MISCELÁNEA MATEMÁTICA **46** (2008) 49–72 SMM

Productos de Euler

Felipe Zaldívar
Departamento de Matemáticas
Universidad Autónoma Metropolitana
Unidad Iztapalapa
09340, México, D. F.
México
fzc@oso.izt.uam.mx

Introducción. El problema de calcular la suma de la serie

$$1+\frac{1}{2^m}+\frac{1}{3^m}+\frac{1}{4^m}+\frac{1}{5^m}+\cdots=\sum_{k=1}^{\infty}\frac{1}{k^m} \tag{1}$$

para $m \geq 2$ entero, había atraído la atención de varios matemáticos desde el siglo XVII, en particular para $m = 2$. En el siglo XVIII se interesaron en este problema matemáticos como Jacob Bernoulli, Daniel Bernoulli y Christian Goldbach, quienes obtuvieron algunos resultados preliminares sobre la suma de esta serie en el caso $m = 2$

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\cdots=\sum_{k=1}^{\infty}\frac{1}{k^2}, \tag{2}$$

los cuales pronto serían superados por Leonhard Euler que, en este marco conceptual, hizo su primer contacto con la serie anterior y pronto mejoraría los cálculos de sus predecesores. El problema de calcular la suma de la serie (2) no era fácil debido a su lenta convergencia, por ejemplo, para calcular el número al que converge, con una precisión de seis decimales, hay que sumar al menos un millón de términos de la serie. En efecto, como

$$\frac{1}{k}-\frac{1}{k+1}=\frac{1}{k(k+1)}<\frac{1}{k^2}<\frac{1}{k(k-1)}=\frac{1}{k-1}-\frac{1}{k},$$

sumando desde $k = n + 1$, por la propiedad telescópica de los extremos de la desigualdad anterior, se tiene que

$$\frac{1}{n+1}<\sum_{k=n+1}^{\infty}\frac{1}{k^2}<\frac{1}{n}$$

de tal forma que aproximar la serie con n lugares decimales requiere calcular la suma de al menos 10^n términos. Finalmente, en 1735, Euler anunció en [1] que

$$\frac{\pi^2}{6} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \cdots = \sum_{k=1}^{\infty} \frac{1}{k^2} \tag{3}$$

un resultado que contribuiría a establecer su prestigio como matemático y que se difundió rápidamente entre los especialistas. Poco después, Euler anunciaría la generalización del cálculo anterior al caso cuando $m = 2n$ en (1), y en los diez años siguientes, debido a críticas y dudas, de sus contemporáneos y de él mismo, revisó y dio varias demostraciones de los cálculos anteriores, hasta obtener un tratamiento enteramente satisfactorio del tema. Una ganancia adicional a los esfuerzos anteriores es que Euler fue llevado a considerar la función gamma que ahora lleva su nombre, y que se obtiene al interpolar el factorial de un entero, y a la consideración de productos infinitos en su relación con ciertas series infinitas. En el artículo [2] presentado a la Academia de San Petersburgo en 1737, Euler estudia varias series, comenzando con una sugerida en su correspondencia con Goldbach, y obtiene una descomposición de la serie (1) en términos de un producto que involucraba a todos los primos, probando el resultado siguiente:

Teorema 1 (Euler)**.** *Si de la serie de primos formamos el producto*

$$\frac{2^n}{(2^n-1)}\frac{3^n}{(3^n-1)}\frac{5^n}{(5^n-1)}\frac{7^n}{(7^n-1)}\cdots$$

entonces su valor es igual a la suma de la serie

$$1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \frac{1}{5^n} + \cdots$$

Es decir,

$$\sum_{k=1}^{\infty} \frac{1}{k^n} = \prod_{p \text{ primo}} \frac{p^n}{p^n - 1}.$$

La *demostración* de Euler es ingeniosa, pero como sucede algunas veces con el manejo liberal que hace Euler de la convergencia de series, es necesario revisarla para hacerla rigurosa. Veamos cuál es la idea de Euler. Para comenzar, escribe

$$x = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \frac{1}{5^n} + \frac{1}{6^n} + \cdots$$

y luego dividiendo entre 2^n obtiene

$$\frac{1}{2^n}x = \frac{1}{2^n} + \frac{1}{4^n} + \frac{1}{6^n} + \frac{1}{8^n} + \frac{1}{10^n} + \cdots$$

que restando de la expresión anterior nos da

$$\frac{2^n - 1}{2^n}x = 1 + \frac{1}{3^n} + \frac{1}{5^n} + \frac{1}{7^n} + \frac{1}{9^n} + \frac{1}{11^n} + \cdots$$

ya que se eliminan todos los términos con denominadores divisibles por 2.

Después divide la expresión anterior por 3^n obteniendo

$$\frac{(2^n - 1)}{2^n}\frac{1}{3^n}x = \frac{1}{3^n} + \frac{1}{9^n} + \frac{1}{15^n} + \frac{1}{21^n} + \frac{1}{27^n} + \cdots$$

que restándola de la expresión anterior nos da

$$\frac{(2^n - 1)(3^n - 1)}{2^n \cdot 3^n}x = \frac{1}{5^n} + \frac{1}{7^n} + \frac{1}{11^n} + \frac{1}{13^n} + \frac{1}{17^n} + \cdots$$

ya que se eliminan todos los términos con denominadores divisibles por 3.

Del mismo modo se eliminan, en el lado derecho, las potencias de los denominadores que son divisibles por 5, 7, 11, etcétera, notando que en cada paso se eliminan los sumandos que tienen la potencia del primo correspondiente y también sus múltiplos, de tal forma, dice Euler, que al final se eliminan todos los términos del lado derecho excepto el primero, a saber el número 1, y del lado izquierdo queda la expresión

$$\frac{(2^n - 1)(3^n - 1)(5^n - 1)(7^n - 1)\cdots}{2^n \cdot 3^n \cdot 5^n \cdot 7^n \cdots}x = 1$$

de donde se obtiene la afirmación del teorema.

El argumento anterior también le sirve a Euler para *probar*, repitiendo los pasos anteriores con $n = 1$, que la serie armónica se puede escribir como el producto siguiente

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots = \frac{2}{(2-1)}\frac{3}{(3-1)}\frac{5}{(5-1)}\frac{7}{(7-1)}\cdots$$

Es decir,

$$\sum_{k=1}^{\infty}\frac{1}{k} = \prod_{p \text{ primo}}\frac{p}{p-1}$$

de donde concluye que, como la serie armónica diverge, el número de primos debe ser infinito.

La *demostración* del teorema de Euler puede hacerse rigurosa y el teorema formularse para la serie de la forma

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

con s un número complejo con parte real mayor que 1, para obtener el teorema siguiente:

Teorema 2 (Euler)**.** *Si $s \in \mathbb{C}$ es tal que $\mathrm{Re}(s) > 1$, entonces*

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

En lugar de dar la demostración usual de este teorema (la cual puede verse en [16], por ejemplo) lo obtendremos como una consecuencia del resultado siguiente que también usaremos más adelante. Recordemos primero que una función $\varphi : \mathbb{N} \to \mathbb{C}$ se dice que es *multiplicativa* si $\varphi(1) = 1$ y si $\varphi(mn) = \varphi(m)\varphi(n)$, para todo par m, n de naturales coprimos. Por ejemplo, la función ϕ de Euler es multiplicativa (recuerde que $\phi(n)$ es el número de enteros entre 1 y n, coprimos con n).

