El diablo de los números

Sección a cargo de

Javier Fresán

La aritmética como tomografía

por

Fernando Rodríguez Villegas

1. Introducción

La ley de reciprocidad cuadrática es uno de los resultados fundamentales de la teoría de números que uno típicamente encuentra en las primeras lecturas sobre el tema. Demos unos pasos hacia atrás reformulando esta ley de la siguiente manera. Consideremos un polinomio $f(x) := ax^2+bx+c$ de grado dos con coeficientes enteros. Dado un primo p, el número de soluciones $N(p)$ de la congruencia

$$f(x) \equiv 0 \text{ mód } p \tag{1}$$

es ciertamente $0, 1$ o 2, dado que $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ es un cuerpo. Lo que la ley de reciprocidad cuadrática nos da es una forma alternativa de describir la función $p \mapsto N(p)$ en términos finitos. Concretamente, tenemos lo siguiente:

Teorema 1.1. *Dado un polinomio cuadrático $f(x) := ax^2 + bx + c$ con $a, b, c \in \mathbb{Z}$, existen un conjunto finito de primos S, un entero m y un homomorfismo*

$$\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \{\pm 1\}$$

tales que, para todo primo $p \notin S$, se tiene

$$N(p) = 1 + \chi(p).$$

Podríamos ser mucho más explícitos en esta descripción, pero lo que queremos es enfatizar un punto esencial. El resultado muestra cómo la función $p \mapsto N(p)$ tiene una estructura oculta, descriptible en términos de algo a priori totalmente ajeno al problema como es el carácter χ módulo m. En efecto, vemos por ejemplo que el número de soluciones de la congruencia (1) solo depende de p módulo m. Más aún,

$\chi(a)$ no es una función arbitraria de a módulo m, sino que tiene mucha estructura: es una función multiplicativa.

Surge naturalmente una pregunta fundamental. ¿Qué podemos decir en el caso de polinomios en general (de grado cualquiera, en más variables, más de uno simultáneamente), sobre el número de soluciones $N(p)$ a congruencias módulo un número primo p como función de p? En este trabajo, hablaremos de lo que se sabe o se conjetura acerca de esta pregunta y de por qué importa, de modo completamente informal (una buena referencia es [11]). Vamos a dividir la pregunta en dos partes:

1. *¿Cuál es la forma general de la función $p \mapsto N(p)$?*
2. *¿Se puede expresar $N(p)$ en términos de otras estructuras matemáticas?*

Hay un aspecto quizás sorprendente de lo que vamos a discutir, y es que la respuesta a estas preguntas tiene un contenido netamente geométrico. Contar soluciones a una congruencia podríamos decir que es algo discreto, mientras que la geometría la asociamos con algo continuo. Lo discreto y lo continuo tienden a considerarse como conceptos opuestos. Es notable entonces que, como veremos, cantidad y forma tengan una relación tan estrecha. Esta relación se expresa de forma precisa en las conjeturas de A. Weil de los años 40 probadas por P. Deligne en 1973.

Una vez, en una pre-entrevista para una posible futura entrevista radial, me presionaron para que diera una explicación de mi trabajo de la manera menos técnica posible, sin apelar a frases hechas o clichés vacíos. Se me ocurrió que había una analogía con la tomografía. En una tomografía, mandamos rayos a través del objeto de interés y observamos el resultado. Repitiéndolo en muchas direcciones distintas, conseguimos reconstruir el objeto, incluido su interior (la razón principal de su uso en medicina).

Podemos pensar en cada número primo como en una dirección, y en contar soluciones a la correspondiente congruencia, como en medir el resultado de los rayos de una tomografía. Esperamos que la información obtenida para muchos primos nos permita deducir algo sobre la geometría de las soluciones complejas o sobre la naturaleza de las soluciones racionales de las correspondientes ecuaciones. Esto se conoce en general como el *principio local-global*.

Consideremos sistemas polinomiales de ecuaciones

$$X: \quad \begin{cases} F_1(x_1, \ldots, x_n) &= 0, \\ \vdots & \\ F_s(x_1, \ldots, x_n) &= 0, \end{cases} \tag{2}$$

donde $F_i(x_1, \ldots, x_n)$ son polinomios de grado arbitrario con coeficientes enteros. Llamamos al conjunto de sus ceros comunes una *variedad algebraica*. Tenemos, por un lado, el conjunto $X(\mathbb{C})$ de las soluciones complejas del sistema y, por otro, el conjunto de soluciones $X(\mathbb{F}_p)$ en el cuerpo finito $\mathbb{F}_p$. Lo que resulta es que la geometría del espacio $X(\mathbb{C})$ está íntimamente ligada a la naturaleza de los números $\#X(\mathbb{F}_p)$.

Hay otro aspecto que destacar. También en problemas diofánticos (la descripción de las soluciones en números racionales $X(\mathbb{Q})$ a sistemas polinomiales de ecuaciones), como en mucha de la teoría de números moderna, los números $\#X(\mathbb{F}_p)$ intervienen de forma fundamental. El caso más impactante es el de la conjetura de

Birch–Swinnerton-Dyer (BSD), uno de los problemas del instituto Clay para el nuevo milenio, que tocaremos en la sección 9.

En este corto trabajo (que sigue en espíritu el punto de vista de [10]) intentaré dar de forma muy breve algo de sustancia a la metáfora de la aritmética como tomografía. Dejo al lector decidir si la analogía es acertada. En todo caso, ¡no fui convocado para la entrevista!

2. Ejemplos

Antes de entrar en más detalle, describamos algunos ejemplos que iremos desarrollando más adelante.

1. Para polinomios generales $f \in \mathbb{Z}[x]$, la función correspondiente $p \mapsto N(p)$, donde $N(p)$ es el número de soluciones a la congruencia $f(x) \equiv 0 \bmod p$, está muy lejos de ser descrita solamente en términos de la clase de congruencia de p módulo un número fijo m. Pero esto sí es verdad para *ciertos* polinomios de grado arbitrario. Veamos algunos casos.

   Para un primo $N > 2$, sea

   $$f_N(x) := \prod_{j=1}^{(N-1)/2} \left(x - 2\cos\left(\frac{2\pi j}{N}\right)\right).$$

   Este es un polinomio con coeficientes enteros. Concretamente, por ejemplo, para $N = 11$ el polinomio es

   $$f_{11}(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

   Aquí tenemos que, para primos $p \neq N$,

   $$N(p) = \begin{cases} \frac{1}{2}(N-1) & \text{si } p \equiv \pm 1 \bmod N, \\ 0 & \text{si } p \not\equiv \pm 1 \bmod N. \end{cases} \tag{3}$$

2. Aun en el caso de un polinomio cúbico, describir $N(p)$ es típicamente complicado. Sea, por ejemplo, $f = x^3 - x^2 + 1$ (no un polinomio precisamente tomado al azar, pero de comportamiento típico). En este caso, tenemos que

   $$N(p) = \begin{cases} 0 \text{ o } 3 & \text{si } \chi(p) = +1, \\ 1 & \text{si } \chi(p) = -1, \end{cases}$$

   donde $\chi(p) = \left(\frac{-23}{p}\right)$ es el símbolo de Legendre módulo p. El número -23 es el discriminante del polinomio f.

