Resumen de la demostración de Deligne de la hipótesis de Riemann para variedades sobre cuerpos finitos

Nicholas M. Katz

Tabla de Contenidos

1. Introducción a las congruencias. El problema fundamental en teoría de números es, sin duda, el de resolver ecuaciones con números enteros. Como este problema está todavía fuera del alcance, nos contentaremos con el problema de resolver congruencias polinómicas módulo p. La idea de considerar congruencias surge naturalmente al intentar probar que una ecuación dada no tiene soluciones enteras. Por ejemplo, la ecuación

$$y^2 = x^3 - x - 1$$

no puede tener soluciones enteras, porque la correspondiente congruencia módulo *tres* no tiene soluciones enteras módulo tres (el miembro izquierdo es 0 o 1 mód. 3, y el derecho es -1 mód. 3).

Ahora bien, cuando consideramos una congruencia módulo p,

$$f(x_1, \ldots, x_n) \equiv 0 \qquad \text{mód } p$$

lo más natural es buscar soluciones no sólo en el cuerpo primo $\mathbb{F}_p$, sino también en todas sus extensiones finitas $\mathbb{F}_{p^n}$. Si identificamos entre sí las soluciones que sean *conjugadas* sobre $\mathbb{F}_p$, llegamos a la noción de "divisor primo" $\mathcal{Y}$ (ideal maximal de $\mathbb{F}_p[x_1, \ldots, x_n]/(f)$). La *norma* de un tal divisor primo, denotada por $N\mathcal{Y}$, es el cardinal de su cuerpo residual. Por tanto, $N\mathcal{Y} = p^{\deg \mathcal{Y}}$, donde $\deg \mathcal{Y}$ es el número de soluciones cojugadas que "hay" en $\mathcal{Y}$.

2. La Función Zeta. Teniendo presente el parecido con la función zeta de Riemann, introducimos como E. Artin [2] el producto infinito

$$\prod_{\mathcal{Y}} \frac{1}{1 - N\mathcal{Y}^{-s}} \qquad \text{convergente para } \mathrm{Re}(s) \gg 0.$$

Si hacemos el cambio de variable $T = p^{-s}$, obtenemos

$$\prod_{\mathcal{Y}} \frac{1}{1 - T^{\deg \mathcal{Y}}}$$

cuyo *logaritmo* se calcula fácilmente y vale

$$\sum_{n \geq 1} \frac{T^n}{n} N_n,$$

donde

$$N_n = \text{el número de soluciones con coordenadas en } \mathbb{F}_{p^n}.$$

Así, para cualquier variedad algebraica X sobre un cuerpo finito $\mathbb{F}_q$ (q es *potencia* de p), introducimos su función zeta

$$Z(X/\mathbb{F}_q, T) \coloneqq \exp\left(\sum \frac{T^n}{n} N_n\right); \qquad N_b = \#X(\mathbb{F}_{q^n})$$

$$= \prod_{\mathcal{Y}} \frac{1}{1 - T^{\deg \mathcal{Y}}}$$

$$= \prod_{\mathcal{Y}} \frac{1}{1 - N\mathcal{Y}^{-s}} \qquad T = q^{-s}$$

como una serie formal en T con coeficientes en $\mathbb{Z}$. Contiene toda la información diofantina que ofrece X.

Calculemos un ejemplo sencillo. Sea $X = \mathbb{A}^r$, el espacio afín r-dimensional sobre $\mathbb{F}_q$, cuyos puntos con valores en $\mathbb{F}_{q^n}$ son simplemente las r-tuplas de elementos de $\mathbb{F}_{q^n}$. Hay q^{rn} tales r-tuplas, por lo que

$$N_n = q^{rn}$$

$$Z(\mathbb{A}^r/\mathbb{F}_q, T) = \exp\left(\sum \frac{T^n}{n} q^{rn}\right) = \frac{1}{1 - q^r T}$$

De hecho, E. Artin (1924) había introducido la función zeta sólo para cuerpos de funciones de *curvas* sobre cuerpos fintios, como un análogo de la función zeta de Dedekind de un cuerpo de números algebraicos cualquiera, respecto de la variable s

$$\zeta(s) = \prod_{\mathcal{Y}} \frac{1}{1 - N\mathcal{Y}^{-s}} = \sum_{\mathcal{D}} N\mathcal{D}^{-s}$$

donde la última suma se extiende sobre todos los "divisores efectivos" del cuerpo de funciones. Fue sólo siete años más tarde (1931) que F. K. Schmidt [40] mostró que el teorema de Riemann-Roch en la propia curva podía usarse para establecer que, para una curva $X/\mathbb{F}_q$ de género g, su función zeta es una función *racional* de $T = q^{-s}$ que tiene la forma precisa

$$\zeta(s) = \frac{P(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})} = \frac{P(T)}{(1 - T)(1 - qT)}$$

donde $P(T) = \prod_{i=1}^{2g}(1 - \alpha_i T)$ es un polinomio de grado $2g$ con coeficientes enteros, cuyas raíces admiten la permutación $\alpha \mapsto q/\alpha$. En términos de la variable compleja s, esto da una ecuación funcional bajo $s \mapsto 1 - s$. La "Hipótesis de Riemann", formulada por primera vez en E. Artin [2], afirma que los ceros de esta función zeta $\zeta(s)$ yacen todos en la recta $\mathrm{Re}(s) = 1/2$, o equivalentemente que

$$|\alpha_i| = \sqrt{q}$$

Si tomamos logaritmos en ambos miembros de la igualdad

$$\exp\left(\sum \frac{N_n}{n} T^n\right) = \frac{\prod_{i=1}^{2g}(1 - \alpha_i T)}{(1 - T)(1 - qT)}$$

obtenemos

$$N_n = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n$$

la expresión de la distribución de primos en términos de los ceros de la función zeta. La Hipótesis de Riemann se vuelve equivalente al enunciado diofantino

$$|N_n - 1 - q^n| \leq 2g\sqrt{q^n}$$

equivalencia señalada por primera vez en Hasse [23].

