencia o no de puntos de p-torsión.

6.2. Resultados de transcendencia

De forma paralela al avance en el conocimiento de los números algebraicos, se produjo un avance en el conocimiento de

los números transcendentes. Si bien la teoría de conjuntos de G. Cantor permite afirmar que los números algebraicos son un subconjunto numerable del conjunto de los números complejos, de ello no se puede deducir la transcendencia de ningún número concreto.

Los primeros resultados de transcendencia son de 1844 y debidos a J. Liouville. Para todo número algebraico irracional $\alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$, Liouville demostró que existe una constante positiva $c = c(\alpha) > 0$ tal que

$$\frac{c}{q^d} \leq \left| \alpha - \frac{p}{q} \right|,$$

para todo $p/q \in \mathbb{Q}$, siendo $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

El resultado anterior motivó la definición siguiente: un número $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ se dice que es de Liouville si existe una sucesión de números racionales $\{p_n/q_n\}_{n \geq 1}$ tal que

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^n}.$$

Por tanto, los números de Liouville son números reales que se aproximan muy bien por racionales. Un ejemplo lo constituye el número

$$\sum_{n=1}^{\infty} 10^{-n!} = 0{,}11000100000000000000000010...$$

El primer resultado de transcendencia obtenido fue que todo número de Liouville es transcendente. Sin embargo, ni el número e ni el número π son de Liouville.

Como es bien sabido, Lindemann probó en 1882 la transcendencia de e y de π. Partiendo de la identidad de Euler $e^{i\pi} = -1$, la demostración de la transcendencia de π se encamina a probar que si π fuera algebraico, existiría una función $J(x)$ que, evaluada en los enteros primos p, satisfacería las desigualdades

$$(p-1)! \leq |J(p)| \leq c^p,$$

siendo $c > 0$ una constante. Pero las desigualdades anteriores son contradictorias si p es suficientemente grande. La demostración de la transcendencia de e puede hacerse de forma parecida.

Lindemann (1882) y Weierstrass (1885) mejoraron los resultados anteriores probando que, dados n números algebraicos distintos $\alpha_1, \ldots, \alpha_n$ en $\overline{\mathbb{Q}}$, los valores tomados en estos argumentos por la función exponencial

$$e^{\alpha_1}, \ldots, e^{\alpha_n}$$

son $\overline{\mathbb{Q}}$-linealmente independientes. Equivalentemente, dados $\alpha_i \in \overline{\mathbb{Q}}$ linealmente independientes sobre $\mathbb{Q}$, entonces las exponenciales $e^{\alpha_1}, \ldots, e^{\alpha_n}$ son algebraicamente independientes sobre $\overline{\mathbb{Q}}$.

Como corolario del resultado anterior se obtiene que si α es un número real algebraico no nulo, entonces $\sin\alpha$ y $\log\alpha$ son transcendentes. A su vez, si α es un número algebraico no real, entonces $\Re(e^\alpha)$ y $\Im(e^\alpha)$ son transcendentes; si α es un número algebraico no nulo, entonces $\tan\alpha$ es transcendente.

Los resultados mencionados, así como otros análogos, permiten formular un principio por el cual las funciones transcendentes (sobre $\mathbb{C}(z)$) tienden a tomar valores transcendentes en argumentos algebraicos no especiales.

En el Problema 7 de su lista, Hilbert pidió demostrar la transcendencia de α^β, para todo α algebraico, $\alpha \neq 0, 1$, y todo β irracional algebraico. Equivalentemente, dados $x, y \in \mathbb{C}$, $y \notin \mathbb{Q}$, se pedía demostrar que

$$\operatorname{gr\,tr}_{\mathbb{Q}} \overline{\mathbb{Q}}\,(y, e^x, e^{xy}) \geq 1.$$

Con ello resultaría que dados α, β elementos algebraicos no nulos, si $\log\alpha$, $\log\beta$ son $\mathbb{Q}$-linealmente independientes, entonces $\log\alpha, \log\beta$ son $\overline{\mathbb{Q}}$-linealmente independientes.

La resolución del Problema 7 de Hilbert fue obtenida por A. Gelfond y T. Schneider en 1934. La demostración de Gelfond usa una función auxiliar, $F(z) = P(e^z, e^{\beta z})$, con un cero de multiplicidad alta. La demostración de Schneider usa una función

auxiliar, $G(z) = Q(z, e^{z \log \alpha})$, con muchos ceros de multiplicidad uno.

Ideas similares permiten probar el teorema de las seis exponenciales, debido a Lang (1966), por el cual, dados dos conjuntos $\{x_1, x_2\}$, $\{y_1, y_2, y_3\}$ de numeros complejos $\mathbb{Q}$-linealmente independientes, se satisface que

$$\operatorname{gr} \operatorname{tr}_{\mathbb{Q}} \overline{\mathbb{Q}}(e^{x_1 y_1}, e^{x_1 y_2}, e^{x_1 y_3}, e^{x_2 y_1}, e^{x_2 y_2}, e^{x_2 y_3}) \geq 1.$$

A. Thue, C. L. Siegel y K. F. Roth mejoraron el teorema de Liouville. En 1955, Roth probó que, para todo número algebraico no racional α y para todo $\varepsilon > 0$, la desigualdad

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon}}$$

se satisface únicamente para un número finito de enteros p, q primos entre si. Por tanto, existe una constante $c = c(\alpha, \varepsilon) > 0$ tal que

$$\frac{c}{q^{2+\varepsilon}} < \left| \alpha - \frac{p}{q} \right|,$$

para todo $p/q \in \mathbb{Q}$. En 1958, Roth recibió la Medalla Fields por este resultado.

6.2.1. Transcendencia de períodos

El teorema de Lindemann relativo a la transcendencia de π es un resultado de transcendencia de períodos: dado el retículo de períodos $\Lambda = \mathbb{Z} \cdot 2\pi$ de la función exponencial e^{iz}, el teorema nos dice que todo elemento no nulo del mismo es transcendente.

En 1937, el teorema de Lindemann fue extendido por Schneider obteniendo resultados de transcendencia para períodos de ciertas funciones elípticas. Concretamente, si $\Lambda = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$ designa un retículo de períodos de una función $\wp(\Lambda, z)$ de Weierstrass que satisface una ecuación diferencial

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

con coeficientes algebraicos: $g_2, g_3 \in \overline{\mathbb{Q}}$, entonces todo período no nulo de $\wp$ es transcendente.

En esta línea, se tienen asimismo resultados de transcendencia de arcos elípticos y de arcos lemniscáticos.

Dada una elipse de semiejes algebraicos

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \quad 0 < b < a, \quad a, b \in \overline{\mathbb{Q}},$$

entonces los arcos de extremos algebraicos

$$s(x_0, x_1) = \int_{x_0}^{x_1} \sqrt{\frac{a^2 - \varepsilon^2 x^2}{a^2 - x^2}}\, dx, \quad x_0, x_1 \in \overline{\mathbb{Q}},$$

en donde $\varepsilon^2 := 1 - b^2/a^2$, son transcendentes.

Dada una lemniscata $(x^2+y^2)^2 = 2a^2(x^2-y^2)$, de parámetro algebraico $0 < a \in \overline{\mathbb{Q}}$, entonces los arcos de extremos algebraicos, $x, x_1 \in \overline{\mathbb{Q}}$,

$$s(x_0, x_1) = a\sqrt{2} \int_{x_0}^{x_1} \frac{dt}{\sqrt{1-t^4}}, \quad t^2 := \frac{x^2 - y^2}{x^2 + y^2},$$

son transcendentes: $s(x_0, x_1) \notin \overline{\mathbb{Q}}$.

En particular, al tener en cuenta el valor de los períodos de la curva elíptica $Y^2 = 4X^3 - 4$,

$$4 \int_0^1 \frac{dt}{1-t^4} = 4\varpi = \frac{1}{\sqrt{2\pi}} \Gamma^2(\frac{1}{4}),$$

se obtienen el siguiente resultado de transcendencia:

$$\pi^{-1/4}\Gamma(1/4) \notin \overline{\mathbb{Q}},$$

en el que aparece el valor de la función Γ de Euler en $s = 1/4$, afectado por una potencia de π.

Consideremos una curva algebraica irreducible $\mathcal{C}$, de género $g > 1$, definida sobre el cuerpo $\overline{\mathbb{Q}}$ de los números algebraicos.

Consideremos su primer grupo de homología entera $H_1(\mathcal{C},\mathbb{Z}) = \langle\gamma_1,\cdots,\gamma_{2g}\rangle$. Sea φ una de las $2g$ diferenciales de segunda especie. En 1941, Schneider demostró que uno al menos de los $2g$ períodos

$$\eta_k := \int_{\gamma_k} \varphi, \quad 1 \leq k \leq 2g,$$

es transcendente. De ello se deduce la transcendencia de valores especiales de la función beta de Euler. Dados $a, b \in \mathbb{Q}$ tales que $a, b, a+b \notin \mathbb{Z}$, entonces

$$B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} \notin \overline{\mathbb{Q}},$$

pues basta tener en cuenta que

$$B(a,b) = \int_0^1 x^{a-1}(1-x)^{b-1}dx.$$

6.2.2. Independencia algebraica

En los años 1970, G. Chudnovsky mejoró los resultados de transcendencia de períodos, anteriormente mencionados, obteniendo resultados de independencia algebraica. Dada una curva elíptica $E/\overline{\mathbb{Q}}$,

$$Y^2 = 4X^3 - g_2X - g_3, \quad g_2, g_3 \in \overline{\mathbb{Q}},$$

y dotada de multiplicación compleja, Chudnovsky demostró que, para todo período $\lambda \in \Lambda(E)$, $\lambda \neq 0$, los números π y λ son algebraicamente independientes sobre $\overline{\mathbb{Q}}$. De este modo, al tener en cuenta la evaluación de los períodos de las curvas elípticas $Y^2 = 4X^3 - 4$, $Y^2 = 4X^3 - 4X$,

$$4\int_0^1 \frac{dt}{1-t^4} = \frac{\Gamma^2\left(\frac{1}{4}\right)}{\sqrt{2\pi}}, \quad 4\int_9^\infty \frac{dt}{4x^3-4} = \frac{\Gamma^3\left(\frac{1}{3}\right)}{\pi},$$

se deduce que $\Gamma(1/4)$ y $\Gamma(1/3)$ son transcendentes. Por tanto, en aquel momento se sabía que $\Gamma(1/2)$, $\Gamma(1/3)$, $\Gamma(1/4)$, $\Gamma(2/3)$ y $\Gamma(3/4)$ son transcendentes.

La teoría de la multiplicación compleja garantiza que si $\tau \in \mathcal{H}$ es un irracional cuadrático, entonces $j(\tau) \in \overline{\mathbb{Q}}$. En 1937, Schneider demostró que, dadas dos funciones de Weierstrass algebraicamente independientes

$$\wp(z) = \wp(g_2, g_3; z), \quad \wp^*(z) = \wp(g_2^*, g_3^*; z),$$

entonces

$$\operatorname{gr\,tr}_{\mathbb{Q}} \overline{\mathbb{Q}}(g_2,\ g_3,\ g_2^*,\ g_3^*,\ \wp(z_0),\ \wp^*(z_0)) \geq 1,$$

para todo z_0 no período de $\wp$ ni de $\wp^*$. Del resultado de Schneider se deduce que si $\tau = \lambda_2/\lambda_1 \in \overline{\mathbb{Q}}$ es el módulo de una curva elíptica para el cual la función j toma valores algebraicos:

$$j(\tau) = 1728\frac{g_2^3(\tau)}{g_2^3(\tau) - 27g_3^2(\tau)} \in \overline{\mathbb{Q}},$$

entonces necesariamente τ es un irracional cuadrático; es decir, $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$.

6.2.3. Períodos de curvas elípticas con MC

En la producción de A. Selberg se encuentra un único trabajo en colaboración: su trabajo con S. Chowla, de 1967, basado en una breve nota de ambos autores, de 1949. El artículo de Selberg y Chowla versa sobre la función zeta de Epstein y en él mejoran una fórmula obtenida por Deuring en 1933.

Dada una forma cuadrática binaria $Q = (a, b, c)$, la función zeta de Epstein se define por

$$Z(Q, s) := \sum_{m,n} \frac{1}{Q(m,n)^s}, \quad \Re(s) > 1,$$

en donde el sumatorio se extiende a todos los pares de enteros $(m, n) \neq (0, 0)$. La función $Z(Q, s)$ admite una prolongación analítica a una función meromorfa de $\mathbb{C}$ con un polo simple en $s = 1$.

En su trabajo, Chowla y Selberg obtienen una fórmula referente a los períodos de las funciones elípticas dotadas de multiplicación compleja. (Al parecer, al mismo resultado habría llegado previamente M. Lerch, un alumno de Weierstrass.)

Sea $\{Q_j(X,Y) = (a_j, b_j, c_j)\}$, $1 \leq j \leq h$, un sistema de representantes de las clases de formas cuadráticas binarias de discriminante fundamental $D < 0$. A partir de la igualdad

$$\sum_{j=1}^{h} Z(Q_j, s) = w\zeta(s)L(\chi_D, s)$$

y del cálculo de los primeros términos del desarrollo de ambas series, Chowla y Selberg obtienen que

$$\prod_{j=1}^{h} \Delta(\tau_j) = \left(\frac{2\pi}{|D|}\right)^{6h} \prod_{j=1}^{h} a_j^6 \left\{ \prod_{m=1}^{|D|} \Gamma\left(\frac{m}{|D|}\right)^{\chi_D(m)} \right\}^{3w},$$

en donde los elementos τ_j son los ceros de las formas cuadráticas binarias situados en el semiplano superior:

$$Q_j(\tau_j, 1) = 0, \quad \tau_j \in \mathcal{H},\ 1 \leq j \leq h(D).$$

En la fórmula de Chowla-Selberg intervienen la forma modular discriminante Δ, el carácter de Kronecker χ_D y el número de raíces de la unidad w contenidas en el cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{D})$.

Por resultados que hemos recordado, era conocido que los períodos de las curvas elípticas con multiplicación compleja por $\mathbb{Q}(i)$ y por $\mathbb{Q}(\rho)$ son expresables por medio de valores de la función Γ en argumentos racionales. Tal como se pondrá de manifiesto a continuación, la fórmula de Chowla-Selberg generaliza este resultado clásico.

Dados dos números complejos no nulos $a, b \in \mathbb{C}^*$, escribiremos $a \sim b$ para indicar que a, b pertenecen a la misma clase de transcendencia; es decir que $ab^{-1} \in \overline{\mathbb{Q}}^*$ o, equivalentemente, que ambos coinciden salvo el producto por números algebraicos.

La teoría clásica de la multiplicación compleja nos dice que la función j toma valores algebraicos en argumentos cuadráticos imaginarios situados en el semiplano superior complejo: si $\tau \in \mathbb{Q}(\sqrt{D}) \cap \mathcal{H}$, entonces $j(\tau) \in \overline{\mathbb{Q}}$. En tal caso, y puesto que la función modular $j(z)$ se expresa como función racional de la función modular $k(z)$, el modelo de Jacobi de la curva elíptica asociada a τ,

$$E : Y^2 = (1 - X^2)(1 - k(\tau)X^2),$$

está definido sobre $\overline{\mathbb{Q}}$. Observemos que $\Lambda(E) = \langle 4K(\tau), 4K(\tau)\tau \rangle$. El modelo de Weierstrass asociado a este retículo estará definido sobre $\overline{\mathbb{Q}}$. Por el teorema de Chudnovsky, para todo período no nulo $\lambda \in \Lambda(E)$, los números λ y π son algebraicamente independientes. Puesto que

$$\Delta(\tau) \sim K(\tau)^{12}, \quad \Delta(\tau_i) \sim \Delta(\tau_j), \quad \text{para } 1 \leq j \leq h(D),$$

y, por Chowla-Selberg, $K(\tau) \sim (\pi \cdot \pi_D)^{1/2}$, en donde

$$\pi_D := \prod_{m=1}^{|D|} \left\{ \Gamma\left(\frac{m}{|D|}\right)^{\chi_D(m)} \right\}^{\frac{w}{2h}},$$

se sigue que π_D es transcendente. Con ello hemos puesto de manifiesto que la fórmula de Chowla-Selberg, unida al teorema de Chudnovsky, permite identificar la clase de transcendencia de los períodos de las curvas elípticas con multiplicación compleja.

En 1978, D. Gross dio una demostración alternativa de la fórmula de Chowla-Selberg, aunque menos precisa que la inicial. Gross dedujo su fórmula a partir del estudio de los períodos de las formas diferenciales regulares definidas por las curvas de Fermat.

6.3. Problemas aritméticos en género superior

6.3.1. La conjetura de Mordell

Después de probar la conjetura de Poincaré relativa a la estructura del grupo de puntos racionales de las cúbicas definidas sobre $\mathbb{Q}$, Mordell conjeturó en 1922 que para toda curva proyectiva $\mathcal{C}$, no singular, de género $g \geq 2$, definida sobre un cuerpo K de números, el conjunto de sus puntos K-racionales $\mathcal{C}(K)$ debía ser finito.

En 1927, A. Weil se fijó como objetivo para su tesis doctoral la demostración de la conjetura de Mordell. Utilizando ideas que se remontaban a Abel y Jacobi, Weil intentó atacar el problema sumergiendo la curva de partida en una variedad algebraica lo más pequeña posible en la que se pudiera llevar a cabo la adición de puntos; es decir, en su jacobiana. Weil pudo generalizar la conjetura de Poincaré sobre las cúbicas probando la generación finita del grupo abeliano $A(K)$ para cualquier variedad abeliana A/K, definida sobre un cuerpo de números K. Pero ello fue insuficiente para resolver el problema planteado por Mordell.

Debido a que el estudio aritmético de las variedades abelianas estaba en sus comienzos, el esfuerzo de Weil en aquella ocasión fue enorme. Tuvo que crear una teoría de alturas en variedades abelianas para practicar a su vez el descenso infinito. Y, lo que constituía la mayor dificultad, la geometría algebraica no disponía todavía de un lenguaje adecuado para el tratamiento de los problemas aritméticos.

La conjetura formulada por Mordell para las curvas de género $g \geq 2$ fue criticada por Weil en el sentido de que era una afirmación que lo mismo podía ser cierta que falsa, pues de la misma se tenía una evidencia numérica muy escasa.

Un posible indicio sobre la posible veracidad de la conje-

tura de Mordell se obtuvo en 1965 a través de un trabajo de D. Mumford que pasó casi desapercibido. En él se probaba que la altura de los puntos racionales de las curvas de género $g \geq 2$ presenta como mínimo un crecimiento exponencial. Tal hecho no ocurre en las curvas de género menor y en ello podía hallarse un indicio por el cual las curvas de género alto no pueden albergar un número demasiado grande de puntos racionales.

6.3.2. El teorema de Siegel

Si se consideran curvas afines definidas sobre cuerpos de números, en lugar de curvas proyectivas, tiene sentido distinguir entre sus puntos racionales y sus puntos de coordenadas enteras

En 1929, Siegel demostró un resultado parcial en favor de la conjetura de Mordell. Siegel demostró que, para toda curva afín $\mathcal{C}/K$ definida sobre un cuerpo de números y de género $g > 0$, el conjunto $\mathcal{C}(\mathcal{O}_K)$ de sus puntos de coordenadas enteras es finito. La demostración de Siegel de este teorema se basa en una combinación del teorema de aproximación diofántica de Thue-Siegel-Roth, juntamente con la versión del teorema de Mordell-Weil para variedades abelianas, puesto que aplicaba dicho teorema a la jacobiana de la curva $\mathcal{C}$. El teorema de Siegel no es efectivo, pues no permite calcular ni los puntos de coordenadas enteras ni su número. Teoremas de efectividad en casos muy particulares fueron obtenidos por A. Baker como corolario de sus impresionantes trabajos sobre medidas de transcendencia en formas lineales en logaritmos, que le valieron la Medalla Fields en 1970.

Capítulo 7

Series L de variedades aritméticas

7.1. Variedades aritméticas

Alrededor de los años 1950, se inició una transición de los métodos clásicos de la teoría de números hacia los métodos que caracterizarían su desarrollo subsiguiente. El lenguaje empleado en 1946 por A. Weil en su libro *Foundations of Algebraic Geometry* había favorecido el desarrollo de una geometría algebraica sobre cuerpos no algebraicamente cerrados. Posteriormente, la creación de la teoría de esquemas por parte de A. Grothendieck conllevó el desarrollo de una geometría algebraica sobre anillos, adecuada para la formulación de problemas aritméticos.

Los cuerpos de funciones abstractos con cuerpos de constantes dados por cuerpos de números se interpretaron, primeramente, como cuerpos de funciones de variedades algebraicas y, más adelante, como las fibras genéricas de esquemas definidos sobre anillos de enteros, subanillos, o bien sus localizados. Por paso a las fibras cerradas, se obtuvieron esquemas definidos sobre cuerpos finitos. Por paso a los completados, esquemas definidos sobre cuerpos locales $\mathfrak{p}$-ádicos.

En cierta forma, los cálculos concretos del pasado que implicaban una gran destreza en el manejo de elaboradas fórmulas decayeron en favor de desarrollos mucho más conceptuales. Los textos se llenaron de sucesiones exactas, diagramas conmutativos, functores representables, espacios de módulos, haces, grupos de homología y de cohomología. Una de las nociones más influyentes fue, sin duda, la creación por parte de Grothendieck de la topología étale de esquemas (en la cual los abiertos ni siquiera deben estar sumergidos en el espacio) y de las cohomologías ℓ-ádicas asociadas, que parecían engullir de una vez por todas los antiguos trabajos sobre puntos de división.

Todavía debíamos asistir a otro cambio significativo bajo el punto de vista conceptual: el producido a partir de los años 1980 con la creación de la denominada geometría de Arakelov. Los objetos principales de estudio de esta teoría son los esquemas aritméticos, que resultan de completar los esquemas algebraicos mediante fibras arquimedianas, las cuales son tratadas mediante métodos propios de la geometría de los números, cuyo origen se remonta a Minkowski.

7.1.1. Funciones zeta locales

Poco después de haber presentado su tesis doctoral, Deuring tuvo la idea de extender los resultados de Hasse acerca de la hipótesis de Riemann sobre cuerpos de funciones elípticas a cuerpos de funciones de una variable sobre un cuerpo de constantes finito, pero de género arbitrario. Ello equivalía a trasladar los resultados de Hasse relativos a curvas elípticas sobre cuerpos finitos a curvas de género arbitrario sobre tales cuerpos. Para ello, Deuring se vio inmerso en el estudio de los anillos de multiplicadores de dichas curvas, lo cual le llevó en 1937 a la creación de una teoría de correspondencias.