Proposición 3. *Si φ es una función multiplicativa y si la serie de números complejos $\sum_{n=1}^{\infty} \varphi(n)$ converge absolutamente, entonces para $s \in \mathbb{C}$ tal que $\mathrm{Re}(s) > 1$ la serie*

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s}$$

converge absolutamente y en su dominio de convergencia tiene una descomposición como un producto infinito

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \prod_{p \text{ primo}} \left(1 + \frac{\varphi(p)}{p^s} + \frac{\varphi(p^2)}{p^{2s}} + \frac{\varphi(p^3)}{p^{3s}} + \cdots\right).$$

Demostración. La convergencia absoluta de la serie se sigue del hecho de que $\varphi(n)$ está acotada y de la convergencia de la serie de números $\sum_{n=1}^{\infty} 1/n^{\alpha}$, para $\alpha > 1$. Para la descomposición en producto infinito (llamado un *producto de Euler*) fijemos un natural N y consideremos un pro-

ducto parcial

$$\begin{aligned}\prod_{p<N}\left(1+\frac{\varphi(p)}{p^s}+\frac{\varphi(p^2)}{p^{2s}}+\frac{\varphi(p^3)}{p^{3s}}+\cdots\right)&=\sum_{e_1}\frac{\varphi(p_1^{e_1})}{p_1^{e_1 s}}\sum_{e_2}\frac{\varphi(p_2^{e_2})}{p_2^{e_2 s}}\cdots\sum_{e_k}\frac{\varphi(p_k^{e_k})}{p_k^{e_k s}}\\&=\sum_{e_1,\ldots,e_k}\frac{\varphi(p_1^{e_1})}{p_1^{e_1 s}}\cdots\frac{\varphi(p_k^{e_1})}{p_k^{e_k s}}\\&=\sum_{e_1,\ldots,e_k}\frac{\varphi(p_1^{e_1}\cdots\varphi(p_k^{e_k})}{p_1^{e_1 s}\cdots p_k^{e_k s}}\\&=\sum_{P(n)<N}\frac{\varphi(n)}{n^s}\end{aligned}$$

donde $p_1,\ldots,p_k$ son los primos menores que N y $P(n)$ es el factor primo mayor de n de tal forma que la última suma es sobre todos los enteros n cuyos factores primos son menores que N. Note que en la tercera igualdad usamos la multiplicatividad de φ. Ahora, como todo natural menor que N no tiene factores mayores que N, entonces

$$\left|\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}-\sum_{P(n)<N}\frac{\varphi(n)}{n^s}\right|\leq\sum_{n=N}^{\infty}\left|\frac{\varphi(n)}{n^s}\right|$$

y el término en la derecha tiende a 0 cuando $N\to\infty$, lo cual da el resultado deseado. □

Corolario 4. *Si $\varphi:\mathbb{N}\to\mathbb{C}$ es una función acotada y* estrictamente multiplicativa*, es decir, si $\varphi(mn)=\varphi(m)\varphi(n)$ para todo $m,n\in\mathbb{N}$, entonces para todo $s\in\mathbb{C}$ tal que $\mathrm{Re}(s)>1$,*

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

Demostración. Para cada primo p, como $\varphi(p^k)=\varphi(p)^k$, en la proposición anterior se tiene que la serie dentro del producto infinito es una serie geométrica que converge a $1/(1-\varphi(p)p^{-s})$. □

Claramente el teorema de Euler se sigue de este corolario al considerar la función multiplicativa constante $\varphi=1$. La expansión en producto de Euler de $\zeta(s)$ guarda el teorema fundamental de la aritmética en una sola ecuación. Esto muestra, de inicio, la importancia aritmética de la función $\zeta(s)$, a la que se conoce como la función *zeta de Riemann*, porque fue Riemann en su único artículo sobre teoría de números quien la estudió como una función de variable compleja y obtuvo varias de sus propiedades importantes,

incluyendo la ecuación funcional que satisface y que permite extenderla a todo al plano complejo, salvo por un polo simple en $s = 1$.

Finalmente, observemos que es de suma importancia determinar cuándo una sucesión de complejos $\varphi(n) = a_n$ es multiplicativa para que la serie (llamada *serie de Dirichlet*) asociada

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

con $\mathrm{Re}(s) > 1$, tenga una descomposición en producto de Euler. En la sección siguiente veremos un caso importante donde esta multiplicatividad está dada y donde algunos ejemplos fueron estudiados por Euler en su artículo [2] que estamos discutiendo, y después de recordar algunos hechos sobre formas modulares daremos la caracterización de Hecke para que φ sea multiplicativa y consecuentemente se tenga esta descomposición de Euler.

Series de Dirichlet. En [2] Euler también calcula la suma de otras series interesantes, pero para verlas en perspectiva, tendremos que adelantarnos casi 100 años cuando Dirichlet introdujo una generalización de la función zeta de Riemann de la forma siguiente, para lo cual recordamos las definiciones pertinentes: si N es un número natural, un *carácter de Dirichlet* módulo N es un homomorfismo

$$\chi : \left(\mathbb{Z}/N\mathbb{Z}\right)^* \to \mathbb{S}^1 = \{z \in \mathbb{C} \ : \ |z| = 1\} \subseteq \mathbb{C}^*$$

del grupo de unidades del anillo de enteros módulo N al círculo unitario en $\mathbb{C}$. El carácter χ se extiende a todo $\mathbb{Z}$, para definir una función multiplicativa $\chi : \mathbb{Z} \to \mathbb{C}$ mediante

$$\chi(n) = \begin{cases} \chi(n \bmod N) & \text{si } \mathrm{mcd}(n, N) = 1, \\ 0 & \text{si } \mathrm{mcd}(n, N) \neq 1. \end{cases}$$

Si $m|N$ y χ' es un carácter módulo m, éste induce la función $\chi : \mathbb{Z} \to \mathbb{C}$ mediante

$$\chi(a) = \begin{cases} \chi'(a \bmod N) & \text{si } \mathrm{mcd}(a, N) = 1, \\ 0 & \text{si } \mathrm{mcd}(a, N) \neq 1 \end{cases}$$

y resulta que χ es un carácter de Dirichlet módulo N el cual decimos que es *inducido* por el carácter χ'. Un carácter de Dirichlet módulo N se dice que es *primitivo* si no es inducido por algún carácter módulo m para todo $m < N$, y también diremos que en este caso N es el *conductor* de χ y lo denotamos por $N = f(\chi)$.

Si χ_1, χ_2 son caracteres de Dirichlet primitivos, de conductores f_1 y f_2, respectivamente, entonces existe un único carácter primitivo χ cuyo conductor f divide al producto $f_1 f_2$ y tal que

$$\chi(a) = \chi_1(a)\chi_2(a)$$

para todo a coprimo con $f_1 f_2$. Al carácter χ anterior se le conoce como el *producto* de χ_1 y χ_2 y se denota por $\chi = \chi_1\chi_2$. Sin embargo, note que si $\mathrm{mcd}(a, f_1 f_2) > 1$ no necesariamente se tiene que $\chi(a) = \chi_1(a)\chi_2(a)$.

El conjunto de caracteres de Dirichlet primitivos es un grupo abeliano con el producto anterior y su neutro es el *carácter trivial o principal* $\chi^0 : \mathbb{Z} \to \mathbb{C}$ dado por $\chi^0(n) = 1$ para todo n. Note que χ^0 es el único carácter con conductor 1. El inverso del carácter primitivo χ es el carácter $\overline{\chi}$ dado por conjugación compleja, es decir, $\overline{\chi}(a) = \overline{\chi(a)}$, para $a \in \mathbb{Z}$.