El primer caso particular de la Hipótesis de Riemann había sido mostrado por Gauss, para la curva elíptica lemniscática $y^2 = x^4 - 1$ sobre cualquier $\mathbb{F}_p$. E. Artin ([2]) verificó algunos casos particulares más, y en 1933 Hasse fue capaz de probarla para curvas elípticas cualesquiera.

Hasse (1933 y 1934) dio dos demostraciones muy diferentes. La primera [22] se basaba en la teoría de la multiplicación compleja, y consistía en levantar la curva elíptica con su endomorfismo de Frobenius a característica cero. Su segunda demostración ([24], [25]) era explícitamente geométrica, basada en un estudio directo del anillo de endomorfismos de la curva elíptica. Hasse y Deuring señalaron ([14bis], [26]) la importancia de la teoría de correspondencias para el caso de curvas de género mayor que uno.

Weil (1940 y 1941) esbozó entonces dos demostraciones diferentes de la Hipótesis de Riemann para una curva de género cualquiera g sobre un cuerpo finito. La primera ([51]) atacaba el problema usando los puntos de orden finito primo con p de la Jacobiana de la curva como una especie de primer grupo de homología de la curva. Siguiendo a Hurwitz, interpretó una correspondencia de la curva consigo misma como un endomorfismo de la Jacobiana, lo que le permitió asociarle una matriz ℓ-ádica $2g \times 2g$ a la correspondencia. Entonces dedujo la Hipótesis de Riemann de la positividad de la "involución de Rosatti"(cf., [38], [61]). La segunda demostración [52], que prescindía de la teoría "transcendente" de Hurwitz (i. e., con matrices ℓ-ádicas y la Jacobiana), estaba basada completamente en la teoría de Severi de las correspondencias de la curva consigo misma. La función zeta se expresaba fácilmente en términos de números de intersección de correspondencias. En términos de estos números de intersección, Weil definió una "función traza" en el anillo de todas las (clases de equivalencia adecuadas de) correspondencias. Entonces, la Hipótesis de Riemann se seguía de una propiedad de positividad de esta traza (desigualdad de Castelnuovo, cf., [61], [37]). En el caso de una curva de género *uno*, esta demostración se reduce esencialmente a la demostración geométrica de Hasse.

Aunque este formalismo de correspondencias y los enunciados de positividad en los que Weil basó sus demostraciones eran "bien conocidos"por los geómetras algebraicos italianos y sus análogos complejos estaban rigurosamente demostrados con métodos trascendentes (cf., [61], pp. 552-5), la falta de fundamentos adecuados para la geometría algebraica abstracta (en el sentido de [61]) llevaron a Weil a escribir sus *Fundamentos de Geometría Algebraica* [53]. Hecho esto, dio tratamientos completos de sus dos demostraciones, la

segunda en *Sobre las curvas algebraicas y las variedades deducidas de ellas* [54] y la primera, generalizada a variedades abelianas cualesquiera, en *Variedades abelianas y curvas algebraicas* [55].

3. Las conjeturas de Weil. Entonces, en 1949, Weil conjeturó lo que debería ser cierto para variedades de dimensión superior [57]. Sea X una variedad proyectiva no singular n-dimensional sobre $\mathbb{F}_q$. Entonces

1. $Z(X/\mathbb{F}_q, T)$ es una función *racional* de T
2. Además, $Z(X/\mathbb{F}_q, T) = \dfrac{P_1(T)P_3(T)\dots P_{2n-1}(T)}{P_0(T)P_2(T)\dots P_{2n}(T)}$, donde $P_i(T) = \prod_{j=1}^{b_i}(1-\alpha_{ij}T)$ y $|\alpha_{ij}| = \sqrt{q}^i$, siendo la última igualdad la "Hipótesis de Riemann" en esta situación.
3. Bajo $\alpha \mapsto q^n/\alpha$, las $\alpha_{i,j}$ se corresponden biyectivamente con las $\alpha_{2n-i,j}$. En términos de la variable compleja s, esto es una ecuación funcional para $s \mapsto n - s$.
4. En caso de que X sea la "reducción módulo p"de una variedad proyectiva no singular $\mathcal{X}$ en característica cero, entonces b_i es el i-ésimo número de Betti topológico de $\mathcal{X}$ como variedad compleja.