Dada una variedad algebraica $X/\mathbb{F}_q$, proyectiva, no singular y definida sobre un cuerpo finito, la información diofántica de

la misma se organiza por medio de su función zeta. Siguiendo el camino iniciado por Hasse en el caso de curvas elípticas, podemos considerar el número $N_m = \#X(\mathbb{F}_{q^m})$ de sus puntos racionales sobre las distintas extensiones finitas $\mathbb{F}_{q^m}|\mathbb{F}_q$. Su función zeta se define por la fórmula

$$Z(X/\mathbb{F}_q, s) := \exp\left(\sum_{m\geq 1}^{\infty} \frac{N_m}{m} q^{-ms}\right), \quad s \in \mathbb{C}.$$

Formuladas en los años 1940, las conjeturas de Weil afirman que $Z(X/\mathbb{F}_q, s)$ es una función racional en $T = q^{-s}$ tal que

$$Z(X/\mathbb{F}_q, s) = \prod_{i=0}^{2n} P_i(q^{-s})^{(-1)^{i+1}}, \quad P_i(T) = \prod_{j=1}^{b_i}(1 - \alpha_{i,j}T).$$

Si la dimensión de X es n, la función zeta satisface una ecuación funcional de la forma

$$Z(X/\mathbb{F}_q, n-s) = \pm q^{A(s)} Z(X/\mathbb{F}_q, s), \quad A(s) := \left(\frac{n}{2} - s\right)\chi(s).$$

Sus ceros y sus polos satisfacen la denominada hipótesis de Riemann en este contexto:

$$|\alpha_{i,j}| = q^{i/2}.$$

Si X procede por reducción de una variedad $\widetilde{X}$ definida sobre un subcuerpo de $\mathbb{C}$, el grado b_i de cada polinomio P_i coincide con el i-ésimo número de Betti de la variedad $\widetilde{X}(\mathbb{C})$.

En 1948, Weil demostró la veracidad de las conjeturas anteriores en el caso de curvas y de variedades abelianas sobre cuerpos finitos, completando de esta forma la labor iniciada por Hasse en el caso de las curvas elípticas. La hipótesis de Riemann para curvas definidas sobre cuerpos finitos fue demostrada por Weil haciendo uso de la teoría de correspondencias de Deuring.

La racionalidad de la función zeta en el caso de variedades de dimensión arbitraria fue obtenida por primera vez por B. Dwork, en 1959, utilizando métodos p-ádicos.

De la ingente labor realizada por Grothendieck y su escuela es especialmente notable la demostración de las conjeturas de Weil. La demostración de la racionalidad de las funciones zeta, su ecuación funcional y su relación con los números de Betti es debida a Grothendieck. La primera se obtuvo expresando dichas funciones en términos de productos alternados de polinomios característicos de elementos de Frobenius operando sobre la cohomología ℓ-ádica de las variedades. La ecuación funcional se obtuvo como resultado de teoremas de dualidad en cohomología. La localización de los ceros y de los polos (hipótesis de Riemann en este contexto), se debe a P. Deligne, y fue probada en 1974 en un auténtico *tour de force* que le valió la Medalla Fields en 1978.

7.1.2. Funciones zeta globales

En 1955, Hasse había asignado a todo cuerpo de funciones algebraicas de una variable definido sobre un cuerpo de números K una función zeta global. Dicha función se define por medio de un producto de Euler cuyos factores son las funciones zeta locales asociadas a los lugares finitos de buena reducción de K. La definición de Hasse puede extenderse a toda variedad X no singular definida sobre un cuerpo de números K, obteniéndose la función $\zeta(X/K, s)$.

La función $\zeta(X/K, s)$ se expresa como un producto alternado de series $L_m(X/K, s)$, $1 \leq m \leq 2\dim X$. La veracidad de las conjeturas de Weil para las variedades algebraicas definidas sobre cuerpos finitos garantiza que el producto de Euler que define estas series converge en el semiplano $\Re(s) \geq 1 + m/2$, definiendo por tanto una función holomorfa y sin ceros en este semiplano.

En 1969, J-P. Serre formuló varias conjeturas acerca de los factores locales de las series $L_m(X/K, s)$ en todos los lugares del cuerpo de definición. Los factores locales en los primos de buena reducción no ofrecen ningún problema y siguen el modelo de

Hasse-Weil. Los casos interesantes son, por un lado, los primos de mala reducción y, por otro, los lugares arquimedianos. En los lugares ultramétricos $\mathfrak{p}$, Serre determina los factores por la acción de los grupos de Galois locales operando sobre la cohomología ℓ-ádica de $X \otimes K_{\mathfrak{p}}$. En los lugares arquimedianos, Serre tiene en cuenta el tipo de Hodge de la cohomología de $X \otimes K_{\mathfrak{p}}$. La conjetura principal afirma que las series $L_m(X/K, s)$ así completadas poseen una prolongación analítica a una función meromorfa y satisfacen una ecuación funcional del tipo

$$L_m(X/K, s) = wL_m(X/K, m + 1 - s), \quad w = \pm 1.$$

En el caso en que $X = \mathrm{Spec}K$ sea un punto, se recupera la función zeta de Dedekind del cuerpo K, para la cual se sabe que satisface la conjetura acerca de su prolongación analítica y ecuación funcional. Si E/K es una curva elíptica, se recupera su serie L de Hasse-Weil.

7.2. Series L de variedades abelianas

7.2.1. Variedades abelianas con MC

El estudio de las variedades abelianas con MC se desarrolló básicamente a partir de trabajos de G. Shimura, K. Taniyama y A. Weil de los años 1950.

Las variedades abelianas con multiplicación compleja definen puntos especiales de espacios de módulos que parametrizan clases de isomorfía de variedades abelianas complejas, polarizadas y dotadas de ciertas estructuras de nivel. Su aritmética está íntimamente relacionada con la naturaleza de los valores que toman ciertas funciones y formas automorfas definidas en estos espacios.

Se sabe que toda variedad abeliana con multiplicación compleja posee un modelo definido sobre un cuerpo de números. Los

distintos tipos de multiplicaciones responden a los distintos tipos posibles de sus anillos de endomorfismos.

Hasse había demostrado en 1954 que, dado un cuerpo de números K y un cuerpo de funciones del tipo de Fermat $F := K(u_1, u_2)$, en donde u_i son indeterminadas que satisfacen $u_1^{m_1} + u_2^{m_2} = 1$, su función zeta global $\zeta(F, s)$ se expresa como producto de funciones zeta de Dedekind $\zeta(K, s)$ por un producto de funciones $L(\psi, s)$ asociadas a caracteres de Hecke. En particular, la función ζ admite en este caso una prolongación analítica y satisface una ecuación funcional.

Shimura y Taniyama calcularon la función ζ de una variedad abeliana con multiplicación compleja en términos de su tipo MC y de funciones L asociadas a caracteres de Hecke, generalizando los resultados de Deuring para las curvas elípticas con MC y de Hasse para las curvas de Fermat. Los teoremas fundamentales de la multiplicación compleja de variedades abelianas describen cómo actúan los automorfismos del grupo de Galois absoluto del cuerpo racional $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sobre las variedades abelianas con multiplicación compleja y sobre sus puntos de torsión. Un tratado pionero en esta teoría fue el texto de Shimura y Taniyama, publicado en 1961.

La teoría de la multiplicación compleja en variedades abelianas de dimensión superior resultó ser bastante más complicada que en dimensión 1, debido a dos tipos de dificultades. Por una parte, los puntos de división proporcionan extensiones abelianas no del cuerpo E de la multiplicación compleja, como en el caso de las curvas elípticas, sino de un segundo cuerpo E^*, denominado el cuerpo reflejo de E. Por otra parte, en dimensiones superiores, la teoría de la multiplicación compleja no proporciona suficientes elementos para generar todas las extensiones abelianas del cuerpo reflejo.

Uno de los puntos cruciales de la teoría de la multiplicación compleja lo constituye la fórmula de Shimura-Taniyama la cual, generalizando resultados previos relativos a congruencias de Kro-

necker y de Deuring para los módulos singulares de las funciones elípticas, proporciona una descripción de los elementos de Frobenius en términos de reducción de multiplicaciones de la variedad:

Sea A/K una variedad abeliana de tipo MC dado por (E, Φ) y definida sobre un cuerpo de números K, extensión de Galois de $\mathbb{Q}$. Sea $E^* \subseteq K$ su cuerpo reflejo. Supongamos que A posee buena reducción en un ideal primo $\mathfrak{P}$ de $\mathcal{O}_K$. Sean $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{E^*}$, $(p) = \mathfrak{p} \cap \mathbb{Z}$ y $q = (\mathcal{O}_E^* : \mathfrak{p})$. Supongamos que p es no ramificado en E, que $\mathfrak{P}$ no lo es en E^* y que $\mathrm{End}(A) \cap E = \mathcal{O}_E$. Sea $\sigma = \mathrm{Frob}(K|E^*, \mathfrak{P})$ el elemento de Frobenius. Entonces, existe una $\mathfrak{a}$-multiplicación $\alpha : A \to \sigma A$, $\mathfrak{a} \subseteq \mathcal{O}_E$, tal que su reducción $\alpha_0 : A_0 \to \sigma(A_0)^{(q)}$ es la aplicación de Frobenius y, además, $\mathfrak{a} = N_\Phi(\mathfrak{p})$.

7.2.2. Representaciones ℓ-ádicas abelianas

La teoría de la multiplicación compleja en dimensión superior fue linealizada por Serre en su libro sobre representaciones ℓ-ádicas, conocido tradicionalmente como McGill. En este texto de 1968, la teoría de la multiplicación compleja es introducida desde un punto de vista próximo al de la posterior teoría de motivos. Haciendo abstracción de construcciones propias de la teoría de los cuerpos de clases y de la teoría de la multiplicación compleja, Serre asocia a cada cuerpo de números K una familia proyectiva $(S_\mathfrak{m})$ de grupos algebraicos conmutativos definidos sobre $\mathbb{Q}$. Para cada módulo $\mathfrak{m}$ de K, en el sentido de la teoría de los cuerpos de clases, Serre demuestra que existe una sucesión exacta de grupos algebraicos conmutativos $1 \to T_\mathfrak{m} \to S_\mathfrak{m} \to C_\mathfrak{m} \to 1$, en la cual $C_\mathfrak{m}$ es un grupo finito y $T_\mathfrak{m}$ es un toro. Los caracteres de $S_\mathfrak{m}$ son, en esencia, los caracteres de Hecke de tipo A_0 cuyo conductor divide a $\mathfrak{m}$.

Serre demuestra que las representaciones lineales de la familia $(S_\mathfrak{m})$ proporcionan todos los sistemas compatibles de representaciones racionales abelianas ℓ-adicas del cuerpo K que son

localmente algebraicas.

Resultados de transcendencia debidos a C. L. Siegel, a S. Lang y a M. Waldschmidt permitieron demostrar que todas las representaciones racionales abelianas y semisimples asociadas a un cuerpo de números K son localmente algebraicas, por lo que el resultado anterior de Serre proporciona un control completo de las mismas.

Dado un sistema compatible de representaciones l-ádicas racionales (abelianas o no), Serre relacionó problemas de equidistribución de clases de conjugación de elementos de Frobenius con la presencia de propiedades analíticas específicas de las series L del sistema.

7.2.3. La conjectura BSD

En los años 1963 y 1965, Birch y Swinnerton-Dyer pusieron de manifiesto por medio de experiencias numéricas realizadas en curvas con multiplicación compleja, que el rango r de una curva elíptica $E/\mathbb{Q}$ coincidía con el orden en el punto $s = 1$ del cero de la función $L(E/\mathbb{Q}, s)$. Conjeturaron que éste bien podría ser un hecho general:

$$r \stackrel{?}{=} \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s).$$

En el momento de su formulación, la conjetura de Birch y Swinnerton-Dyer parecía excesivamente arriesgada, pues comparaba una cantidad desconocida, el rango de la curva elíptica, con otra, el valor $L(E/\mathbb{Q}, 1)$, que ni siquiera estaba definido, ya que la serie que define $L(E/\mathbb{Q}, s)$ converge sólamente para $\Re(s) > 3/2$ y su prolongación analítica distaba de ser probada.

Los cálculos de Birch y Swinnerton-Dyer hicieron posible una formulación mucho más precisa de su conjetura, que incorpora no sólo el orden del cero de la función L en $s = 1$, sino que describe minuciosamente la parte principal del mismo, según una fórmula que recuerda la fórmula analítica del número de clases.

Más generalmente, la conjetura BSD se formula hoy para toda variedad abeliana A/K definida sobre un cuerpo K de números. La conjetura afirma que

$$\frac{L^r(A,1)}{r! \cdot \Omega(A)} = \frac{\prod c_{\mathfrak{p}} \cdot \mathrm{Reg}(A) \cdot \#\mathrm{sha}(A)}{\#A(K)_{\mathrm{tor}} \cdot \#A^{\vee}(K)_{\mathrm{tor}}},$$

en donde $r = \mathrm{ord}_{s=1} L(A,s)$ denota el rango analítico de A; $c_{\mathfrak{p}}$ es el número de Tamagawa de A en $\mathfrak{p}$ (igual al número de componentes racionales de la reducción del modelo de Néron de A en $\mathfrak{p}$); $\Omega(A)$ es el valor absoluto de la integral sobre $A(\mathbb{R})$ de $\omega := \omega_1 \wedge \cdots \wedge \omega_d$, siendo $\{\omega_i\}$ una base de 1-diferenciales holomorfas de A; $\mathrm{Reg}(A)$ es el regulador de A, que mide el volumen del retículo de la parte libre de $A(K)$; y $\mathrm{sha}(A)$ es el grupo de Tate-Shafarevich de A. En la fórmula interviene asimismo el orden de la torsión racional de A y de la variedad dual $A^{\vee}$. Mediante algoritmos sofisticados, creados en gran parte por W. Stein, digamos que se empieza a conseguir evidencia numérica para la conjetura BSD para variedades abelianas modulares. La ventaja de tratar con este tipo de variedades es que su función L admite una prolongación analítica y, por tanto, está definida en $s = 1$.

Por su parte, la conjetura BSD forma parte de un programa general, conocido como conjeturas de Beilinson las cuales, formuladas a partir de los años 1980, proporcionan un significado aritmético en términos de reguladores superiores a los distintos valores especiales de las funciones L de motivos aritméticos.

Como curiosidad, la conjetura BSD en la primera formulación que hemos dado de ella (es decir, para curvas elípticas sobre $\mathbb{Q}$ y solamente atendiendo al rango r), es uno de los denominados Siete Problemas del Milenio, propuestos por el Instituto Clay de Matemáticas. Como comentaremos más adelante, hoy sabemos (gracias a A. Wiles *et al.*) que para toda curva elíptica $E/\mathbb{Q}$ su función L admite una prolongación analítica, con lo cual el valor $L(E/\mathbb{Q},1)$, como mínimo, sabemos que está definido.

7.3. Demostración de la conjetura de Mordell

Sesenta años después de que Mordell formulara su controvertida conjetura sobre la finitud del número de puntos K-racionales de las curvas de género $g > 2$, proyectivas, no singulares y definidas sobre un cuerpo de números K, G. Faltings logró demostrar que Mordell estaba en lo cierto.

En un espectacular trabajo publicado en 1983, que le valió la concesión de la Medalla Fields en 1986, Faltings demostró por primera vez tres famosas conjeturas: la mencionada conjetura de Mordell (1922), la de Shafarevich (1962) y la de Tate (1966).

En el Congreso Internacional de Matemáticos de 1962, celebrado en Estocolmo, Shafarevich había formulado la pregunta de si sería válido en el caso de curvas algebraicas un teorema análogo a un teorema de Hermite para cuerpos de números. De ser así, fijado un género $g > 1$ y un conjunto de degeneración S formado por un número finito de lugares de un cuerpo de números K, el conjunto de clases de isomorfía de curvas algebraicas definidas sobre K con buena reducción fuera de S sería finito. La importancia de la denominada conjetura de Shafarevich se puso de manifiesto en un trabajo de Parshin de 1968, en el que, a través de una ingeniosa construcción, probaba que la conjetura de Shafarevich implicaba la conjetura de Mordell. La construcción de Parshin permite remitir el problema del cómputo del número de puntos K-racionales al de un número equivalente de curvas definidas sobre K.

De las tres conjeturas probadas por Faltings en 1983, la conjetura de Tate es la más técnica, pero también la que después ha tenido una repercusión mayor. Dada una variedad abeliana A definida sobre un cuerpo de números K, la conjetura de Tate caracteriza la clase de isogenia de A a través de su función zeta de Hasse-Weil $\zeta(A/K, s)$: dos variedades abelianas A/K, B/K son isógenas si, y solamente si, sus respectivas funciones zeta

$\zeta(A/K, s)$, $\zeta(B/K, s)$ poseen idénticos factores de Euler salvo, a lo sumo, en un número finito de lugares de K.

Faltings inicia su trabajo con la demostración de la conjetura de Tate. Su principal logro es la definición y el control de una noción de altura $h(A)$ para las variedades abelianas, entendidas ahora como puntos del espacio de módulos M_g de las clases de isomorfía de las variedades abelianas principalmente polarizadas de dimensión g. La altura $h(A)$ da cuenta de los volúmenes de las variedades $A/\overline{K}_v$ cuando v recorre el conjunto de los lugares arquimedianos de K. El espacio de módulos M_g no es compacto. Si se compactifica (mediante el proceso de Satake o de Chai, por ejemplo) las métricas sobre su fibrado canónico adquieren singularidades en los bordes. Sin embargo, al ser éstas suficientemente suaves (de tipo logarítmico) permitieron definir a Faltings una altura casi invariante por isogenias. Al hacer una inmersión proyectiva de M_g en un espacio proyectivo conveniente $\mathbf{P}^n_K$ (por medio de formas modulares K-racionales), la altura usual de $\mathbf{P}^n_K$ define una segunda función altura en M_g. Para poder probar los resultados de finitud, es esencial el hecho que las contribuciones de ambas alturas sobre M_g en los lugares ultramétricos $v_\mathfrak{p}$ de K difieren únicamente en una cantidad acotada.

El resto de la demostración de la conjetura de Tate es un ingenioso cálculo en el que se conjugan resultados de Raynaud y del propio Tate sobre grupos $\mathfrak{p}$-divisibles y el teorema de densidad de Chebotarev, así como la demostración de que la representación de Galois definida por el módulo de Tate ℓ-ádico $V_\ell(A)$ es semisimple.

A partir de la recién probada conjetura de Tate y de teoremas de Weil, Faltings dedujo un teorema de finitud para las clases de isogenia, primero, y para las clases de isomorfía, después, de las variedades abelianas principalmente polarizadas definidas sobre K, una vez fijados su dimensión g y su conjunto de degeneración. El clásico teorema de Torelli, según el cual toda curva es determinable a partir de la polarización canónica de su jacobiana, permite a Faltings recuperar las curvas y probar la conjetura

de Shafarevich a partir de su teorema de finitud para las clases de isomorfía de las variedades abelianas.

A cada punto K-racional P de una curva $\mathcal{C}$, definida sobre K y con buena reducción fuera de S, la construcción de Parshin le asocia un recubrimiento $\varphi_P : \mathcal{C}_P \to \mathcal{C}$ en el cual la curva recubridora $\mathcal{C}_P$ tiene género acotado y buena reducción fuera de S. Al considerar que, para cada $\mathcal{C}_P$, el número de morfismos φ_P es finito y la aplicación $P \to (X_P, \varphi_P)$ es inyectiva, a partir de la conjetura de Shafarevich, ya probada, Faltings logra demostrar la conjetura de Mordell.

Con posterioridad a Faltings, P. Vojta y E. Bombieri obtuvieron demostraciones alternativas de la conjetura de Mordell. Sus demostraciones se basan en técnicas de aproximación diofántica cercanas a las de Siegel y, en el caso de Vojta, hace uso de una teoría aritmética de intersección. Sin embargo, ninguna de las demostraciones conocidas hasta la fecha de la conjetura de Mordell es cuantitativa, en el sentido de producir cotas calculables para el número de puntos racionales de la curva dada.

Capítulo 8

Formas modulares y aritmética

8.1. Formas modulares

Los orígenes de las formas modulares deben buscarse en fórmulas de Jacobi para el cómputo del número representaciones de enteros como suma de cuadrados, en las funciones thetafuchsianas de Poincaré y en cálculos diversos debidos a S. Ramanujan. En un principio, las formas modulares resultaron algo marginales en teoría de números, pero en el transcurso de los años se han convertido en objetos cada vez más imprescindibles.

Como veremos, las formas modulares o, más generalmente, las formas automorfas proporcionan las funciones necesarias para efectuar la representación integral de series L aritméticas, proporcionando así resultados de prolongación analítica y ecuaciones funcionales para las mismas.

8.1.1. Grupos fuchsianos aritméticos

Se denominan fuchsianos los subgrupos $\Gamma \subseteq \mathbf{PSL}(2,\mathbb{R})$ que operan de forma discontínua en el semiplano superior complejo. Ello significa que las órbitas Γz, $z \in \mathcal{H}$, no contienen puntos de acumulación en el semiplano superior complejo, aunque pueden contenerlos en el eje real $\mathbf{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$. Los grupos fuchsianos cuyo conjunto límite es $\mathbf{P}^1(\mathbb{R})$ se dice que son de primera especie; en particular, ello ocurre cuando el espacio cociente $\Gamma\backslash\mathcal{H}$ posee volumen finito.

Entre los grupos fuchsianos de primera especie con más relevancia para la aritmética se encuentran el grupo modular y sus subgrupos de congruencia:

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{SL}(2,\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \mid a \equiv 1 \pmod{N} \right\},$$

$$\Gamma(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(N) \mid b \equiv 0 \pmod{N} \right\}.$$

Notemos que se satisfacen las inclusiones

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N).$$

Los ejemplos anteriores corresponden a grupos fuchsianos aritméticos. Para dar una definición más general de éstos debemos recordar algunos conceptos básicos de álgebra no conmutativa.

Consideremos un álgebra de cuaternios $\left(\frac{a,b}{F}\right)$, de centro un cuerpo F, con base $\{1, \mathrm{I}, \mathrm{J}, \mathrm{K}\}$ y producto definido por las reglas

$$\mathrm{I}^2 = a,\ \mathrm{J}^2 = b,\ \mathrm{IJ} = -\mathrm{JI} = \mathrm{K}, \quad a, b \in F^*.$$

Las álgebras de cuaternios son ejemplos de álgebras simples, pues carecen de ideales bilaterales no triviales. Se trata de álgebras de rango cuatro sobre su centro. El primer ejemplo histórico son los cuaternios de Hamilton, $H = \left(\frac{-1,-1}{\mathbb{R}}\right)$, que son, además, un cuerpo no conmutativo. El álgebra de matrices $M(2,F) \simeq \left(\frac{1,b}{F}\right)$ proporciona otro ejemplo.