Dado un carácter de Dirichlet (primitivo) χ, se define su *L-serie de Dirichlet* mediante

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

para un complejo s tal que $\mathrm{Re}(s) > 1$. Observe que si χ^0 es el carácter trivial, entonces $L(s, \chi^0) = \zeta(s)$ es la función zeta de Riemann. En forma análoga a como se demostró el teorema de Euler, se puede probar que $L(\chi, s)$ converge absoluta y uniformemente en un semiplano de $\mathbb{C}$ y define una función holomorfa en el semiplano $\mathrm{Re}(s) > 1$. De hecho, si $\chi \neq \chi^0$ es primitivo, a diferencia del caso de la función zeta de Riemann, se prueba que $L(\chi, s)$ tiene una continuación analítica a todo $\mathbb{C}$. Más aún, la multiplicatividad de χ, *i.e.*, $\chi(mn) = \chi(m)\chi(n)$ y la condición de que $|\chi(n)| \leq 1$, implican la existencia de un producto de Euler:

$$L(\chi, s) = \prod_{p \text{ primo}} \left(1 - \chi(p)p^{-s}\right)^{-1}.$$

En el artículo [2], Euler considera el ejemplo $L(\chi, s)$ para el carácter de Dirichlet no trivial módulo 4

$$\chi : (\mathbb{Z}/4\mathbb{Z})^* = \{1, 3\} \to \mathbb{S}^1$$

dado por $\chi(1) = 1$ y $\chi(3) = -1$, por lo que su extensión a todo $\mathbb{Z}$ es la función

$$\chi(n) = \begin{cases} (-1)^{(n-1)/2} & \text{si } n \text{ es impar,} \\ 0 & \text{si } n \text{ es par} \end{cases}$$

y así la L-serie de Dirichlet asociada es

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} + \cdots$$

cuya evaluación, en el caso cuando $s = 1$, la cita Euler en el teorema 11 de [2], y es un cálculo debido a Leibniz, y cuya factorización en producto de Euler está en este teorema 11 de [2] (de nuevo, en el caso $s = 1$, que es el único que Euler considera), y el resultado neto es

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots = \frac{3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdots}{4 \cdot 4 \cdot 8 \cdot 8 \cdot 12 \cdot 12 \cdots} = \prod_{p \text{ primo impar}} \frac{p}{p \pm 1}$$

donde el signo en el denominador de los términos del producto está determinado por la congruencia

$$p \pm 1 \equiv 0 \pmod 4$$

como explícitamente escribe Euler en la demostración del teorema. Para una deducción del resultado anterior, además de consultar a Euler, el artículo [8] es de lectura deliciosa.

Formas modulares para $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Para comenzar, recordemos que el grupo lineal especial $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, *i.e.*, el grupo de matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ con entradas enteras y con determinante 1, actúa en el semiplano complejo superior $\mathcal{H}$, es decir, en el conjunto de números complejos z cuya parte imaginaria $\mathrm{Im}(z) > 0$, mediante las transformaciones de Möbius. Más aún, como $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ es la matriz identidad, la acción de $\pm I$ induce la función identidad, y si $g \in \mathrm{SL}_2(\mathbb{Z})$ induce la función identidad, entonces $g = \pm I$. En otras palabras, si consideramos el grupo cociente

$$\overline{\Gamma} := \mathrm{SL}_2(\mathbb{Z}) / \pm I,$$

éste *actúa fielmente* sobre $\mathcal{H}$, es decir, ningún elemento distinto de la identidad actúa trivialmente. El grupo $\overline{\Gamma}$ está generado por las clases laterales de las matrices $T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ y $S := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ cuya acción en $\mathcal{H}$ está dada por: $T : z \mapsto z + 1$ y $S : z \mapsto -1/z$. Así, T genera a todas las traslaciones y S es la negativa de una inversión.

Consideremos ahora una función holomorfa $f(z)$ en el semiplano superior $\mathcal{H}$ y sea k un entero. Supongamos que $f(z)$ satisface la relación

$$f(\gamma z) = (cz + d)^k f(z) \quad \text{para todo} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}). \qquad (9)$$

Supongamos además que $f(z)$ es *holomorfa en infinito*, lo que quiere decir que en la expansión de Fourier de f

$$f(z) = \sum_{n\in\mathbb{Z}} a_n q^n \quad \text{donde} \quad q = e^{2\pi i z}, \tag{10}$$

se tiene que $a_n = 0$ para todo $n < 0$. Una función $f(z)$ que satisface las condiciones (9) y (10) anteriores se llama una *forma modular de peso k para* el grupo modular $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Si además, $a_0 = 0$, *i.e.*, f se anula en infinito entonces $f(z)$ se llama una *forma parabólica (o cuspidal) de peso k para* Γ.

Observemos ahora que si k es impar, tomando $\gamma = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ se tiene que $\gamma z = z$ por definición de la acción de $\mathrm{SL}_2(\mathbb{Z})$; y si $f(z)$ es una forma modular, al substituir γ en (9) se obtiene que

$$f(\gamma z) = f(z) = (-1)^k f(z) = -f(z),$$

(ya que k es impar) y por lo tanto $f(z) = -f(z)$, lo cual implica que $f(z) = 0$, y así no hay formas modulares no triviales de peso k impar, y sólo consideraremos el caso cuando k es par.

Ahora, si $f(z)$ es una forma modular de peso k, en particular, para $\gamma = T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ y $\gamma = S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ la relación (9) anterior implica

$$f(z+1) = f(z) \qquad \text{y} \qquad f(-1/z) = (-z)^k f(z), \tag{11}$$

y se prueba también, usando que $\overline{\Gamma}$ está generado por S y T, que (11) implica (9).

Finalmente, notamos que las condiciones (9) y (11) se preservan bajo la suma y la multiplicación escalar, *i.e.*, los conjuntos de formas modulares y formas parabólicas para algún peso fijo k son espacios vectoriales sobre $\mathbb{C}$. El producto de una forma modular de peso k_1 y una forma modular de peso k_2 es una forma modular de peso $k_1 + k_2$.

Series de Dirichlet asociadas a formas modulares. Si $f(z)$ es una forma modular de peso $2k$ con serie de Fourier

$$f(z) = a_0 + \sum_{n=1}^{\infty} a_n q^n \qquad \text{donde } q = e^{2\pi i z},$$

se le asocia la L-serie de Dirichlet

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

y se prueba, ver [13], que la serie anterior converge en el semiplano $\mathrm{Re}(s) > k+1$ si $f(z)$ es una forma parabólica y en el semiplano $\mathrm{Re}(s) > 2k$ si $f(z)$ no es parabólica. Más aún, si los coeficientes a_n de $f(z)$ satisfacen la propiedad multiplicativa $a_{mn} = a_m a_n$, entonces la L-serie de Dirichlet asociada tiene una representación como producto de Euler de la forma

$$L(f,s) = \prod_{p \text{ primo}} \frac{1}{1 - a_p p^{-s} + p^{2k-1}p^{-2s}},$$

donde notamos que los factores de Euler son polinomios cuadráticos en p^{-s}.