   Vemos que al menos un aspecto de la función $N(p)$ está gobernado por congruencias. Pero distinguir los casos 0 y 3 cuando $\chi(p) = 1$ requiere algo más sofisticado, algo que no puede determinarse con una congruencia. Se tiene que

   $$N(p) = \begin{cases} 3 & \text{si } p = x^2 + xy + 6y^2 \quad (x, y \in \mathbb{Z}), \\ 0 & \text{en caso contrario,} \end{cases} \qquad \chi(p) = +1. \tag{4}$$

Por ejemplo, en el rango $2 \leq p \leq 150$, el único primo de la forma $x^2+xy+6y^2$ con x e y enteros es $p = 59$.

¿Qué hace que, en el caso de f_N del primer ejemplo, un sistema de congruencias sea suficiente para describir $N(p)$, pero no en el caso de $f = x^3 - x^2 + 1$? Veremos que la diferencia crucial está en que el grupo de Galois del polinomio f_N es abeliano, mientras que el de f no lo es.

3. Sea $f(x_0, \ldots, x_3) \in \mathbb{Z}[x_0, \ldots, x_3]$ un polinomio cúbico homogéneo en cuatro variables cuyas derivadas parciales $\partial f/\partial x_0, \ldots, \partial f/\partial x_3$ no tienen ningún cero no trivial en común. El conjunto de ceros complejos de f define una superficie algebraica no singular X en el espacio proyectivo complejo $\mathbb{P}^3(\mathbb{C})$.

   Si, en cambio, consideramos el número de puntos de X en el cuerpo finito $\mathbb{F}_p$, tomando la ecuación módulo p obtenemos que, para primos p fuera de un cierto conjunto finito,

$$\#X(\mathbb{F}_p) = p^2 + t_p p + 1, \tag{5}$$

   donde t_p es un número entero de valor absoluto $|t_p| \leq 7$.

   Explicar cómo el número t_p depende del primo p requiere más detalles, pero digamos por ahora que involucra las famosas 27 rectas contenidas en toda superficie cúbica.

4. Una matriz cuadrada A se dice *nilpotente* si satisface $A^N = 0$ para algún entero positivo N. Si la matriz es de tamaño $n \times n$, alcanza con saber si $A^n = 0$. En términos de las entradas de A vistas como variables, la condición $A^n = 0$ determina n^2 ecuaciones con coeficientes enteros.

   Por ejemplo, cuando $n = 2$, si escribimos $A = (a_{i,j})$, la condición $A^2 = 0$ es equivalente al sistema de ecuaciones

$$\mathcal{N}_2 := \begin{cases} a_{1,1}^2 + a_{2,1}a_{1,2} &= 0, \\ a_{1,2}a_{1,1} + a_{2,2}a_{1,2} &= 0, \\ a_{2,1}a_{1,1} + a_{2,2}a_{2,1} &= 0, \\ a_{2,1}a_{1,2} + a_{2,2}^2 &= 0. \end{cases}$$

   En este caso, el número $N(p)$ de soluciones de esas ecuaciones módulo p es el número de matrices nilpotentes sobre $\mathbb{F}_p$. Se sabe que este número es p^{n^2-n} para todo primo p, con lo que la dependencia de $N(p)$ en p es básicamente trivial, aunque las ecuaciones en consideración no lo sean.

   Notemos que, por el teorema de Cayley-Hamilton, una forma alternativa de determinar si A es nilpotente es pedir que su polinomio característico sea igual a T^n. Para $n = 2$, esto determina el sistema de ecuaciones mucho más sencillo

$$\mathcal{N}_2' := \begin{cases} a_{1,1} + a_{2,2} &= 0, \\ a_{1,1}a_{2,2} - a_{1,2}a_{2,1} &= 0. \end{cases}$$

   Hagamos un pequeño paréntesis para notar una de las dificultades a la hora de considerar sistemas polinomiales de ecuaciones arbitrarios. En rigor, estos dos sistemas de ecuaciones $\mathcal{N}_2$ y $\mathcal{N}_2'$ no son equivalentes. Por ejemplo, la ecuación

$a_{1,1} + a_{2,2}$ de $\mathcal{N}_2'$ no se puede expresar polinomialmente en términos de las ecuaciones de $\mathcal{N}_2$ (este sí es el caso para $(a_{1,1} + a_{2,2})^3$). Sin embargo, las soluciones de ambos sistemas con $a_{i,j}$ en un cuerpo dado cualquiera son las mismas. Aunque no sea evidente a simple vista, lo que tenemos es similar a considerar la ecuación $x = 0$ en lugar de $x^2 = 0$.

5. En la famosa última anotación del 7 de julio de 1814 en su *Tagebuch* matemático, Gauss menciona lo siguiente. Consideremos la congruencia

$$x^2 + y^2 + x^2y^2 \equiv 1 \text{ mód } p$$

para p primo, y sea $N(p)$ el número de soluciones con $x, y \in \mathbb{F}_p$. Gauss notó, seguramente basado en la evidencia numérica (*observatio per inductionem facta gravissima*), algo equivalente a lo siguiente. Escribamos $N(p) = p - 3 - a_p$ (veremos luego el porqué de esta elección). Para $p \equiv 1$ mód 4, se tiene

$$a_p = (-1)^{\frac{1}{2}(u+v-1)} 2u, \tag{6}$$

donde escribimos p como $u^2 + v^2$ con u y v enteros y v par. Para primos $p \equiv 3$ mód 4, tenemos $a_p = 0$.

Weil se refiere a Gauss en relación a sus conjeturas. En su articulo *Two lectures on number theory, past and present* [15], dice textualmente:

> *In 1947, in Chicago, I felt bored and depressed and, not knowing what to do, I started reading Gauss's two memoirs on biquadratic residues, which I had never read before... This led me in turn to some conjectures.*

Estas conjeturas son las que ahora se conocen como *conjeturas de Weil*. Formuladas en los años 40, dieron un inmenso impulso al desarrollo de la Geometría Algebraica moderna. Nos dan una respuesta precisa a nuestra primera pregunta. Las retomamos más adelante.

6. Ecuaciones de la forma

$$E\colon \quad y^2 = x^3 + ax + b, \qquad 27b^2 + 4a^3 \neq 0,$$

para a y b fijos, se conocen como *curvas elípticas* y juegan un papel central en la teoría de números. Tomemos $a, b \in \mathbb{Z}$ y escribamos, de forma análoga al ejemplo anterior de Gauss, $\#E(\mathbb{F}_p) = p + 1 - a_p$ (agregamos en este cómputo el único punto extra, en el infinito, de la versión proyectiva de la ecuación).

¿Qué podemos decir de a_p como función de p? Esta resulta ser una pregunta profunda cuya respuesta fue dada por el trabajo de Wiles y otros sobre la *modularidad* de tales curvas elípticas previamente conjeturada. Como es sabido, la consecuencia más espectacular de este trabajo fue la resolución del último teorema de Fermat, uno de los problemas emblemáticos de la teoría de números.

En pocas palabras, la modularidad de una curva elíptica dice que a_p es el coeficiente de q^p de una *forma modular* asociada, una función del semiplano

superior complejo que satisface ciertas condiciones de simetría muy particulares. Por ejemplo, la curva elíptica

$$E: \quad y^2 + y = x^3 - x^2$$

está asociada a la forma modular

$$F(q) = q \prod_{n\geq 1} (1-q^n)^2(1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 + \cdots .$$

En el caso $p = 97$, el coeficiente de q^{97} de $F(q)$ es -7 y, efectivamente, el número de soluciones de la congruencia $y^2 + y \equiv x^3 - x^2$ mód 97 con $x, y \in \mathbb{F}_{97}$ es $104 = 97 - (-7)$.

Recalquemos el paralelo con la ley de reciprocidad cuadrática con la que empezamos. El número de soluciones a una congruencia viene expresado en términos de un objeto matemático altamente estructurado que, a priori, le es completamente ajeno.