Dada un álgebra de cuaternios H de centro un cuerpo de números K, el número de lugares $\mathfrak{p}$ de K en los que H ramifica (es decir, en los que el álgebra $H \otimes K_{\mathfrak{p}}$ no es isomorfa a un álgebra de matrices) es finito. El producto de estos lugares se denomina el discriminante D_H de H. Los subanillos de H de rango cuatro, sobre el anillo de enteros $\mathcal{O}_K$ de K, reciben el nombre de órdenes de H. Dado un orden $\mathcal{O}$ de un álgebra de cuaternios, designaremos por $\mathcal{O}_1^*$ el grupo multiplicativo de sus unidades de norma 1. Los subgrupos Γ de H^* conmensurables con $\mathcal{O}_1^*$ son, por definición, grupos fuchsianos aritméticos.

Veamos el primer ejemplo: el álgebra de cuaternios más sencilla de centro el cuerpo racional es el álgebra de matrices $M(2,\mathbb{Q})$. Su discriminante es $D = 1$. Las matrices de coeficientes enteros $\mathcal{O} = M(2,\mathbb{Z})$ constituyen un orden maximal. El grupo multiplicativo de las unidades de norma 1 de este orden es, exactamente, el grupo modular $\mathcal{O}_1^* = \mathbf{SL}(2,\mathbb{Z})$.

Dado un grupo fuchsiano aritmético Γ, el cuerpo $\mathbb{C}(\Gamma)$ de todas las funciones Γ-automorfas es el cuerpo de funciones de una curva algebraica, $X(\Gamma)$, definida sobe un cuerpo de números. Sus puntos complejos $X(\Gamma)(\mathbb{C})$ están en correspondencia biyectiva con los puntos de $\Gamma\backslash\mathcal{H}^*$, en donde $\mathcal{H}^*$ se obtiene a partir de $\mathcal{H}$ por adición de los puntos parabólicos de Γ. Los primeros ejemplos los proporcionan las curvas modulares, definidas por los subgrupos de congruencia del grupo modular antes mencionados. Tal como es habitual, escribiremos $X_0(N) := X(\Gamma_0(N))$, $X_1(N) := X(\Gamma_1(N))$, $X(N) := X(\Gamma(N))$. Más generalmente, las curvas $X(\Gamma)$ asociadas a grupos fuchsianos aritméticos se deno-

minan curvas de Shimura.

En el caso de la curva modular $X_0(N)$, se tiene un isomorfismo

$$(j, j_N) : \Gamma_0(N)\backslash\mathcal{H}^* \simeq X_0(N)(\mathbb{C}) \subseteq \mathbf{P}^2(\mathbb{C}).$$

Las funciones j, $j_N(z) := j(Nz)$ definen una parametrización analítica de la misma y dan lugar al polinomio modular de nivel N, $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$, como ecuación definidora de $X_0(N)$.

Entre les curvas modulares y las curvas de Shimura cuaterniónicas ($D \neq 1$) se dan notables diferencias. Los grupos fuchsianos que definen las curvas modulares contienen traslaciones, pero los grupos fuchsianos que definen las curvas de Shimura en el caso cuaterniónico no contienen este tipo de transformaciones. Como consecuencia de ello, las funciones y las formas automorfas respecto de grupos fuchsianos aritméticos son desarrollables en serie de Fourier únicamente en el caso modular.

8.1.2. Conjeturas de Ramanujan

Vamos a empezar considerando cómo las acciones de los grupos fuchsianos sobre $\mathcal{H}$ se transmiten a las funciones definidas en este semiplano. Dada una matriz $\gamma = \begin{bmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{bmatrix}$ en $\mathbf{SL}(2, \mathbb{Z})$, se define el factor de automorfía $j(\gamma, z)$ como

$$j(\gamma, z) = c_\gamma z + d_\gamma, \quad z \in \mathcal{H}.$$

Dado un entero k, para cada matriz γ se define el operador de peso k en las funciones $f : \mathcal{H} \to \mathbb{C}$ mediante la fórmula

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

Dados un subgrupo de congruencia $\Gamma \subseteq \mathbf{SL}(2, \mathbb{Z})$ y un entero k, una función $f : \mathcal{H} \to \mathbb{C}$ se denomina una forma modular de peso k respecto de Γ cuando satisface las condiciones siguientes:

(1) La función f es holomorfa.

(2) La función f es invariante bajo la acción de los operadores $[\gamma]_k$, para todo $\gamma \in \Gamma$.

(3) La función $f[\alpha]_k$ es holomorfa en el infinito, para todo $\alpha \in \mathbf{SL}(2,\mathbb{Z})$.

Si el subgrupo Γ contiene traslaciones de la forma

$$\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} : z \mapsto z + h,$$

se obtiene que las formas modulares poseen en el entorno de ∞ desarrollos de Fourier de la forma

$$f(z) = \sum_{n=0}^{\infty} a_n q_h^n, \quad q_h = e^{2\pi i z/h}.$$

Una forma modular se dice que es parabólica o cuspidal cuando se anula en todos los puntos parabólicos. Las formas modulares de peso k respecto de Γ constituyen un espacio vectorial, que denotamos por $\mathcal{M}(\Gamma, k)$. Las formas modulares parabólicas constituyen un subespacio del mismo, que denotamos por $\mathcal{S}(\Gamma, k)$.

Las series de Eisenstein G_k, para $k \geq 4$ par, son elementos de $\mathcal{M}(\Gamma_0(1), k)$; se definen por

$$\begin{aligned} G_k(z) &:= \sum_{(m,n)\neq 0} \frac{1}{(mz+n)^k} \\ &= 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\right), \end{aligned}$$

en donde $\zeta(s)$ es la función zeta de Riemann, B_k son los números de Bernoulli y $\sigma_k(n) := \sum_{d|n} d^k$ es la k-ésima función suma de divisores. Se suele escribir

$$g_2(z) = 60G_4(z), \quad g_3(z) = 140G_6(z).$$

Los espacios de formas modulares parabólicas $\mathcal{S}(\Gamma_0(1), k)$ son cero para $k < 12$. La función discriminante $\Delta(z)$ es una forma

parabólica no nula de $\mathcal{S}(\Gamma_0(1), 12)$, siendo este espacio vectorial de dimensión 1. Los coeficientes de Fourier de Δ en el infinito definen la célebre función τ de Ramanujan:

$$\frac{1}{(2\pi)^{12}}\Delta(z) = q\prod(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$$

$$= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + O(q^7).$$

Ramanujan llegó al estudio de la función τ a través del problema de averiguar el número $r_{24}(n)$ de representaciones distintas de un entero n como suma de 24 cuadrados. El papel de $\tau(n)$ en este problema es el de un término de error. Ramanujan calculó los 30 primeros valores $\tau(n)$ y, a la vista de los resultados obtenidos, dedujo que la función τ debía tener las propiedades siguientes:

(i) $\tau(mn) = \tau(m)\tau(n)$, si $\text{mcd}(m,n) = 1$,

(ii) $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$, si p es primo y $n \geq 1$,

(iii) $|\tau(p)| \leq 2p^{11/2}$, para todo primo p.

El deseo de probar las conjeturas de Ramanujan hizo avanzar enormemente el estudio de las formas modulares y llevó al descubrimiento de importantes estructuras aritméticas.

En 1917, Mordell probó las conjeturas (i) y (ii) de Ramanujan. El resultado de Mordell fue ampliamente generalizado por Hecke en 1936. Los espacios de formas parabólicas están dotados del denominado producto escalar de Petersson. Hecke definió un álgebra de operadores hermíticos que actúan en estos espacios, con lo cual las propiedades (i) y (ii) probadas por Mordell para la función τ reflejan que la forma Δ es una función propia de todos los operadores de Hecke.

Dado un carácter de Dirichlet χ módulo N, se define

$$\mathcal{M}(N,k,\chi) =$$

$$\{f \in \mathcal{M}(\Gamma_1(N),k) : f[\gamma]_k(z) = \chi(d_\gamma)f, \text{para todo } \gamma \in \Gamma_0(N)\}.$$

Los espacios $\mathcal{M}(\Gamma_1(N), k)$ descomponen en suma directa de subespacios propios asociados a caracteres de Dirichlet; así se satisface que

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

Los elementos de $\mathcal{M}(N, k, \chi)$ se denominan formas modulares de tipo (N, k, χ). Para que los subespacios $\mathcal{M}(N, k, \chi)$ sean no nulos es necesario que se cumpla la relación $\chi(-1) = (-1)^k$. En general, las dimensiones de estos espacios se determinan o bien por medio del teorema de Riemann-Roch, o mediante versiones explícitas de la fórmula de las trazas de Selberg. En particular, destaquemos que

$$\mathcal{S}(\Gamma_0(N), 2k) \simeq H^0(X_0(N), \Omega^{\otimes k})$$

por lo que

$$\dim_{\mathbb{C}} \mathcal{S}(\Gamma_0(N), 2) = \text{género de } X_0(N).$$

8.1.3. Funciones L de formas modulares

A cada forma modular parabólica $f \in \mathcal{S}(\Gamma_1(N), k)$ se le puede asociar una serie L de Dirichlet. Si $f(z) = \sum_{n=1}^{\infty} a_n q^n$, se define

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

La serie $L(f, s)$ converge absolutamente para todo s en el semiplano $\Re(s) > (k+1)/2$.

Dada $f \in \mathcal{S}(\Gamma_0(N), k, \chi)$, se satisface que f es un vector propio normalizado ($a_1 = 1$) de todos los operadores de Hecke si, y solamente si, la serie $L(f, s)$ admite la siguiente descomposición en forma de producto de Euler:

$$L(f, s) = \prod_{p} \frac{1}{1 - a_p p^{-s} + \chi(p) p^{k-1-2s}}, \quad \Re(s) > \frac{k+1}{2}.$$

Los espacios de formas parabólicas poseen, además de las acciones de los operadores de Hecke, una involución importante, definida por un operador autoadjunto:

$$W_N : \mathcal{S}(\Gamma_1(N)) \to \mathcal{S}(\Gamma_1(N)), \quad f \mapsto i^k N^{1-k/2} f \left[\begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}\right]_k.$$

Definiendo

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

la acción de W_N permite demostrar que, para toda forma parabólica de peso k que sea vector propio de W_N, su función $\Lambda(f,s)$ se prolonga a una función analítica de todo $\mathbb{C}$ y satisface una ecuación funcional de la forma

$$\Lambda(f,s) = \pm\Lambda(f,k-s), \quad \text{siendo } W_N(f) = \pm f.$$

La demostración de este hecho se consigue de manera análoga a la demostración que en su día hizo Riemann de la ecuación funcional satisfecha por la función zeta que lleva su nombre.

8.1.4. La conjetura de modularidad STW

En la sesión de problemas de un simposio internacional sobre teoría algebraica de números, celebrado en Tokyo-Nikko en 1955, un joven matemático llamado Taniyama propuso averiguar si las curvas elípticas definidas sobre un cuerpo de números son parametrizables mediante funciones automorfas. De ser así, éste podía ser un camino para probar la conjetura de Hasse-Weil relativa a la prolongación analítica y ecuación funcional de la serie $L(E,s)$. La precisión a lo largo de los años del enunciado del problema propuesto por Taniyama dio lugar a la conjetura de Shimura-Taniyama-Weil (STW).

En 1964, Shimura delimitó el enunciado del problema de Taniyama considerando únicamente curvas elípticas E definidas sobre el cuerpo racional $\mathbb{Q}$ y preguntando si serían parametrizables por funciones modulares. De ser así, la función L de una curva

elíptica $E/\mathbb{Q}$ se obtendría como transformada de Mellin de una forma modular f_E de peso 2, por lo que su función L satisfacería la conjetura de Hasse-Weil. En 1967, Weil precisó el nivel N_E de la hipotética forma modular f_E; siendo éste igual al conductor de E. Los divisores primos del conductor coinciden con los primos de mala reducción de E y el exponente con el cual un primo divide al conductor depende del símbolo de Kodaira de la fibra geométrica del modelo de Néron de E en p; su cálculo se efectúa mediante el algoritmo de Tate. Con ello quedó precisada la conjetura STW según la cual todas las curvas elípticas $E/\mathbb{Q}$ debían ser modulares. El hecho de que E sea una curva elíptica semiestable equivale a que N_E sea un entero libre de cuadrados.

Posteriormente se fueron encontrando formulaciones equivalentes a la conjetura STW; entre ellas mencionamos las siguientes:

a) Para toda curva elíptica $E/\mathbb{Q}$, existe un morfismo

$$X_0(N_E)_{/\mathbb{Q}} \to E_{/\mathbb{Q}},$$

en donde N_E es el conductor de E.

b) Toda curva elíptica $E/\mathbb{Q}$ es isógena sobre $\mathbb{Q}$ a un factor de la jacobiana $J_0(N_E)$ de la curva modular $X_0(N_E)$.

c) Existen funciones modulares $\xi, \eta \in \mathbb{Q}(j, j_{N_E})$ tales que

$$E \ : \xi(z)^2 = \eta(z)^3 + a\eta(z) + b.$$

d) Si $L(E/\mathbb{Q}, s) = \sum_{n\geq 1} \frac{a_n}{n^s}$, entonces $f(q) := \sum_{n\geq 1} a_n q^n$ es una forma parabólica de $\mathcal{S}(\Gamma_0(N_E), 2)$.

Paulatinamente, y a partir del los años 1970, se logró una gran evidencia numérica en favor de esta conjetura. Como en el caso de la formulación de la conjetura BSD, los ordenadores desempeñaron un papel muy importante en este proceso.

La conjetura STW proporcionaba pues un camino para probar la conjetura de Hasse-Weil. En particular, de ser STW cierta, las integrals elípticas asociadas a curvas elípticas definidas sobre $\mathbb{Q}$ se han de poder obtener por reducción de integrales abelianas asociadas a curvas modulares. Si esto es así, entonces la función L admite una representación integral cuyo núcleo integral viene dado por la forma modular f_E (función thetafuchsiana) de peso 2:

$$L(E/\mathbb{Q}, s) = (2\pi)^s \Gamma(s)^{-1} \int_0^{i\infty} (-iz)^s f_E(z) \frac{dz}{z},$$

siendo $f_E(z)dz \in H^0(X_0(N), \Omega^1)$. Esta representación integral es la que permite la prolongación analítica de la función L y la demostración de la ecuación funcional, de manera análoga, tal como se ha comentado, al caso de la función zeta de Riemann.

La conjetura STW adquirió una relevancia inesperada cuando, gracias a resultados de Frey (1986), de Serre (1987) y de Ribet (1990), se puso de manifiesto que no solamente implicaba la conjetura de Hasse-Weil sino que, *cum grano salis*, implicaba el teorema de Fermat.

8.2. Curvas modulares y aritmética

El estudio de las curvas modulares ha dado lugar a una extensa literatura en la que han intervenido numerosos autores. Tanto las curvas modulares como su generalización, las curvas de Shimura, se han convertido en objetos imprescindibles para el tratamiento actual de problemas aritméticos.

Los artículos de Shimura publicados hasta la fecha han sido recopilados en cuatro volúmenes por la editorial Springer; además, Shimura es autor de diversos libros sobre estos temas.

8.2.1. Las congruencias de Eichler-Shimura

En una exposición en el Séminaire Delange–Pisot–Poitou, acaecida en 1969, Serre formuló la notable conjetura según la cual ciertas congruencias satisfechas por la función τ de Ramanujan podrían ser explicadas por la existencia, para cada primo ℓ, de una representación ℓ-ádica de dimensión 2

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(V_\ell),$$

no ramificada fuera de ℓ, y tal que

$$\mathrm{Tr}(\rho_\ell(F_p)) = \tau(p), \quad \det(\rho_\ell(F_p)) = p^{11},$$

para cada elemento de Frobenius F_p, siendo $p \neq \ell$ un primo cualquiera.

Previamente, Weil había sugerido que la desigualdad conjeturada por Ramanujan acerca de la función τ:

$$|\tau(p)| \leq 2p^{11/2}$$

podía deberse a una estimación de valores propios del automorfismo de Frobenius operando en un espacio de dimensión 2 proveniente de la cohomología 11 de cierta variedad.

En 1971, y como consecuencia de su demostración de las conjeturas de Weil, Deligne logró demostrar la conjetura de Ramanujan siguiendo el camino trazado por Weil y Serre. El estudio de la cohomología ℓ-ádica de las curvas modulares y la interpretación cohomológica de las formas modulares permitió asociar a toda forma modular parabólica, vector propio de todos los operadores de Hecke (es decir, a toda forma modular nueva), representaciones de Galois ℓ-ádicas, de acuerdo con las predicciones hechas por Serre; por otra, la demostración de todas las conjeturas de Weil (por parte de Grothendieck y Deligne) permitió la deducción de la desigualdad conjeturada por Ramanujan acerca de la función τ, así como afirmaciones análogas para formas modulares nuevas de cualquier peso, nivel y carácter. La

construcción de representaciones ℓ-ádicas asociadas a formas automorfas fue proseguida por M. Ohta en 1982.

En general, las representaciones ℓ-ádicas ρ_ℓ asociadas a formas modulares nuevas dejan invariante un retículo de V_ℓ y, por tanto, puede interpretarse como representaciones valoradas en el grupo lineal $\mathbf{GL}(2, \mathbb{Z}_\ell)$. Las imágenes de ρ_ℓ suelen ser grandes; en este caso, todo el grupo lineal. Los primos para los cuales ello no ocurre se denominan primos excepcionales, de los cuales se demuestra que son en número finito. En el caso de las representaciones asociadas a la función τ de Ramanujan, Swinnerton-Dyer demostró que los primos excepcionales son $2, 3, 5, 7, 23, 691$. Por ejemplo,

$$\tau(p) \equiv 1 + p^{11} \pmod{691}$$

es una de las congruencias descubiertas por Ramanujan. Como consecuencia, el valor de $\tau(p) \pmod{\ell}$ no puede ser deducido a partir de ninguna congruencia en p, cuando ℓ no es un primo excepcional.

8.2.2. Puntos de torsión de curvas elípticas

En el año 1977, Mazur obtuvo un resultado fundamental sobre los posibles grupos de torsión de las curvas elípticas definidas sobre $\mathbb{Q}$, que completaba resultados previos debidos a muchos otros autores. En un artículo innovador por su metodología, Mazur demostró que toda curva elíptica $E/\mathbb{Q}$ posee a lo sumo 16 puntos de torsión de coordenadas racionales, y precisó, de acuerdo con una conjetura formulada por A. Ogg, las posibles 15 estructuras de los grupos correspondientes:

$$E(\mathbb{Q})_{\text{tor}} \simeq \begin{cases} \mathbb{Z}/N\mathbb{Z}, \ 1 \leq N \leq 10, \ N = 12, \\ \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \ 1 \leq N \leq 4\,. \end{cases}$$

Mazur planteó la resolución de este problema en términos de un problema diofántico relativo a las curvas modulares $X_0(N)$.

Dada la interpretación de las curvas modulares como espacios de módulos de curvas elípticas con estructuras de nivel, los valores de N citados coinciden con los valores para los cuales la curva modular $X_0(N)$ tiene puntos racionales no parabólicos.

Para obtener su resultado, Mazur introdujo el ideal de Eisenstein $\mathcal{I}$ del álgebra de Hecke $\mathbb{T}$ operando en la jacobiana $J_0(N)$ de la curva modular $X_0(N)$. Un punto esencial de la prueba lo constituye el hecho de que el subgrupo de torsión de $J_0(N)(\mathbb{Q})$ es un grupo cíclico de orden igual al numerador de $(N-1)/12$ y generado por la clase del divisor cuspidal $(0)-(\infty)$. Como herramientas, Mazur hace uso de la teoría de esquemas en grupos (utilizando aquellos que son finitos y planos), de formas modulares sobre anillos (lo cual fue muy novedoso para la época), así como de resultados previos debidos a D. Kubert y a Ogg, principalmente.

8.2.3. Resultados sobre la conjetura BSD

Entre los resultados parciales demostrados a favor de la conjetura de Birch y Swinnerton-Dyer se incluyen dos importantes teoremas: el teorema de Coates-Wiles, del año 1977, y el teorema de Gross-Zagier, del año 1986. Ambos teoremas se refieren a curvas elípticas $E/\mathbb{Q}$.

Coates y Wiles demostraron que si $E/\mathbb{Q}$ es una curva elíptica dotada de multiplicación compleja por un cuerpo cuadrático imaginario K con número de clases $h_K = 1$, entonces si su función L no se anula en $s = 1$, el rango de la curva es cero:

$$L(E/\mathbb{Q}, 1) \neq 0 \Longrightarrow \mathrm{rg}E(\mathbb{Q}) = 0.$$

La demostración consiste en trasladar a los cuerpos obtenidos a partir de los puntos de división de las curvas elípticas resultados aritméticos probados por Kummer y K. Iwasawa en el caso ciclotómico. Para ello, Coates y Wiles trabajan en el marco de la teoría de los grupos formales de Lubin-Tate asociados a curvas elípticas y de la multiplicación compleja formal, utilizan resultados previos debidos a Deuring y a R. Damerell, relativos a valores

especiales de las series L de las curvas elípticas con multiplicación compleja, hacen un uso adecuado de las unidades elípticas, construidas por G. Robert en 1973 (las cuales desempeñan un papel análogo al de las unidades ciclotómicas) y trabajan con una generalización *ad hoc* del concepto de primo irregular, debido a Kummer. La condición de que el cuerpo de la multiplicación compleja fuera de número de clases 1 fue eliminada poco después por Nicole Arthaud. Las hipótesis sobre el cuerpo de definición de la curva elíptica fueron debilitadas por K. Rubin en 1981, quien obtuvo una generalización notable del teorema de Coates-Wiles al refinar las técnicas de su demostración.

Gross y Zagier, en su artículo memorable de 1986, partieron de una curva elíptica $E/\mathbb{Q}$ parametrizable por medio de funciones modulares. (Hoy, gracias a la demostración completa de la conjetura STW, sabemos que esta condición no es restrictiva.) Demostraron que si la función L posee un cero simple en $s = 1$, entonces el rango de la curva elíptica es mayor o igual que 1:

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 1 \Longrightarrow \mathrm{rg} E(\mathbb{Q}) \geq 1.$$

El modelo sobre $\mathbb{Q}$ de la curva modular $X_0(N)$ puede ser descrito como la compactificación del espacio de módulos de las curvas elípticas dotadas de un subgrupo cíclico de orden N. Consideremos un cuerpo cuadrático imaginario K de discriminante D_K, que supondremos primo con N; sea $\mathcal{O}_K$ su anillo de enteros y h_K su número de clases. Un punto MC de $X_0(N)$ de discriminante D_K es un diagrama $x = (E \to E')$ en el que E y E' son curvas elípticas con multiplicación compleja por $\mathcal{O}_K$ y la flecha es una isogenia de orden N. Tales puntos existen si, y solamente si, D_K es un cuadrado módulo $4N$; en este caso, se tienen exactamente $2^t h_K$ puntos, siendo t el número de primos distintos que dividen a N. Todos los puntos MC de discriminante D son racionales sobre el cuerpo de clases de Hilbert $H = K(j(E))$; ello significa que E, E' y la isogenia entre ambas están definidas sobre H.

