Función zeta de variedades algebraicas

por

José Miguel Echarri, Universidad del País Vasco-Euskal Herriko Unibertsitatea

1. Introducción

Los casos en los que los métodos analíticos proporcionan información acerca de cuestiones de naturaleza algebraica, son usualmente instancias del principio enunciado por Hecke:

"... el preciso conocimiento del comportamiento de una función analítica en una vecindad de sus puntos singulares es fuente de teoremas aritméticos".

Este principio continúa inspirando investigaciones y conjeturas hoy en día, ya que muchos problemas puramente algebraicos son abordados por métodos analíticos.

Uno de los más sorprendentes fenómenos en teoría de números es precisamente el hecho, de que un gran número de profundas propiedades aritméticas, de una amplia clase de objetos, están codificadas dentro de una simple función analítica, su función zeta. Por esta razón, la función zeta, como sus generalizaciones (las L-series) han acaparado un primer plano en la escena aritmética de hoy, y más que nunca, son el foco de investigaciones aritmético-teóricas.

Esta función tiene una forma simple, pero no está dispuesta a revelar sus mis-

terios. Sin embargo, cada vez, que intentamos desentrañar alguna de sus bien guardadas verdades, podemos esperar vernos recompensados por la revelación de algunas fascinantes y maravillosas relaciones, cargadas de significativos resultados. El prototipo fundamental de tales funciones es la *función zeta de Riemann.*

La *función zeta de Riemann clásica*, es la función de variable compleja,

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s},$$

definida para $\Re(s) > 1$ y que satisface la relación de Euler,

$$\zeta(s) = \prod_{p} (1 - p^{s})^{-1},$$

donde el producto se halla extendido a todos los primos. La identidad de Euler expresa, en una simple ecuación, la ley de factorización única en primos de los números naturales. Esto ya demuestra la importancia teórico-numérica de la función zeta.

Riemann demostró que ζ podía ser extendida a una función meromorfa en el plano complejo con un polo simple en $s = 1$ y que si

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

entonces ξ es una función entera que satisface la ecuación funcional $\xi(s) = \xi(1-s)$. Más aún, conjeturó que todos los ceros de ξ se hallaban sobre la línea $\Re(s) = \frac{1}{2}$.

Más tarde, Dedekind generaliza la función de Riemann a un cuerpo arbitrario de números $\mathbb{K}$ (extensión finita de $\mathbb{Q}$), por definir

$$\zeta_{\mathbb{K}}(s) = \sum_{\mathcal{I}} (N\mathcal{I})^{-s}$$

donde $\mathcal{I}$ recorre todos los ideales del anillo de enteros $\mathcal{A}$, del cuerpo numérico $\mathbb{K}$, y la norma $N\mathcal{I}$ es el número de elementos del anillo cociente $\mathcal{A}/\mathcal{I}$. Y obtuvo la relación de Euler,

$$\zeta_{\mathbb{K}}(s) = \prod_{\mathfrak{P}} (1 - N\mathfrak{P})^{-s})^{-1} \tag{2.1}$$

donde el producto se extiende a todos los ideales primos $\mathfrak{P}$ de $\mathcal{A}$ y muchos años después, Hecke demuestra que $\zeta_{\mathbb{K}}$ puede ser extendida a una función meromorfa

y satisface una ecuación funcional (mucho más complicada) generalizando a la de Riemann. Tenemos así, un análogo de la función zeta para cualquier cuerpo de números. La función zeta de Riemann (y las L-series de Dirichlet) están asociadas al cuerpo $\mathbb{Q}$.

Formalmente, la relación (2.1) sólo hace uso de dos propiedades del anillo $\mathcal{A}$:

(1) que es un anillo de Dedekind,

(2) que el cuerpo $\mathcal{A}/\mathfrak{P}$ es finito para todos los primos, siendo además la norma N una función completamente multiplicativa.

Estas ζ-funciones fueron el punto de arranque para la definición de la función zeta de una variedad algebraica y la formulación de las famosas *conjeturas de Weil* para variedades sobre cuerpos finitos, relativas al número de soluciones de ecuaciones polinómicas sobre dichos cuerpos. Sentó las bases de una nueva geometría algebraica en su lenguaje de esquemas y la cohomología étale (en particular de la cohomología l-ádica).