3. Forma general de $N(p)$

Para p primo, sea $N(p)$ el número de soluciones de la congruencia

$$\begin{cases} F_1(x_1, \ldots, x_n) & \equiv & 0 & \text{mód } p, \\ \qquad\vdots & & & \\ F_s(x_1, \ldots, x_n) & \equiv & 0 & \text{mód } p, \end{cases}$$

donde $F_i(x_1, \ldots, x_n)$ son polinomios de grado arbitrario con coeficientes enteros.

Recordemos nuestra primera pregunta:

¿Cuál es la forma general de la función $p \mapsto N(p)$?

La respuesta es una consecuencia de las conjeturas de Weil. Aquí conviene hacer una digresión y extender la pregunta a todos los cuerpos finitos. En efecto, la estructura que queremos describir emerge considerando no solo el cuerpo finito $\mathbb{F}_p$ con p dado, sino también la torre de cuerpos finitos que lo contienen. Un tal cuerpo está determinado por su tamaño q, que es de la forma p^r con r entero; lo denotamos $\mathbb{F}_q$. Extendemos entonces la pregunta a la forma de la función $q \mapsto N(q)$, donde $N(q)$ representa el número de soluciones al sistema de ecuaciones

$$\begin{cases} F_1(x_1, \ldots, x_n) & = & 0, & \\ \qquad\vdots & & & (x_i \in \mathbb{F}_q), \\ F_s(x_1, \ldots, x_n) & = & 0. & \end{cases}$$

considerando $F_i(x_1, \ldots, x_n)$ en su reducción módulo p.

Como primera aproximación, la respuesta es la siguiente:

Teorema 3.1. *Existen un conjunto finito de primos S, números complejos $\xi_1, \ldots, \xi_k$ y signos $\epsilon_1 = \pm 1, \ldots, \epsilon_k = \pm 1$ tales que*

$$N(p^r) = \epsilon_1 \xi_1^r + \cdots + \epsilon_k \xi_k^r \tag{7}$$

para todo $r \geq 1$ y para todo primo $p \notin S$.

Hay una forma elegante de expresar este resultado en términos de series generatrices. Consideremos la serie de potencias en una variable T definida como

$$Z(T) := \exp\left(\sum_{r \geq 1} N(p^r) \frac{T^r}{r}\right).$$

No es difícil comprobar que la validez de (7) para todo $r \geq 1$ es equivalente a la propiedad de que $Z(T)$ sea el desarrollo de Taylor de una función racional, o más precisamente que tengamos

$$Z(T) = \prod_{i=1}^{k} (1 - \xi_i T)^{-\epsilon_i}.$$

Por ejemplo, en el caso de una curva elíptica obtenemos la igualdad

$$Z(T) = \frac{1 - a_p T + pT^2}{(1 - T)(1 - pT)} \qquad (p \notin S), \tag{8}$$

donde, como antes, $\#E(\mathbb{F}_p) = p + 1 - a_p$. Es decir, que los números (ξ_i, ϵ_i) son $(1, 1), (p, 1), (\alpha, -1), (\beta, -1)$, donde α y β son las raíces del numerador de $Z(T)$, o sea, que satisfacen $\alpha\beta = p$ y $\alpha + \beta = a_p$.

Esta función se llama la *función zeta* de nuestro sistema de ecuaciones y es una forma muy conveniente de codificar todos los números $N(p^r)$ al mismo tiempo. En esta forma, el resultado fue demostrado por B. Dwork [3] en 1959.

Aquí conviene destacar un punto sorprendente e importante que se desprende del resultado de Dwork. La expresión (7) implica que $N(p^r)$ está a priori unívocamente determinada por sus valores $N(p), N(p^2), \ldots, N(p^k)$. En el caso de una curva elíptica, de hecho alcanza con el valor de $N(p) = \#E(\mathbb{F}_p)$ para determinar toda la sucesión $N(p^r)$, ya que conocer a_p es suficiente.

Una segunda consecuencia de las conjeturas de Weil, más profunda, es que los números ξ_i no son completamente arbitrarios. Este fue uno los de aportes principales de Deligne. Como segunda aproximación, tenemos lo siguiente:

Teorema 3.2. *La función $Z(T)$ tiene la forma*

$$Z(T) = \prod_i P_i(T)^{-\eta_i}, \qquad \eta_i = \pm 1, \tag{9}$$

donde $P_i(T)$ es un polinomio con coeficientes enteros de la forma

$$P_i(T) = \prod_j (1 - \xi_{i,j} T), \qquad |\xi_{i,j}| = p^{w_i/2},$$

con w_i un entero no negativo. En particular, para todo entero $r \geq 1$,

$$N(p^r) = \sum_{i,j} \eta_i \, \xi_{i,j}^r, \qquad |\xi_{i,j}| = p^{w_i/2}, \qquad \eta_i = \pm 1.$$

Este resultado se conoce como la *hipótesis de Riemann* para variedades sobre cuerpos finitos, dado que si tomamos $T = p^{-s}$ con $s \in \mathbb{C}$, entonces los ceros de $P_i(p^{-s})$ están todos situados en la recta vertical $\mathrm{Re}(s) = w_i/2$.

Notemos que $\xi_{i,j}$ es una raíz del polinomio $P_i^*(T) := T^{d_i} P_i(T^{-1})$, donde d_i es el grado de P_i. Este polinomio $P^*(T)$ es mónico con coeficientes enteros, con lo que $\xi_{i,j}$ es un entero algebraico. Decimos que $\xi \in \mathbb{C}$ es un *número de Weil de peso w* si es un entero algebraico tal que

$$|\xi^\sigma| = p^{w/2}$$

para todo conjugado de Galois ξ^σ de ξ. Por ejemplo, por un teorema de Kronecker, un número de Weil de peso cero es necesariamente una raíz de la unidad.

4. Polinomios de una variable

Volvamos al caso de polinomios de una variable. Sea $f \in \mathbb{Z}[x]$ un polinomio de grado n que, sin pérdida de generalidad, podemos suponer irreducible. Podemos describir la función $N(q)$ para la ecuación $f(x) = 0$ de la siguiente manera.

Dado un primo p que no divida al discriminante $\mathrm{disc}(f)$ de f, su factorización módulo p es de la forma

$$f(x) \equiv f_1(x) \cdots f_l(x) \bmod p,$$

con $f_i(x) \in \mathbb{F}_p[x]$ polinomios irreducibles distintos de grado, digamos, n_i. Podemos asumir que $n_1 \geq n_2 \geq \cdots \geq n_l$ y claramente $n = n_1 + \cdots + n_l$, con lo que $\tau_p := [n_1, n_2, \ldots, n_l]$ es una partición de n. Es un ejercicio sencillo verificar que la función zeta del polinomio f está dada por

$$Z(T) = \frac{1}{(1 - T^{n_1}) \cdots (1 - T^{n_l})}.$$

Es decir, que todos los $\xi_{i,j}$ correspondientes son números de Weil de peso cero.

Lo que querríamos describir es entonces la función $p \mapsto \tau_p$ para $p \notin S$, donde S es el conjunto de primos que dividen a $\mathrm{disc}(f)$. Notemos que este es precisamente el contexto de la ley de reciprocidad cuadrática formulada como en el teorema 1.1 cuando f es un polinomio de grado $n = 2$. En este caso, hay solo dos particiones posibles, $\tau_p = [1, 1]$ y $[2]$, lo que simplifica mucho las cosas. En general, el número de particiones $p(n)$ crece muy rápido con n.