Sea $J = J_0(N)$ la variedad jacobiana de $X_0(N)$. La teoría de

Néron relativa a las alturas, formulada en 1965, da lugar a una forma bilineal $\langle\ ,\ \rangle$ en $J(H) \times J(H)$ que depende del divisor $2(\Theta)$ de J. Dado un punto x de multiplicación compleja de discriminante D_K, Gross y Zagier proceden en una primera parte del artículo al cálculo del símbolo $\langle c, T_m d^\sigma \rangle$, en donde $c := (x) - (\infty)$ y $d := (x) - (0)$ son divisores de grado cero asociados a x; T_m denota el m-ésimo operador de Hecke operando en J y σ es un automorfismo del grupo de Galois $\mathrm{Gal}(H/K)$. Cuando los divisores c y $T_m d^\sigma$ poseen soportes disjuntos, el símbolo global puede calcularse por medio de la suma de símbolos locales $\langle c, T_m d^\sigma \rangle_v$, en donde v recorre los lugares de H. El cálculo de los símbolos locales es completamente distinto según que v sea o no una lugar arquimediana de H.

El cálculo de los símbolos locales arquimedianos $\langle c, T_m d^\sigma \rangle_v$ se efectúa mediante la teoría del potencial. Para ello es necesario introducir una función de Green adecuada en la superficie de Riemann $X_0(N)(\mathbb{C})$. En la construcción de esta función intervienen la función de Legendre de segunda especie y la serie de Eisenstein de peso 0 relativa al punto parabólico ∞ de $\Gamma_0(N)$. Denotemos por $\mathcal{A}$ la clase de ideales que corresponde al automorfismo σ por la teoría de cuerpos de clases. Al evaluar la función de Green normalizada en pares de puntos de Heegner, se obtiene una expresión del símbolo local $\langle c, T_m d^\sigma \rangle_v$ en función de los números $r_{\mathcal{A}}(n)$ y $R_{\mathcal{A}}(n)$ de ideales enteros de norma n contenidos en la clase $\mathcal{A}$ y en el género que contiene a $\mathcal{A}$, respectivamente. Al evaluar el símbolo $\langle c, T_m d^\sigma \rangle_\infty$, definido por suma de todos los símbolos locales en los lugares arquimedianos, se obtiene una expresión en términos de la derivada logarítmica de la función zeta de Riemann (en $s = 2$) y de la derivada logarítmica de la función de Dirichlet $L(\chi_D, s)$ (en $s = 1$). En el caso en que los divisores c y $T_m d^\sigma$ no son primos entre sí, las fórmulas deben ser modificadas con unos términos correctivos en los que se hace uso de la función η de Dedekind y de la primera fórmula límite de Kronecker.

El cálculo de los símbolos locales no arquimedianos $\langle c, T_m d^\sigma \rangle_v$

se obtiene a partir de una teoría de intersección aritmética. Para ello debe considerarse un modelo entero $\mathcal{X}$ de la curva modular, definido sobre $\mathbb{Z}$, y las secciones $\underline{x}$ y $\underline{x}^\sigma$ en $X \otimes \mathcal{O}_{H,\sigma}$ definidas por los puntos c y d^σ. El modelo $\mathcal{X}$ se obtiene a partir del modelo propuesto por Deligne-Rapoport, en el caso en que N es libre de cuadrados, y del modelo propuesto por Katz-Mazur, en el caso general. La descripción de las fibras de mala reducción de X está basada en las clásicas congruencias de Kronecker para los polinomios modulares. El modelo $\mathcal{X}$ es regular sobre $\mathbb{Z}$ salvo en los puntos supersingulares en característica p, cuando $p \mid N$. El valor de los números de intersección locales $(\underline{x} \cdot \underline{x}^\sigma)$ se obtiene recurriendo a anillos de Witt para un cálculo del número de homomorfismos de grado m entre las correspondientes curvas elípticas. A su vez, este número se obtiene a partir del estudio de la aritmética de ciertos órdenes en álgebras de cuaternios definidas, interviniendo en su obtención la fórmula de congruencia debida a Eichler. Si los divisores no son primos entre sí, las fórmulas deben ser modificadas mediante el uso de la función η de Dedekind. En ambos casos hay tres tipos de fórmulas, según el tipo de descomposición en el cuerpo K que presenta el primo p tal que $v|p$.

Dada una forma modular parabólica nueva $f \in \mathcal{S}(\Gamma_0(N), 2k)$ y una clase de ideales $\mathcal{A}$ en el cuerpo cuadrático K, en el artículo que nos ocupa se pasa a definir una serie $L_{\mathcal{A}}(f, s)$ a partir de la serie $L(\chi_D, s)$ y de la convolución de $L(f, s)$ con la función zeta parcial de Dedekind $\zeta_{\mathcal{A}}(K, s)$ asociada a $\mathcal{A}$. Se prueba que la función $L_{\mathcal{A}}(f, s)$, corregida convenientemente con factores Γ, se extiende analíticamente a una función entera de s y satisface una ecuación funcional. Ello se logra a partir de una representación integral de $L_{\mathcal{A}}(f, s)$ cuyo núcleo está formado por el producto de una función theta parcial por una serie de Eisenstein. A continuación se deducen fórmulas para los valores de las funciones $L_{\mathcal{A}}(f, s)$ y $L'_{\mathcal{A}}(f, s)$, en $s = k$, que es el centro de simetría de la ecuación funcional. En el caso particular en que $k = 1$, en el cual f es de peso 2, los valores especiales $L_{\mathcal{A}}(f, 1)$ y $L'_{\mathcal{A}}(f, 1)$ se expresan por medio del producto escalar de Petersson de f

con una forma modular parabólica $\Phi_{\mathcal{A}}(z) = \sum_{m=1}^{\infty} a_{m,\mathcal{A}} e^{2\pi i m z}$ de peso 2 y de nivel N.

Al sumar las fórmulas obtenidas para todas las contribuciones arquimedianas y las no arquimedianas en el símbolo de Néron y tener en cuenta las fórmulas anteriores en el caso $k = 1$, se obtiene que:

$$\langle c, T_m c^{\sigma} \rangle = u^2 a_{m,\mathcal{A}},$$

en donde u es igual a $1/2$ del número de unidades de K. Esta igualdad es la que permite a Gross y Zagier obtener su resultado relativo a la conjetura BSD.

Gross y Zagier consideran una curva elíptica E definida sobre $\mathbb{Q}$ que sea modular; es decir para la cual existe un morfismo no trivial $\varphi : X_0(N) \to E$. En este caso existe una forma modular parabólica $f_E \in \mathcal{S}(\Gamma_0(N), 2)$ tal que $L(E/\mathbb{Q}, s) = L(f_E, s)$. Con ello, la conjetura de Hasse-Weil es cierta para E y la función $L(E, s)$ está definida para todo $s \in \mathbb{C}$. Traduciendo los resultados anteriores a este caso, Gross y Zagier deducen la existencia de un punto racional $P \in E(\mathbb{Q})$ para el cual

$$L'(E/\mathbb{Q}, 1) = \alpha \, \Lambda \, \langle P, P \rangle,$$

siendo $\alpha \in \mathbb{Q}^*$ un número racional no nulo, Λ el período real de una diferencial regular de $E/\mathbb{Q}$ y $\langle P, P \rangle$ el producto escalar definido por las alturas canónicas en E. En particular, si la función L posee en $s = 1$ un cero simple ($m = 1$), se deduce que $\langle P, P \rangle \neq 0$. Por las propiedades de la altura, ello implica que P debe ser un punto de orden infinito en E; o sea, el rango de E es $r \geq 1$.

Sólo nos resta precisar que el punto racional P de E se obtiene a partir de las trazas de puntos de multiplicación compleja situados en la variedad jacobiana $J_0(N)$ de la curva modular. Si x es un punto MC de discriminante D, entonces

$$P_K := \sum_{\sigma \in \mathrm{Gal(H/K)}} \varphi(x)^{\sigma},$$

y $P := P_K + \overline{P}_K$.

Un resultado posterior debido a Rubin demostró que, bajo las mismas condiciones, si el rango de E es $r \geq 2$, entonces la multiplicidad del cero en $s = 1$ es $m \geq 2$. En consecuencia, se tiene que $m = 1$ implica $r = 1$.

En el mismo trabajo, Gross y Zagier proporcionaron un ejemplo de una curva elíptica $E/\mathbb{Q}$ para la cual $m = r = 3$.

En la actualidad, todavía no se han podido dar ejemplos de curvas elípticas $E/\mathbb{Q}$ con rango analítico $m \geq 4$, aunque se tienen multitud de ejemplos de curvas elípticas con rango aritmético r alto. Un hito destacable en este sentido fué el conseguido por J. Quer en 1987 al construir una curva elíptica del tipo $Y^2 = X^3 + k$ de rango aritmético 12.

En 2006, N. Elkies batió el récord de los valores de r conocidos mediante la construcción de una curva elíptica de rango aritmético 28 dada por la ecuación

$$Y^2 + XY + Y = X^3 - X^2$$

$$-2006776241557552658503320820933854275093 0$$

$$230312178956502X$$

$$+3448161179503055646703298569039072037485 59$$

$$4435931918036126600829629193944873224342 9.$$

8.3. Las conjeturas de modularidad de Serre

La conjetura de Shimura-Taniyama-Weil, ya mencionada, forma parte de una extensa familia de conjeturas conocidas bajo la denominación genérica de conjeturas de modularidad. Entre

éstas, nos limitaremos a mencionar la conjetura de modularidad de Serre.

Una representación de Galois irreducible, continua y con determinante impar,

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}(2, R),$$

en la que $R = \overline{\mathbb{Z}}_p$, o bien $\overline{\mathbb{F}}_p$, se denomina modular de tipo (N, χ, k) si los polinomios característicos asociados a los elementos de Frobenius de $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ proceden de los coeficientes de Fourier de una forma modular parabólica de tipo (N, χ, k), bien porque son iguales, en el caso de característica cero, o bien porque se obtienen por reducción, en el caso de característica p.

En 1987, Serre formuló la conjetura por la cual toda representación $\rho : G_{\mathbb{Q}} \to \mathbf{GL}(2, \overline{\mathbb{F}}_p)$, irreducible e impar, debía ser modular y, además, de un tipo muy preciso $(N(\rho), k(\rho), \chi(\rho))$. El nivel $N(\rho)$ es el conductor de Artin de ρ, privado del primo p; el peso $k(\rho)$ se determina a partir de la configuración de Hodge-Tate de la restricción de ρ al grupo de inercia en p, y el carácter $\chi(\rho)$ se obtiene privando al determinante de ρ de la parte ramificada en el ideal (p).

En 1990, Ribet demostró un caso muy particular de la conjetura de modularidad de Serre, conocido como conjetura *epsilon*. Supongamos que $p \geq 3$ y que ρ es una representación de la cual sabemos que es modular y de tipo $(N\ell, 2, 1)$, siendo ℓ un número primo que no divide a N. Si $\ell \neq p$, supongamos que ρ es no ramificada en ℓ; si $\ell = p$, supongamos que ρ es finita en p. Bajo estas condiciones, Ribet demostró que ρ es modular de tipo $(N, 2, 1)$, de acuerdo con la conjetura de Serre. Notemos que el teorema de Ribet permite simplificar el primo ℓ del nivel cuando se dan las condiciones de ramificación apropiadas.

Aunque el teorema de Ribet demuestra únicamente un caso muy particular la conjetura de modularidad de Serre, se trata de un resultado muy notable por dos razones: por una parte, por las técnicas empleadas en su demostración y, por otra, porque de él

se dedujo que la conjetura STW implica el teorema de Fermat, tal como recordamos a continuación.

8.3.1. STW implica Fermat

Supongamos que (a, b, c) fuera una hipotética solución de la ecuación de Fermat $X^p + Y^p = Z^p$, para un exponente primo $p \geq 5$. Se tendría que

$$a^p + b^p = c^p, \quad a, b, c \in \mathbb{Z}, \quad abc \neq 0.$$

En 1986, G. Frey había asociado a una tal solución la curva elíptica:

$$E_{a,b,c} : \ Y^2 = X(X - a^p)(X + b^p).$$

Notemos que se trata de una curva elíptica definida sobre $\mathbb{Q}$. Frey observó que dicha curva parecía contradecir la conjetura STW. Como consecuencia del trabajo de Serre y de Ribet se pudo probar que, efectivamente, en el caso de existir una solución no trivial ($abc \neq 0$) de la ecuación de Fermat, la curva de Frey $E_{a,b,c}$ no sería modular. Las razones para ello son las siguientes: un cálculo del conductor $N_{a,b,c}$ de $E_{a,b,c}$ pone de manifiesto que éste es igual al radical de abc, o sea a un producto de la forma $2p_1 \cdots p_r$, siendo p_i los primos impares dos a dos distintos que dividen a abc. En particular, $E_{a,b,c}$ sería una curva elíptica de las denominadas semiestables. Si esta curva fuera modular (de acuerdo, con STW), existiría una forma modular $f_{a,b,c}$ en $\mathcal{S}(\Gamma_0(N_{a,b,c}), 2, 1)$ tal que

$$L(E_{a,b,c}, s) = L(f_{a,b,c}, s).$$

Miremos ahora la extensión de Galois de $\mathbb{Q}$ proporcionada por los puntos de p-división de $E_{a,b,c}$. Se tiene que

$$\mathbb{Q} \subseteq \mathbb{Q}(e^{2\pi i/p}) \subseteq \mathbb{Q}(E_{a,b,c}[p]).$$

La representación de Galois ρ_p correspondiente resulta ser irreducible, impar, no ramificada fuera de $2p$ y poco ramificada en

p. El cálculo de las constantes de Serre de la representación proporciona $N(\rho_p) = 2$, $k(\rho_p) = 2$, $\varepsilon(\rho_p) = 1$. Si la curva elíptica $E_{a,b,c}$ fuera modular, la representación ρ_p sería modular y, por el teorema de Ribet, debería provenir de una forma modular de tipo $(2, 2, 1)$, pues todos los primos p_i, salvo el 2 decaerían del nivel. Pero ello no puede ser, ya que al ser la curva modular $X_0(2)$ de género cero, el espacio de formas parabólicas $\mathcal{S}(\Gamma_0(2), 2, 1)$ es de dimensión cero.

Con ello quedó claro en 1990 que STW implicaba el teorema de Fermat y que, de hecho, para probar Fermat era suficiente demostrar STW para las curvas elípticas semiestables.

8.3.2. Demostración de la conjetura STW

La conjetura de Shimura-Taniyama-Weil (STW) se convirtió en un teorema gracias al impresionante trabajo de Wiles [1993], Taylor-Wiles [1993], Diamond [1996], Conrad-Diamond-Taylor [1998] y Breuil-Conrad-Diamond-Taylor [1999].

El método de la demostración de la modularidad de las curvas elípticas definidas sobre $\mathbb{Q}$ se basó en crear una teoría de deformaciones de representaciones de Galois gracias a la cual se pudo contagiar la modularidad a todas las curvas elípticas $E/\mathbb{Q}$, primero en el caso semiestable y, después, en el caso general, a partir de la modularidad conocida de ciertas representaciones de Galois en características 3 y 5.

Dada un curva elíptica $E/\mathbb{Q}$, un anillo universal de deformaciones $R_{\mathcal{D}}$ controla todas las deformaciones de representaciones en característica 3 o 5 asociadas a la 3-torsión, o a la 5-torsión de E y que pertenecen a un tipo $\mathcal{D}$ preciso, que se calcula a partir de la ramificación de la representación de Galois. El carácter modular de estas representaciones residuales se establece gracias a teoremas de Langlands (1980) y de Tunnell (1981) relativos a la conjetura de Artin, en los casos octaédrico y en ciertos casos icosaédricos. Este carácter modular permite establecer la existencia

de una flecha

$$\varphi : R_{\mathcal{D}} \twoheadrightarrow \mathbb{T}_{\mathcal{D}},$$

en donde $\mathbb{T}_{\mathcal{D}}$ es un anillo universal que controla todas las deformaciones que son modulares y de tipo $\mathcal{D}$. Bajo condiciones muy precisas para el tipo $\mathcal{D}$, φ es un isomorfismo. De ello, Wiles deduce la modularidad, en caracterísica cero, de la representación de Galois asociada a toda la p-torsión de E, para un primo conveniente, lo cual es equivalente a la modularidad de E.

En una primera estimación de los trabajos anteriores, cabría pensar que los grupos fuchsianos que intervienen en la demostración de STW se reducen a los subgrupos de congruencia del grupo modular o bien, equivalentemente, que las únicas curvas que juegan un papel relevante en la demostración de STW son las curvas modulares. Pero el hecho es que otra familia importante de subgrupos fuchsianos aritméticos y las curvas asociadas intervienen por partida doble en la demostración de la conjetura STW. Se trata de las curvas de Shimura, que ya hemos mencionado y de las cuales nos ocuparemos en el capítulo siguiente.

Digamos, al mismo tiempo, que las técnicas de Wiles y sus múltiples ramificaciones no solamente han permitido demostrar STW y, con ello, el teorema de Fermat, sino que se están utilizando para probar la conjetura de modularidad de Serre, en toda su generalidad.

Capítulo 9

Formas automorfas y aritmética

9.1. Variedades de Shimura

El estudio de las curvas modulares se generalizó en varias direcciones, dando lugar, todavía en un contexto clásico, al estudio de las variedades de Siegel y al de las variedades de Hilbert. Posteriormente, el estudio de dichas variedades se ha englobado en el de las variedades de Shimura. Se trata de variedades algebraicas que tienden a poseer buenos modelos aritméticos, caracterizados precisamente por su comportamiento frente a fenómenos de multiplicación compleja.

La definición general de una variedad de Shimura parte de un grupo algebraico reductivo G definido sobre el cuerpo racional y de una clase X de $G(\mathbb{R})$-conjugación de homomorfismos

$$\mathbb{S} \to G_{\mathbb{R}}$$

que dotan al álgebra de Lie $\mathfrak{g}$ de G de una estructura de Hodge conveniente. En la definición, $\mathbb{S}$ denota el grupo multiplicativo $\mathbb{C}^*$, interpretado como un toro sobre $\mathbb{R}$. Cada componente conexa X_i de X es isomorfa a un espacio simétrico hermítico. Para

cada subgrupo K del grupo de adeles $G(\mathbb{A}_f)$ de G, se tiene una variedad compleja

$$\mathrm{Sh}_K(G,X) = \bigcup \Gamma_i \backslash X_i.$$

Un teorema debido a Baily-Borel (1966) afirma que cada cociente aritmético $\Gamma\backslash X$ posee una estructura natural de variedad cuasi-proyectiva.

Al variar los subgrupos aritméticos Γ en G se obtiene un sistema proyectivo de variedades $\mathrm{Sh}(G,X)$, que admite la descripción siguiente:

$$\mathrm{Sh}(G,X) = G(\mathbb{Q})\backslash X \times G(\mathbb{A}_{\mathbb{Q},f}),$$

en donde $\mathbb{A}_{\mathbb{Q},f}$ denota el anillo de las adeles finitas del cuerpo racional. Con frecuencia, por variedad de Shimura se entiende el sistema proyectivo $\mathrm{Sh}(G,X)$.

El grupo de todos los puntos adélicos $G(\mathbb{A}_{\mathbb{Q},f})$ opera en la variedad de Shimura $\mathrm{Sh}(G,X)$. Su acción da lugar a que cada variedad $\Gamma\backslash X$ posea una familia suficientemente amplia de correspondencias de Hecke.

El sistema proyectivo $\mathrm{Sh}(G,X)$ está definido de manera natural sobre un cuerpo de números $E(G,X)$, denominado el cuerpo reflejo de la variedad. Ello se traduce en el hecho de que cada uno de los niveles finitos $\Gamma\backslash X$ está definido sobre una extensión específica de $E(G,X)$.

Las variedades de Shimura $\mathrm{Sh}(G,X)$ están dotadas de abundantes puntos MC o de multiplicación compleja, cuya definición generaliza en este contexto la del caso modular. La descripción de la acción del grupo de Galois absoluto $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ en los puntos MC y en el conjunto $\pi_0(\mathrm{Sh}(G,X))$ de componentes conexas de la variedad de Shimura da lugar a la denominada ley de reciprocidad de Shimura.

De entrada, las variedades $M = \Gamma\backslash X$ pueden ser proyectivas. En el caso contrario, admiten compactificaciones diversas.

De acuerdo con teoremas de Baily-Borel, la compactificación minimal M^* proporciona una variedad proyectiva. La compactificación de Borel-Serre $\overline{M}$ proporciona una variedad con esquinas. Entre $\overline{M}$ y M^* pueden darse distintas compactificaciones de tipo Satake. Las compactificaciones toroidales $\widetilde{M}$ se obtienen a partir de M^* por resolución de singularidades. Además se tienen aplicaciones naturales $\overline{M} \to M^*$, $\widetilde{M} \to M^*$.

En general, la cohomología compleja de las variedades de Shimura $H^*(\mathrm{Sh}(G,X),\mathbb{C})$ puede ser computada a través de la cohomología de álgebras de Lie. Las simetrías provenientes de los grupos adélicos $G(\mathbb{A}_{\mathbb{Q},f})$ proporcionan información sobre los grupos de cohomología étale $H^*(\mathrm{Sh}(G,X)),\mathbb{Q}_\ell)$. Puede decirse que los grupos de cohomología étale de las variedades de Shimura son una fuente natural para la producción de representaciones de Galois con buenas propiedades.

Bajo condiciones específicas, las variedades de Shimura admiten interpretaciones modulares como espacios que parametrizan motivos.

Se espera que la teoría de las variedades de Shimura pueda proporcionar la existencia de modelos canónicos definidos sobre el anillo de enteros $\mathcal{O}_E$ del cuerpo reflejo, que deberían ser lisos salvo en un conjunto concreto de primos. Las fibras de mala reducción se detectarían a partir de propiedades p-ádicas de los objetos que parametrizan. Las correspondencias de Hecke provenientes de la parte coprima con p, $G(\mathbb{A}^p_{\mathbb{Q},f})$, deberían poder extenderse a los modelos enteros canónicos locales para los primos p de buena reducción. Asimismo, los modelos canónicos enteros deberían estar provistos de buenas compactificaciones, tanto minimales como toroidales.