La caracterización de Hecke de la multiplicatividad de la sucesión $a(n) = a_n$ que define la serie de Dirichlet

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

está dada en términos de la forma modular que definen estos coeficientes, a saber, de la función cuya serie de Fourier es

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z},$$

donde estamos suponiendo, para conveniencia de la exposición, que $f(z)$ es una forma parabólica. Para dar la caracterización deseada, Hecke introduce una familia de operadores lineales $T(p)$ en el espacio de formas modulares de un peso $2k$ dado y prueba el resultado fundamental siguiente:

Teorema 5 (Hecke)**.** *Supongamos que*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$$

es una forma modular parabólica de peso $2k$ y que $a_1 = 1$. Entonces, los a_n son multiplicativos si y sólo si $f(z)$ es un vector propio de los operadores de Hecke $T(p)$ con valores propios a_p. Se tiene además que

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ primo}} \frac{1}{1 - a_p p^{-s} + p^{2k-1}p^{-2s}}.$$

□

Hacia 1967 A. Weil [14] extiende los teoremas de Hecke [9] para considerar no sólo formas modulares asociadas al grupo $\mathrm{SL}_2(\mathbb{Z})$ sino también a los subgrupos de congruencia tales como

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

donde recordamos que estos grupos tienen, en general, muchos generadores, a diferencia de $\overline{\Gamma}$ que, como vimos, tiene sólo dos generadores. Para una muestra de la relevancia de estos resultados de Weil, recordaremos a continuación cómo se definen otras funciones L, sólo que esta vez con un origen aritmético-geométrico, que de nuevo se remonta hasta Euler.

La función L de Hasse-Weil de una curva elíptica. Dos días antes de la navidad de 1751 en la Academia de Berlín se recibió una copia de las Obras Matemáticas de G. de Fagnano la cual se le dio a Euler. En algunos de los artículos incluidos, Fagnano estudiaba algunas integrales elípticas, en particular aquéllas asociadas a la longitud de arco de la lemniscata

$$\int \frac{dz}{\sqrt{1-z^4}}$$

y que había publicado entre 1714 y 1720 en algunas revistas italianas de poca circulación; en estos artículos Fagnano obtiene, esencialmente, una fórmula para duplicar un arco de lemniscata dado y Euler, que había estado siguiendo el trabajo de sus contemporáneos acerca de integrales elípticas, se interesó de inmediato por las fórmulas de Fagnano de tal forma que cinco semanas después, el 27 de enero de 1752, presentó a la Academia los resultados de [4] donde explica y comienza a extender los resultados de Fagnano y el 30 abril de 1753 presenta los resultados del artículo [5] donde obtiene una fórmula para sumar dos longitudes de arco arbitrarias de la lemniscata, guiado por la analogía con la longitud de arco de la circunferencia, digamos, $x^2 + y^2 = 1$, de radio 1 y centro el origen $(0, 0)$, por lo que la longitud de arco en el primer cuadrante está dada por la integral

$$s(r) = \int_0^r \frac{dx}{\sqrt{1-x^2}}$$

y en este caso se sabe que un cambio de variable trigonométrico permite calcular estas integrales. Sin embargo, existe una forma más sistemática de calcular las integrales anteriores, parametrizando el círculo usando la pendiente de las rectas que pasan por uno de sus puntos, digamos $A = (-1, 0)$, donde después de resolver las ecuaciones polinomiales correspondientes el

cambio de variable que se sugiere es

$$x = \frac{2m}{1+m^2}$$

que al substituir en la integral para la longitud de arco del círculo, racionaliza el integrando ya que

$$s(r) = \int_0^r \frac{dr}{\sqrt{1-x^2}} = \int_0^t \frac{2dm}{1+m^2}, \quad \text{para} \quad t = \frac{2r}{1+r^2},$$

que se calcula elementalmente. Ahora, para la lemniscata cuyas ecuaciones paramétricas podemos escribir como

$$2x^2 = m^2 + m^4$$
$$2y^2 = m^2 - m^4$$

(despejando x y y en términos del parámetro m), y restringiéndonos al primer cuadrante donde el parámetro varía en $[0,1]$, resulta que la longitud de arco correspondiente es

$$s = s(r) = \int_0^r \frac{dx}{\sqrt{1-x^4}}$$

y procediendo por analogía con el caso de la longitud de arco del círculo, observando que ahora se tiene $\sqrt{1-x^4}$ en lugar de $\sqrt{1-x^2}$, esto sugiere el cambio de variable

$$x = \frac{2m^2}{1+m^4},$$

(que, en efecto, es monótona y suprayectiva en $0 \leq m \leq 1$) y que al hacer las substituciones correspondientes en la integral anterior nos da

$$s = s(r) = \int_0^r \frac{dx}{\sqrt{1-x^4}} = \sqrt{2}\int_0^t \frac{dm}{\sqrt{1+m^4}},$$

donde notamos que, a diferencia del caso del círculo, el cambio de variable propuesto no racionalizó el integrando. Sin embargo, Fagnano y Euler consideran ahora la integral del lado derecho para la cual el cambio de variable análogo que se sugiere es

$$m = \frac{2u^2}{1-u^4}$$

que al substituirlo en la integral del lado derecho nos da

$$s = s(r) = \int_0^r \frac{dx}{\sqrt{1-x^4}} = \sqrt{2}\int_0^t \frac{dm}{\sqrt{1+m^4}} = \sqrt{2}\sqrt{2}\int_0^v \frac{du}{\sqrt{1-u^4}}$$

es decir,

$$s(r) = 2\ s(v)$$

donde (Euler [4], Teorema 5, página 72)

$$r = \frac{2v\sqrt{1-v^4}}{1+v^4}. \qquad (*)$$

Así, a pesar de que no se puede racionalizar el integrando de la longitud de arco de la lemniscata, se tiene una fórmula $(*)$ que permite *duplicar* la longitud de arco de la misma. En el artículo [5] Euler generaliza lo anterior para obtener una fórmula para *sumar dos longitudes de arco* arbitrarias de la lemniscata. Estos resultados de Euler pueden leerse, después de Abel y Jacobi, como *inversión de integrales abelianas*, que en el caso de la integral de la longitud de arco del círculo unitario

$$s(r) = \int_0^r \frac{dx}{\sqrt{1-x^2}}$$

pensada como una función de r, su *función inversa* (en el intervalo correspondiente) es $r = \operatorname{sen}(s)$ y ésta satisface la *fórmula de aditividad*

$$\operatorname{sen}(\alpha+\beta) = \operatorname{sen}\alpha\cos\beta + \cos\alpha\operatorname{sen}\beta$$

donde poniendo $x = \operatorname{sen}\alpha$ y $y = \operatorname{sen}\beta$, se tiene que $\cos\alpha = \sqrt{1-x^2}$ y $\cos\beta = \sqrt{1-y^2}$, por lo que $\operatorname{sen}(\alpha+\beta) = x\sqrt{1-x^2} + y\sqrt{1-y^2}$, y así, para

$$z := \alpha+\beta = \operatorname{sen}^{-1}(\operatorname{sen}(\alpha+\beta))$$

se tiene la *fórmula de aditividad*

$$\int_0^x \frac{dr}{\sqrt{1-r^2}} + \int_0^y \frac{dt}{\sqrt{1-t^2}} = \int_0^z \frac{du}{\sqrt{1-u^2}}$$

donde

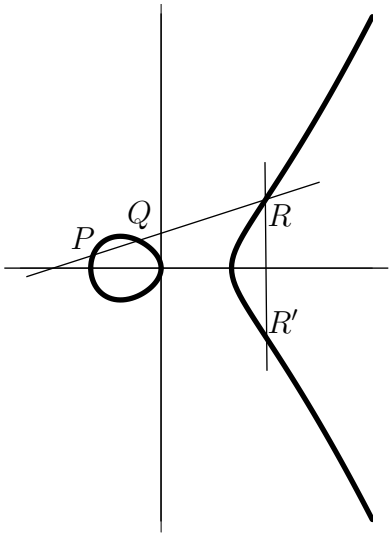
$$z = x\sqrt{1-x^2} + y\sqrt{1-y^2}.$$

Estas son las fórmulas de aditividad para la integral

$$\int_0^t \frac{dt}{\sqrt{1-t^2}}$$

y son las que Euler generalizó para la lemniscata y otros polinomios de grado 4. Estos resultados de Euler pueden considerarse el nacimiento del estudio de la ley de grupo en una curva elíptica, en este caso dada por la retícula en $\mathbb{C}$ asociada a los dos períodos de la integral elíptica considerada.