Como insinuamos en la sección 2, entender cómo varía τ_p con p pasa a través del grupo de Galois G del polinomio f. Este grupo G actúa permutando las raíces de f, lo cual determina una inyección (no canónica) $\iota\colon G \longrightarrow S_n$ en el grupo de permutaciones de n elementos. La conexión con τ_p es la siguiente:

Teorema 4.1. *Para $p \notin S$, existe un elemento $\mathrm{Frob}_p \in G$ definido módulo conjugación tal que la descomposición en ciclos de $\iota(\mathrm{Frob}_p) \in S_n$ es τ_p.*

La clase de conjugación (bien definida) de Frob_p se llama la *clase de conjugación de Frobenius en p*. Una elección de Frob_p en esta clase se conoce a menudo, algo imprecisamente, como el *automorfismo de Frobenius en p*.

Si pensamos en S_n actuando en $\mathbb{C}^n$ en su representación natural, es decir, para $\sigma \in S_n$ hacemos que $\sigma e_i := e_{\sigma i}$, donde $e_1, \ldots, e_n$ es la base estándar de $\mathbb{C}^n$, entonces

$$\det(1 - \sigma T) = (1 - T^{n_1}) \cdots (1 - T^{n_l}),$$

donde $(n_1, \ldots, n_l)$ son las longitudes de la descomposición en ciclos de σ. Deducimos:

$$Z(T) = \det(1 - \mathrm{Frob}_p\, T)^{-1}. \tag{10}$$

Notemos que el lado derecho no depende de qué elemento Frob_p en su clase de conjugación elegimos. Ahora podemos ser precisos:

Teorema 4.2. *La particion τ_p para $p \notin S$ está unívocamente determinada por la clase de congruencia de p módulo un entero positivo m fijo si y solo si el grupo de Galois G es abeliano. En ese caso, tenemos un homomorfismo sobreyectivo $(\mathbb{Z}/m\mathbb{Z})^\times \to G$.*

Por ejemplo, para los polinomios f_N del ejemplo 1 de la sección 2, una forma más precisa de (3) consiste en decir que la partición τ_p es igual a $\tau_p = [d, \ldots, d]$, donde d es el orden de p en $(\mathbb{Z}/N\mathbb{Z})^\times/(\pm 1)$.

Sin entrar en gran detalle, el resultado clave es el teorema de Kronecker-Weber que dice que toda extensión abeliana de $\mathbb{Q}$ es una subextensión de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, donde ζ_m es una raíz primitiva m-ésima de la unidad para algún m. La recíproca, que toda subextensión de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ es abeliana, es también válida (y mucho más sencilla de demostrar). En efecto, el grupo de Galois de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ es precisamente $(\mathbb{Z}/m\mathbb{Z})^\times$, y todo cociente de un grupo abeliano es también abeliano.

Este resultado, parte de la gran teoría de cuerpos de clase de la teoría algebraica de números, nos da una nueva perspectiva sobre la reciprocidad cuadrática. Esperamos una descripción de $N(p)$, o lo que en este caso es lo mismo τ_p, en términos de congruencias gracias a que toda extensión cuadrática es de Galois con grupo de Galois cíclico (¡abeliano!) de orden dos.

En general, un polinomio al azar de grado n tiene típicamente grupo de Galois S_n, que no es abeliano si $n > 2$. Esto pasa con nuestro ejemplo 2 de la sección 2, es decir $f(x) = x^3 - x^2 + 1$, cuyo grupo de Galois es S_3. Aclaremos que la descripción concreta que dimos en (4), que va más allá de congruencias, tampoco se generaliza fácilmente; es específica a casos donde el grupo de Galois es diedral [12]. (En grado tres, el grupo de Galois es o bien cíclico o bien diedral.)

No existe entonces, en general, una descripción de τ_p en términos de congruencias. Pero la paridad de $\iota(\mathrm{Frob}_p) \in S_n$ sí tiene siempre tal descripción gracias a la reciprocidad cuadrática. Veamos esto en un caso concreto de grado cuatro. Sea $f = x^4 + x + 1$, de discriminante 229, con grupo de Galois S_4. Si $\theta_1, \ldots, \theta_4$ son las raíces de f en $\mathbb{C}$, su discriminante es $\mathrm{disc}(f) = \prod_{i<j}(\theta_i - \theta_j)^2$. Consideremos

$$\Delta := \prod_{i<j}(\theta_i - \theta_j).$$

Claramente, $\Delta^2 = \operatorname{disc}(f) = 229$, con lo que $F := \mathbb{Q}\left(\sqrt{229}\right)$ es un subcuerpo de $L = \mathbb{Q}(\theta_1, \ldots, \theta_4)$. Por otro lado, una permutación $\sigma \in S_4$ actúa en Δ como

$$\Delta^\sigma = \epsilon(\sigma)\Delta,$$

donde $\epsilon(\sigma)$ es el signo de σ. En términos de $\tau_p = [n_1, \ldots, n_l]$, tenemos $\epsilon(\sigma) = (-1)^{n-l}$.

De acuerdo con la reciprocidad cuadrática, para un primo $p \neq 229$ se tiene que

$$\epsilon(\mathrm{Frob}_p) = \chi(p),$$

donde $\chi(p) = \left(\frac{229}{p}\right)$ es el símbolo de Legendre módulo p. En otras palabras, Frob_p es una permutación par si y solo si p es un cuadrado módulo 229. Esto se puede ver claramente en la siguiente tabla con los primeros valores:

p	τ_p	$\chi(p)$	p	τ_p	$\chi(p)$	p	τ_p	$\chi(p)$
2	[4]	−1	13	[4]	−1	31	[4]	−1
3	[3, 1]	1	17	[3, 1]	1	37	[2, 2]	1
5	[3, 1]	1	19	[3, 1]	1	41	[4]	−1
7	[4]	−1	23	[2, 1, 1]	−1	43	[3, 1]	1
11	[3, 1]	1	29	[2, 1, 1]	−1	47	[2, 1, 1]	−1

5. Proyectiva y no singular

Si en el sistema de ecuaciones (2) todos los polinomios son homogéneos, el conjunto de soluciones $X(\mathbb{C})$ determina una variedad algebraica compacta del espacio proyectivo $\mathbb{P}^{n-1}(\mathbb{C})$. Si las derivadas parciales $\partial F_i/\partial x_j$ no tienen ceros en común, entonces $X(\mathbb{C})$ es no singular. Sea $d := \dim(X)$ la dimensión de $X(\mathbb{C})$. En este caso, la conjetura de Weil toma una forma más precisa:

Teorema 5.1. *Para primos p fuera de un conjunto finito, la función $Z(T)$ toma la forma*

$$Z(T) = \prod_{i=0}^{2d} P_i(T)^{(-1)^{i+1}},$$

donde $P_i(T)$ es un polinomio con coeficientes enteros de la forma

$$P_i(T) = \prod_{j=1}^{b_i}(1 - \xi_{i,j}T), \qquad |\xi_{i,j}| = p^{i/2},$$

y de grado $b_i := \dim H^i(X(\mathbb{C}), \mathbb{Q})$. En particular, para todo entero $r \geq 1$,

$$N(p^r) = \sum_{i=0}^{2d}(-1)^i \sum_{j=1}^{b_i} \xi_{i,j}^r. \tag{11}$$

Más aún, tenemos la ecuación funcional

$$Z(1/q^d T) = (-1)^\chi q^{\frac{1}{2}d\chi} Z(T), \qquad \chi := \sum_{i=0}^{d}(-1)^i b_i. \tag{12}$$

Los espacios vectoriales de cohomología $H^i(X(\mathbb{C}), \mathbb{Q})$ son invariantes geométricos de la variedad $X(\mathbb{C})$, cuyas dimensiones b_i, conocidas como los números de Betti de $X(\mathbb{C})$, miden en algún sentido su *forma*. El número χ es la característica de Euler (topológica) de $X(\mathbb{C})$, y la simetría (12) es un reflejo de la dualidad de Poincaré.