Después de 25 años de intenso trabajo por un grupo de eminentes matemáticos bajo la batuta de A. Grothendieck (en el Instituto de Estudios Científicos Superiores, IHES, en París), durante el cual resultados parciales fueron obtenidos, fué en 1973 cuando, P. Deligne encontró una prueba de la última conjetura de Weil, la llamada *hipótesis de Riemann-Weil para variedades sobre cuerpos finitos*. Una de las razones de la elegancia de las conjeturas de Weil es la intrigante conexión indirecta entre las propiedades topológicas y geométricas de la variedad (característica de Euler-Poincaré χ, ...) consideradas sobre los complejos y las propiedades teórico-numéricas (el número de puntos de la variedad) consideradas sobre un cuerpo finito.

La función zeta de una variedad algebraica y las conjeturas de Weil son uno de los más bellos ejemplos de unidad e imaginación en la historia de las matemáticas.

2. Variedades sobre cuerpos finitos

Como muchos problemas de teoría de números, la historia comienza con Gauss. En su trabajo sobre las leyes de reciprocidad, introduce las llamadas *sumas de Gauss* (siendo la más conocida

$$\sum_{x=0}^{p-1} \exp\left(\frac{2\pi i x^2}{p}\right), \text{con} \quad p \quad \text{primo}).$$

Para evaluar estas sumas, necesita conseguir (mediante métodos elementales) el número de soluciones en $\mathbb{F}_p$ de las congruencias,

$$ax^3 - by^3 \equiv 1, \quad ax^4 - by^4 \equiv 1, \quad y^2 \equiv ax^4 - b(\mathrm{mod}\, p).$$

Poco después, Jacobi invierte el proceso y usando propiedades elementales de las sumas de Gauss, trata de estimar el número de soluciones de cierto tipo de congruencias, donde los métodos elementales resultan engorrosos.

Cuando Hardy y Littlewood estudian el *problema de Waring*, se enfrentan al problema de estudiar el comportamiento asintótico del número de soluciones de la congruencia

$$x_1^k + \ldots + x_r^k = 0(\mathrm{mod}\, p)$$

y para este propósito, hicieron uso del *método de Jacobi*.

Más generalmente, en 1949, Hua-Vandiver y A. Weil simultáneamente, dieron el estimado $N = q^r + O\left(q^{\frac{r-1}{2}}\right)$ para el número de soluciones N de las ecuaciones

$$a_0 x_0^{k_0} + \ldots + a_r x_r^{k_r} = 0, \quad a_0 a_1 \ldots a_r \neq 0,$$

en cualquier cuerpo finito $\mathbb{F}_q$ con $q = p^f$ elementos. Resultados similares fueron obtenidos por Davenport (1931) y Mordell (1933) para la ecuación $y^m = P_n(x)$ en $\mathbb{F}_p$, donde $P_n(x)$ es un polinomio de grado n, estimando $N = p + O(p^{\phi(m,n)})$ con $\frac{1}{2} < \phi(m,n) < 1$.

En su tesis (1921), E. Artin observó que las congruencias algebraicas en dos variables módulo un primo p, podían ser interpretadas como ecuaciones algebraicas en el cuerpo primo $\mathbb{F}_p$ y que existía una notable analogía entre el anillo de polinomios $\mathbb{F}_p[X]$ y el anillo de enteros $\mathbb{Z}$.

Para explotar esta analogía, Artin consideró entonces el cuerpo finito $\mathbb{F}_q$ (extensión finita de $\mathbb{F}_p$) y trabajó con el anillo definido por la clausura entera, $\mathcal{A}$, del anillo $\mathbb{F}_q[X]$ en el cuerpo de descomposición del polinomio $Y^2 - f(X) \in \mathbb{F}_q[X,Y]$ (extensión cuadrática de $\mathbb{F}_q[X]$), donde $f(X) \in \mathbb{F}_q[X]$ y sin raices múltiples. Este anillo $\mathcal{A}$ es un *dominio de Dedekind*, es decir, todo ideal posee una factorización única en producto de ideales primos y todo ideal primo es maximal. Esta situación es completamente análoga al caso de cuerpo de números.

Esto le permite a Artin definir la ζ-función $\zeta_c(s)$ de la curva $c : Y^2 - f(X) = 0$ como sigue:

Definición Sea $c : Y^2 - f(X) = 0$, $f(X) \in \mathbb{F}_q[X]$. Entonces, la ζ-función de c es

$$\zeta_c(s) = \sum_{\mathcal{I}} (N\mathcal{I})^{-s}, \quad \Re(s) \gg 0$$

donde $N\mathcal{I}$ es la norma del ideal $\mathcal{I} \subset \mathcal{A}$, es decir la cardinalidad del anillo cociente $\mathcal{A}/\mathcal{I}$. De nuevo obtuvo una representación de $\zeta_c(s)$ como un producto

$$\zeta_c(s) = \prod_{\mathfrak{P}} (1 - N\mathfrak{P})^{-s})^{-1}, \quad \Re(s) \gg 0 \tag{2.2}$$

donde el producto está tomado en los ideales primos de $\mathcal{A}$, los cuales son maximales (por ser $\mathcal{A}$ anillo de Dedekind). Por lo tanto $\mathcal{A}/\mathfrak{P}$ es una extensión finita $\mathbb{F}_{q^\nu}$, de $\mathbb{F}_q$ y $N\mathfrak{P} = q^{deg(\mathfrak{P})}$ donde $deg(\mathfrak{P}) = \nu$ es el grado del punto cerrado x de c, correspondiente al primo $\mathfrak{P} \in Spec(\mathcal{A})$ (conjunto de ideales primos de $\mathcal{A}$).

Artin notó que la teoría de su ζ_c-función zeta era esencialmente más simple que para la $\zeta_{\mathbb{K}}$-función de Dedekind. Para su función, comprobó que podía ser escrita $\zeta_c(s) = Z(q^{-s})$, con $Z(T)$ una función racional con coeficientes en $\mathbb{Q}$, que la ecuación funcional para ζ_c, expresaba el cociente $Z((1/qT)/Z(T)$ como una función racional con ceros y polos conocidos y conjeturó que todos los ceros de $Z(T)$ se hallaban sobre el círculo $|T| = q^{\frac{1}{2}}$, verificando la conjetura para muchos polinomios $f(X)$ de bajo grado.

Ahora, los primos $\mathfrak{P}$ para los que $\mathcal{A}/\mathfrak{P}$ es isomorfo a $\mathbb{F}_q$ (es decir, $N\mathfrak{P} = q$), corresponden biyectivamente con los homomorfismos $\mathcal{A} \to \mathbb{F}_q$ y cualquiera de ellos envía $(x, y) \to (a, b) \in \mathbb{F}_q^2$, donde $b^2 = f(a)$, es decir, que el número de soluciones de la ecuación $Y^2 - f(X) = 0$ en $\mathbb{F}_q$ es exactamente el número N_1 de estos primos. Por oto lado de la relación (2.2) se sigue que

$$\log Z(T) = N_1 T + \ldots,$$

en un entorno de $T = 0$, de donde el conocimiento de $Z(T)$ implica el de N_1 y la hipótesis de Riemann implicaba que

$$|N_1 - q| \leq cq^{\frac{1}{2}}, \quad (N_1 = q + O(q^{\frac{1}{2}})),$$

coincidiendo sus resultados con los trabajos de congruencias de Gauss.

Para una variedad arbitraria no singular X sobre un cuerpo finito $\mathbb{F}_q$, $q = p^f$, Weil (1949) usó esta fórmula producto para definir la expresión de la ζ-función, $\zeta_X(s)$ de X. Ésta se define por:

Definición Para una variedad algebraica no singular $X/\mathbb{F}_q$,

$$\zeta_X(s) = \prod_{x\in|X|}(1-N(x)^{-s})^{-1} = \prod_{x\in|X|}\left(1-q^{-s.deg(x)}\right)^{-1}$$

donde el producto corre en los puntos cerrados $|X|$ de X, $N(x)$ denota el número de elementos del cuerpo residual $k(x)$ de X en x, y $deg(x) = [k(x) : \mathbb{F}_q]$. Haciendo $T = q^s$ y $Z(T) = Z(X/\mathbb{F}_q, T) = \zeta_X(s)$, no es difícil demostrar que

$$Z(T) = \exp\left(\sum_{\nu\geq 1}\frac{N_\nu}{\nu}T^\nu\right)$$

donde, $N_\nu = \sum_{deg(x)/\nu} deg(x)$, es el número de puntos de X con coordenadas $\mathbb{F}_{q^\nu}$, es decir, $X(\mathbb{F}_{q^\nu})$.

3. Conjeturas de Weil

Tenemos entonces el siguiente profundo teorema, primeramente conjeturado por Weil (probado por él mismo para curvas y variedades abelianas, y probado completamente por Deligne en 1974):

Teorema *Sea $X/\mathbb{F}_q$ una variedad proyectiva no-singular de dimension d. Entonces, se verifican las propiedades:*

1. Racionalidad de la función zeta: *la serie $Z(T)$ es una función racional de T, es decir, $Z(T) \in \mathbb{Q}(T)$,*
2. Ecuación Funcional: *existe un entero χ (llamado la característica de Euler de X), tal que $Z(1/(q^dT)) = \pm q^{d\chi/2}T^\chi Z(T)$, donde para $l \neq p$ es*

$$\chi = \sum_{i=0}^{2d}(-1)^i dim H^i(X_{et}, \mathbb{Q}_l),$$

3. Localización de ceros y polos: *la función racional $Z(T)$ factoriza*

$$Z(T) = \frac{P_1(T)P_3(T)\ldots P_{2d-1}(T)}{P_0(T)P_2(T)\ldots P_{2d}(T)},$$

donde para todo i, $P_i(T) \in Z(T)$, $P_0(T) = 1-T$, $P_{2d} = 1-q^dT$, y para los otros i, $P_i = \prod_j(1-\omega_{ij}T)$, con $|\omega_{ij}| = q^{i/2}$.