Un siglo después de Euler, se puede ya definir a una *curva elíptica* E como el lugar geométrico de los puntos de $\mathbb{C}^2$ que satisfacen un polinomio cúbico en dos variables, que para simplificar, podemos pensar que es de la forma $y^2 = x^3 + bx + c$ y donde el polinomio cúbico en x tiene sus tres raíces diferentes, de tal forma que E es una curva lisa y más aún, tiene género $g = 1$, al considerarla no como curva afín sino en el plano proyectivo $\mathbb{P}^2$ al tomar el polinomio homogéneo asociado $y^2z = x^3 + bxz^2 + cz^3$. La fórmula de adición que había encontrado Euler corresponde al hecho de que los puntos de la curva E se pueden *sumar* de tal manera que E tiene estructura de grupo abeliano, una propiedad que no tienen otras curvas de género distinto de 1. La operación de grupo en E se define como sigue: dados dos puntos P y Q en E, considerando la recta secante que pasa por ellos (tangente, si $P = Q$), sea R el tercer punto donde esta recta corta a E (este punto existe por el teorema de Bezout) y luego consideremos la recta que pasa por R y el *punto al infinito* $\mathbf{0} = (0, 1, 0)$ y sea R' el tercer punto donde esta recta (que hemos dibujado como una recta vertical en la figura siguiente) interseca a E. La suma $P + Q$ se define como R'. Se prueba directamente que, con esta operación, E es un grupo abeliano, donde la única parte laboriosa es la demostración de la asociatividad de la operación, pero todo lo anterior se puede simplificar mediante una demostración más conceptual usando los elementos de la geometría algebraica.



Desde el punto de vista de la teoría de números interesa considerar curvas elípticas definidas por polinomios con coeficientes racionales que, después de eliminar denominadores y cambiar variables adecuadamente, se pueden considerar como curvas definidas por polinomios con coeficientes

enteros. En geometría diofantina el problema principal es estudiar el conjunto de puntos de E que tienen coordenadas racionales o enteras y en nuestro caso se sabe que el conjunto de puntos con coordenadas racionales de E, denotado $E(\mathbb{Q})$, es un grupo abeliano finitamente generado (el teorema de Mordell-Weil) y para el estudio de la aritmética de estas curvas conviene en ocasiones escoger un modelo de la curva definida sobre $\mathbb{Z}$ (mínimo en un cierto sentido) y reduciendo sus coeficientes módulo un primo p podemos considerar la curva reducida $\widetilde{E}: \ y^2 = x^3 + \overline{b}x + \overline{c}$ definida ahora sobre el campo finito $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, la cual puede o no ser lisa. En cualquier caso, como $\mathbb{F}_p$ es finito podemos contar el número de puntos con coordenadas en $\mathbb{F}_p$ que tiene la curva $\widetilde{E}$. Esto lo hacemos también con todas las extensiones finitas $\mathbb{F}_{p^n}$ de $\mathbb{F}_p$ y denotamos el número de puntos con coordenadas en este campo con $\#\widetilde{E}(\mathbb{F}_{p^n})$. La idea es considerar la función generadora asociada a la sucesión de enteros $\#\widetilde{E}(\mathbb{F}_{p^n})$

$$Z(E,u) := \exp\left(\sum_{n=1}^{\infty} \frac{\#\widetilde{E}(\mathbb{F}_{p^n})}{n} \cdot u^n\right).$$

Se prueba que esta función es de la forma siguiente

$$Z(E,u) = \begin{cases} \dfrac{1 - a_p u + p u^2}{(1-u)(1-pu)} & \text{si } E \text{ tiene buena reducción en } p, \textit{ i.e.}, \ \widetilde{E} \text{ es lisa} \\ \\ \dfrac{1 - a_p u}{(1-u)(1-pu)} & \text{si } E \text{ tiene mala reducción en } p, \textit{ i.e.}, \ \widetilde{E} \text{ no es lisa} \end{cases}$$

donde $a_p = p + 1 - \#\widetilde{E}(\mathbb{F}_p)$. Notamos entonces que en esta función zeta sólo el entero a_p depende de la curva E por lo que sólo los numeradores nos dan información sobre la curva. Tomando estos numeradores, variando los primos p y substituyendo $u = p^{-s}$ para $s \in \mathbb{C}$, se define la función L de Hasse-Weil de E como el producto de Euler

$$L(E,s) := \prod_{p \text{ malos}} \frac{1}{1 - a_p p^{-s}} \prod_{p \text{ buenos}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

y con respecto a la convergencia de este producto infinito se tiene

Teorema 6 (Hasse)**.** *Para todo primo p se tiene que $|a_p| < 2\sqrt{p}$ y consecuentemente $L(E,s)$ converge para $\mathrm{Re}(s) > 3/2$.* □

Hasse había conjeturado que la función $L(E,s)$ tiene una continuación analítica a todo $\mathbb{C}$ y satisface una ecuación funcional de la forma

$$L(E,s) \sim L(E, 2-s)$$

donde $\sim$ denota igualdad salvo factores gamma elementales.

Note que la función L de Hasse-Weil se *define* como un producto de Euler y no como una serie. De hecho, existen varias conjeturas acerca de la forma que debe tener la expansión de Taylor (vea unos párrafos abajo por qué la función L anterior es entera) de esta función, incluyendo la información sobre la curva E que, conjeturalmente, se encuentra en el primer coeficiente de la expansión de Taylor alrededor de $s = 1$, a saber, las conjeturas de Birch y Swinnerton-Dyer.