La *moraleja* es que la topología de los puntos complejos de $\mathcal{X}$, expresada a través de los grupos de cohomología clásicos $H^i(\mathcal{X}, \mathbb{C})$, determina la forma de la función zeta de X, i. e., determina la forma diofantina de X. Hay un argumento heurístico para esto, como sigue (cf. [61]). Entre todos los elementos del cierre algebraico de $\mathbb{F}_p$, los elementos de $\mathbb{F}_q$ se distinguen por ser los puntos fijos del morphismo de Frobenius $x \mapsto x^q$. Con mayor generalidad, si $\mathbf{x} = (\dots, x_i, \dots)$ es una solución de algunas ecuaciones que están definidas sobre $\mathbb{F}_q$, la $F(\mathbf{x}) \coloneqq (\dots, x_i^q, \dots)$ será también una solución de las *mismas* ecuaciones, y el punto $\mathbf{x}$ tendrá coordenadas en $\mathbb{F}_q$ precisamente cuando $F(\mathbf{x}) = \mathbf{x}$. Por tanto F es un endomorfismo de nuestra variedad X sobre $\mathbb{F}_q$, y

$$N_n = \#\text{Fijos}(F^n);$$
$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum \frac{T^n}{n}\#\text{Fijos}(F^n)\right)$$

Supongamos que se considera entonces una variedad compacta compleja $\mathcal{X}$, y un endomorfismo F de $\mathcal{X}$ con puntos fijos razonables. Entonces la fórmula de los puntos fijos de Lefschetz nos daría

$$\#\text{Fijos}(F^n) = \sum(-1)^i \text{ traza}(F^n|H^i(\mathcal{X}, \mathbb{C})),$$

que es formalmente equivalente a la identidad

$$\exp\left(\sum \frac{T^n}{n}\#\text{Fijos}(F^n)\right) = \prod_{i=0}^{2n} \det\left(\text{Id} - TF|H^i(\mathcal{X}, \mathbb{C})\right)^{(-1)^{i+1}}$$

La búsquedad de una "teoría de cohomología para variedades sobre cuerpos finitos" que pudiera justificar este argumento heurístico ha sido responsable, directa e indirectamente, de buena parte del progreso tremendo hecho en geometría algebraica estos últimos

veinticinco años. Las demostraciones de Weil de la Hipótesis de Riemann para curvas sobre cuerpos finitos ya había necesitado sus *Fundamentos*. Durante la misma época, Zariski también había empezado a enfatizar la necesidad de una geometría algebraica abstracta; su desencanto con la falta de rigor en la escuela italiana había llegado tras escribir su famosa monografía *Superficies Algebraicas* [63], que daba el "estado de la cuestión" en 1934 (cf., [64]). La posibilidad de trasponer a variedades algebraicas abstractas con su "topología de Zariski" los potentes métodos topológicos y de teoría de haces que habían sido desarrollados por Picard, Lefschetz, Hodge, Kodaira, Leray, Cartan, ... tratando con variedades complejas estaba implícita en las notas de Weil de 1949 "*Fibrados en Geometría Algebraica*"[58]. La trasposición fue llevada a cabo por Serre en su famoso artículo "Haces Algebraicos Coherentes"[41]. Desde el punto de vista de las conjeturas de Weil, sin embargo, esta teoría era todavía inadecuada, pues al aplicarla a variedades en característica p daba grupos de cohomología que eran espacios vectoriales en característica p, así que sólo daban fórmulas de trazas "mód. p", es decir, sólo podían dar congruencias "mód. p"para números de puntos racionales.

4. Cohomología ℓ-ádica. Tras varias salidas en falso (como la cohomología de vectores de Witt de Serre [42], [43]) y la demostración "fuera de guion"(por no ser aparentemente cohomológica) de Dwork [16] de la conjetura de racionalidad (1) para *cualquier* variedad sobre $\mathbb{F}_q$, M. Artin y A. Grothendieck desarrollaron una teoría "buena" de cohomología [3], basada en la noción de revestimiento étale y que generalizaba las matrices ℓ-ádicas de Weil. De hecho, desarrollaron un *montón* de teorías, una para cada número primo $\ell \neq p$, cuyo cuerpo de coeficientes es el cuerpo $\mathbb{Q}_\ell$ de números ℓ-ádicos. *Cada* teoría daba una factorización de zeta

$$Z(T) = \prod_{i=0}^{2n} P_{i,\ell}(T)^{(-1)^{i+1}}$$

en un producto alternado de polinomios $\mathbb{Q}_\ell$-ádicos, satisfaciendo la conjetura (3). En el caso en que X pudiera levantarse a $\mathcal{X}$ en característica cero, probaron que $P_{i,\ell}$ era un polinomio de grado $b_i(\mathcal{X})$. *No* probaron qe los $P_{i,\ell}$ de hecho tenían coeficientes en $\mathbb{Q}$, ni a fortiori que los $P_{i,\ell}$ eran independientes de ℓ. Esto significaba que en la factorización de un $P_{i,\ell}$ individual

$$P_{i,\ell}(T) = \prod_{j=1}^{b_i}(1 - \alpha_{i,j,\ell}T)$$

las raíces $\alpha_{i,j,\ell}$ sólo eran algebraicas sobre $\mathbb{Q}_\ell$, pero posiblemente *no* algebraicas sobre $\mathbb{Q}$, por lo que podrían no *tener* siquiera valores absolutos arquimedianos. (Por supuesto, por un teorema de Fatou, los ceros y polos recíptocos de la función racional $Z(T)$ son enteros algebraicos, el problema es que podría haber *cancelaciones* entre los diversos $P_{i,\ell}$ en la factorización ℓ-ádica de zeta.)