En algunos casos, Shimura ha podido establecer la existencia de modelos canónicos definidos sobre cuerpos de números para las variedades que llevan su nombre, y expresar sus funciones L en términos de formas automorfas respecto del grupo G que define la variedad y otro grupo ${}^LG$ deducido de G mediante una

relación de dualidad. Estos problemas han sido tratados especialmente en el caso de las variedades modulares de Siegel, de Hilbert y en el caso de las variedades de tipo PEL.

En general, las variedades de Siegel se uniformizan por medio de cocientes del espacio de Siegel $\mathcal{H}_g$ por la acción de subgrupos de congruencia del grupo modular simpléctico $\mathbf{Sp}(2g, \mathbb{Z})$. Admiten una interpretación modular en tanto que parametrizan variedades abelianas dotadas de estructuras de nivel. Una de las variedades de Siegel más básica es $\mathcal{A}_g$, el espacio de módulos de todas las variedades abelianas principalmente polarizadas y de dimensión g.

Las variedades de Hilbert admiten una uniformización por cocientes de copias del semiplano superior complejo bajo la acción de subgrupos de congruencia del grupo modular de Hilbert $\mathbf{SL}(2, \mathcal{O}_K)$, en donde K designa un cuerpo de números totalmente real. Son también espacios de módulos en tanto que parametrizan variedades abelianas dotadas de multiplicaciones reales.

9.2. Curvas de Shimura

Muchas de las propiedades conjeturales para las variedades de Shimura ya se conocen bien en el caso de dimensión uno.

Shimura interpreta las curvas $X(\Gamma)$, definidas a partir de la acción en $\mathcal{H}$ de grupos aritméticos, como espacios de módulos de superficies abelianas dotadas de multiplicación cuaterniónica y de estructuras de nivel. Esta interpretación modular es especialmente relevante para el estudio de la existencia de modelos enteros.

El estudio teórico de las curvas de Shimura permite definir una clase de funciones automorfas que generalizan de manera natural las funciones modulares elípticas. Los cuerpos generados por los valores especiales de estas funciones se identifican con cuerpos de clases radiales (en el sentido de la teoría de cuerpos

de clases) de cuerpos de números de tipo MC.

Sea F un cuerpo de números totalmente real de grado $n = [F : \mathbb{Q}]$. Sea B un álgebra de cuaternios sobre F totalmente indefinida; es decir, un álgebra B de dimensión 4 sobre F tal que $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \bigoplus_{i=1}^{n} \mathrm{M}_2(\mathbb{R})$. En este caso su discriminante $\mathrm{disc}(B) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2r}$ es producto de un número par de ideales primos distintos de F y $r \geq 1$. Designemos por $\mathcal{O}$ un orden maximal en B. Una variedad abeliana con multiplicación cuaterniónica por $\mathcal{O}$ sobre $\overline{\mathbb{Q}}$ es una variedad abeliana $A/\overline{\mathbb{Q}}$ tal que $\mathrm{End}(A) \simeq \mathcal{O}$ y $\dim(A) = 2n$. La elección de un cuaternio puro $\mu \in \mathcal{O}$ tal que $\mu^2 = -uD$, para cierta unidad de F totalmente positiva, permite considerar el siguiente problema de módulos: clasificar las clases de isomorfía de triples $(A, \iota, \mathcal{L})$ tales que: 1) A es una variedad abeliana de dimensión $g = 2n$; $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ es un homomorfismo de anillos y $\mathcal{L}$ es una polarización principal de A deducida de μ y que conmuta con la involución de Rosati: $\iota(\beta)^\circ = \iota(\mu^{-1}\overline{\beta}\mu)$, para todo $\mu \in \mathcal{O}$.

Fue probado por Shimura que el functor de módulos asociado al problema anterior es representable por un esquema cuasiproyectivo, reducido e irreducible, $\mathcal{X}_\mu/\mathbb{Q}$ definido sobre $\mathbb{Q}$ y de dimensión n. Además, si el álgebra B no es conmutativa, la variedad es completa. Si designamos por $\mathcal{H}$ el semiplano de Poincaré, la teoría de Shimura implica la existencia de un isomorfismo analítico

$$\mathcal{O}^1 \backslash \mathcal{H}^n \simeq \mathcal{X}_\mu(\mathbb{C}),$$

para el cual debe identificarse el grupo $\mathcal{O}^1$ de las unidades de $\mathcal{O}$ de norma 1 con un subgrupo totalmente discontinuo de $\mathbf{SL}(\mathbb{R})^n$.

9.2.1. Modelos canónicos

Algunas de las variedades de Shimura más útiles aparecen como espacios de módulos de esquemas abelianos, con estructuras de nivel extras, de la misma manera que las curvas modulares se interpretan como espacios de módulos de curvas elípticas. En

los años 1960, un generalización adecuada de la teoría de la multiplicación compleja en el caso modular condujo a Shimura a la creación de su teoría de los modelos canónicos.

Una de las primeras aplicaciones de las curvas de Shimura apareció en el artículo de Ribet de 1990, en el que probó la conjetura ε, como parte de la conjetura de modularidad de Serre. A su vez, las curvas de Shimura juegan un papel muy sutil en la misma demostración de Wiles de la conjetura STW. En ambos casos deben compararse las fibras de modelos enteros de jacobianas de curvas modulares con las fibras de modelos enteros de jacobianas de curvas de Shimura.

9.2.2. Funciones automorfas

Debido a su interés creciente, las variedades de Shimura han empezado a ser estudiadas desde un punto de vista efectivo. Incluso en el caso de dimensión 1, este estudio plantea diferencias notables respecto del caso modular. La teoría de Shimura establece la existencia de modelos en los cuales los puntos MC son algebraicos, aunque la teoría en sí no permite la construcción efectiva de los mismos.

Como era ya bien sabido por los clásicos, las funciones y las formas modulares poseen q-desarrollos en el infinito, en términos de la función $q(z) = e^{2\pi iz}$. Sin embargo, la falta de puntos parabólicos en las curvas de Shimura no modulares, o bien, si se prefiere, la no presencia de traslaciones en el grupo fuchsiano que las define, impide la utilización de desarrollos de Fourier para el tratamiento analítico de las funciones y de las formas automorfas involucradas en su estructura.

El estudio de las curvas de Shimura fue emprendido en Barcelona en la década de los 90, como continuación natural de los trabajos desarrollados en el caso de las curvas modulares. [1]

[1] Una muestra de los resultados obtenidos en el caso modular pude encon-

En dos tesis doctorales, de M. Alsina (2000) y de V. Rotger (2002), se trabajó la construcción de dominios fundamentales y su interpretación como espacios de módulos de superficies abelianas con multiplicación cuaterniónica. Aspectos fundamentales relativos a puntos MC fueron considerados en ambos trabajos.

En la tesis de Alsina y en una monografía de Alsina y Bayer publicada por la AMS en 2003, se puso de manifiesto que los puntos MC de una curva de Shimura están en correspondencia biyectiva con una clase de formas cuadráticas binarias con coeficientes algebraicos semienteros asociados a cada curva; además se hizo patente la existencia de unos puntos MC especiales, en número finito. Se formuló una teoría de reducción de formas cuadráticas binarias con coeficientes algebraicos semienteros que permite un tratamiento computacional de los puntos MC, paralelo al que en su día desarrollara Gauss en sus *Disquistiones arithmeticæ*.

Para asignar propiamente a cada curva de Shimura las formas cuadráticas binarias que le pertenecen debe recurrirse a otra interpretación de los puntos MC. Tales puntos vienen determinados a partir de inclusiones optimales de órdenes cuadráticos en órdenes cuaterniónicos, siendo útil en este estudio los resultados de Eichler que dan cuenta del número de tales inmersiones, convenientemente clasificadas. Para llevar a cabo una teoría de la reducción de tales formas o, equivalentemente, para entender los puntos como órbitas bajo la acción de grupos fuchsianos, es necesario describir estos grupos por generadores y relaciones. En cada caso concreto, ello equivale al cálculo de un dominio fundamental en el semiplano superior complejo $\mathcal{H}$ bajo la acción del grupo fuchsiano Γ. Los dominios fundamentales se obtuvieron gracias a la elaboración por parte de Alsina de software adecuado para trabajar con cuaternios. Se obtienen así polígonos hiperbólicos de un número par de lados, que son geodésicas, y dos a dos identificados. Las formas cuadráticas binarias asociadas a Γ son reducidas si, y solamente si, sus ceros con parte imaginaria

trarse en el monográfico especial del año 2000 que la Revista de la Academia dedicó a la teoría de números.

positiva caen en el interior de tales dominios. Notemos que en el caso modular el polígono que corresponde al grupo modular es la figura de Gauss.

En 2006, Bayer y J. Guàrdia desarrollaron un método que condujo a la obtención explícita de ecuaciones de curvas elípticas falsas asociadas a puntos MC de curvas de Shimura, siendo esencial en el mismo el uso de funciones theta con características y con variables en el espacio de Siegel $\mathcal{H}_2$. En este trabajo se hizo patente el papel de las estructuras de tipo PEL que permiten a Shimura dar una interpretación modular de sus curvas. Las iniciales P, E, L responden a la fijación de polarizaciones, endomorfismos y nivel. Si se parte de un punto MC de la curva de Shimura, se tiene un punto τ en $\mathcal{H}$. Las multiplicaciones cuaterniónicas y sus acciones permiten crear a partir de τ un retículo de dimensión 4. La elección de un cuaternio de norma 1 permite polarizar este retículo. A partir de la polarización del retículo y de normalizaciones adecuadas de éste, se construyen funciones theta explícitas que proporcionan una parametrización analítica de curvas de género 2 y que permiten obtener para las mismas ecuaciones con coeficientes algebraicos. Las jacobianas de tales curvas son los puntos clasificados por $X(\Gamma)$; es decir las curvas elípticas falsas.

Bayer y Travesa (2007) han establecido un método que permite la obtención de las funciones automorfas definidoras de curvas de Shimura mediante desarrollos adecuados alrededor de puntos MC. Se han efectuado los cálculos en el caso de la curva de Shimura básica ($N = 1$) asociada a un orden maximal del álgebra de cuaternios racional de discriminante $D = 6$ y alrededor de los puntos MC especiales. Las funciones automorfas del modelo canónico de Shimura se obtienen a partir de la integración de ecuaciones diferenciales de tercer orden, que se construyen a su vez a partir de los dominios fundamentales obtenidos y de cocientes suyos por involuciones. Una serie de recubrimientos de Galois asociados a tales cocientes permite la determinación de los parámetros accesorios que aparecen, de entrada, en las ecua-

ciones diferenciales asociadas a los dominios. Bayer y Travesa (2008) han demostrado recientemente la transcendencia de las constantes inherentes a los parámetros de uniformización local, análogas por tanto a π en el parámetro de uniformización local $q = e^{2\pi iz}$ del caso modular cuspidal. Mediante una interpretación adecuada de la fórmula de Chowla-Selberg, se calculan dichas constantes en términos de valores especiales de la función Γ de Euler.

9.3. Leyes de reciprocidad de Shimura

La teoría de la multiplicación compleja debida a Shimura distingue tres casos distintos: **SP** (simpléctico), **UT** (unitario), **UB** (unitario acotado), según sea el comportamiento de un grupo reductivo G en cada lugar arquimediana. Los casos se corresponden con los grupos $\mathbf{Sp}(n, \mathbb{R})$, $\mathbf{U}(n, n)$, $\mathbf{U}(m, n)$ y cada uno de ellos tiene su propia teoría de multiplicación compleja.

En general, Shimura establece la noción de punto de multiplicación compleja en espacios simétricos asociados a los grupos anteriores, de manera que se generalicen las definiciones clásicas. En los casos más tratables, tales puntos se definen a partir de variedades abelianas con un exceso de simetría.

Shimura ha desarrollado una teoría de funciones automorfas y de formas automorfas racionales sobre $\overline{\mathbb{Q}}$, de modo que los espacios de las formas automorfas están generados por formas automorfas con coeficientes algebraicos. En los casos **SP** y **UT**, la noción de $\overline{\mathbb{Q}}$-racionalidad está asociada a la naturaleza algebraica de los coeficientes de Fourier; en el caso **UB**, el concepto de $\overline{\mathbb{Q}}$-racionalidad se define en términos de propiedades de estas funciones en cada uno de los puntos de multiplicación compleja.

En los casos **SP**, **UT**, Shimura obtiene una ley de reciprocidad relativa a los valores de las funciones automorfas $\mathbf{f}$, $\overline{\mathbb{Q}}$-

racionales, valoradas en los puntos w de multiplicación compleja, que se expresa en un lenguaje adélico. La ley de reciprocidad describe la acción del grupo de Galois sobre los valores $\mathbf{f}(w)$ por medio del valor de una segunda función automorfa en w. Dado un elemento del grupo de Galois, esta segunda función es la imagen de $\mathbf{f}$ bajo un automorfismo del cuerpo de todas las funciones automorfas $\overline{\mathbb{Q}}$-racionales que se asocia al elemento de grupo de Galois. Para ello resulta de suma importancia un estudio previo de las variedades abelianas con MC.

Shimura también ha investigado las propiedades aritméticas de formas automorfas evaluando las derivadas de sus funcions zeta en puntos MC. Par ello debe previamente introducirse una familia adecuada de operadores diferenciales. Con ello se consigue cubrir el estudio de las series de Eisenstein.

En los casos **SP**, **UT**, una teoría de Hecke convenientemente generalizada permite asociar una familia de funciones $\mathcal{Z}(s, \mathbf{f}, \chi)$ a toda forma propia de Hecke. Completadas con factores Γ adecuados, estas funciones zeta admiten un prolongación analítica a todo el s-plano como funciones meromorfas con un número finito de polos, todos ellos simples.

En los tres casos, **SP**, **UT** y **UB**, dada una forma parabólica holomorfa $\mathbf{f}$ que sea una forma propia de todos los operadores de Hecke y que sea $\overline{\mathbb{Q}}$-racional, en cada punto crítico σ_0, el valor $\mathcal{Z}(\sigma_0, \mathbf{f}, \chi)/\mathbf{q}\langle \mathbf{f}, \mathbf{f}\rangle$, multiplicado por una potencia de π, es algebraico. En esta fórmula, $\langle \mathbf{f}, \mathbf{f}\rangle$ denota una generalización conveniente del producto escalar de Petersson, definido de una manera canónica y $\mathbf{q}$ es un cierto período, que es igual a 1 en los casos **SP**, **UT**.

9.4. Leyes de reciprocidad de Langlands

Como habrá podido observarse a través de los distintos capítulos de esta memoria, una de las características de la teoría de números del siglo XX ha sido el papel preponderante ejercido por las funciones zeta y las funciones L. Paulatinamente, se han ido interpretando las leyes de reciprocidad como igualdades entre dos familias de series L: una series L definidas a partir de datos diofánticos proporcionados por variedades algebraicas definidas sobre cuerpos de números, y otras series L definidas a partir de datos analíticos proporcionados por formas automorfas con respecto de grupos fuchsianos aritméticos. Tal como hemos indicado, la ley de reciprocidad de Artin admite esta formulación. Lo propio ocurre con las leyes de reciprocidad de Shimura.

En un trabajo de 1974 titulado *Some contemporary problems with origins in the Jugendtraum*, R. Langlands expresó su opinión de que una interpretación moderna del *Sueño de Juventud* de Kronecker debía dilucidar la naturaleza analítica de las funciones L de Hasse-Weil de las variedades de Shimura. Para ello estableció unas pautas encaminadas al tratamiento del tema en años sucesivos. El denominado Programa de Langlands, conocido también como filosofía de Langlands, constituye uno de los campos más fértiles de la producción actual en teoría de números.

Restringido al estudio de las extensiones abelianas de los cuerpos de números, el programa de Langlands reproduce la teoría clásica de cuerpos de clases. Por tanto, desde el punto de vista aritmético, el programa de Langlands responde a una posible extensión no abeliana de dicha teoría. De las distintas afirmaciones conjeturales que contempla, nos limitaremos a formular la ley de reciprocidad de Langlands.

Dada una extensión de Galois $K|E$ de cuerpos de números y una representación lineal irreducible compleja de dimensión n de

su grupo de Galois (o, más generalmente, de su grupo de Weil),

$$\rho : \mathrm{Gal}(K|E) \longrightarrow \mathrm{GL}(V),$$

la conjetura de reciprocidad de Langlands implica la existencia de una representación automorfa cuspidal π_ρ del grupo lineal adélico $\mathbf{GL}(n, \mathbb{A}_E)$ tal que

$$L(\pi_\rho, s) = L(\rho, s),$$

en donde $L(\rho, s)$ es la función L de Artin de la representación ρ.

El lado izquierdo de la ley de reciprocidad de Langlands es aritmético y la fuente natural de las representaciones que en él aparecen serían las representaciones de Galois proporcionadas por la cohomología ℓ-ádica de las variedades de Shimura. En el caso clásico, en este lado de la igualdad aparecen los productos de Euler, convergentes, en general, en ciertos semiplanos.

En el lado derecho se concentra el análisis y en él se insertan resultados anteriores de Harish-Chandra y I. Gelfand sobre representaciones de grupos de Lie semisimples. Al concepto de representación automorfa cuspidal se llega tras un largo camino, que se inicia con el concepto de serie de Dirichlet asociada a un carácter, de serie L asociada a un carácter de Hecke, de forma automorfa (en particular, modular, de Hilbert o de Siegel) y, finalmente, de representación automorfa cuspidal. En el caso clásico estas series poseen prolongación analítica y satisfacen ecuaciones funcionales.

Pero el Programa de Langlands no se reduce a los términos anteriores. Por una parte, podemos cambiar el cuerpo base por un cuerpo local o por un cuerpo de funciones en una variable y de característica positiva. Se tienen entonces el Programa local de Langlands. Por otra parte, pueden cambiarse los grupos lineales por otros grupos reductivos G, en cuyo caso, la teoría contempla, además del grupo G, su grupo dual de Langlands ${}^L G$. En este caso, las funciones L se construyen asociadas a representaciones cuspidales de G y a representaciones finitas del

grupo dual. Además debe satisfacerse un principio de functorialidad que conecta las teorías asociadas a los distintos grupos de manera natural.

Las ideas anteriores se trasladan asimismo al denominado Programa geométrico de Langlands. En los casos considerados como más asequibles, este programa relaciona ciertas representaciones ℓ-ádicas del grupo fundamental de una curva algebraica compleja con objetos de la categoría derivada de haces ℓ-ádicos sobre espacios de módulos de fibrados vectoriales sobre la curva.

Cronología

Pierre de **Fermat** (1601-1665)

John **Wallis** (1616-1703)

Giovanni **Cassini** (1625-1712)

Ehrenfried Walther **von Tschirnhaus** (1646-1716)

Jacob **Bernoulli** (1654-1705)

John **Bernoulli** (1667-1748)

Giulio **Fagnano** (1707-1766)

Leonhard **Euler** (1707-1783)

Joseph-Louis de **Lagrange** (1736-1813)

Adrien-Marie **Legendre** (1752-1833)

Lazare **Carnot** (1753-1823)

Gaspard **de Prony** (1755-1839)

Paolo **Ruffini** (1765-1822)

Jean-Baptiste-Joseph **Fourier** (1768–1830)

Carl Friedrich **Gauss** (1777-1855)

Nicolaï Ivanovitch **Lobatschevski** (1792-1856)

Christoph **Gudermann** (1798-1852)

Niels Henrik **Abel** (1802-1829)

Carl Gustav Jacob **Jacobi** (1804-1851)

George Birch **Jerrard** (1804-1863)

Gustav Peter Lejeune **Dirichlet** (1805-1859)

William R. **Hamilton** (1805-1865)

Joseph **Liouville** (1809-1882)

Ernst Eduard **Kummer** (1810-1893)

Évariste **Galois** (1811-1832)

Adolph **Göpel** (1812-1847)

Karl **Weierstrass** (1815-1897)

Johann Georg **Rosenhain** (1816-1887)

Charles **Hermite** (1822-1901)

Ferdinand Gotthold Max **Eisenstein** (1823-1852)

Leopoldt **Kronecker** (1823-1891)

Enrico **Betti** (1823-1892)

Francesco **Brioschi** (1824-1897)

Georg Friedrich Bernhard **Riemann** (1826-1866)

Julius Wilhelm Richard **Dedekind** (1831-1916)

Immanuel Lazarus **Fuchs** (1833-1902)

C. J. **Thomae** (1840-1921)

Friedrich Emil **Prym** (1841-1915)

Marius Sophus **Lie** (1842-1899)

Heinrich **Weber** (1842-1913)

Hermann Amandus **Schwarz** (1843-1921)

William Kingdom **Clifford** (1845-1879)

Georg **Cantor** (1845-1918)

Georg Ferdinand **Frobenius** (1849-1917)

Felix **Klein** (1849-1925)

Ludwig **Stickelberger** (1850-1936)

Henri **Poincaré** (1854-1912)

Charles Emile **Picard** (1856-1941)

Mathias **Lerch** (1860-1922)

Robert **Fricke** (1861-1930)

David **Hilbert** (1862-1943)

Axel **Thue** (1863-1922)

Hermann **Minkowski** (1864-1909)

Wilhelm **Wirtinger** (1865-1945)

Philipp **Furtwängler** (1869-1940)

Louis **Bachelier** (1870-1946)

Teiji **Takagi** (1875-1960)

Srinivasa **Ramanujan** (1877-1920)

Rudolf **Fueter** (1880-1950)

Gustav **Herglotz** (1881-1953)

Emmy **Noether** (1882-1935)

Solomon **Lefschetz** (1884-1972)

Heinrich **Brandt** (1886-1954)

Erich **Hecke** (1887-1947)

Louis Joel **Mordell** (1888-1972)

Grigorevich **Chebotarev** (1894-1947)

Carl Ludwig **Siegel** (1896-1981)

Emil **Artin** (1898-1962)

Helmut **Hasse** (1898-1979)

Richard **Brauer** (1901-1977)

Alexander **Gelfond** (1906-1968)

André **Weil** (1906-1998)

Max **Deuring** (1907-1984)

Sarvadaman **Chowla** (1907-1995)

Claude **Chevalley** (1909-1984)

Theodor **Schneider** (1911-1988)

Martin **Eichler** (1912-1992)

Izráil **Gelfand** (1913-)

Kunihiko **Kodaira** (1915-1997)

Kenkichi **Iwasawa** (1917-1998)

Atle **Selberg** (1917-2007)

Harish-Chandra (1923-1983)

Armand **Borel** (1923-2003)

Igor **Shafarevich** (1923-)

Klaus Friedrich **Roth** (1925-)

John **Tate** (1925-)

Jean-Pierre **Serre** (1926-)

Yukata **Taniyama** (1927-1958)

Serge **Lang** (1927-2005)

Peter **Swinnerton-Dyer** (1927-)

Alexander **Grothendieck** (1928-)

Goro **Shimura** (1930-)

Bryan John **Birch** (1931-)

Robert **Langlands** (1936-)

Alan **Baker** (1937-)

Barry **Mazur** (1937-)

David **Mumford** (1937-)

Enrico **Bombieri** (1940-)

Andrew P. **Ogg** (1943-)

Pierre **Deligne** (1944-)

Gerhard **Frey** (1944-)

John Henry **Coates** (1945-)

David **Chudnovsky** (1947-)

Don Bernhard **Zagier** (1951-)

Gregory **Chudnovsky** (1952-)

Andrew John **Wiles** (1953-)

Gerd **Faltings** (1954-)

Karl **Rubin** (1956-)

Paul **Vojta** (1957-)

Noam **Elkies** (1966-)

Bibliografía

[1] Abel, N. H.: Recherches sur les fonctions elliptiques *J. reine u. angew. Math.***2** (1827), 101-181. *J. reine u. angew. Math.***3** (1828), 160-190.