Por ejemplo, en el caso de curvas algebraicas ($d = 1$), el espacio $X(\mathbb{C})$ puede verse como una superficie de Riemann. Estas están caracterizadas por su número g (el *género*) de agujeros. Tenemos que

$$b_0 = 1, \qquad b_1 = 2g, \qquad b_2 = 1.$$

Como ilustración, una curva elíptica considerada como variedad algebraica es de dimensión $d = 1$ (una curva) y de género $g = 1$ (un solo agujero). Vemos efectivamente que la expresión (8) para $Z(T)$ que ya mencionamos es la que nos dan las conjeturas de Weil generales.

Todo esto muestra lo que decíamos en la introducción: el número de puntos $\#X(\mathbb{F}_q)$ está íntimamente ligado a la geometría de $X(\mathbb{C})$. Una manifestación importante de este principio es la cota superior para $N(p)$ que se deduce de (11). Por ejemplo, para una curva algebraica de genero g se tiene que

$$|N(q) - q - 1| \leq 2g\sqrt{q}. \tag{13}$$

Una forma de pensar en este resultado es que la diferencia entre el número de puntos $N(q)$ de una curva (proyectiva, no singular) sobre $\mathbb{F}_q$ y el de una recta $(q + 1)$ está acotada por el producto de una constante (que depende de su geometría) y $\sqrt{q}$.

Explicar en detalle cómo entran en la discusión los espacios $H^i(X(\mathbb{C}), \mathbb{Q})$ nos llevaría demasiado lejos. Damos en cambio una breve indicación. Evitando, como siempre, un número finito de primos, dado p tenemos para cada $0 \leq i \leq 2d$ un automorfismo de Frobenius Frob_p que actúa linealmente sobre un espacio vectorial $H^i(X)$ de dimensión b_i. Una primera complicación es que, por razones técnicas, este no es un espacio vectorial sobre $\mathbb{C}$ (esto no se podría obtener de forma natural), sino sobre un cuerpo l-ádico $\mathbb{Q}_l$ para un primo $l \neq p$ cualquiera. En todo caso, lo que sucede es que tenemos el análogo de (10), es decir,

$$P_i(T) = \det(1 - \mathrm{Frob}_p|_{H^i(X)}\, T)$$

independientemente de l. Desde este punto de vista, los $\xi_{i,j}$ son los valores propios del operador Frob_p^{-1} actuando sobre $H^i(X)$ y son números de Weil de peso i.

Consideremos el caso de una superficie cúbica X como en el ejemplo 3 de la sección 2. Los números de Betti de X son

$$b_0 = 1, \qquad b_1 = 0, \qquad b_2 = 7, \qquad b_3 = 0, \qquad b_4 = 1.$$

Como decíamos, una superficie cúbica contiene 27 rectas, uno de los resultados importantes de la Geometría Algebraica clásica. Cada una de estas rectas determina una clase de cohomología en $H^2(X, \mathbb{Q})$, y estas generan todo el espacio. Aunque, como supusimos, la ecuación cúbica que define X tenga coeficientes enteros, definir estas rectas típicamente requiere pasar a una extensión finita de $\mathbb{Q}$.

La acción del grupo de Galois correspondiente permuta las rectas y, en particular, Frob_p aparece como una permutación de las 27 rectas. Esta permutación induce, a su vez, una transformación lineal σ_p de $H^2(X, \mathbb{Q})$. Esta acción de Frob_p es en paralelo a la acción en el espacio l-ádico $H^2(X)$ que da la teoría general. Más precisamente, tenemos

$$P_2(T) = \det(1 - \mathrm{Frob}_p|_{H^2(X)}\, T) = \det(1 - \sigma_p p T). \tag{14}$$

Notemos que σ_p es de orden finito y, por lo tanto, sus valores propios son raíces de la unidad (números de Weil de peso cero), mientras que, por la teoría general, Frob_p^{-1} actuando sobre $H^2(X)$ tiene valores propios de peso dos. Esto es consistente con la igualdad (14), ya que si ζ es una raíz de la unidad, entonces ζp es un número de Weil de peso dos.

Este proceso en donde el peso cambia en dos y los valores propios se multiplican por p se conoce como el *torcimiento de Tate*. Es un fenómeno bastante común que una acción de Frob_p^{-1} de cierto peso w (en nuestro ejemplo, $w = 0$) aparezca en la cohomología $H^d(X)$ de una variedad X de dimensión $d > w$ (en nuestro ejemplo, $d = 2$) por medio de una iteración de tal torcimiento. Tendríamos $d = w+2k$ para un entero k, mientras que los valores propios se multiplican por p^k. Un caso interesante es el de una variedad cúbica no singular de dimensión tres $X \subseteq \mathbb{P}^4$. La acción de Frobenius en $H^3(X)$ proviene, a través de un torcimiento de Tate, de una acción de peso uno análoga a la del H^1 de una curva de genero cinco [1].

Volviendo a nuestra superficie cúbica X, la acción de Frob_p en los demás espacios $H^i(X)$ es más simple, y tenemos que $P_1(T) = P_3(T) = 1$ y

$$P_0(T) = 1 - T, \qquad P_4(T) = 1 - p^2 T.$$

Concluimos que

$$Z(T) = \frac{1}{(1-T)\det(1 - \sigma_p p T)(1 - p^2 T)}.$$

Si desarrollamos esta igualdad en series de potencias en T y observamos el coeficiente de T encontramos que

$$\#X(\mathbb{F}_p) = p^2 + \mathrm{tr}(\sigma_p)p + 1.$$

Es decir, $t_p = \mathrm{tr}(\sigma_p)$ es la traza de la transformación σ_p, en la notación de (5).

Como σ_p actúa en un espacio de dimensión 7 y sus valores propios son raíces de la unidad, deducimos que $|t_p| \leq 7$ como mencionamos. Pero podemos ser más precisos. El grupo de simetrías del conjunto de 27 rectas es isomorfo a $W(E_6)$, el grupo de Weyl de E_6 de orden 51840. Este grupo actúa naturalmente y de forma irreducible sobre un espacio V de dimensión 6 por medio de reflexiones. Los únicos valores posibles de la traza de un elemento de $W(E_6)$ en esta acción son $-3, -2, -1, 0, 1, 2, 3, 4, 6$. Bajo la acción de $W(E_6)$, el espacio $H^2(X(\mathbb{C}), \mathbb{Q})$ se descompone como $U \oplus V$, donde U es de dimensión uno y acción trivial. Sumando uno, la traza en U, a los valores precedentes, concluimos que t_p puede solo tomar los valores $-2, -1, 0, 1, 2, 3, 4, 5, 7$.

6. Formulación cohomológica

Intentamos en esta sección dar una idea básica, necesariamente superficial, de los ingredientes que entran en la formulación cohomológica de las conjeturas de Weil y que son la base de una estrategia para su demostración. Aquí, X es una variedad algebraica general.