Así que la cuestión pasó a ser cómo introducir consideraciones *arquimedianas* en la teoría ℓ-ádica. Incluso antes de que se desarrollara la teoría ℓ-ádica, Serre (1960), siguiendo una sugerencia de Weil ([61], p. 556), había formulado y probado un análogo Kahleriano

de las conjeturas de Weil, haciendo uso esencial del teorema del Índice de Hodge. En parte inspirado por esto, y en parte inspirado por su propia observación (1958) de que la desigualdad de Castelnuovo usada por Weil era una consecuencia del teorema del Índice de Hodge en una superficie ([20], [37]), Grothendieck a principios de los sesenta formuló varias conjeturas muy díficiles de positiviad y existencia sobre ciclos algebraicos, las llamadas "conjeturas estándar"(cf. [15], [31]) cuya demostración implicaría tanto la independencia de ℓ como la Hipótesis de Riemann.

Para sorpresa de casi todo el mundo cuando Deligne probó sus teoremas, Deligne consiguió *evitar* estas conjeturas por completo, excepto para *deducir* una de ellas, el teorema de Lefschetz "difícil" que da la existencia de la "descomposición primitiva" de la cohomología de una variedad proyectiva no singular, un resultado conocido anteriormente sólo sobre $\mathbb{C}$, y ahí por la teoría de Hodge de integrales armónicas. Las demás "conjeturas estándar" continúan abiertas. De hecho, el dogma generalmente aceptado de que la Hipótesis de Riemann no podía demostrarse sin estas conjeturas (cf. [15], I, p. 224 por ejemplo) probablemente tuvo el efecto de retrasar por unos años la demostración de la Hipótesis de Riemann.

Es bastante chocante notar que en la deducción de Deligne del teorema de Lefschetz difícil a partir de la Hipótesis de Riemann para variedades sobre cuerpos finitos, hace uso esencial de un resultado célebre de análisis clásico, el método de Hadamard-de la Vallée Poussin de probar que la función zeta de Riemann usual no tiene ceros en la recta $\mathrm{Re}(s) = 1$. Fue conducido a este método al estudiar la prueba de Yoshida [62] del análogo para cuerpos de funciones de la conjetura de Sato-Tate sobre la distribución de los *ángulos* de los autovalores de Frobenius en *familias* de curvas elípticas. Yoshida necesitaba probar que cierta función L no tenía ceros en la recta $\mathrm{Re}(s) = 1$, y lo hizo usando algunas estimaciones potentes de Selberg. Deligne se dio cuenta de que los resultados de Selberg daban mucho más de lo que se necesitaba para la cuestión de equidistribución, y comprobó que los argumentos clásicos de Hadamard-de la Vallée Poussin podían usarse en su lugar. Después observó que el método podía usarse para mejorar notablemente la desigualdad de Lang-Weil para los valores absolutos de los autovalores de Frobenius en el H^2 de una superficie proyectiva lisa de $|\alpha| \leq q^{3/2}$ a $|\alpha| < q^{3/2}$. (La Hipótesis de Riemann en este caso es $|\alpha| = q$.)

5. Los ingredientes nuevos. Entonces, ¿qué fue lo que permitió finalmente probar la Hipótesis de Riemann para variedades sobre cuerpos finitos? Hubo dos ingredientes principales.

5.1. Monodromía de pinceles de Lefschetz. En el gran trabajo de Lefschetz [35] sobre la topología de variedades algebraicas, introdujo la técnica de "fibrar" sistemáticamente una variedad proyectiva por sus secciones hiperplanas, y después expresar la cohomología de la variedad en términos de la cohomología de esas fibras. La teoría general de Lefschetz fue trasladada exitosamente a la cohomología ℓ-ádica, pero no llegó a dar frutos diofantinos hasta que Kazhdan-Margouls [30] probaron que el "grupo de monodromía" de un pincel de Lefschetz con dimensión relativa impar era "lo más grande posible". Deligne se dio cuenta de que si el *mismo* resultado fuese cierto también para dimensión relativa

par, entonces sería posible probar inductivamente la independencia de ℓ y la racionalidad de los $P_{i,\ell}$ de X, recuperándolos como los "máximos comunes divisores" de los $P_{i,\ell}$ de las secciones hiperplanas. Pero la demostración de Kazhdan-Margoulis estaba basada en la teoría de álgebras de Lie, vía los logaritmos de las diversas transformaciones de Picard-Lefschetz en el grupo de monodromía. La restricción a dimensión relativa impar era necesaria porque en ese caso las transformaciones de Picard-Lefschetz eran *unipotentes*, así que tenían logaritmos interesantes, mientras que en dimensión relativa par eran *de orden finito*. Poco después, A'Campo [1] encontró un contraejemplo a una conjetura de Brieskorn de que la monodromía local de singularidades aisladas siempre debería tener orden finito. Cambiando la tristeza por alegría, Deligne se dio cuenta de que el ejemplo de A'Campo se podía usar para construir pinceles (no de Lefschetz) que *tendrían* monodromía local unipotente. Los usó para conseguir que la prueba de Kazhdan-Margoulis funcionase también en dimensión relativa par, y así establecer la "independencia de ℓz racionalidad de los $P_{i,\ell}$ (cf., [50]).

Con este resultado, la importancia de las consideraciones de monodromía para las cuestiones diofantinas quedó firmemente establecida.