[2] Alsina, M.: *Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de Shimura.* Tesis. Dir. P. Bayer. Universitat de Barcelona, 2000.

[3] Alsina, M.; Bayer, P.: *Quaternion orders, quadratic forms and Shimura curves.* CRM Monograph Series **22**. American Mathematical Society, Providence, RI, 2004. xvi+196 pp. ISBN: 0-8218-3359-6.

[4] Arenas, A.; Bayer, P.: Heegner points on modular curves. *Rev. R. Acad. Cienc. Exactas Fís. Nat.* **94** (2000), no. 3, 323–332.

[5] Arenas, A.; Bayer, P.: Complex multiplication points on modular curves. *Rev. R. Acad. Cienc. Exactas Fís. Nat.* 94 (2000), no. 3, 333–338.

[6] Artin, E.: Quadratische Körper im Gebiete der höheren Kongruenzen I, II. *Math. Z.* **19** (1924), 153-206.

[7] Ayoub, R.: The lemniscate and Fagnano's contributions to elliptic integrals. *Arch. Hist. Exact Sci.* **29** (1984), no. 2, 131-149.

[8] Bachelier, L.: *Théorie de la spéculation. Théorie mathématique du jeu*, 1900. Éditions Jacques Gabay, 1995.

[9] Bayer, P.: Uniformization of certain Shimura curves. *Differential Galois Theory*, Bedlewo, 2001, T. Crespo and Z. Hajto (eds.). Banach Center Publications **58** (2002), 13-26. Polish Acad. Sci., Warsaw, 2002.

[10] Bayer, P.: Jean-Pierre Serre: An Overwiew on his Work. *The Abel Prize 2003-2007. The first five years: 2003-2007*, pp. 33–80. H. Holden and R. Piene (editors). Springer, 2010. ISBN: 978-3-642-01372-0.

[11] Bayer, P.; Guàrdia, J.: A la recerca de pi. *But. Soc. Catalana Mat.* **17** (2002), no. 2, 7–19.

[12] Bayer, P.; Guàrdia, J.: On equations defining fake elliptic curves. *J. Théor. Nombres Bordeaux* 17(2005), no. 1, 57–67.

[13] Bayer, P.; Guàrdia, J.: Uniformization of Fermat curves. *Ramanujan J.* **12** (2006), 207-223.

[14] Bayer, P.; Travesa, A. (eds.): *Curves modulars: Taules.* Notes del Seminari de Teoria de Nombres **1**, ISBN: 84-604-3577-6. Barcelona, 1992.

[15] Bayer, P.; Travesa, A.: Órdenes matriciales generados por grupos de congruencia. *Rev. R. Acad. Cienc. Exactas Fís. Nat.* **94** (2000), no. 3, 339–346.

[16] Bayer, P.; Travesa, A.: Formas cuadráticas ternarias e inmersiones matriciales de órdenes cuadráticos. *Rev. R. Acad. Cienc. Exactas Fís. Nat.* **94** (2000), no. 3, 347–355.

[17] Bayer, P.; Travesa, A.: Inmersiones de órdenes cuadráticos en el orden generado por $\Gamma_0(N)$. *Rev. R. Acad. Cienc. Exactas Fís. Nat.* **94** (2000), no. 3, 357–376.

[18] Bayer, P.; Travesa, A.: Uniformization of triangle modular curves. *Publ. Mat.*, extra vol. (2007), 43-106.

[19] Bayer, P.; Travesa, A.: Uniformizing functions for certain Shimura curves, in the case $D = 6$. *Acta Arith.* **126** (2007), no. 4, 315-339.

[20] Bayer, P.; Travesa, A.: On Local Constants Associated to Arithmetical Functions. *Pure Appl. Math. Q.* **4** (2008), no. 4, 1107-1132. [Special issue: in honor of Jean-Pierre Serre, Part 1 of 2].

[21] Beilinson, A. A.: Higher regulators and values of L-functions. *Current problems in mathematics*, Vol. 24, 181–238, Itogi Nauki i Tekhniki, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform. Moscow, 1984.

[22] Bombieri, E.: The Mordell conjecture revisited. *Ann. Scuola Norm. Sup. Pisa* Cl. Sci. **17** (1990), no. 4, 615–640.

[23] Breuil, C.; Conrad, B.; Diamond, F.; Taylor, R.: On the modularity of elliptic curves over $\mathbb{Q}$, or wild 3-adic exercicies. *J. Amer. Math. Soc.* **14** (2001), no. 4, 843–939.

[24] Browder, F. E.(ed.): *Mathematical developments arising from Hilbert problems.* Symposium in Pure Mathematics. Northern Illinois University, 1974. Proceedings of Symposia in Pure Mathematics, v. 28. Americal Mathematical Society, 1976.

[25] Chebotarev, N.: Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substituionsklasse gehören. *Math. Ann.* **95** (1925), 191–228.

[26] Chudnovsky, G. V.: *Proceedings of the International Congress of Mathematicians.* Helsinki 1978, pp- 339-350. Acad. Sci. Fennica, Helsinki, 1980.

[27] Chudnovsky, D. V.; Chudnovsky, G. V.: *Transcendental Methods and Theta Functions.* Proc. Symp. Pure Mathematics 49 (1989), 167-232.

[28] Coates, J.; Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* **39** (1977), no. 3, 223–251.

[29] O'Connor, J. J.; Robertson, E. F.: The MacTutor History of Mathematics archive. http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Legendre.html.

[30] Conrad, B.; Diamond, F.; Taylor, R.: *Modularity of certain potentially Barsotti-Tate Galois representations* (1999). *J. Amer. Math. Soc.* **12** (1999), no. 2, 521–567.

[31] Cox, D. A.: *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication.* A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. xiv+351 pp. ISBN: 0-471-50654-0; 0-471-19079-9.

[32] Davenport, H.; Hasse, H.: Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen *J. reine u. angew. Math.* **172** (1935), no. 1, 151-182. *Mathematische Abhandlungen.* Bd. 3. Walter de Gruyter, 1975.

[33] Dedekind, R.: Schreiben an Herrn *Borchardt* über die Theorie der elliptischen Modul-Functionen. *J. für reine u. angew. Math.* **83** (1877), 265-292.

[34] Deligne, P.: Travaux de Shimura. *Séminaire Bourbaki*, 23ème année (1970/71), Exp. No. 389, pp. 123–165. Lecture Notes in Math., Vol. 244, Springer, Berlin, 1971.

[35] Deligne, P.: La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.* No. 43 (1974), 273–307.

[36] Deuring, M.: Zur arithmetischen Theorie der algebraischen Funktionen. *Math. Ann.* **106** (1932), 103-106.

[37] Deuring, M.: Zur Theorie der Idealklassen in algebraischen Funktionenkörpern. *Math. Ann.* **106** (1932), 103-106.

[38] Deuring, M.: Galoische Theorie und Darstellunstheorie. *Math. Ann.* **107** (1932), 140-144.

[39] Deuring, M.: Anwendungen der Darstellungen von Gruppen durch lineare Substitutionen auf die galoissche Theorie. *Math. Ann.* **113** (1937), no. 1, 40-47.

[40] Deuring, M.: Invarianten und Normalformen elliptischer Funktionenkörper. *Math. Z.* **47** (1940), 47-56.

[41] Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197-272.

[42] Deuring, M.: Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers. *Math. Z.* **47** (1942), 643-654.

[43] Deuring, M.: Die Anzahl der Typen von Maximalordnungen in einer Quaternionenalgebra von primer Grundzahl. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. Math. Phys. Chem. Abt. 1945* (1945), 48-50.

[44] Deuring, M.: Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung. *Comment. Math. Helv.* **19** (1946), 74-82.

[45] Deuring, M.: Zur Theorie der elliptischen Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg* **15** (1947), 211-261.

[46] Deuring, M.: Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl. *Jber. Deutsch. Math. Verein.* **54** (1950), 24-41.

[47] Deuring, M.: Die Struktur der elliptischen Funktionenkörper und die Klassenkörper der imaginären quadratischen Zahlkörper. *Math. Ann.* **124** (1952), 393-426.

[48] Deuring, M.: Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins I, II, III, IV. *Nachr. Akad. Wiss. Göttingen. Math. Phys., Kl. Math. Phys. Chem. Abt., 1953* (1953), 85-94. *Nachr. Akad. Wiss. Göttingen. Math. Phys., Kl. IIa, 1955* (1955), 13-42. *Nachr. Akad. Wiss. Göttingen. Math. Phys., Kl. IIa, 1956* (1956), 37-76. *Nachr. Akad. Wiss. Göttingen. Math. Phys., Kl. IIa, 1957* (1957), 55-80.

[49] Deuring, M.: Zur Transformationstheorie der elliptischen Funktionen. *Akad. Wiss. Mainz. Abh. Math.-Nat. Kl. 1954* (1954), 95-104.

[50] Deuring, M.: On the zeta-function of an elliptic function field with complex multiplications. *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955*, pp. 47-50. Science Council of Japan, Tokyo, 1956.

[51] Deuring, M. Die Klassenkörper der komplexen Multiplikation. *Enzyklopädie der mathematischen Wissenschaften: Mit Einschluss ihrer Anwendungen, Band I 2, Heft 10, Teil II (Article I 2, 23)* B. G. Teubner Verlagsgesellschaft, Stuttgart 1958.

[52] Dieudonné Jean (ed.): *Abrégé d'histoire des mathématiques 1700–1900.* Tome I. Hermann, Paris, 1978. x+392 pp. ISBN: 2-7056-5870-X. Tome II. Hermann, Paris, 1978. vii+469 pp. ISBN: 2-7056-5871-9.

[53] Eichler, M.: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Arch. Math.* **5** (1954), 355–366.

[54] Eisenstein, G.: Beiträge zur Theorie der elliptischen Funktionen I: Ableitung des biquadratischen Fundamentaltheorems aus der Theorie der Lemniskatenfunctionen, nebst Bemerkungen zu den Multiplications- und Transformationsformeln. *J. reine u. angew. Math.* **30** (1846), 185–210.

[55] Elkies, N. D.: *Shimura curves computations.* Lecture Notes in Computer Sciences 1423, Springer, 1998, 1-49.

[56] Euler, L.: De comparatione arcuum curvarum irrectificabilium (Sobre la comparación de los arcos de curva no rectificables). *Novi commentarii academiae scientiarum Petropolitanae* 6(1756/57), 58-84. *Opera Postuma* 1, 1862, pp. 452-486. *Opera Omnia*: Series 1, Volume 21, pp. 296 - 357.

[57] Euler, L.: *Introductio in analysin infinitorum.* Traducción española: *Introducción al análisis de los infinitos.* A. J. Durán Guardeño; F. J. Pérez Fernández (eds.). Traducido por José Luis Arantegui Tamayo y anotado por Antonio José Durán Guardeño. SAEM "Thales". Real Sociedad Matemática Española, 2000. ISBN: 84-923760-3-1; 84-923760-4-X.

[58] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73** (1983), no. 3, 349–366.

[59] Frey, G.: Links between stable elliptic curves and certain diophantine equations. *Ann. Univ. Saraviensis, Math. Ser.* **1** (1986), 1-40.

[60] Frobenius, F. G.: *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe.* Sitzungsberichte Königl. Preussisch. Akad. Wissenschaft. Berlin (1896), 689-703. Gesammelte Abhandlungen II, 719-733. Springer, 1968.

[61] Fuchs, L.: Zur Theorie der linearen Differentialgleichungen mit veränderlichen Coefficienten. *J. für reine u. angew. Math.* **66** (1866), 121-160.

[62] Fuchs, L.: Ueber eine Klasse von Funktionen mehrerer Variablen, welche durch Umkehrung der Integrale von Lösungen der linearen Differential Gleichungen mit rationalen Coeffizienten entstehen *J. für reine u. angew. Mathematik*, **89** (1880), 151-169.

[63] Gauss, C. F.: *Disquisitiones arithmeticæ*. Lipsiae, 1801. Traducción catalana: *Disquisicions aritmètiques*. Traducció i pròleg de Griselda Pascual Xufré. Societat Catalana de Matemàtiques, 1996. ISBN 84-7283-313-5.

[64] Gauss, C. F.: Gauss'wissenschaftliches Tagebuch 1796-1814. Mit Anmerkungen herausgegeben von Felix Klein. *Math. Ann.* **57** (1903), 1–34.

[65] Gross, B. H.: On the periods of abelian integrals and a formula of Chowla and Selberg. With an appendix by David E. Rohrlich. *Invent. Math.* **45** (1978), no. 2, 193-211.

[66] Hasse, H.: Zum Hauptidealsatz der komplexen Multiplikation. *Monatsh. Math. Phys.* **38** (1931), no. 1, 315-322. *Mathematische Abhandlungen.* Bd. 3. Walter de Gruyter, 1975.

[67] Hasse, H.: Ein Satz über die Ringklassenkörper der komplexen Multiplikation. *Monatsh. Math. Phys.* **38** (1931), no. 1, 323-330. *Mathematische Abhandlungen.* Bd. 3. Walter de Gruyter, 1975.

[68] Hasse, H.: Das Zerlegungsgesetz für die Teiler des Moduls in den Ringklassenkörpern der komplexen Multiplikation. *Monatsh. Math. Phys.* **38**(1931), no. 1, 331-344. *Mathematische Abhandlungen.* Bd. 3. Walter de Gruyter, 1975.

[69] Hasse, H.: Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern. *Abh. Math. Sem. Hamburg* **10** (1934), 325-348. *Mathematische Abhandlungen.* Bd. 3. Walter de Gruyter, 1975.

[70] Hasse, H.: Zur Theorie der abstrakten elliptischen Funktionenkörper I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung. *J. reine u. angew. Math.* **175** (1935), no. 1, 55-62. *Mathematische Abhandlungen.* Bd. 3. Walter de Gruyter, 1975.

[71] Hasse, H.: Zur Theorie der abstrakten elliptischen Funktionenkörper II. Automorphismen und Meromorphismen. Das Additionsthm. *J. reine u. angew. Math.* **175** (1935), no. 1, 151-182. *Mathematische Abhandlungen.* Bd. 3. Walter de Gruyter, 1975.

[72] Hasse, H.: Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die struktur des Meromophismenrings. Die Riemannsche Vermutung. *J. reine u. angew. Math.* **175** (1935), no. 1, 151-182. *Mathematische Abhandlungen.* Bd. 3. Walter de Gruyter, 1975.

[73] Hasse, H.: Der n-Teilungskörper eines abstrakten elliptischen Funktionenkörpers als Klassenkörper, nebst Anwendung auf den Mordell-Weilschen Endlichkeitssatz. *Math. Z.* **48** (1942), 48-66. *Mathematische Abhandlungen.* Bd. 3. Walter de Gruyter, 1975.

[74] Hasse, H.: Zetafunktion und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus. *Abh. Deutsch. Akad. Wiss. Berlin., Kl. Math. Nat.* 1954 (1954), no. 4, 70 pp. (1955). *Mathematische Abhandlungen.* Bd. 3. Walter de Gruyter, 1975.

[75] Hermite, Ch.: *Œuvres complètes*, 4 volúmenes. Émile Picard (ed.). Académie des sciences de France. Gauthier-Villards, 1905-1917.

[76] Herglotz, G.: Über das quadratische Reziprozitätsgestz in imaginären quadratische Zahlkörpern. Ges. Werke 396-410. FdM 48 (1921/22).

[77] Hilbert, D.: Einer neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper. *Nachr. K. Ges. Wiss. Göttingen* (1896), 29–39. *Ges. Abh.* I, pp. 53-62.

[78] Hilbert, D.: *The theory of algebraic number fields.* Translated from the German and with a preface by Iain T. Adam-

son. With an introduction by Franz Lemmermeyer and Norbert Schappacher. Springer-Verlag, Berlin, 1998. xxxvi+350 pp. ISBN: 3-540-62779-0. Traducción del *Zahlbericht* cuya primera edición apareció en 1897.

[79] Ihara, I.: Schwarzian equations, *J. Fac. Sci. University of Tokyo* **21** (1974), 97-118.

[80] Jacobi, C. G. J.: *Fundamenta nova theoriae functionum ellipticarum*, 1829. Gesammelte Werke, Bd. 1. Berlin, 1881.

[81] Jacobi, C. G. J.: Gesammelte Werke. 8 Bände. Chelsea 1969.

[82] Klein, F.: Ueber die Transformation der elliptischen Functionen und die Auflösung der Gleichungen fünften Grades. *Math. Ann.* **14** (1879), 111-145.

[83] Klein, F.: *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade.* Reprogr. Nachdr. der Ausg. Leipzig, Teubner 1884. Hrsg. mit einer Einf. und mit Kommentaren von Peter Slodowy. Birkhäuser, 1993. ISBN: 3-7643-2454-6.

[84] Klein, F.: *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert.* 2 Bde. (GMW, Bde. 24 u. 25). Springer, Berlin, 1926-1927. Reimpresión, Springer, 1979.

[85] Klein, F.: *Vorlesungen über nicht-euklidische Geometrie. Neu bearbeitet von W. Rosemann.* GMW, Bd.26. Springer, Berlin, 1928.

[86] Klein, F.: *Vorlesungen über die hypergeometrische Funktion gehalten an der Universität Göttingen im Wintersemester 1893/1894.* GMW Bd. 39. Springer, Berlin 1933.

[87] Klein, F.; Fricke, R.: *Vorlesungen Über die Theorie der elliptischen modulfunktionen I und II.* Teubner Stuttgart, 1966. Reimpresión de 1890/92.

[88] Krazer, A.: *Lehrbuch der Thetafunktionen* Chelsea, 1970. Primera edición: Leipzig, 1903.

[89] Kronecker, L.: Über die algebraisch auflösbaren Gleichungen. *Monatsber. Akad. Berlin* (1853), 365-374; Werke IV, pp. 3–11.

[90] Kronecker, L.: Über Abelsche Gleichungen. *Monatsber. Akad. Berlin* (1877), 845-851; Werke IV, pp. 63-71.

[91] Kronecker, L.: Carta a Dedekind del 15 de marzo de 1880. Werke V, pp. 453-457.

[92] Lange, H.; Birkenhake, C.: *Complex Abelian Varieties.* GMW **302**, 1992.

[93] Langlands, R. P.: Some contemporary problems with origins in the Jugendtraum. *Mathematical developments arising from Hilbert problems.* F. E. Browder (ed.). Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974, pp. 401–418. Amer. Math. Soc., Providence, R. I., 1976.

[94] Langlands, R. P.: Automorphic representations, Shimura varieties, and motives. Ein Märchen. *Automorphic forms, representations and L-functions.* Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977, Part 2, pp. 205–246, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.

[95] Lawden, D. F.: *Elliptic Functions and Applications.* Colledge Press, 1998.

[96] Lefschetz, S.: On certain numerical invariants of algebraic varieties with application to abelian varieties. *Trans. Amer. Math. Soc.* **22** (1921), no. 3 327-406; **22** (1921), no. 4, 407-482.

[97] Legendre, A. M.: Recherches d'analyse indéterminée. *Histoire de l'Académie Royale des Sciences de Paris* (1785), 465-559, Paris 1788.

[98] Lehner, J.: *Discontinuous Groups and Automorphic Functions.* Mathematical Surveys and Monographs **8**. AMS, 1964.

[99] Lemmermeyer, F.: *Reciprocity Laws: from Euler to Eisenstein.* Springer, 2000. ISBN: 3-540-66967-4.

[100] Mazur, B.: Modular curves and the Eisenstein ideal. *Inst. Hautes études Sci. Publ. Math.* **47** (1977), 33–186.

[101] Mordell, L. J.: On the rational solutions of the indeterminate equations of the third and four degrees. *Proc. Cambridge Phil. Soc.* **22** (1922), 179-192

[102] Neukirch, J.: *Algebraische Zahlentheorie.* Springer, 1992. ISBN: 3-540-54237-6.

[103] Poincaré, H.: *Œuvres de Henri Poincaré.* Gauthier-Villars, 1916-1954.

[104] Poincaré, H.: Sur les propriétés arithmétiques des courbes algébriques. *Journal de Mathématiques* t. **7** (1901), 161-233.

[105] Poincaré, H.; Picard, E.: Sur un théorème de Riemann relatif aux fonctions de n variables indépendentes admettant $2n$ systèmes de périodes. *Comptes rendus de l'Académie des Sciences* **97** (1883), 1284-1287.

[106] Quer, J.: Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12. *C. R. Acad. Sci. Paris.* Sér. I Math. **305** (1987), no. 6, 215–218.

[107] Rotger, V.: *Abelian varities with quaternionic multiplication and their moduli.* Tesis. Dir. P. Bayer. Universitat de Barcelona, 2002.

[108] Rotger, V.: On the group of automorphisms of Shimura curves and applications. *Compositio Math.* **132** (2002), no. 2, 229–241.

[109] Rotger, V.: Quaternions, polarization and class numbers. *J. reine u. angew. Math.* **561** (2003), 177–197.

[110] Rotger, V.: Modular Shimura varieties and forgetful maps. *Trans. Amer. Math. Soc.* **356** (2004), no. 4, 1535–1550.

[111] Rotger, V.: Shimura curves embedded in Igusa's threefold. *Modular curves and abelian varieties*, 263–276, Progr. Math. 224. Birkhäuser, Basel, 2004.

[112] Riemann, B.: Theorie der Abel'schen Functionen. *Gesammelte mathematische Werke.* Teuber, 1892.