Primero veamos más concretamente cómo pensar en el automorfismo de Frobenius Frob_p, que es la herramienta fundamental. Sea $X(\overline{\mathbb{F}}_p)$ el conjunto de soluciones del sistema polinomial X de ecuaciones (2) sobre una clausura algebraica $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$. Si $x = (x_1, \ldots, x_n) \in X(\overline{\mathbb{F}}_p)$ es una tal solución, como los coeficientes de cada F_i son enteros, resulta que $\mathrm{Frob}_p(x) := (x_1^p, \ldots, x_n^p)$ también lo es. Esta es la magia de los cuerpos finitos: la correspondencia $x \mapsto x^p$ es un automorfismo de cualquier cuerpo intermedio $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \overline{\mathbb{F}}_p$ que es la identidad sobre $\mathbb{F}_p$. Es decir, Frob_p es un elemento del grupo de Galois de la extensión $\mathbb{F}_q/\mathbb{F}_p$ y es, de hecho, un generador de este grupo cíclico.

La segunda observación es que podemos caracterizar en términos de Frob_p las soluciones $X(\mathbb{F}_q)$ del sistema X en un cuerpo $\mathbb{F}_q$ dado. En efecto, el cuerpo $\mathbb{F}_{p^r}$ es el cuerpo fijo por Frob_p^r. En general, tenemos

$$X(\mathbb{F}_{p^r}) = \{x \in X(\overline{\mathbb{F}}_p) \,:\, \mathrm{Frob}_p^r(x) = x\}.$$

En particular, $N(p^r) := \#X(\mathbb{F}_{p^r})$ es igual al número de puntos fijos de Frob_p^r actuando sobre $X(\overline{\mathbb{F}}_p)$.

Aquí es donde apelamos a la cohomología. Buscamos contar puntos fijos de Frob_p^r usando un análogo de la formula de Lefschetz en topología. Esta relaciona los puntos fijos de una función continua $\phi\colon U \longrightarrow U$ de un espacio topológico U apropiado con la traza de la función inducida ϕ_* en los grupos de homología $H_i(U, \mathbb{Q})$. Concretamente, el número relevante es el número de Lefschetz de ϕ, dado por

$$L(\phi) := \sum_{i \geq 0} (-1)^i \,\mathrm{tr}(\phi_*|_{H_i(U,\mathbb{Q})}). \tag{15}$$

Un caso muy simple, pero no trivial, de esta situación es la de un grupo finito G actuando por medio de permutaciones en un conjunto finito U. Esta acción da lugar a una representación lineal ρ de G en el espacio vectorial de funciones

$$F(U) := \{f\colon U \longrightarrow \mathbb{C}\}$$

de la forma natural:

$$\rho(g)(f)(u) := f(g^{-1}u), \qquad g \in G,\ f \in F(U),\ u \in U.$$

La traza de $\rho(g)$ es efectivamente el número de elementos de $F(U)$ fijados por $\rho(g)$. Para ver esto, basta tomar como base de $F(U)$ las funciones delta

$$\delta_u(v) = \begin{cases} 1 & \text{si } u = v, \\ 0 & \text{si } u \neq v, \end{cases} \qquad u, v \in U,$$

y notar que $\rho(g)\delta_u = \delta_u$ si y solo si $gu = u$. La matriz de $\rho(g)$ en esta base tendrá entonces un 1 en la diagonal si u es fijado por g y un 0 si no. Tenemos un caso en donde solo el término $i = 0$ contribuye a la suma (15) del número de Lefschetz.

En todo caso, para aplicar estas ideas se necesita una teoría cohomológica adecuada. Esta fue desarrollada en los años 60 por Grothendieck y sus colaboradores. Como dijimos en la sección 5, los grupos de cohomología a usar resultan ser espacios vectoriales sobre un cuerpo l-ádico, donde l es un primo fijo distinto de p. Grothendieck demostró que el número de Lefschetz $L(\mathrm{Frob}_p^r)$ en esta cohomología l-ádica es, como se espera, igual a $\#X(\mathbb{F}_{p^r})$.

Combinando este resultado con el desarrollo en serie de potencias

$$\det(1 - AT)^{-1} = \exp\left(\sum_{r\geq 1} \mathrm{tr}\,(A^r)\,\frac{T^r}{r}\right),$$

válida para cualquier transformación lineal A de un espacio vectorial de dimensión finita, obtenemos

$$Z(T) = \prod_{i=0}^{2d} P_i(T)^{(-1)^{i+1}},$$

donde $P_i(T) := \det(1 - \mathrm{Frob}_p\,|_{H^i(X)}T)$. Esto está muy cerca de la afirmación (9). El problema es que, a priori, solo podemos afirmar que $P_i(T)$ es un polinomio con coeficientes en $\mathbb{Q}_l$ y además podría depender de la elección de l. Aunque se espera que no haya tal dependencia de l y que los coeficientes estén en $\mathbb{Z} \subseteq \mathbb{Q}_l$, para una variedad X general esto todavía se desconoce. (Pero sí se conoce en el caso en que X es proyectiva y no singular, como indicamos en la sección 5.)

Completar la demostración de los teoremas 3.2 y 5.1, sobre todo en lo que respecta al peso de los valores propios de Frob_p, requiere ideas adicionales que fueron uno de los aportes cruciales de Deligne y exceden este breve resumen.

7. Conteo polinomial

Dado un sistema de ecuaciones (2), supongamos que para todo primo $p \notin S$ con S un conjunto finito vale lo siguiente:

$$\#X(\mathbb{F}_q) = a_0 + a_1 q + \cdots + a_m q^m, \qquad q = p^r, \quad r \geq 1, \tag{16}$$

donde $a_0, a_1, \ldots, a_m$ son números complejos independientes de p. Diremos en este caso que la correspondiente variedad X es de *conteo polinomial* y llamaremos $N(q)$ al polinomio $a_0 + a_1 q + \cdots + a_m q^m$, ahora con q como variable.

No es difícil comprobar que, necesariamente, $a_k \in \mathbb{Z}$. Si además, como en la sección 5, X es proyectiva y no singular, entonces como consecuencia de (11) obtenemos:

Teorema 7.1. *Si X es una variedad de conteo polinomial, proyectiva y no singular de dimensión d, entonces $b_i = 0$ si i es impar y*

$$b_{2k} = a_k, \qquad k = 0, \ldots, d,$$

donde $b_i := \dim H^i(X(\mathbb{C}), \mathbb{Q})$ *y* a_k *es como en* (16). *En particular,*

$$N(1) = \chi,$$

donde χ *es la característica de Euler de* $X(\mathbb{C})$ *y*

$$q^d N(1/q) = N(q),$$

o, equivalentemente,

$$a_k = a_{2d-k}, \qquad k = 0, \ldots, d. \tag{17}$$

Estos quizás sean los casos más contundentes de la relación entre la geometría compleja de $X(\mathbb{C})$ y el número de puntos de $X(\mathbb{F}_q)$. Un ejemplo típico de la situación es la variedad grassmaniana $X = G_{n,m}$ que parametriza subespacios vectoriales de dimensión m dentro de un espacio vectorial de dimensión n fijo. Es un lindo ejercicio calcular el número de tales subespacios sobre un cuerpo finito $\mathbb{F}_q$. Se obtiene que

$$\#G_{n,m}(\mathbb{F}_q) = \left[\begin{array}{c} n \\ m \end{array} \right] := \frac{(1-q)\cdots(1-q^n)}{(1-q)\cdots(1-q^m)(1-q)\cdots(1-q^{n-m})},$$

donde el lado derecho, que es en efecto un polinomio en q, representa la *versión* q del número binomial $\binom{n}{m}$. Muchas construcciones sobre $\mathbb{F}_q$ son análogas de otras más sencillas en las que se puede pensar como su límite cuando q tiende a 1. Se dice entonces que las primeras son la versión q de las segundas. En nuestro ejemplo, hay una analogía evidente con el hecho de que $\binom{n}{m}$ represente el número de subconjuntos de tamaño m dentro de un conjunto fijo de n elementos. Esto es típico y, de hecho, se especula que habría una teoría geométrica de variedades sobre un inexistente cuerpo con solo un elemento [13].