La primera afirmación fué probada por B. Dwork unos años antes que Deligne, haciendo uso de técnicas elementales de análisis p-ádico y tiene profundas implicaciones prácticas para resolver sistemas de ecuaciones polinómicas sobre cuerpos finitos. Viene a decir que existen un conjunto finito de números complejos $\alpha_1, \ldots, \alpha_t$, $\beta_1, \ldots, \beta_u$ tal que para todo $\nu = 1, 2, \ldots$, se tiene que $N_\nu = \sum_1^t \alpha_t - \sum_1^u \beta_i$.

En otras palabras, una vez que determinamos los α_i, β_i con un número finito de los N_ν, se tiene una simple fórmula para predecir el resto de los N_ν.

Los espacios de cohomología considerados en el segundo párrafo son los étales, sobre el cuerpo l-ádico $\mathbb{Q}_l$, donde l es un primo diferente a la característica p de la variedad X. Grothendieck fue capaz de generalizar en una forma muy original, los conceptos de topología y de haz, para asociar a cada variedad X un grupo de cohomología étale $H^i(X_{et}, \mathbb{Q}_l)$ con coeficientes en $\mathbb{Q}_l$.

Pero, la parte más dura del teorema corresponde a la última afirmación, que dice que $|\omega_{ij}| = q^{\frac{i}{2}}$. Ésta es la llamada *hipótesis de Riemann* para variedades sobre cuerpos finitos. Haciendo $\zeta(s) = Z(q^{-s})$, la relación $|\omega_{ij}| = q^{\frac{i}{2}}$ es equivalente a la afirmación $\Re(s_{ij}) = \frac{1}{2}$ ($q^{-s_{ij}} = \frac{1}{\omega_{ij}}$), es decir que los ceros de $\zeta(s)$ se hallan sobre la línea $\Re(s) = \frac{1}{2}$, tomando una forma similar a la conjetura de los ceros de la función zeta, lo cual explica el nombre de conjetura de Riemann.

Notar que si el teorema es cierto para hipersuperficies proyectivas implica su validez para variedades proyectivas, como consecuencia de las simples relaciones:

$$N_\nu = N_\nu^* + N_\nu^{**} \Longrightarrow Z(T) = Z(T)^* Z(T)^{**}$$

$$N_\nu = N_\nu^* - N_\nu^{**} \Longrightarrow Z(T) = Z(T)^* / Z(T)^{**}$$

$$N_\nu(f, g) = N_\nu(f) + N_\nu(g) - N_\nu(fg)$$

donde $N_\nu(f, g, \ldots)$ designa el número de soluciones del sistema de ecuaciones $\{f = 0, g = 0, \ldots\}$ en el cuerpo finito $\mathbb{F}_{q^\nu}$.

Finalmente, si los coeficientes de las ecuaciones que definen a X fueran la clase mod p de enteros, (coeficientes de ecuaciones de una variedad no singular X_0 en $\overline{\mathbb{Q}^r}$) el grado de cada P_i sería el i-ésimo número de Betti de la variedad X_0.

Estas conjeturas sugieren una profunda conexión entre la aritmética de las variedades algebraicas definidas sobre cuerpos finitos y la topología de variedades

algebraicas definidas sobre los números complejos. Weil apuntó, que si se tuviese una adecuada teoría de cohomología para variedades abstractas, análoga a la cohomología ordinaria de variedades definidas sobre los complejos, entonces se podrían deducir sus conjeturas desde varias propiedades estandard de la teoría de cohomología.

Esta observación ha sido una de las principales motivaciones para introducir varias teorías de cohomología en geometría algebraica. En 1963, A. Grothendieck fué capaz de mostrar que su cohomología l-ádica tenía suficientes propiedades que implicaban parte de las conjeturas de Weil (la racionalidad de la función zeta), pero fué Deligne quien demostró el resto de las conjeturas (especificamente el análogo a la hipótesis de Riemann, considerada como la culminación del estudio de la cohomología l-ádica, comenzada por A. Grothendieck, M. Artin y otros).