5.2. Formas modulares, método de Rankin, y teoría cohomológica de las series L. En los años posteriores a las conjeturas de Weil, expertos en la teoría de formas modulares comenzaron a sosprechar una relación fuerte entre las conjeturas de Weil y la conjetura de Ramanujan sobre el orden de magnitud de $\tau(n)$, Recuérdese que los $\tau(n)$ son los coeficientes de la q-expansión de la única forma cuspidal Δ de peso doce en $SL_2(\mathbb{Z})$:

$$\Delta(q) = q\left(\prod_{n\geq 1}(1-q^n)\right)^{24} = \sum \tau(n)q^n$$

Como función aritmética, $\tau(n)$ aparece esencialmente como *término de error* en la fórmula para el número de representaciones de n como suma de 24 cuadrados. La conjetura de Ramanujan es que

$$|\tau(n)| \leq n^{11/2}d(n), \quad d(n) = \#\text{divisores de } n.$$

De acuerdo con la teoría de Hecke (que había sido "predescubierta" por Mordell para Δ) la serie de Dirichlet correspondiente a Δ admite un producto de Euler:

$$\sum_{n\geq 1}\tau(n)n^{-s} = \prod_p \left(\frac{1}{1-\tau(p)p^{-s}+p^{11-2s}}\right)$$

La certeza de la conjetura de Ramanujan para todo $\tau(n)$ es entonces una consecuencia formal de su certeza para todo $\tau(p)$ con p primo:

$$|\tau(p)| \leq 2p^{11/2}$$

Esta última desigualdad podría interpretarse como sigue. Considérese el polinomio $1-\tau(p)T+p^{11}T^2$ y factorícese:

$$1 - \tau(p)T + p^{11}T^2 = (1 - \alpha(p)T)(1 - \beta(p)T).$$

Entonces la conjetura de Ramanujan para $\tau(p)$ es equivalente a la *igualdad*

$$|\alpha(p)| = |\beta(p)| = p^{11/2}$$

Si existiese una variedad proyectiva lisa X sobre $\mathbb{F}_p$ tal que el polinomio $1-\tau(p)T+p^{11}T^2$ divide a $P_{11}(X/\mathbb{F}_p, T)$, entonces la Hipótesis de Riemann para X implicaría la conjetura de Ramanujan para $\tau(p)$. La búsqueda de esta X fue llevada a cabo por Eichles, Shimura, Kuga e Ihara (cf., [29],[32]). Construyeron una X que "debería haber funcionado", pero como dicha X era *no compacta* y no tenía una compactificación obvia, su polinomio P_{11} no tenía necesariamente todas las raíces con valor absoluto correcto. Deligne entonces mostró cómo compactificar X y cómo ver que el polinomio de Hecke $1 - \tau(p)T + p^{11}T^2$ dividía a cierto factor de P_{11}, cuyas raíces tendrían los valores absolutos "correctos" si las conjeturas de Weil fuesen ciertas. Por tanto, la certeza de la conjetura de Ramanujan se convirtió en consecuencia de la certeza universal de la Hipótesis de Riemann para variedades sobre cuerpos finitos.

En 1939, Rankin [39] había obtenido la mejor estimación (del momento) para $\tau(n)$ (concretamente $\tau(n) = O(n^{29/5})$) estudiando los polos de la serie de Dirichlet

$$\sum (\tau(n))^2 n^{-s}$$

Langlands [34] señaló que la idea de la demostración de Rankin podía usarse fácilmente para probar la conjetura de Ramanujan, siempre que uno supiera lo suficiente sobre la localización de los polos de una colección infinita de series de Dirichlet deducidas de Δ tomando potencias tensoriales pares: para cada entero par $2n$ uno necesitaba conocer los polos de la función representada por el producto de Euler

$$\prod_p \prod_{i=0}^{2n} \left(\frac{1}{1 - \alpha(p)^i \beta(p)^{2n-i} p^{-s}} \right)^{\binom{2n}{i}}$$

Deligne estudió el artículo original de Rankin intentando entender las observaciones de Langlands. Se dio cuenta de que para las series L de curvas sobre cuerpos finitos (en vez de sobre $\mathrm{Spec}(\mathbb{Z})$), la teoría cohomológica de Grothendieck [19] de tales series L junto con el resultado de monodromía de Kazhdan-Margoulis daba un control a priori de los polos: los métodos de Rankin podían por tanto combinarse con técnicas de monodromía de pinceles de Lefschetz para obtener la Hipótesis de Riemann para variedades sobre cuerpos finitos, y con ella la conjetura de Ramanujan-Peterson como corolario.

6. La demostración de Deligne en un caso particular

6.1. Formulación del problema. Ahora me gustaría explicar la idea de la demostración de Deligne tratando el caso particular de una hipersuperficie no singular de dimensión impar (¡incluyendo así el caso de curvas planas no singulares!). Este caso particular, que fue de hecho el primer caso tratado por Deligne, ilustra las ideas principales sin abrumar al novato cohomológico. En el caso general, las ideas explicadas aquí aparecen como el "Lema Principal".