Por ejemplo, los números de Betti pares b_{2k} de $G_{5,2}$, una variedad de dimensión $6 = 2 \cdot (5-2)$, son los coeficientes del polinomio

$$\left[\begin{array}{c} 5 \\ 2 \end{array} \right] = q^6 + q^5 + 2q^4 + 2q^3 + 2q^2 + q + 1.$$

En general, podemos decir que si conocemos $N(q)$ con suficiente detalle, el teorema 3.2 mismo puede usarse para calcular los números de Betti de una variedad proyectiva no singular. Casos muy importantes de este proceso son, por ejemplo, [5, 4].

En la dirección contraria, saber que un polinomio dado, por ejemplo definido de forma puramente combinatoria, al evaluarlo en q es igual a $\#X(\mathbb{F}_q)$, con X proyectiva no singular, implica que sus coeficientes son enteros no negativos. En efecto, por el teorema 7.1 sus coeficientes son la dimensión de ciertos espacios vectoriales. Además, la dualidad de Poincaré (12) nos dice que el polinomio es palindrómico (17). Hay aquí también casos importantes donde esta estrategia dio frutos sorprendentes [2, 7]. En general, probar este tipo de resultados puede ser muy difícil.

Más aún, otro hecho muy importante de la geometría compleja, el teorema duro de Lefschetz, permite en algunos casos también deducir que los coeficientes de ciertos polinomios son unimodales. Es decir, crecen hasta un punto intermedio y luego decrecen [14].

¿Qué podemos decir si la variedad X no es proyectiva o es singular? Los coeficientes a_i son necesariamente enteros, pero ahora pueden ser negativos y no satisfacer la simetría $a_k = a_{d-k}$; la conexión con los espacios de cohomología es más complicada. En completa generalidad, en todo caso, el polinomio $N(q) = a_0 + a_1 q + \cdots + a_m q^m$ que da el número de puntos sigue teniendo un significado geométrico (es lo que se conoce como el polinomio E de X [8]). Pero, típicamente, este no alcanza para deducir los números de Betti de X.

En el caso de la variedad de matrices nilpotentes que consideramos en el ejemplo 4 de la sección 2, tenemos una variedad singular que tiene el mismo número de puntos sobre $\mathbb{F}_q$ que un espacio afín de su misma dimensión, mientras que es poco claro cuál es la relación geométrica entre ambos, si es que la hay. De todas formas, contar puntos sobre cuerpos finitos es una técnica poderosa para estudiar la geometría de espacios de interés [8, 6].

8. Programa de Langlands

El monumental programa de Langlands aritmético busca dar de forma precisa una respuesta a la segunda pregunta de nuestra introducción:

¿Se puede expresar $N(p)$ en términos de otras estructuras matemáticas?

La propuesta de Langlands es que estas estructuras son las formas automorfas. En vez de un fútil intento de describir qué son estas formas automorfas y cómo se relacionan con $N(p)$ en general, vamos a precisarlo en los ejemplos 5 y 6 de la sección 2.

El ejemplo 5 de la última entrada del *Tagebuch* de Gauss es, de hecho, un caso particular del ejemplo 6. En efecto, la curva afín de ecuación

$$C\colon \qquad x^2 + y^2 + x^2 y^2 = 1$$

es una curva elíptica menos algunos de sus puntos. Usando manipulaciones simples, se obtiene que C es birracional a la curva elíptica de ecuación

$$E\colon \qquad y^2 = x^3 + 4x.$$

Resulta que, si a_p es como en la notación del ejemplo 6 para la curva elíptica E, entonces $\#C(\mathbb{F}_p) = p - 3 - a_p$, en coherencia con la definición del ejemplo 5.

La curva elíptica E tiene una propiedad distintiva: tiene un automorfismo de orden cuatro dado por $(x, y) \mapsto (-x, iy)$. Es decir, que la curva satisface un caso particular de lo que se conoce clásicamente como *multiplicación compleja*. El grueso de las curvas elípticas no tienen multiplicación compleja. Resumiendo brutalmente la teoría, lo que obtenemos es que, para un primo $p \equiv 1$ mód 4, el automorfismo de Frobenius Frob_p actuando sobre $H^1(E)$ está representado por un elemento $\pi \in \mathbb{Z}[i]$. Este elemento satisface $\pi\bar{\pi} = p$ y $\pi + \bar{\pi} = a_p$.

Sabiendo solamente que $\pi \in \mathbb{Z}[i]$ satisface $\pi\bar{\pi} = p$ no alcanza para determinarlo, ni siquiera módulo conjugación, ya que cualquiera de las cuatro opciones $\pm\pi, \pm i\pi$ serviría igualmente. El descubrimiento de Gauss (6) nos dice que π varía de forma

coherente como función de $p \equiv 1$ mód 4. Una forma compacta de reescribir (6) es la siguiente:

$$\pi = u + iv \in \mathbb{Z}[i], \qquad \pi\bar{\pi} = p, \qquad \pi \equiv 1 \text{ mód } (1+i)^3.$$

Conviene ir más lejos y organizar esta definición directamente en términos de $\mathbb{Z}[i]$. Sea ϵ el carácter de $\mathbb{Z}[i]$ módulo $(1+i)^3$ con valores en $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$ tal que, para todo $\alpha \in \mathbb{Z}[i]$ coprimo con $1+i$, se tiene que $\epsilon(\alpha)\alpha \equiv 1$ mód $(1+i)^3$. Extendemos su definición poniendo $\epsilon(\alpha) := 0$ si α no es coprimo con $(1+i)$. Finalmente, definimos

$$\begin{array}{rccc} \psi\colon & \mathbb{Z}[i] & \longrightarrow & \mathbb{C} \\ & \alpha & \longmapsto & \epsilon(\alpha)\alpha \end{array}$$

y consideramos la serie generatriz

$$F(q) := \tfrac{1}{4} \sum_{\alpha \in \mathbb{Z}[i]} \psi(\alpha) q^{|\alpha|^2}. \tag{18}$$

La función ψ se conoce como un *Grössencharacter* o carácter de Hecke. En esta fórmula, $q = e^{2\pi i\tau}$ con $\mathrm{Im}(\tau) > 0$ es una variable y no debe confundirse con el orden de los cuerpos finitos de la sección 3.

En términos de F, todas las observaciones sobre el valor de a_p se resumen en lo siguiente:

a_p es igual al coeficiente de q^p en la serie $F(q)$.

Este hecho, debido a Hecke, ya es en sí mismo no trivial y está en el espíritu de la reciprocidad cuadrática expresada como en el teorema 1.1, pero su profundidad se manifiesta en la naturaleza de la serie $F(q)$. No se trata de una simple serie generatriz, sino que es una *forma modular*.

Hasta aquí hemos presentado el ejemplo 5 como un caso particular del ejemplo 6. En ambos casos, a_p es el coeficiente de q^p de una cierta forma modular asociada, lo que llamamos *modularidad*. Sin embargo, hay entre ambos ejemplos una diferencia fundamental debida a la existencia de multiplicación compleja en el caso considerado por Gauss.