Podemos ahora explicar la relevancia del trabajo de Weil de 1967 sobre funciones L de Dirichlet asociadas a formas modulares: Weil conjetura que la función L de Hasse-Weil de la curva elíptica E definida sobre $\mathbb{Q}$ debe ser la función L de Dirichlet asociada a una forma modular parabólica $f(z)$ de peso 2 para un grupo de congruencia $\Gamma_0(N)$

$$L(E, s) = L(f, s),$$

de tal manera que la aritmética de la curva elíptica E está determinada por la aritmética de las formas modulares, lo cual enfatiza, si hiciera falta, la relevancia del estudio de estas funciones. No está de más mencionar que esta conjetura ya había sido adelantada por los matemáticos japoneses Y. Taniyama y G. Shimura, pero fue Weil quien dio la primera evidencia propia de su validez. El año 1999, continuando el trabajo de Wiles-Taylor en su demostración de la conjetura de Fermat, se anunció la demostración de la conjetura de Shimura-Taniyama-Weil y como consecuencia de esto se tiene que la conjetura de Hasse es verdadera: para toda curva elíptica $E/\mathbb{Q}$, la función $L(E, s)$ se extiende a una función entera. Quizá no esté de más recordar que Euler fue atraído hacia la teoría de números por varios problemas que Fermat había dejado, y que en ocasiones Euler tenía que reconstruir las demostraciones de Fermat, lo cual sucedió en particular con la conjetura de Fermat para el exponente 4 y, como Jacobi menciona en [10], es tentador suponer que Euler no puede haber dejado de ver la analogía[1] entre la no existencia de soluciones racionales no triviales a la ecuación diofantina $y^2 = 1 - x^4$, o lo que es lo mismo, la no existencia de soluciones enteras no triviales de la ecuación $x^4 - z^4 = y^2$, lo cual Euler [3] ya había demostrado en 1738 al reconstruir la demostración de Fermat, por descenso infinito, de la no existencia de soluciones enteras no triviales de la ecuación de Fermat

$$x^4 + y^4 = z^4,$$

[1] «esta coincidencia digna de notarse difícilmente se le haya escapado al autor», [10], p. 353.

y la no integrabilidad en términos de funciones elementales de la longitud de arco de la lemniscata

$$\int \frac{dz}{\sqrt{1-z^4}},$$

ya que cualquier substitución que transforme la diferencial anterior en una diferencial racional podría dar soluciones racionales de $y^2 = 1 - x^4$, lo cual a su vez daría soluciones enteras de la ecuación de Fermat.

Funciones zeta de Dedekind. Dedekind generaliza la función zeta de Riemann a cualquier campo de números K (una extensión finita de $\mathbb{Q}$) de la forma siguiente: Sea $K/\mathbb{Q}$ una extensión finita de grado n y sea $\mathcal{O}_K$ el anillo de enteros de K. Para cada ideal $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ el cociente $\mathcal{O}_K/\mathfrak{a}$ es finito, y así

$$N(\mathfrak{a}) := |\,(\mathcal{O}_K/\mathfrak{a})\,| < \infty.$$

Se define entonces la *función zeta de Dedekind de* K como:

$$\zeta_K(s) := \sum_{\mathfrak{a}} 1/N(\mathfrak{a})^s,$$

donde la suma corre sobre los ideales distintos de cero de $\mathcal{O}_K$. Nótese que si $K = \mathbb{Q}$, $\zeta_{\mathbb{Q}}(s)$ es la función zeta de Riemann. Se sabe que ζ_K converge en el semiplano complejo $\mathrm{Re}(s) > 1$ y se puede continuar meromorfamente a todo $\mathbb{C}$, y como $\mathcal{O}_K$ es un anillo de Dedekind, *i.e.*, todos sus ideales propios $\neq 0$ se pueden factorizar en forma única como producto de ideales primos, entonces ζ_K tiene un producto de Euler dado por

$$\zeta_K(s) = \prod_{\mathfrak{P}\text{ primo}} \left(1 - N(\mathfrak{P})^{-s}\right)^{-1}.$$

Ahora, si $K/\mathbb{Q}$ es la m-ésima extensión ciclotómica, se tiene una inyección del grupo de caracteres de Dirichlet de $(\mathbb{Z}/m\mathbb{Z})^*$ en el grupo de caracteres del grupo de Galois $\mathrm{Gal}(K/\mathbb{Q})$, compatible con extensiones de campos ciclotómicos. Se tiene la fórmula siguiente que relaciona las funciones L de Dirichlet con la función zeta de Dedekind de campos ciclotómicos $K/\mathbb{Q}$:

$$\zeta_K(s) = \prod_{\chi} L(s, \chi) \tag{13}$$

donde χ recorre los caracteres de Dirichlet módulo m.

Funciones L de Artin. En todos los casos anteriores sólo hemos considerado una serie L asociada a un campo de números K dado y a continuación veremos cómo Emil Artin asocia una función L a una extensión finita K/F

de campos de números. La construcción de Artin [7] fue motivada por su demostración (y formulación) de esa vasta generalización de la ley de reciprocidad cuadrática de Gauss (y cuyos orígenes se pueden trazar a Legendre y Euler) que es la ley de reciprocidad abeliana de Artin o teoría de campos de clases. En este marco de ideas, se considera una extensión ciclotómica $\mathbb{Q}(\mu_m)$ de $\mathbb{Q}$ y se observa que su grupo de Galois es isomorfo al grupo de unidades de $\mathbb{Z}/m\mathbb{Z}$

$$G = \text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^*,$$

donde el isomorfismo hace corresponder a la clase residual módulo m de cada primo p que no divide a m con el automorfismo de Frobenius Fr_p de $\mathbb{Q}(\mu_m)$ que manda a $\zeta \in \mu_m$ a $\text{Fr}_p(\zeta) = \zeta^p$. Usando el isomorfismo anterior podemos interpretar un carácter de Dirichlet módulo m, $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ como un homomorfismo

$$\chi : G = \text{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \to \text{GL}_1(\mathbb{C}) = \mathbb{C}^* \tag{14}$$

es decir, como una representación de dimensión 1 del grupo de Galois G, y la descomposición en producto de Euler de la serie L de Dirichlet asociada al carácter χ módulo m

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}}$$

la podemos escribir en términos de teoría de Galois como

$$L(\chi, s) = \prod_{p \nmid m} \frac{1}{1 - \chi(\text{Fr}_p)p^{-s}} \tag{15}$$

lo cual llevó a Artin a la generalización que describiremos a continuación, comenzando con el caso de extensiones finitas de la forma $K/\mathbb{Q}$, donde un problema básico es la descripción de cómo se factoriza un (ideal) primo racional $p \in \mathbb{Z}$ en ideales primos del anillo de enteros de una extensión finita K de $\mathbb{Q}$. Se sabe que el anillo de enteros $\mathcal{O}_K \subseteq K$ satisface que todo ideal se factoriza en forma única como un producto de ideales primos y así, para la extensión $K/\mathbb{Q}$

$$\begin{array}{ccccc} p\mathcal{O}_K & \hookrightarrow & \mathcal{O}_K & \hookrightarrow & K \\ \downarrow & & \downarrow & & \downarrow \\ \langle p \rangle & \hookrightarrow & \mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

y para la extensión $p\mathcal{O}_K$ del ideal $\langle p \rangle$ de $\mathbb{Z}$ se tiene que