Consideremos una hipersuperficie no singular $X_0 \subset \mathbb{P}^{2n}$ de grado d, sobre el cuerpo $\mathbb{F}_q$. Su función zeta es de la forma

$$Z(X_0/\mathbb{F}_q, T) = \frac{P(X_0/\mathbb{F}_q, T)}{\prod_{i=0}^{2n-1}(1 - q^i T)}$$

donde $P(X_0/\mathbb{F}_q, T)$ es un polinomio con coeficientes enteros y término constante 1, cuyo grado $b = \deg P$ es el número de Betti intermedio de cualquier hipersuperficie compleja lisa de grado d y dimensión $2n - 1$. Explícitamente,

$$b = \frac{((d-1)^{2n} - 1)(d-1)}{d}$$

Sobre $\mathbb{C}$, podríamos factorizarlo

$$P(X_0/\mathbb{F}_q, T) = \prod_{i=1}^{b}(1 - \alpha_i T)$$

De acuerdo con la ecuación funcional, $\alpha \mapsto q^{2n-1}/\alpha$ permuta los α_i. La Hipótesis de Riemann para X_0 es la afirmación de que los valores absolutos de los α_i vienen dados todos por

$$|\alpha_i| = \sqrt{q}^{2n-1} \qquad i = 1, \ldots, b$$

A la vista del hecho de que $\alpha \mapsto q^{2n-1}/\alpha$ *permuta* las α_i, estas igualdades son equivalentes a las desigualdades

$$|\alpha_i| \leq \sqrt{q}^{2n-1} \qquad i = 1, \ldots, b$$

Si igualamos las expresiones cohomológica y diofantina de la función zeta, obtenemos

$$Z(X_0/\mathbb{F}_q, T) = \exp\left(\sum_{r \geq 1} \frac{T^r}{r} N_r\right) = \frac{\prod_{i=1}^{b}(1 - \alpha_i T)}{\prod_{i=0}^{2n-1}(1 - q^i T)}$$

Igualando coeficientes de los logaritmos, obtenemos

$$N_r - \sum_{i=0}^{2n-1} q^{ri} = -\sum_{i=1}^{b} \alpha_i^r,$$

de modo que la Hipótesis de Riemann para X_0 es equivalente a las estimaciones diofantinas

$$\left| N_r - \sum_{i=0}^{2n-1} q^{ri} \right| \leq b\sqrt{q^r}^{2n-1}, \quad r = 1, 2, \ldots$$

Sin embargo, la formulación equivalente de la Hipótesis de Riemann para X_0 más fructífera resulta ser la siguiente forma $*$ de la desigualdad $|\alpha_i| \leq \sqrt{q}^{2n-1}$:

$$*\text{La serie de potencias } \frac{1}{P(X_0/\mathbb{F}_q, T)} \in \mathbb{Q}[[T]] \text{ converge}$$
$$\text{(en el sentido arquimediano) para } |T| < 1/\sqrt{q}^{2n-1}.$$

6.2. Una construcción geométrica . El primer paso para probar la Hipótesis de Riemann para X_0 es considerar no sólo la propia X_0, sino toda una familia uniparamétrica (de hecho, un pincel de Lefschetz) X_t de hipersuperficies en el mismo espacio proyectivo ambiente. La idea de probar *simultáneamente* la Hipótesis de Riemann para *todas* las variedades en una familia adecuada que contenga la de interés inicial le fue sugerida a Deligne porque Bombieri le dijo que Swinnerton-Dyer había obtenido estimaciones débiles en el caso de curvas elípticas considerando ciertas series L asociadas a "la" *familia universal* de curvas elípticas, y relacionándolas con formas modulares (!).

Supóngase que X_0 está definida por una forma homogénea F de grado dd. Escójase cualquier otra forma G del mismo grado también definida sobre $\mathbb{F}_q$, y considérese la familia uniparamétrica de formas $F + tG$. Denótese por X_t la hipersuperficie correspondiente.

No es difícil ver que, cambiando $\mathbb{F}_q$ por una extensión finita si es necesario, podemos escoger G de manera que

1. la hipersuperficie de ecuación G es lisa e interseca X_0 transversalmente.
2. para todo t salvo un conjunto finito en el cierre algebraico de $\mathbb{F}_q$, la hipersuperficie X_t es lisa, mientras que para los valores restantes tiene un único punto singular, que además es un punto doble ordinario.

Denotaremos por $\mathbb{A}^1$ la t-recta afín sobre $\mathbb{F}_q$, y por $S \subset \mathbb{A}^1$ el conjunto finito de valores del parámetro *excepcionales*. Probaremos *simultáneamente* las conjeturas de Weil para *todas* las X_t, $t \in \mathbb{A}^1 - S$, haciendo uso del "pegamento" ℓ-ádico que las mantiene juntas. Este pegamento es una cierta representación ℓ-ádica de cierto grupo fundamental aritmético.

6.3. El papel de la monodromía.

El contexto clásico. Supóngase primero que el cuerpo base es $\mathbb{C}$ en vez de $\mathbb{F}_q$. Entonces los diversos X_t, $t \in \mathbb{A}^1 - S$, encajan juntos para formar una fibración sobre $\mathbb{A}^1 - S$ que es localmente (sobre $\mathbb{A}^1 - S$) trivial en el sentido $\mathcal{C}^\infty$. Los grupos de cohomología intermedios $H^{2n-1}(X_t, \mathbb{Q})$ forman por tanto un *sistema de coeficientes locales* en $\mathbb{A}^1 - S$, o lo que es lo mismo una vez escogido un punto base $t_0 \in \mathbb{A}^1 - S$, dan una *representación* de $\pi_1(\mathbb{A}^1 - S)$ en $H^{2n-1}(X_{t_0}, \mathbb{Q})$. Esta representación *respeta* la forma de intersección antisimétrica $\langle , \rangle$ en $H^{2n-1}(X_{t_0}, \mathbb{Q})$, así que da un homomorfismo de $\pi_1(\mathbb{A}^1 - S)$ en el grupo simpléctico $Sp = \mathrm{Aut}(H^{2n-1}(X_{t_0}, \mathbb{Q}), \langle , \rangle)$. El teorema de Kazhdan-Margoulis afirma que la imagen de π_1 en Sp es *Zariski-densa*: toda función polinómica en Sp que se anule en la imagen de π_1 es idénticamente nula.