Probar que la serie $F(q)$ definida en (18) es una forma modular del tipo esperado (de peso 2 y algún nivel N) es relativamente rutinario. La propiedad clave es que los exponentes de q están dados por $|\alpha|^2 = u^2 + v^2$ si $\alpha = u + iv$, que es una forma cuadrática positiva definida en las variables u y v. La demostración sigue la del caso básico de la función theta de Riemann

$$\theta(\tau) := \sum_{n \in \mathbb{Z}} e^{\pi i n^2 \tau}, \qquad \mathrm{Im}(\tau) > 0,$$

que satisface

$$\theta(-1/\tau) = \sqrt{-i\tau}\,\theta(\tau).$$

Este resultado clásico usa la fórmula de Poisson y depende, en última instancia, del hecho de que una distribución gaussiana normalizada apropiadamente es su propia transformada de Fourier.

Cuando la curva elíptica no tiene multiplicación compleja como en el ejemplo 6 (el caso típico), demostrar la modularidad de la correspondiente serie generatriz requiere técnicas *completamente* distintas y muy sofisticadas. Este fue el resultado del impresionante trabajo de Wiles y otros.

¿Qué podemos decir entonces en el caso general? Dicho mal y pronto, Langlands propone que $N(p)$ puede ser descrito en términos de una vasta generalización de las formas modulares asociadas a curvas elípticas. Aunque se ha hecho enorme progreso en esa dirección, estamos todavía lejos de tener un panorama completo.

9. La conjetura de Birch y Swinnerton-Dyer

Una curva elíptica E, además de ser una variedad algebraica, tiene de forma natural una estructura de grupo abeliano. Más precisamente, si fijamos un punto de E como la identidad, podemos a partir de dos puntos cualesquiera producir un tercero de forma algebraica. La operación resultante, que remonta al menos a Fermat, le da a los puntos de E la estructura de un grupo abeliano. Aquí, por puntos nos referimos a soluciones de las ecuaciones que definen la curva con coeficientes y coordenadas en un cuerpo fijo K cualquiera.

Si $K = \mathbb{C}$, el conjunto de los puntos $E(\mathbb{C})$ es topológicamente un toro complejo (una superficie de Riemann con solo un agujero). Alternativamente, podemos describir $E(\mathbb{C})$ como el cociente $\mathbb{C}/L$, donde $L \subseteq \mathbb{C}$ es un retículo (un subgrupo discreto isomorfo a $\mathbb{Z}^2$). Con esta descripción, la estructura de grupo de $E(\mathbb{C})$ es la visible heredada de sumar en $\mathbb{C}$.

Si $K = \mathbb{F}_p$, tenemos un grupo abeliano finito $E(\mathbb{F}_p)$ con una operación de suma dada de forma algebraica. Estos grupos son una fuente importantísima para todo tipo de aplicaciones prácticas, por ejemplo en criptografía.

Si, en cambio, $K = \mathbb{Q}$, describir $E(\mathbb{Q})$ es uno de los problemas centrales del análisis diofántico. Un teorema de Mordell nos dice que el grupo $E(\mathbb{Q})$ es finitamente generado, con lo que $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$ para un grupo finito T (la *torsión*) y un entero no negativo r (el *rango*). La torsión de curvas elípticas sobre $\mathbb{Q}$ se conoce bien gracias al trabajo de Mazur [9]. El rango, en cambio, es mucho más errático, y no se sabe por ejemplo cuán grande puede ser. Determinar el rango de una curva elíptica en la práctica es difícil.

En los años 60, Birch y Swinnerton-Dyer tuvieron la brillante idea de comparar el crecimiento de $N(p) := \#E(\mathbb{F}_p)$ a medida que p aumenta con el rango r. La intuición era que, cuanto más grande sea r, más rápido debería crecer $N(p)$ con p. De nuevo, esperamos que la variación de $N(p)$ con p nos aporte información sobre una pregunta global.

La forma concreta en la que Birch y Swinnerton-Dyer hicieron esta comparación fue la siguiente. Consideremos el producto normalizado

$$\pi(x) := \prod_{p \leq x} \frac{N(p)}{p}$$

(recordemos que la cota superior (13) nos dice que cada factor en el producto es a lo más de orden $1 + 2/\sqrt{p}$). Lo que los ejemplos numéricos parecían sugerir era que

$$\pi(x) \sim C \log^r(x), \qquad x \to \infty.$$

Eventualmente, esto dio lugar a la conjetura precisa BSD que propone que el rango de E es igual al orden del cero en $s = 1$ de una serie de Dirichlet $L(E, s)$ asociada. Esta serie, definida en términos de $N(p)$, converge originalmente solo para $\mathrm{Re}(s) > 3/2$. La modularidad implica que se extiende a todo el plano complejo y, por lo tanto, tiene sentido hablar de su comportamiento en $s = 1$.

Referencias

[1] E. Bombieri y H. P. F. Swinnerton-Dyer, On the local zeta function of a cubic threefold, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **21** (1967), 1–29.

[2] W. Crawley-Boevey y M. Van den Bergh, Absolutely indecomposable representations and Kac-Moody Lie algebras, con un apéndice de H. Nakajima, *Invent. Math.* **155** (2004), 537–559.

[3] B. Dwork, On the rationality of the zeta function of an algebraic variety, *Amer. J. Math.* **82** (1960), 631–648.

[4] L. Göttsche, The Betti numbers of the Hilbert scheme of points on a smooth projective surface, *Math. Ann.* **286** (1990), 193–207.

[5] G. Harder y M. S. Narasimhan, On the cohomology groups of moduli spaces of vector bundles over curves, *Math. Ann.* **212** (1974/75) 215–248.

[6] T. Hausel, E. Letellier y F. Rodríguez Villegas, Arithmetic harmonic analysis on character and quiver varieties, *Duke Math. J.* **160** (2011), no. 2, 323–400.

[7] T. Hausel, E. Letellier y F. Rodríguez Villegas, Positivity of Kac polynomials and DT-invariants of quivers, *Ann. of Math. (2)* **177** (2013), no. 3, 1147–1168.

[8] T. Hausel y F. Rodríguez Villegas, Mixed Hodge polynomials of character varieties, con un apéndice de N. Katz, *Invent. Math.* **174** (2008), 555–624.

[9] B. Mazur, Modular curves and the Eisenstein ideal, con un apéndice de B. Mazur y M. Rapoport, *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186 (1978).

[10] F. Rodríguez Villegas, *Experimental Number Theory*, Oxford Graduate Texts in Mathematics, 13, Oxford University Press, Oxford, 2007.

[11] J-P. Serre, *Lectures on* $N_X(p)$, Chapman & Hall/CRC Research Notes in Mathematics, 11, CRC Press, Boca Raton, FL, 2012.

[12] J-P. Serre, Modular forms of weight one and Galois representations, *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, 193–268, Academic Press, London, 1977.

[13] C. Soulé, Les variétés sur le corps à un élément, *Mosc. Math. J.* **4** (2004), 217–244.

[14] R. Stanley, Combinatorial applications of the hard Lefschetz theorem, *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, 447–453, PWN, Warsaw, 1984.

[15] A. Weil, Two lectures on number theory, past and present, *Enseign. Math.* **20** (1974), no. 2, 87–110.

Fernando Rodríguez Villegas, The Abdus Salam International Centre for Theoretical Physics, Strada Costiera 11, Trieste 34151, Italia

Correo electrónico: villegas@ictp.it

Página web: https://users.ictp.it/~villegas/