Pero, ¿cómo conecta esta hipótesis para variedades con el problema inicial de Gauss y con las cotas para el número de soluciones de congruencias sobre cuerpos finitos?.

Pues muy sencillo, el teorema de Deligne (hipótesis de Riemann) implica, mediante un fácil cálculo, que el número de puntos de grado uno, N_1, (es decir, $X(\mathbb{F}_q)$) de una variedad proyectiva no singular de dimensión d sobre $\mathbb{F}_q$ tiene el estimado $|N_1 - (1+q+\ldots+q^d)| \leq bq^{\frac{d}{2}}$, donde la constante b puede ser computada explícitamente, esta es el d-ésimo número de Betti de la variedad sobre los complejos que tiene el mismo grado que X. Este estimado coincide o mejora los trabajos desde Gauss a Artin.

4. La función zeta global de una variedad

Sea $X/\mathbb{K}$ una variedad (proyectiva y no-singular) de dimension d, definida por ecuaciones con coeficientes en $\mathbb{K}$, un cuerpo numérico (extensión finita de $\mathbb{Q}$). Después de eliminar denominadores, podemos asumir que nuestra variedad tiene coeficientes en $\mathcal{A}$ (el anillo de enteros de $\mathbb{K}$). Para todo primo $\mathfrak{P}$, consideremos la variedad $X(\mathfrak{P})/\mathbb{F}_q$ obtenida por reducir los coeficientes módulo $\mathfrak{P}$, siendo $q = N\mathfrak{P}$, la cardinalidad de $\mathcal{A}/\mathfrak{P}$ (puede ocurrir que la variedad obtenida sea singular, lo cual ocurre para un número finito de $\mathfrak{P}$).

Para todo $\nu \geq 1$, sea $N_\nu(\mathfrak{P})$ el número de puntos de $X(\mathfrak{P})$ definida sobre el

cuerpo finito $\mathbb{F}_{q^\nu}$ y consideremos la serie formal de potencias, en la variable T:

$$Z_{\mathfrak{P}}(T) = \exp\left(\sum_{\nu \geq 1} \frac{N_\nu(\mathfrak{P})}{\nu} T^\nu\right).$$

Ahora, con todas las $Z_{\mathfrak{P}}(T)$ locales podemos formar la función zeta global de variable compleja s (con $\Re(s) \gg 0$, es decir, suficientemente grande) por

$$\zeta(X, s) = \prod_{\mathfrak{P}} Z_{\mathfrak{P}}(q^{-s})$$

donde el producto se halla extendido sobre los primos $\mathfrak{P}$ de $\mathcal{A}$, donde X posee buena reducción, es decir donde $X(\mathfrak{P})$ es no-singular (que X no posea buena reducción sólo en un número finito de primos, es un resultado clave).

De esta forma, la función zeta global codifica gran cantidad de información aritmética.

Muy poco se conoce de la función zeta general. Se cree (¿se puede conjeturar cuando sólo unos pocos casos han sido corroborados?) que puede ser extendida analíticamente a una función meromorfa con una ecuación funcional (siempre que los factores locales, en donde la variedad posea mala reducción, sean definidos en una forma alternativa) y satisface la hipótesis de Riemann, es decir aparte de los ceros triviales, todos los demás ceros y polos están en una cierta linea vertical en el plano complejo.

Notar que se puede recuperar la clásica función zeta de Riemann, considerando X el punto 0 y en forma general, se puede recobrar la función zeta de Dedekind de un campo numérico $\mathbb{K}$, por tomar para X la variedad 0-dimensional, definida en la línea proyectiva por $P = 0$, donde P es el polinomio mónico con coeficientes enteros definiendo el cuerpo sobre $\mathbb{Q}$.

Bibliografía

[H] W.J.W. Hulsbergen, *Conjectures in Arithmetic Algebraic Geometry. A Survey*, Aspects of Mathematics, vol. 18, 1992.

[K1] N. Koblitz, *p-adic numbers, p-adic Analysis and zeta-functions*, Graduate Texts in mathematics. Springer-Verlag, vol. 58, 1977.

[K2] N. Koblitz, *Introduction to Elliptic curves and Modular Forms*, Graduate Texts in Mathematics, Springer-Verlag, vol. 97, 1984.

[N] J. Neukirch, *Algebraic Number Theory*, A series of comprehensive studies in Mathematics, Springer-Verlag, vol. 322, 1999.

[W] M. Waldschmidt, *From Number theory to Physics*, Springer-Verlag, 1992.