[113] Riemann, B.: Ueber die Anzahl der Primzahlen unter einer gegebenen Größe. *Monatsberichte der Berliner Akademie* (1859), 671-680. *Gesammelte mathematische Werke.* Teuber, 1892.

[114] Selberg, A.; Chowla, S.: On Epstein's zeta-function. *J. Reine Angew. Math.* **227** (1967), 86-110.

[115] Serre, J-P.: Une interprétation des congruences relatives à la fonction τ de Ramanujan. 1967/68 *Séminaire Delange-Pisot-Poitou*: Théorie des Nombres, Exp. 14. Secrétariat mathématique, Paris. *Oeuvres. Collected Papers*, v. 2. Springer, 1986.

[116] Serre, J-P.: Facteurs locaux des fonctions zeta des variétés algébriques (définitions et conjectures). 1969/70 *Séminaire Delange-Pisot-Poitou*: Théorie des Nombres, Exp. 19. Secrétariat mathématique, Paris. *Oeuvres. Collected Papers*, v. 2. Springer, 1986.

[117] Serre, J-P. *Abelian l-adic representations and elliptic curves.* Benjamin, 1968, edited in collaboration with W. Kuyk and J. Labute; 2nd ed. AK Peters, 1998.

[118] Serre, J-P. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.* **54** (1987), no. 1, 179–230. *Oeuvres. Collected Papers*, v. 4. Springer, 2000.

[119] Shimura, G.: Correspondances modulaires et les fonctions ζ de courbes algébriques. *J. Math. Soc. Japan* **10** (1958), 1–28. Collected Papers. Springer, 2002-2003.

[120] Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions.* Iwanami Shoten and Princeton University Press, 1971.

[121] Shimura, G.: *Abelian Varieties with Complex Multiplication and Modular Functions.* Princeton Mathematical Series **46**. Princeton University Press, 1998.

[122] Shimura, G.; Taniyama, Y.: *Complex multiplication of abelian varieties and its applications to number theory.* Publications of the Mathematical Society of Japan, 6. The Mathematical Society of Japan, Tokyo 1961, xi+159 pp.

[123] Schwarz, H. A.: Ueber diejenigen Fälle, in welchen die *Gauss*ische hypergeometrische Reihe eine *algebraische* Function ihres vierten Elementes darstellt. *J. für reine u. angew. Math.* **75** (1873), 292-335.

[124] Takagi, T.: *Collected papers.* With a preface by S. Iyanaga. Second edition. Edited and with a preface by Iyanaga, K. Iwasawa, K. Kodaira and K. Yosida. With appendices by Iyanaga, Iwasawa and Yosida. Springer-Verlag, Tokyo, 1990. xvi+376 pp. ISBN: 4-431-70057-9.

[125] Takeuchi, K.: Arithmetic triangle groups. *J. Math. Soc. Japan* **29** (1977), 91-106.

[126] Taylor, R; Wiles, A.: Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.* **141** (1995), 553-572.

[127] Vladut, S. G.: *Kronecker's Jugendtraum and modular functions.* Translated from the Russian by M. Tsfasman. Studies in the Development of Modern Mathematics, 2. Gordon and Breach Science Publishers, New York, 1991. x+411 pp. ISBN: 2-88124-754-7.

[128] Vojta, P.: Mordell's conjecture over function fields. *Invent. Math.* **98** (1989), no. 1, 115–138.

[129] Vojta, P.: Siegel's theorem in the compact case. *Ann. of Math.* (2) **133** (1991), no. 3, 509–548.

[130] Vojta, P.: Arithmetic and hyperbolic geometry. Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), 757–765, Math. Soc. Japan, Tokyo, 1991.

[131] Wallis, J.: *The arithmetic of infinitesimals.* Traducido del latín *Arithmetica Infinitorum* y con una introducción por Jaequeline A. Stedall. Sources and Studies in the History of Mathematics and Physical Sciences. Springer-Verlag, New York, 2004. xxxiv+192 pp. ISBN: 0-387-20709-0.

[132] Weber, H.: Zur Theorie der zyklischen Zahlkörper, II. *Math. Ann.* 70 (1911), 459–470.

[133] Weber, H.: *Lehrbuch der Algebra*, Bd.I-II-III. Chelsea, 1895-1896-1908.

[134] Weil, A.: *Foundations of Algebraic Geometry.* American Mathematical Society Colloquium Publications, vol. 29. American Mathematical Society, New York, 1946. xix+289 pp.

[135] Weil, A.: *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités Sci. Ind., no. 1041; Publ. Inst. Math. Univ. Strasbourg 7 (1945). Hermann et Cie., Paris, 1948. iv+85 pp.

[136] Weil, A.: Jacobi sums as "Grössencharaktere". *Trans. Amer. Math. Soc.* **73** (1952), 487–495. *Scientific works. Collected papers.* Vol. II. Springer, 1979.

[137] Weil, A.: Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Ann.* **168** (1967), 149–156. *Scientific works. Collected papers.* Vol. III. Springer, 1979.

[138] Weil, A.: *Elliptic functions according to Eisenstein and Kronecker.* Reprint of the 1976 original. Classics in Mathematics. Springer-Verlag, Berlin, 1999. viii+93 pp. ISBN: 3-540-65036-9.

[139] Wiles, A.: Modular elliptic curves and Fermat's Last Teorem. *Ann. of Math.* **141** (1995), 443-551.

CONTESTACIÓN DEL EXCMO. SR. D. MANUEL LÓPEZ PELLICER

Excmo. Sr. Presidente,

Excmo. Sr. Presidente de Honor,

Excmos. Sres. Académicos,

Señoras, Señores:

Agradezco a la Academia el haber sido designado para contestar el excelente discurso de la Profesora Pilar Bayer Isant, pues es para mí un motivo de profunda satisfacción y alegría responder en nombre de nuestra Corporación a la nueva Académica, a quien le expreso, en nombre de todos, la más efusiva bienvenida a esta casa.

Tras un esbozo de su obra concluiré con una breves consideraciones sobre Teoría de Números.

ENCOMIUM

En 1967 la Profesora Pilar Bayer obtuvo el título de Profesora de Piano por el Conservatorio Superior Municipal de Música de Barcelona. Desde 1990 hasta 2004 ha participado como pianista solista o acompañante en todas la ediciones del Concert de Primavera de los estudiantes y profesores de la Facultad de Matemáticas de la Universidad de Barcelona, donde en 1968 terminó su licenciatura en Matemáticas. A continuación inició un período de especialización en Teoría de Números bajo la dirección del Profesor Enrique Linés Escardó, ilustre Académico que

fue de nuestra Corporación, y en colaboración con D.ª Griselda Pascual Xufré, que había sido su profesora de matemáticas en el Instituto Nacional de Enseñanza Media Maragall de Barcelona a lo largo de todo el Bachillerato. Se doctoró en Matemáticas en 1975 por la Universidad de Barcelona (presentando su tesis doctoral el mismo día que la Profesora Griselda Pascual) y siendo el Profesor Rafael Mallol Balmaña el director de su tesis.

Entre 1968 y 1977 ocupó distintos puestos en la Universitat de Barcelona y en la Universitat Autònoma de Barcelona. Entre 1977 y 1980 fue Profesora Asistente en la Universität Regensburg de Alemania. De 1980 a 1981 fue Profesora Agregada numeraria en la Universidad de Santander. Desde 1981 es Catedrática numeraria, primero en la Universitat Autònoma de Barcelona y desde 1982 en la Universitat de Barcelona, donde ha dirigido el Departamento de Álgebra y Geometría de la Facultad de Matemáticas en varios períodos, con una participación muy activa en la vida académica, pues ha sido miembro del Comitè Acadèmic y de la Comissió de Reclamacions de la Universitat de Barcelona y desde 2004 es miembro de la Junta Consultiva de dicha universidad. Ha dirigido 10 tesis doctorales, de las que dos han obtenido el Premio Extraordinario de la Facultad de Matemáticas de la Universidad de Barcelona, a otras dos se les concedió el Premi Josep Teixidor por parte del Institut d'Estudis Catalans y otra tesis fue premiada por la Fundación Conde de Barcelona. Además a una de las tesis con Premio Extraordinario se le otorgó el Accésit al Premio Claustro de Doctores de la Universidad de Barcelona. En la actualidad se encuentra dirigiendo otras 3 tesis doctorales.

Nombramientos y Premios

Fue nombrada Académica correspondiente de la Real Academia de Ciencias Exactas, Físicas y Naturales de Madrid (1994), Acadèmica numerària de la Reial Acadèmia de Doctors (1994), Acadèmica numerària de la Reial Acadèmia de Ciències i Arts

(elegida en 1996, leyó su discurso de ingreso en 2001) y miembro del Institut d'Estudis Catalans (2001). En el año 2001 fue elegida Académica numeraria de la Real Academia de Ciencias de Madrid.

En 1998 recibió la Medalla Narcís Monturiol de la Generalitat de Catalunya otorgada al mérito científico y tecnológico.

Investigación

Su primera línea de investigación se desarrolló en el marco de la *Teoría de cuerpos de clases*, desde principio de los 70. En esta década investigó sobre *Formas cuadráticas*, *Cohomología étale y l-ádica*, *Teoría de Iwasawa* y el *Problema inverso de la Teoría de Galois*.

Las líneas de investigación desarrolladas por la Profesora Bayer en la década de los 80 fueron *Formas modulares*, *Aritmética de curvas elípticas* y *Aritmética de curvas modulares*.

En los últimos 20 años ha hecho destacadas aportaciones al estudio de las *Variedades aritméticas*, *Representaciones de Galois* y *Representaciones automorfas* y *Curvas de Shimura*. En la actualidad trabaja también en *Aplicaciones de la teoría de números a la física teórica*, estando especialmente interesada en las repercusiones en física del denominado *Programa de Langlands*, que representa la versión más avanzada (en gran parte conjetural) de la *Teoría de cuerpos de clases*.

Todo ello está recogido en más de 50 artículos de investigación y en más de 50 capítulos de libros y en libros. Entre los más recientes destacaría la invitación que recibió de la Abel Prize Foundation para escribir el extenso artículo *Jean-Pierre Serre: An Overview of his Work*, publicado en 2010 en el libro *The Abel Prize. The first five years: 2003–2007*, editado por Springer, así como su artículo *On Local Constants Associated to Arithmetical Functions*, publicado en Pure and Applied Mathematics Quarterly **4** (2008), n. 4, 1107–1132 (Special issue in

honor of Jean-Pierre Serre), en colaboración con su cuarto doctorando Artur Travesa, todo ello como invitación especial por la concesión a Jean-Pierre Serre del Premio Abel de Matemáticas.

Algunas de las revistas donde están publicados sus artículos son: *Acta Arithmetica, Archiv der Mathematik, Banach Center Publications, Compositio Mathematica, Comptes Rendues de l'Académie des Sciences, Experimental Mathematics, Inventiones Mathematicae, Journal für die Reine und Angewandte Mathematik, Journal de Théorie des Nombres de Bordeaux, Journal of Number Theory, L'Enseignement Mathématique, Mathematische Annalen, Mathematische Zeitschrift, Pure and Applied Mathematics Quarterly y The Ramanujan Journal.*

Entre sus contribuciones a libros, además del texto antes mencionado editado por Springer, destacan el capítulo *Embedding problems with kernel of order two*, publicado por Birkhäuser en 1989, en el número 75 de la serie Progress in Mathematics, y el libro *Quaternion orders, quadratic forms and Shimura curves*, escrito en colaboración con Monserrat Alsina, a quien dirigió su Tesis Doctoral. Este libro está publicado en 2004 por la American Mathematical Society (en la serie de monografías del Centre de Recherches Mathématiques, Université de Montréal).

Seminario de Teoría de Números

En 1986 fundó el Seminari de Teoria de Nombres, habiéndolo dirigido a lo largo de más de 20 años. En la actualidad, este Seminario está vinculado a las Universidades de Barcelona, Autònoma de Barcelona y Politècnica de Catalunya. Parte del trabajo desarrollado por sus miembros está escrito en diversas publicaciones, recopiladas sistemáticamente desde 1992 en las Notes del Seminari de Teoria de Nombres, que cuentan en la actualidad con una veintena de volúmenes accesibles *on line*. Además, la Profesora Bayer ha asumido las dirección científica de numerosas actividades anuales del Seminario, de ámbito nacional, y presidió el Comité Organizador de las decimonovenas *Journées Arithméti-*

ques, de ámbito internacional, celebradas en Barcelona en 1995 y organizadas por este Seminario.

Otras actividades relacionadas con la investigación

Ha sido varias veces miembro del jurado de importantes premios y becas, como el Premio CEOE a las Ciencias; el Premi Évariste Galois, el Premi Ferran Sunyer i Balaguer y el Premi Josep Teixidor de Matemàtiques otorgados por el Institut d'Estudis Catalans, así como del Premio Nacional de Investigación Julio Rey Pastor en el área de Matemáticas y Tecnología de la Información y las Comunicaciones. Ha participado en el jurado para la adjudicación de la Savilian Professorship of Geometry y de la Professorship of Pure Mathematics de la Universidad de Oxford.

Ha sido miembro de los comités de evaluación o asesoramiento del programa Stimulaton Action de la CEE y de la ponencia de Física y Matemáticas de la Dirección General de Investigación Científica y Técnica de la ANEP. Ha sido miembro de la Comissió d'Assessorament del Centre de Recerca Matemàtica de Barcelona y de la Associació per al Foment de la Ciència. Ha sido vocal del Comitè avaluador del Pla de Recerca de la Generalitat de Catalunya. Es miembro consultor del Gobierno Vasco y miembro de la comisión para la adjudicación de becas del País Vasco. Es asimismo miembro del Comité Científico de Atomium Culture (the Permanent Platform for European Excellence) de la Unión Europea.

Editora invitada de la Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales, dejando parte de su producción científica y de su escuela en el número 3, volumen 94 del año 2000 de nuestra Revista. Ha sido miembro de los Comités Editoriales de Publicacions de la UAB, de la Revista Matemática de la Universidad Complutense de Madrid y de la revista Debats Tecnològics del Col·legi d'Enginyers Tècnics Industrials de Barcelona. Es miembro del Comité editorial de la Revista Ma-

temática Iberoamericana y del Journal of Number Theory. Ha realizado trabajos de asesoramiento para la editorial Springer.

En 2004 fue contratada en la Cátedra Emmy Noether de la Universidad de Göttingen.

Además de haber impartido conferencias y cursos en casi todas nuestras Universidades, ha sido invitada en Universidades o Centros de Investigación de Anogeia, Berkeley, Besançon, Cobourg, Essen, Ginebra, Göttingen, Graz, Heidelberg, Karlsruhe, Limoges, Lisboa, Luminy, Oberwolfach, París, Regensburg y Saarbrücken.

Ha sido investigadora principal en catorce proyectos, de los que cuatro son acciones integradas o ayudas a la investigación de la Universitat de Barcelona y de la Generalitat de Catalunya y diez son ministeriales.

Divulgación científica

Es bien sabido que nuestra nueva académica es una excelente profesora que no ha descuidado la divulgación científica en todos los medios de comunicación. Nos ofreció una panorámica asequible y completa de la teoría de números en su artículo *¿Para qué sirven hoy los números?* en el libro *2000: Año Mundial de las Matemáticas*, publicado por Espasa en la serie Horizontes Culturales, Las Fronteras de la Ciencia de nuestra Real Academia de Ciencias (2002), páginas 87–107, que he utilizado en esta contestación. Además ha colaborado con El País en artículos del Circuito Científico y con La Vanguardia, ha participado en programas divulgativos de radio y televisión, como el programa *Redes* de TV2, y ha colaborado con la Academia en los programas de *Difusión de la cultura científica y tecnológica* y de *Detección y estímulo del talento precoz en Matemáticas*, fundado por Miguel de Guzmán y más conocido por *Estalmat*, su acrónimo. No tengo ninguna duda que los alumnos de Estalmat aún recuerdan el regalo de la magnífica lección de apertura de la

Profesora Bayer del curso 1999-2000.

Una visión rápida de la teoría de números hasta 1800

Creo que todos nos habremos preguntado en alguna ocasión cómo sería nuestro Universo sin números. La respuesta de los pitagóricos vendría determinada por su convicción de que todas las cosas son, en esencia, números. Parece que uno de ellos, Hipaso de Metaponto, probó que $\sqrt{2}$ no era racional en un momento en que los pitagóricos creían que los números racionales eran capaces de describir toda la geometría del universo. Su muerte puede estar relacionada con la revelación de su descubrimiento, rompiendo el silencio impuesto por los pitagóricos respecto a su hallazgo.

Los números están muy popularizados gracias a las tecnologías digitales que codifican una conversación, una sinfonía o un partido en una sucesión de ceros y unos, que puede ser transmitida a velocidad de la luz. El sistema de numeración de dos dígitos se llama *binario* y fue utilizado implícitamente por los egipcios para resolver el problema de la multiplicación reduciéndola a una sucesión de multiplicaciones por dos, previa la descomposición de uno de los factores en una suma de potencias de dos. Así, por ejemplo:

$$\begin{aligned} 19 \times 13 &= (2^4 + 2 + 1) \times 13 = (2^4 \times 13) + (2 \times 13) + (1 \times 13) \\ &= 208 + 26 + 13 = 247. \end{aligned}$$

Aunque este sencillo método es un claro antecedente del sistema de numeración binario, el sistema de numeración egipcio usado en la escritura jeroglífica, hacia el 3000 a.C., era un sistema de base diez, de siete cifras y que carecía del 0. Sumaban dos cantidades reuniendo los guarismos correspondientes y sustituyendo diez unidades de un orden por otra de orden superior. La escritura jeroglífica egipcia evolucionó a las escrituras hierática y demótica, que incrementaron el número de símbolos para representar los números, con la finalidad de evitar la repetición

de símbolos. El Papiro Rhind, cuya fuente intelectual podría ser Imhotep, contiene abundantes reglas de cálculo y una colección de 84 problemas.

El sistema de numeración sumerio era posicional y mucho más avanzado que el egipcio. Su matemática nos ha llegado a través de tablillas de arcilla grabadas en escritura cuneiforme. En la conocida como Plimton 322, que data de la época de Hammurabi (hacia 1800 a.C.) y se conserva en la Universidad de Columbia, aparecen quince ternas pitagóricas, que son quince soluciones enteras de la ecuación $X^2 + Y^2 = Z^2$, lo que nos hace sospechar que trece siglos antes de Pitágoras algún matemático sumerio ya estaba familiarizado con el teorema de Pitágoras.

Los sistemas de numeración griego y romano eran alfabéticos resultando poco operativos a la hora de calcular, lo que originó la creación de instrumentos mecánicos de cálculo, desde piedras (*calculi*) hasta el ábaco. De su producción científica nos han llegado, entre otros, los *Elementos*, que son trece tomos escritos por Euclides (315–225 a.C.), la *Sintaxis Matemática* de Tolomeo de Alejandría (h. 90–h. 160), obra más conocida por su nombre árabe *Almagesto*, que significa "el más grande", y la *Aritmética* de Diofanto de Alejandría (h. 200–h. 284). Los Elementos están concebidos como un libro para aprender geometría, si bien en los libros VII, VIII y IX se tratan cuestiones básicas sobre divisibilidad, máximo común divisor y mínimo común múltiplo, y propiedades de los números primos que eran ya conocidas por los pitagóricos. Euclides demostró que existen infinitos números primos al probar que existen más números primos que cualquier cantidad fijada de antemano. En el *Almagesto* de Tolomeo aparece una tabla de cuerdas de arcos de medio en medio grado equivalente a una tabla de senos de cuarto en cuarto grado. La *Aritmética* de Diofanto consta de más de 150 problemas sobre propiedades de los números[2]. El problema II-8 se ocupa de las

[2]No es fácil contar los problemas de la Aritmética de Diofanto. En la versión castellana, editada por Aguilar en Clásicos Griegos, su número es 189, repartidos en seis capítulos; sin embargo, en esta traducción algunos proble-

ternas pitagóricas.

La cuna de nuestro sistema de numeración decimal está en la civilización india. En la obra *Aryabhatiya* de Aryabhata, escrita alrededor del año 500, se encuentran abundantes reglas de cálculo. Un siglo después, en la obra de Brahmagupta, se sistematizan esas reglas de cálculo para números positivos y negativos, incluido el 0 . En la Casa de la Sabiduría de Bagdad, fundada por los califas Harun-al-Rasid y Al-Mamun, se tradujeron al árabe las obras griegas a su alcance. Muhammad ibn Musa al-Khwarizmi, muerto hacia el 845, fue el matemático más destacado de aquella institución y con su obra *De numero indorum*, escrita alrededor del 820, consolidó las cifras indo-arábigas, el sistema decimal de posición y sus reglas de cálculo. El texto original árabe se ha perdido, y la traducción más antigua que se conserva de esta obra es del siglo XII y fue hecha por la Escuela de Traductores de Toledo.

Leonardo de Pisa (1180–1250), más conocido como Fibonacci, era hijo del mercader Bonaccio que poseía negocios en el norte de África. Allí aprendió a calcular con las cifras indo-arábigas y estudio los *Elementos* de Euclides. En 1202 dio a conocer su *Liber abaci*, que no está dedicado al aprendizaje del ábaco, sino al cálculo con cifras indias y constituyó el compendio de las matemáticas medievales.

La operatividad del sistema de numeración decimal permitió incrementar la precisión de los cálculos. Al-Kasi (1380–1429) obtuvo una aproximación del número π con 14 cifras decimales. En 1614, y tras más de 14 años de trabajo, John Napier publicó sus tablas de logaritmos, cuya definición fue modificada

---

mas aparecen agrupados de dos en dos, cosa que no ocurre en otras versiones. Pero hay otra cuestión: las traducciones árabes incluyen un capítulo VII y hay historiadores que hablan, incluso, de que la obra completa constaba de un total de trece capítulos. Como curiosidad, se ha dicho también que las traducciones árabes podrían haber incluido los comentarios de Hypatia de Alejandría, por cuyo motivo són más largas que los textos griegos conservados.

ligeramente por Briggs creando los logaritmos de base 10. En 1624 publicó sus tablas de logaritmos, con catorce cifras decimales. Briggs fue el primer *Savilian Professor* de la Universidad de Oxford. Kepler dijo que la invención de los logaritmos duplicaba la vida de los astrónomos al permitirles duplicar el número de cálculos que eran capaces de realizar. Las tablas de logaritmos junto a las tablas de senos y cosenos mejoraron la seguridad de los viajes marítimos al permitir el cálculo preciso y rápido de longitudes y latitudes.