$$p\mathcal{O}_K = \prod \mathfrak{P}_i \tag{16}$$

donde los $\mathfrak{P}_i$ son ideales primos de $\mathcal{O}_K$ y la colección $\{\mathfrak{P}_i\}$ está completamente determinada por el primo p. Más aún, si $K/\mathbb{Q}$ es una extensión normal, su grupo de Galois $G = \text{Gal}(K/\mathbb{Q})$ permuta transitivamente los primos $\mathfrak{P}_i$ arriba de p, de tal forma que el tipo de factorización de p en $\mathcal{O}_K$ está completamente determinado por los subgrupos estabilizadores $G_{\mathfrak{P}_i}$ que fijan a $\mathfrak{P}_i$ y éstos son conjugados en G. El subgrupo de inercia $I_{\mathfrak{P}_i} = \{g \in G_{\mathfrak{P}_i} \ : \ g(a) = a \mod \mathfrak{P}_i \text{ para todo } a \in \mathcal{O}_K\} \subseteq G_{\mathfrak{P}_i}$ toma en cuenta la ramificación del primo correspondiente. Por ejemplo, si todos los primos $\mathfrak{P}_i$ arriba de p son distintos, en cuyo caso decimos que p no se ramifica en K, entonces los grupos de inercia son triviales y los grupos estabilizadores son cíclicos y se tienen isomorfismos $G_{\mathfrak{P}_i} \simeq k_{\mathfrak{P}_i}/\mathbb{F}_p$, donde $k_{\mathfrak{P}_i}$ y $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ son los campos residuales asociados a los primos correspondientes. Así, los $G_{\mathfrak{P}_i}$ están generados por los *automorfismos de Frobenius* $\text{Fr}_{\mathfrak{P}_i}$ asociados, bajo el isomorfismo anterior, a los automorfismos de $k_{\mathfrak{P}_i}$ dados por $\alpha \mapsto \alpha^{q_i}$ donde $q_i = |k_{\mathfrak{P}_i}|$. Así, el tipo de factorización (16) de p está determinado por el automorfismo de Frobenius (en general, cuando hay ramificación, por su clase de conjugación $\{\text{Fr}_p\}$), y se desea dar una descripción de $\{\text{Fr}_p\}$ en términos de p y de la aritmética de $\mathbb{Q}$. Algunos ejemplos donde esto se puede hacer se remontan a Fermat y Euler [6], por ejemplo en el caso de la extensión cuadrática $K = \mathbb{Q}[i] = \{a + bi \in \mathbb{C} \ : \ a, b \in \mathbb{Q}\}$, cuyo anillo de enteros es $\mathbb{Z}[i] = \{a + bi \ : \ a, b \in \mathbb{Z}\}$ (el anillo de enteros gaussianos) y cuyo grupo de Galois es $G = \text{Gal}(\mathbb{Q}[i]/\mathbb{Q}) = \{\text{id}, c\}$, donde $c : \mathbb{Q}[i] \to \mathbb{Q}[i]$ es la conjugación compleja. Es fácil ver que en este ejemplo, si p es un primo impar,

$$\text{Fr}_p = \begin{cases} \text{id} & \text{si } -1 \text{ es un residuo cuadrático módulo } p, \\ c & \text{en otro caso} \end{cases}$$

de tal forma que, poniendo $G \simeq \{+1, -1\}$ por medio del isomorfismo obvio, entonces

$$\text{Fr}_p = \left(\frac{-1}{p}\right)$$

es el *símbolo de Legendre*, que en el caso cuando el primo p es no ramificado en $\mathbb{Q}[i]$ tiene el valor

$$\text{Fr}_p = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

y por lo tanto

$$\text{Fr}_p = (-1)^{(p-1)/2} = 1 \Leftrightarrow p \equiv 1 \pmod 4$$

lo cual describe Fr_p en términos de p y de la aritmética de $\mathbb{Z}$, en este caso módulo 4. Una consecuencia de lo anterior, debida a Fermat y Euler [6], es

que como los ideales de $\mathbb{Z}[i]$ son principales de la forma $\langle n\rangle$ ó $\langle m+ni\rangle$, entonces p se descompone totalmente en $\mathbb{Z}[i]$ si y sólo si $\mathrm{Fr}_p = \mathrm{id}$ y por lo tanto:

Teorema 7 (Fermat-Euler)**.** *Si p es un primo impar, entonces p es la suma de dos cuadrados $p = m^2 + n^2$ si y sólo si $p \equiv 1 \pmod 4$.*

Así, en este ejemplo, el tipo de factorización de p depende de si p está o no en la progresión aritmética módulo 4. En general, para cualquier extensión finita $K/\mathbb{Q}$ se quisiera tener una tal descripción de $\{\mathrm{Fr}_p\}$, por ejemplo, en términos de una progresión aritmética módulo un cierto entero N. Esto no será posible en general, pero para el caso cuando la extensión $K/\mathbb{Q}$ es abeliana, *i.e.*, cuando el grupo de Galois $\mathrm{Gal}(K/\mathbb{Q})$ es abeliano, sí se tiene una tal descripción, y es el contenido de la teoría de campos de clases en la forma en que la concibió E. Artin, al generalizar la función L de (15) asociada a la representación ciclotómica (14), para considerar ahora una representación arbitraria de dimensión 1 del grupo de Galois abeliano

$$\rho : G = \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^* \tag{17}$$

y definir la función L de Artin asociada como el producto de Euler

$$L(\rho, s) = \prod_p \frac{1}{1 - \rho(\mathrm{Fr}_p)p^{-s}}, \tag{18}$$

donde $\rho(\mathrm{Fr}_p)$ es la imagen del Frobenius en el subespacio invariante $\mathbb{C}^{I_p}$ (que es de dimensión 0 ó 1) y que toma en cuenta la posible ramificación de p. El resultado principal en este contexto es

Teorema 8 (Artin)**.** *Sea $K/\mathbb{Q}$ una extensión abeliana finita con grupo de Galois G y sea $\rho : G \to \mathbb{C}^*$ una representación de dimensión 1. Si $L(s, \rho)$ es la función L de Artin asociada, entonces existe un entero N, que depende de ρ, y un carácter de Dirichlet primitivo χ_ρ con conductor N tal que*

$$L(\rho, s) = L(\chi_\rho, s)$$

donde en la derecha se tiene la función L de Dirichlet asociada a χ_ρ. Dicho en otras palabras, el carácter de Dirichlet χ satisface que $\rho(\mathrm{Fr}_p) = \chi_\rho(p)$, para todos los primos p no ramificados. □

El teorema de Artin se puede interpretar como una ley de reciprocidad, y es conocido que implica la ley de reciprocidad cuadrática general, conjeturada por Euler y Legendre y probada por primera vez por Gauss, y también las leyes de reciprocidad superiores.

De hecho, Artin considera una situación más general tomando una extensión finita de Galois F/K de campos de números con grupo de Galois $G = \text{Gal}(F/K)$ no necesariamente abeliano. En forma análoga a lo discutido anteriormente, para $\mathfrak{p}$ un ideal primo de K, si $\mathfrak{P}$ es un ideal primo de F arriba de $\mathfrak{p}$, lo cual denotamos por $\mathfrak{P}|\mathfrak{p}$, sean $G_{\mathfrak{P}}$ e $I_{\mathfrak{P}}$ el grupo de descomposición y el grupo de inercia de $\mathfrak{P}|\mathfrak{p}$. Se tiene un isomorfismo canónico $G_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \text{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ sobre el grupo de Galois de la extensión de campos finitos dada por los campos residuales de $\mathfrak{P}$ y $\mathfrak{p}$, respectivamente. Se sigue que el grupo cociente $G_{\mathfrak{P}}/I_{\mathfrak{P}}$ está generado por el automorfismo de Frobenius $\text{Fr}_{\mathfrak{P}}$ cuya imagen en el grupo cíclico $\text{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ es el morfismo $\alpha \mapsto \alpha^q$, donde $q = |k_{\mathfrak{P}}| =: N(\mathfrak{P})$.