El contexto ℓ-ádico. Sobre el cuerpo base $\mathbb{F}_q$, si fijamos un número primo ℓ primo con q, la teoría de cohomología ℓ-ádica de Grothendieck proporciona una estructura similar e incluso más rica.

Recuérdese que el grupo fundamental aritmético π_1^{arit} de $\mathbb{A}^1 - S$ es un grupo compacto totalmente disconexo, definido como el cociente del grupo de Galois del cierre algebraico $\overline{\mathbb{F}_q(t)}$ sobre $\mathbb{F}_q(t)$ por el subgrupo cerrado generado por los subgrupos de inercia asociados a todos los lugares de $\overline{\mathbb{F}_q(t)}$ por encima de puntos de $\mathbb{A}^1 - S$, El subgrupo $\pi_1^{\text{geom}} \subset \pi_1^{\text{arit}}$ es el correspondiente cociente del grupo de Galois de $\overline{\mathbb{F}_q(t)}$ sobre $\overline{\mathbb{F}}_q(t)$. Es este "grupo fundamental geométrico" el que es análogo al grupo fundamental del caso clásico. Es un subgrupo normal cerrado de π_1^{arit}, con grupo cociente $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \hat{\mathbb{Z}}$, siendo el generador canónico el automorfismo de Frobenius $a \mapsto a^q$ de $\overline{\mathbb{F}}_q$.

$$0 \to \pi_1^{\text{geom}} \to \pi_1^{\text{arit}} \xrightarrow{\text{"grado"}} \hat{\mathbb{Z}} \to 0$$

Igual que en teoría algebraica de números, a cada punto cerrado $x \in \mathbb{A}^1 - S$ y a cada lugar $\bar{x}$ de $\overline{\mathbb{F}}_q(t)$ por encima de él, le corresponde un elemento de Frobenius $\mathcal{F}_{\bar{x}} \in \pi_1^{\text{arit}}$ cuyo grado en $\hat{\mathbb{Z}}$ es el entero $\deg(x) := [\mathbb{F}_q(x)/\mathbb{F}_q]$. Si cambiamos $\bar{x}$ pero no x, el elemento $\mathcal{F}_{\bar{x}}$ cambia por conjugación. Por desgracia, necesitaremos considerar no los $\mathcal{F}_{\bar{x}}$ sino sus *inversos*, que llamaremos $F_{\bar{x}} := (\mathcal{F}_{\bar{x}})^{-1}$. Denotaremos por F_x la clase de conjugación en π_1^{arit} de todos los $F_{\bar{x}}$ para puntos $\bar{x}$ por encima de un x fijo; el *grado* de F_x en $\hat{\mathbb{Z}}$ es el entero $-\deg(x)$.

La teoría ℓ-ádica proporciona los siguientes datos:

1. un $\mathbb{Q}_\ell$-espacio b-dimensional V con una representación continua de π_1^{arit} en $\text{Aut}(V)$, tal que para cada punto cerrado $x \in \mathbb{A}^1 - S$, recuperamos el numerador de la función zeta de $X_x/\mathbb{F}_q(x)$ por la fórmula

$$\det(\text{Id} - TF_x|V) = P(X_x/\mathbb{F}_q(x), T) \in \mathbb{Q}[T]$$

2. una forma de intersección simpléctica en V con valores en $\mathbb{Q}_\ell(1-2n)$, *compatible* con la acción de π_1^{arit}. Esto *significa* que $\langle , \rangle$ es una autodualidad sobre $\mathbb{Q}_\ell$ tal que para $g \in \pi_1^{\text{arit}}$, $v, w \in V$, tenemos que

$$\langle gv, gw \rangle = q^{(1-2n)\deg(g)} \langle v, w \rangle$$

Por tanto

$$\begin{cases} \langle \gamma v, \gamma w \rangle = \langle v, w \rangle \text{ para } \gamma \in \pi_1^{\text{geom}} \\ \langle F_{\bar{x}} v, F_{\bar{x}} w \rangle = q^{(2n-1)\deg x} \langle v, w \rangle \text{ para cada } F_{\bar{x}} \end{cases}$$

La versión ℓ-ádica del teorema de Kazhdan-Margoulis es que la *imagen* de π_1^{geom} en $\text{Aut}(V)$ es Zariski densa (de hecho, ℓ-ádicamente abierta) en el grupo simpléctico $Sp(V, \langle , \rangle)$.

6.4. La demostración: una heurística. Nos proponemos demostrar la Hipótesis de Riemann para todos los $X_x/\mathbb{F}_q(x)$, $x \in \mathbb{A}^1 - S$. Como ya hemos observado, esto es equivalente a probar que para cada punto cerrado $x \in \mathbb{A}^1 - S$, la serie

$$\frac{1}{\det(\mathrm{Id} - T^{\deg x} F_x | V)} = \frac{1}{P(X_x/\mathbb{F}_q(x, T^{\deg x}))} \in \mathbb{Q}[[T]]$$

converge arquimedianamente si $|T| < 1/\sqrt{q}^{2n-1}$.