Pierre de Fermat (1601–1665) fue un abogado que cultivaba las matemáticas por afición y enviaba a sus coetáneos reflexiones sobre diversos problemas de la *Artimética* de Diofanto relativas a propiedades de números enteros. Muchas de sus afirmaciones fueron probadas y otras desmentidas por Euler (1707–1783), Legendre (1752–1833) y por Gauss (1777–1855). Por ejemplo, Fermat conjeturó que todos los números de la forma

$$2^{2^n}+1$$

son primos. En 1732, Euler demostró que $2^{32}+1$ no es primo, pues es múltiplo de 641. A Euler le debemos la igualdad

$$\sum_{n\geq 1}\frac{1}{n^s}=\prod_{p}\frac{1}{1-\frac{1}{p^s}},\quad \mathrm{Re}(s)>1,$$

en cuyo segundo miembro aparecen todos los números primos una sola vez, lo que supuso el comienzo de la Teoría Analítica de Números. Su primer miembro define la función zeta de Riemann[3].

[3]En el capítulo 5 de la memoria se estudian con detalle cuestiones relacionadas con la función zeta de Riemann y con la distribución de los números primos. En 1859, Riemann formuló por primera vez su famosa hipótesis sobre la distribución de los ceros de la función zeta de Riemann, que sigue siendo uno de los problemas abiertos más importantes de la Matemática. En su tesis de 1920, Artin conjeturó el análogo de la hipótesis de Riemann en cuerpos de funciones elípticas definidas sobre cuerpos de constantes finitos, que fue probado por Hasse en 1934. Respecto a la distribución de los números primos, la demostración de que toda progresión aritmética

Fermat pensó alrededor del problema II-8 de la *Aritmética* de Diofanto y anotó en este libro que tenía una preciosa prueba de que la ecuación

$$X^n + Y^n = Z^n$$

carecía de soluciones enteras (no triviales) cuando $n > 2$, pero que no la escribía por la estrechez del margen de página. Entre sus papeles sólo se encontró que por medio de su método del descenso infinito había probado la certeza de su teorema para $n = 3$. La Profesora Bayer nos ha expuesto en su discurso que el teorema de Fermat no ha podido ser demostrado hasta 1994, tras un primer anuncio de demostración por Wiles en 1993, cuya primera versión necesitó correcciones posteriores[4]. La dificultad de la demostración de Wiles nos hace dudar de que Fermat tuviese una prueba sencilla de su hoy teorema.

El discurso de la Profesora Bayer Isant entre 1800 -1950

La profesora Bayer ha comenzado su discurso alrededor de Gauss, quien decidió su vocación por las Matemáticas después de descubrir a los diecinueve años que el polígono regular de diecisiete lados se puede construir con regla y compás. Su obra *Disquisitiones arithmeticae* (1801) es un compendio de sus investigaciones en sus años de aprendizaje en la Universidad de Gotinga y con ella comienza la utilización de números algebraicos y funciones especiales para la investigación de propiedades de los números enteros. Motivado por los resultados de Fermat

$\{a + tN : t > 0\}$ con $\mathrm{mcd}(a, N) = 1$ contiene infinitos números primos se debe a Dirichlet. Este resultado fue generalizado de forma sorprendente por Chebotarev; su primera demostración se basaba en un proceso de reducciones sucesivas a extensiones ciclotómicas en las que imitaba la demostración del teorema de la progresión aritmética de Dirichlet. Hoy se demuestra como un corolario de la teoría de cuerpos de clases, que estudia la clasificación de las extensiones abelianas de los cuerpos de números.

[4]Las investigaciones de Kummer sobre la ecuación de Fermat $X^n + Y^n = Z^n$ le llevaron a distinguir entre números primos irregulares y regulares. Para los exponentes primos regulares consiguió demostrar el teorema de Fermat, si bien aún se desconoce si su número es infinito.

y de Euler sobre caracterización de números expresables como suma de cuadrados, Gauss estudia los números n representables por una forma cuadrática

$$n = aX^2 + bXY + cY^2$$

y obtiene la ley de reciprocidad cuadrática[5], caracteriza los polígonos de N lados que pueden construirse con regla y compás (N debe ser el producto de una potencia de 2 por un producto de números primos de Fermat distintos, que son de la forma $1+2^{2^r}$) y se da cuenta de que lo elaborado para las funciones seno y coseno es aplicable a otras funciones trascendentes. Así el cambio de la circunferencia por la lemniscata le llevó a introducir el seno lemniscático, origen del descubrimiento de las funciones elípticas, que, con las funciones abelianas y las funciones modulares elípticas, las ha desarrollado la Profesora Bayer en los capítulos 2, 3 y 4 de su memoria.

A continuación, la nueva académica describe los problemas de cálculo infinitesimal que llevaron a las integrales elípticas, cuyo integrando es una función racional de dos variables, t y una raíz cuadrada de un polinomio de grado 3 o 4 y sin raíces múltiples, que Legendre redujo a tres formas canónicas que aplicó a la resolución de múltiples problemas de Mecánica. La integral elíptica de segunda especie nos proporciona la longitud de un arco de elipse. Por inversión de las integrales elípticas se obtienen las funciones elípticas, que Jacobi expresó como cociente de funciones theta, ya utilizadas por Fourier en su estudio de 1822

[5]Afirma que dados dos números primos p y q, distintos de 2, el carácter cuadrático de p módulo q queda determinado por el de q módulo p. Esta ley fue generalizada por Jacobi, Eisenstein, Dedekind, Kummer, Hilbert y Herglotz. En el problema 9 de su lista de 1900, Hilbert planteó la formulación de una ley de reciprocidad general que fuera válida para cualquier cuerpo de números. Artin, en 1923, y basándose en los trabajos de Furtwängler, Takagi y Hasse, descubrió un teorema que incluía como casos especiales todas las leyes de reciprocidad conocidas hasta aquella fecha, completando la demostración tres años después a través de la introducción de unas funciones, llamadas las series L de Artin.

sobre la ecuación del calor y posteriormente en la tesis de L. Bachelier de 1900, considerada un antecedente de la matemática financiera. La función elíptica $\wp$ de Weierstrass es solución de la ecuación diferencial

$$\left(\frac{d\wp}{du}\right)^2 = 4\wp^3 - g_2\wp - g_3$$

que, junto con su derivada, proporciona una parametrización meromorfa de la curva elíptica de ecuación

$$Y^2 = 4X^3 - g_2X - g_3.$$

La memoria describe la aplicación de las funciones elípticas en las investigaciones de Poincaré de 1901 sobre la determinación de la estructura del grupo de los puntos de coordenadas racionales de una curva elíptica definida sobre el cuerpo $\mathbb{Q}$ de los números racionales, que dieron lugar a la llamada *conjetura de Poincaré para curvas elípticas*, que nunca formuló explícitamente como tal. Afirma que el referido grupo es finitamente generado. Mordell la demostró en 1922 utilizando un método de descenso midiendo el número de dígitos necesarios para escribir las coordenadas de los puntos racionales de la curva elíptica y propuso como nueva conjetura que en toda curva proyectiva $\mathcal{C}$, no singular, de género $g \geq 2$, definida sobre un cuerpo K de números, el conjunto de sus puntos K-racionales debía ser finito.

En 1927, Weil se fijó como objetivo para su tesis doctoral probar la conjetura de Mordell. No lo consiguió tal vez por estar en sus comienzos el estudio aritmético de las variedades abelianas, por no disponer la geometría algebraica de un lenguaje adecuado para los problemas aritméticos o por ser entonces escasas las evidencias numéricas en favor de la conjetura. La solución de la conjetura de Mordell llegó en 1983 con un teorema de Faltings, que contribuiría a la larga a resolver el problema de Fermat[6].

[6]En un espectacular trabajo publicado en 1983, que le valió la concesión de la Medalla Fields en 1986, Faltings demostró por primera vez tres famosas conjeturas: la ya mencionada de Mordell (1922), la de Shafarevich (1962) y

La forma general de una integral abeliana es

$$\int f(x,y)dx$$

donde las funciones x e y verifican que $F(x,y) = 0$, siendo $F(X,Y)$ un polinomio irreducible y no constante. Por inversión de las integrales abelianas se obtienen funciones abelianas, que tienen un retículo de períodos de dimensión par $2g$ y proporcionan parametrizaciones analíticas de ciertas variedades abelianas complejas de dimensión g, las cuales están dotadas de una ley de adición algebraica y conmutativa. El caso $g = 1$ corresponde a las curvas elípticas. El caso más sencillo de integrales abelianas son las integrales hiperelípticas, que tienen la forma:

$$\int \frac{R(x)}{\sqrt{P(x)}}dx,$$

donde $R(x)$ es una función racional y $P(x)$ es un polinomio de grado menor o igual al 6. Se debe a Picard y Poincaré la representación de las funciones abelianas periódicas como un cociente de funciones theta abelianas, que son la generalización de las funciones de Jacobi, que corresponden al caso $g = 1$. A Poincaré debemos el estudio de la reducción de integrales abelianas, que llevó al concepto de isogenia de variedades abelianas y al teorema de reducibilidad completa, que afirma que toda variedad abeliana es el producto de variedades abelianas simples, que son las que no se pueden descomponer en producto de otras dos variedades de dimensión menor.

---

la de Tate (1966).

En el congreso Internacional de Matemáticos de 1962 celebrado en Estocolmo, Shafarevich formuló la pregunta de si sería válido en el caso de curvas algebraicas un teorema análogo al de Hermite para cuerpos de números. La importancia de la denominada conjetura de Shafarevich se puso de manifiesto en un trabajo de Parshin de 1968, en el que a través de una ingeniosa construcción probaba que la conjetura de Shafarevich implicaba la conjetura de Mordell. La conjetura de Tate es muy técnica y afirma que dada una variedad abeliana A definida sobre un cuerpo de números K, la clase de isogenia de A se caracteriza a través de su función zeta de Hasse-Weil.

La profesora Bayer ha dedicado el capítulo 4 de su discurso a las funciones modulares elípticas, que son funciones meromorfas periódicas respecto a subgrupos discretos de movimientos hiperbólicos. Nos ha descrito como llegaron a estas funciones Gauss, Dedekind[7] y Poincaré quien, en correspondencia mantenida con Fuchs, trató de averiguar cuando el cociente de dos soluciones independientes de la ecuación diferencial

$$\frac{d^2w}{dx^2} - Q(x)w = 0$$

define por inversión una función meromorfa. En este capítulo nos ha descrito tres aplicaciones de las funciones modulares. Nos ha recordado que en 1799, Ruffini publicó su *Teoria generale delle equazioni*, donde trata la imposibilidad de la resolución por radicales de la ecuación general de grado mayor o igual a cinco y que Galois caracterizó la resolubilidad de una ecuación polinómica por radicales mediante la resolubilidad de su grupo de transformaciones, de lo que dedujo que una ecuación general de grado mayor o igual a cinco no es resoluble por radicales. En 1859, Hermite utilizó las transformaciones de Tschirnhaus (1683) y de Jerrard (1834) para reducir la ecuación de grado cinco a la forma trinómica

$$z^5 + az + b = 0$$

que, si bien no es resoluble por radicales, resultó ser resoluble por funciones modulares elípticas. La segunda aplicación hace referencia al estudio de la ecuación de grado cinco hecho por Klein en 1884, relacionando el grupo de isometrías del icosaedro, la teoría de Galois y las funciones modulares elípticas. Klein utilizó una proyección estereográfica de la esfera unidad en el plano complejo de manera que los doce vértices de un icosaedro inscrito en la esfera se proyectasen en los puntos

$$0, \quad \infty, \quad \varepsilon^v(\varepsilon + \varepsilon^4), \quad \varepsilon^v(\varepsilon^2 + \varepsilon^3), \qquad 0 \leq v \leq 4$$

[7]Por integración de una ecuación diferencial de segundo orden de tipo fuchsiano, Dedekind construyó en 1877 una función especial que denominó *Valenz Funktion*. Su normalización es la función modular elíptica j, a la que se conoce como invariante j de Klein. Se la considera el primer ejemplo de función modular.

siendo ε una raíz quinta de la unidad. La tercera aplicación hace referencia al llamado *Sueño de Juventud* de Kronecker, quien en un artículo de 1853, manifestó el notable resultado de que las soluciones de cualquier ecuación polinómica con coeficientes enteros y grupo de Galois abeliano son expresables como funciones racionales de raíces de la unidad. Esta intuición correcta supuso el comienzo de un largo camino hasta la elaboración de la primera prueba aceptada, debida a Hilbert en 1896[8].

Parte de los resultados del capítulo sexto se han comentado ya. Contiene una exposición muy clara de los principales avances en el conocimiento de los números trascendentes.

Principales resultados del discurso de la Profesora Bayer Isant obtenidos a partir de 1950

Alrededor de los años 1950 comenzó una transición de los métodos clásicos de la teoría de números hacia nuevos métodos que caracterizarían su desarrollo subsiguiente. El libro de A. Weil, Foundations of Algebraic Geometry, de 1946, y la teoría de esquemas de Grothendieck favorecieron que los elaborados cálculos del pasado cedieran lugar a desarrollos mucho más conceptuales, siendo dos de las nociones más influyentes la creación

[8]Este resultado se conoce como teorema de Kronecker-Weber, ya que Weber logró diversas demostraciones anteriores a la de Hilbert, que no estuvieron exentas de críticas. Los intentos posteriores de generalización del teorema de Kronecker-Weber dieron lugar al nacimiento de la teoría de la multiplicación compleja. Kronecker deseaba probar que toda extensión abeliana de un cuerpo cuadrático imaginario se genera mediante módulos singulares, correspondientes a valores especiales de funciones modulares elípticas, y los valores de división, dados por funciones elípticas. Esta afirmación constituye el teorema de completitud de la teoría de la multiplicación compleja en el caso cuadrático imaginario. Su demostración correcta, tras varias aproximaciones erráticas de Fueter, fue obtenida por Takagi en 1920. La teoría de la multiplicación compleja en el caso cuadrático imaginario alcanzó su formulación actual entre los años 1940–1950, cuando Hasse y Deuring lograron expresar sus resultados en términos de las funciones L de las curvas elípticas dotadas de multiplicación compleja.

de Grothendieck de la topología étale de esquemas y de las cohomologías l-ádicas asociadas. De la gran labor realizada por Grothendieck y su escuela es especialmente notable la demostración de las conjeturas de Weil. La demostración de la racionalidad de las funciones zeta, su ecuación funcional y su relación con los números de Betti se debe al propio Grothendieck. La localización de ceros y polos (es decir la hipótesis de Riemann en este contexto) se debe a Deligne en 1974, por lo que recibió la Medalla Fields en 1978.

En la sesión de problemas de un simposio internacional sobre teoría algebraica de números celebrado en Tokyo-Nikko en 1955, un joven matemático llamado Taniyama propuso averiguar si las curvas elípticas definidas sobre un cuerpo de números son parametrizables mediante funciones automorfas, lo que podría ser un camino para probar la conjetura de Hasse-Weil. Shimura en 1964 y Weil en 1967 delimitaron la conjetura a curvas elípticas definidas sobre el cuerpo racional preguntando si serían parametrizables mediante funciones modulares. Así nació la conjetura de modularidad STW (Shimura-Taniyama-Weil) que, en principio, proporcionaba un camino para probar la conjetura de Hasse-Weil, pero después de los resultados de Frey (1986), de Serre (1987) y de Ribet (1990) se puso de manifiesto que, además, implicaba el teorema de Fermat, ya que en 1986 Frey observó que si (a, b, c) fuese una hipotética solución entera de la ecuación de Fermat $X^p + Y^p = Z^p$, para un exponente $p \geq 5$, la curva elíptica definida sobre $\mathbb{Q}$

$$Y^2 = X\,(X - a^p)\,(X + b^p)$$

parecía contradecir la conjetura STW, lo que efectivamente se demostró como consecuencia de los resultados de Serre y Ribet mencionados.

Así quedó claro en 1990 que STW implicaba el teorema de Fermat, siendo suficiente para probar este teorema demostrar STW para las curvas elípticas semiestables.

La conjetura de Shimura-Taniyama-Weil (STW) se convir-

tió en un teorema gracias al impresionante trabajo de Wiles (1995), Taylor-Wiles (1995), Diamond (1996), Conrad-Diamond-Taylor (1998) y Breuil-Conrad-Diamond-Taylor (1999). Con ello no sólo quedó probado el teorema de Fermat sino que, además, se dio un paso para resolver uno de los siete Problemas del Milenio propuestos por el Instituto Clay de Matemáticas, la conjetura BSD[9].

No estamos en el final de un camino, pues la propia conjetura de Shimura-Taniyama-Weil forma parte de una extensa familia de conjeturas conocidas como *conjeturas de modularidad*. Lo que probó Ribet en 1990 fue la llamada *conjetura* ε, que sólo es un caso muy particular de la conjetura de modularidad que formuló Serre en 1987. Las técnicas de Wiles y sus múltiples ramificaciones se están utilizando para probar la conjetura de Serre en toda su generalidad.

Y para terminar vamos a volver al trabajo del Grupo de Teoría de Números de la Universidad de Barcelona. En la actualidad, el estudio de las curvas modulares se ha generalizado en varias direcciones, dando lugar al estudio de las variedades de Hilbert y de Siegel, que se han englobado posteriormente en las variedades de Shimura, ya bien estudiadas en el caso de dimensión uno en las llamadas curvas de Shimura. El estudio teórico de las curvas de Shimura permite definir una clase de funciones automorfas que generalizan de manera natural las funciones modulares elípticas. Las curvas de Shimura están presentes en el artículo de Ribet de 1990 sobre la conjetura ε y tienen un papel muy sutil en la demostración de Wiles de la conjetura STW.

Precisamente el estudio de las curvas de Shimura ha sido uno de los objetivos del Grupo de Teoría de Números de la Universidad de Barcelona en la última década, como continuación natural de los trabajos desarrollados en el caso de curvas modulares, re-

[9]Tras experiencias numéricas realizadas en curvas con multiplicación compleja, en los años 1963 y 1965, Birch y Swinnerton-Dyer conjeturaron que el rango r de una curva elíptica $E/\mathbb{Q}$ coincidía con el orden en el punto $s = 1$ del cero de la función $L(E/\mathbb{Q}, s)$.

tió en un teorema gracias al impresionante trabajo de Wiles (1995), Taylor-Wiles (1995), Diamond (1996), Conrad-Diamond-Taylor (1998) y Breuil-Conrad-Diamond-Taylor (1999). Con ello no sólo quedó probado el teorema de Fermat sino que, además, se dio un paso para resolver uno de los siete Problemas del Milenio propuestos por el Instituto Clay de Matemáticas, la conjetura BSD[9].

No estamos en el final de un camino, pues la propia conjetura de Shimura-Taniyama-Weil forma parte de una extensa familia de conjeturas conocidas como *conjeturas de modularidad*. Lo que probó Ribet en 1990 fue la llamada *conjetura* ε, que sólo es un caso muy particular de la conjetura de modularidad que formuló Serre en 1987. Las técnicas de Wiles y sus múltiples ramificaciones se están utilizando para probar la conjetura de Serre en toda su generalidad.

Y para terminar vamos a volver al trabajo del Grupo de Teoría de Números de la Universidad de Barcelona. En la actualidad, el estudio de las curvas modulares se ha generalizado en varias direcciones, dando lugar al estudio de las variedades de Hilbert y de Siegel, que se han englobado posteriormente en las variedades de Shimura, ya bien estudiadas en el caso de dimensión uno en las llamadas curvas de Shimura. El estudio teórico de las curvas de Shimura permite definir una clase de funciones automorfas que generalizan de manera natural las funciones modulares elípticas. Las curvas de Shimura están presentes en el artículo de Ribet de 1990 sobre la conjetura ε y tienen un papel muy sutil en la demostración de Wiles de la conjetura STW.

Precisamente el estudio de las curvas de Shimura ha sido uno de los objetivos del Grupo de Teoría de Números de la Universidad de Barcelona en la última década, como continuación natural de los trabajos desarrollados en el caso de curvas modulares, re-

[9]Tras experiencias numéricas realizadas en curvas con multiplicación compleja, en los años 1963 y 1965, Birch y Swinnerton-Dyer conjeturaron que el rango r de una curva elíptica $E/\mathbb{Q}$ coincidía con el orden en el punto $s = 1$ del cero de la función $L(E/\mathbb{Q}, s)$.

cogidos en parte en el antes citado número 3 del volumen 94 del año 2000 de la centenaria revista de la Real Academia de Ciencias, que además del trabajo ilusionado de todos los académicos de esta casa, debería contar con el apoyo de la administración para convertir a nuestra revista en un referente destacado de la ciencia actual.

En dos tesis doctorales que la Profesora Bayer dirigió a M. Alsina (2000) y a V. Rotger (2002), se trabajó en la construcción de dominios fundamentales respecto de grupos fuchsianos cuaterniónicos y en la interpretación como espacios de módulos de superficies abelianas de las curvas de Shimura correspondientes.

En la monografía de Alsina y Bayer, publicada por la AMS en 2004, se puso de manifiesto que los puntos con multiplicación compleja de una curva de Shimura estaban en correspondencia biyectiva con una clase de formas cuadráticas binarias y para estas formas con coeficientes algebraicos se formuló una teoría de reducción que permite un tratamiento computacional de los puntos con multiplicación compleja, paralelo al que en su día desarrollara Gauss en sus *Disquisitiones arithmeticae*. Para asignar explícitamente a cada curva de Shimura las formas cuadráticas binarias que le pertenecen, fue necesario el cálculo de dominios fundamentales en el semiplano superior complejo bajo la acción de grupos fuchsianos Γ. Los dominios fundamentales se obtuvieron gracias a la elaboración por Alsina del software necesario para trabajar con cuaternios.

En 2006, Bayer y Guàrdia desarrollaron un método que condujo a la determinación de las superficies abelianas asociadas a los puntos con multiplicación compleja de curvas de Shimura. Para ello construyeron funciones theta explícitas que proporcionan una parametrización analítica de curvas de género 2.

Bayer y Travesa (2007) han establecido un método que permite la obtención explícita de las funciones automorfas que parametrizan las curvas de Shimura mediante desarrollos adecuados alrededor de puntos de multiplicación compleja. Tales desarro-

llos se obtienen por integración de ecuaciones diferenciales que se calculan a través del conocimiento de los dominios fundamentales. Recientemente, en 2008, han demostrado la trascendencia de las constantes inherentes a los parámetros de uniformización local, análogas por tanto a π en el parámetro de uniformización local $q = e^{2\pi iz}$ del caso modular cuspidal. Con una interpretación adecuada de la fórmula de Chowla-Selberg, calculan dichas constantes en términos de valores especiales de la función Γ de Euler.

Creo, sinceramente, que la Academia de Ciencias de Madrid está hoy de enhorabuena por la incorporación, tanto tiempo deseada, de la Profesora Pilar Bayer, quien por generosidad, excelentes cualidades científicas y laboriosidad va a prestar excelentes servicios a esta Institución.

He dicho.