Guiado por su formulación de la ley de reciprocidad en el caso abeliano y reconociendo la utilidad de estudiar un grupo arbitario por medio de sus representaciones, Artin considera ahora una representación compleja de G de dimensión n, es decir, considera un $\mathbb{C}$-espacio vectorial V de dimensión n y un homomorfismo de grupos

$$\rho : G \to \text{GL}(V) \simeq \text{GL}_n(\mathbb{C})$$

donde $\text{GL}(V)$ es el grupo de isomorfismos de V en sí mismo (y por lo tanto corresponden a matrices $n \times n$ con determinante no nulo). Después, observa que la imagen del automorfismo de Frobenius, $\rho(\text{Fr}_{\mathfrak{P}}) \in \text{GL}(V)$, induce por restricción un endomorfismo $\rho(\text{Fr}_{\mathfrak{P}})|_{V^{I_{\mathfrak{P}}}} : V^{I_{\mathfrak{P}}} \to V^{I_{\mathfrak{P}}}$ del subespacio vectorial de invariantes $V^{I_{\mathfrak{P}}}$ de V y observamos que su polinomio característico

$$\det(1 - \rho(\text{Fr}_{\mathfrak{P}})|_{V^{I_{\mathfrak{P}}}} t)$$

sólo depende del ideal primo $\mathfrak{p}$ de K y no del ideal $\mathfrak{P}$ arriba de él, ya que para cualquier otro ideal de F arriba de $\mathfrak{p}$ los grupos de descomposición y de inercia asociados son conjugados de los correspondientes de $\mathfrak{P}$ y por lo tanto los endomorfismos de los subespacios de invariantes son conjugados también y consecuentemente tienen el mismo polinomio característico. Artin define la L-serie asociada a la extensión de campos de números F/K y a la representación $\rho : \text{Gal}(F/K) \to \text{GL}_n(V)$ como el producto de Euler

$$L(F/K, \rho, s) = \prod_{\mathfrak{p}} \frac{1}{\det(1 - \rho(\text{Fr}_{\mathfrak{P}})|_{V^{I_{\mathfrak{P}}}} N(\mathfrak{p})^{-s})} \tag{19}$$

donde $\mathfrak{p}$ recorre todos los ideales primos de K.

Note que si $K/\mathbb{Q}$ es una extensión finita (de Galois) y si $\rho\colon \text{Gal}(K/\mathbb{Q}) \to \text{GL}_1(\mathbb{C}) = \mathbb{C}^*$ es la representación trivial $\rho(\sigma) = 1$, para todo $\sigma \in \text{Gal}(K/\mathbb{Q})$, la L-serie de Artin correspondiente

$$L(K/\mathbb{Q}, \rho, s) = \zeta_K(s)$$

es la función zeta de Dedekind de K y por lo tanto las funciones de Artin generalizan a éstas. Es importante notar que, en general, las L-series de Artin, *definidas como un producto de Euler*, no tienen una expresión aditiva como las de las funciones zeta de Dedekind

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}.$$

Un largo camino se ha recorrido desde la factorización en producto de Euler de la función zeta de Riemann hasta la definición de las L-series de Artin como productos de Euler.

Se demuestra que las L-series de Artin convergen absoluta y uniformemente en el semiplano $\mathrm{Re}(s) \geq 1 + \varepsilon$, para todo $\varepsilon > 0$ y así definen una función holomorfa en el semiplano $\mathrm{Re}(s) > 1$. Una conjetura importante de Artin, y que todavía sigue abierta, es que para cualquier representación irreducible ρ, la L-serie de Artin define una función holomorfa en todo $\mathbb{C}$.

El problema que plantea Artin es el de obtener la ley de reciprocidad correspondiente para extensiones no abelianas, es decir, cuáles serían los análogos n-dimensionales de los caracteres de Dirichlet y sus correspondientes funciones L. Con la perspectiva que da el tiempo, sabemos ahora que casi simultáneamente con Artin, E. Hecke había construido análogas 2-dimensionales de las funciones L de Dirichlet asociadas a lo que ahora llamamos caracteres de Hecke y se tuvo que esperar hasta finales de la década de 1960, para que R. P. Langlands formule una serie de conjeturas que incluyen ciertas representaciones automorfas, de dimensión arbitraria del grupo GL_n definido sobre los adeles de $\mathbb{Q}$ como las generalizaciones apropiadas de los caracteres de Dirichlet, y asocia a estas representaciones automorfas π funciones L que generalizan las de Dirichlet y conjetura que se tiene la igualdad

$$L(F/K, \rho, s) = L(\pi, s)$$

como parte de un gran programa que pone la noción de representación automorfa en el centro de atención de la teoría de números.

El desarrollo de las ideas anteriores, por A. Weil, R. P. Langlands, J.-P. Serre y muchos otros matemáticos, está en el centro de mayor actividad de la teoría de números del siglo XX y de lo que va del siglo actual. Nada mal para algunas de las ideas que se originaron con un matemático que este año cumple 300.

Referencias

1. Euler, L., *De summis serierum reciprocarum*. Comm. Acad. Sci. Imp. Petropol. **7** (1740) 123-134. Opera Omnia I. 14, 73-68. **E41** en la clasificación de Eneström.

2. Euler, L., *Variae observationes circa series infinitas*. Comm. Acad. Sci. Imp. Petropol. **9** (1744), 1737, 160-188. Opera Omnia I. 14, 216-244. **E72** en la clasificación de Eneström.

3. Euler, L., *Theorematum quorundam arithmeticorum demonstrationes*. Comm. Acad. Sci. Petropol. **10** (1747), 1752, 125-146. Opera Omnia I. 2, 38-58. **E98** en la clasificación de Eneström.

4. Euler, L., *Observationes de comparatione arcuum curvarum irrectificabilium*. Novi Comm. Acad. Sci. Petropol. **6** (1761), 1752, 58-84. Opera Omnia I. 20, 80-107. **E252** en la clasificación de Eneström.

5. Euler, L., *De integratione aequationis differentialis* $\frac{mdx}{\sqrt{1-x^4}} = \frac{ndy}{\sqrt{1-y^4}}$. Novi Comm. Acad. Sci. Petropol. **6** (1761), 1753, 37-57. Opera Omnia I. 20, 58-79. **E251** en la clasificación de Eneström.

6. Euler, L., *Demonstratio theorematis Fermatiani omnem numerum primum formae 4n+1 esse summam duorum quadratorum*. Novi Comm. Acad. Sci. Petropol. **5** (1760), 1754, 3-13. Opera Omnia I. 3, 328-337. **E241** en la clasificación de Eneström.

7. Artin, E., *Über eine neue Art von L-Reihen*. Hamb. Abh. (1923), 89-108. Collected Papers, 105-124. Addison-Wesley, Reading, 1965.

8. Barajas, A., *π y los primos*. Revista Matemática, Segunda Serie **1** (1968), 33-36.

9. Hecke, E., *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung*. Math. Ann. **112** (1936), 664-699. Mathematische Werke, 591-626. Vandenhoeck und Ruprecht, Götingen, 1959.

10. Jacobi, C. G. J., *De usu theoria integralium ellipticorum et integralium abelianorium in analysi Diophantea*. Journal für die Reine und Andgewandte Math. **13** (1835), 353-355.

11. Langlands, R. P., *Euler products*. Yale University Press, New Haven, 1967.

12. Langlands, R. P., *Problems in the theory of automorphic forms*. Lecture Notes in Mathematics **170**, 18-86, Springer Verlag, Berlín, 1970.

13. Serre, J.-P., *A Course in Arithmetic*. Springer Verlag, Berlín, 1993.

14. Weil, A., *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*. Math. Ann. **168** (1967), 149-156. Œuvres Scientifiques, Vol. III, 165-172. Springer Verlag, Berlín, 1979.

15. Weil, A., *Number theory: An approach through history from Hammurapi to Legendre*. Birkhäuser Verlag, Boston, 2001.

16. Zaldívar, F., *La función zeta de Riemann*. Misc. Mat. **36**, 63-82, (2002).