Para aclarar la idea básica, comencemos explicando cómo podríamos deducir esta última estimación directamente si dos suposiciones aparentemente falsas fueran simultáneamente ciertas (cf. la Observación al final de la demostración). La primera suposición es que cada serie $1/\det(\mathrm{Id} - T^{\deg x} F_x | V) \in \mathbb{Q}[[T]]$ tiene coeficientes *positivos*. La segunda es que el producto infinio

$$L(V, T) \coloneqq \prod_x \frac{1}{\det(\mathrm{Id} - T^{\deg x} F_x | V)} \in \mathbb{Q}[[T]]$$

converge arquimedianamente para $|T| < 1/\sqrt{q}^{2n-1}$ cuando se considera como serie de potencias. Con estas suposiciones, observaríamos simplemente que cada factor $1/\det(\mathrm{Id} - T^{\deg x} F_x | V)$ es una serie con término constante *uno*, la suposición de que los coeficientes son *positivos* significa que la serie de potencias de $L(V, T)$ también tiene coeficientes positivos que son término a término mayores o iguales que los coeficientes de cualquier factor. Por tanto, la supuesta convergencia arquimediana de $L(V, T)$ para $|T| < 1/\sqrt{q}^{2n-1}$ implicaría que cada factor $1/\det(\mathrm{Id} - T^{\deg x} F_x | V)$ es arquimedianamente convergente para $|T| < \sqrt{q}^{2n-1}$.

6.5. La demostración de verdad: "cuadrados". Ahora debemos explicar cómo sortear el hecho de que nuestras suposiciones no son ambas ciertas. La no positividad de los coeficientes del factor individual $1/\det(\mathrm{Id} - T^{\deg x} F_x | V)$ se resuelve *reemplazando* V por cualquiera de sus potencias tensoriales *pares* $V^{\otimes 2k}$. (Reemplazar V por $V^{\otimes 2k}$ es análogo al reemplazo por Rankin de $\sum \tau(n) \cdot n^{-s}$ por $\sum \tau(n)^2 \cdot n^{-s}$.) Para ver que $1/\det(\mathrm{Id} - T^{\deg x} F_x | V^{\otimes 2k})$ tiene coeficientes positivos, argumentamos como sigue. Para cada entero $m \geq 1$, tenemos la fórmula

$$1/\det(\mathrm{Id} - T^{\deg x} F_x | V^{\otimes m}) = \exp\left(\sum_{n \geq 1} \frac{T^n}{n} \mathrm{traza}(F_x^n | V^{\otimes m})\right)$$

$$= \exp\left(\sum_{n \geq 1} \frac{T^n}{n} \mathrm{traza}(F_x^n | V)^m\right)$$

Para $m = 1$, esta fórmula, junto con el hecho de que la serie $1/\det(\mathrm{Id} - T^{\deg x} F_x | V)$ tiene coeficientes racionales muestra que todos números $\mathrm{traza}(F_x^n | V)$ son racionales. Esta racionalidad, junto con la fórmula de arriba para $m = 2k$, muestra que $1/\det(\mathrm{Id} - T^{\deg x} F_x | V^{\otimes 2k})$ es la exponencial de una serie con coeficientes positivos, y por tanto tiene coeficientes positivos también.

6.6. Recordatorio sobre series L Por tanto, para poder aplicar el argumento, necesitamos información sobre el radio de convergencia de la serie de potencias

$$L(V^{\otimes 2k}, T) \coloneqq \prod_x \frac{1}{\det(\mathrm{Id} - T^{\deg x} F_x | V^{\otimes 2k})}.$$

Por suerte, esta información se deduce de la expresión cohomológica de Grothendieck para la función $L(M,T)$ asociada a *cualquier* representación finito-dimensional continua $\mathbb{Q}_\ell$-adica de π_1^{arit}. Grothendieck da una *fórmula* para $L(M,T)$, que la da como una función racional de T y que, con mayor importancia, da un control a priori de sus polos, como sigue.

Sea $M_{\pi_1^{geom}}$ el mayor espacio cociente de M en el que π_1^{geom} actúa trivialmente:

$$M_{\pi_1^{\mathrm{geom}}} = M / \sum_{\gamma \in \pi_1^{\mathrm{geom}}} (\mathrm{Id} - \gamma) M$$

Este espacio cociente es una representación de $\pi_1^{\mathrm{arit}}/\pi_1^{\mathrm{geom}} \simeq \hat{\mathbb{Z}}$, así que el único elemento $F \in \hat{\mathbb{Z}}$ de grado -1 (el *inverso* del automorfismo $a \mapsto a^q$ de $\overline{\mathbb{F}}_q$) actúa en él. La fórmula de Grothendieck de las funciones L afirma que el producto

$$\det(\mathrm{Id} - qTF | M_{\pi_1^{\mathrm{geom}}}) \cdot L(M,T)$$

es un *polinomio*.

6.7. Fin de la demostración. Ajora aplicamos esto a $M = V^{\otimes 2k}$. El punto clave es calcular $(V^{\otimes 2k})_{\pi_1^{\mathrm{geom}}}$ y la acción de F sobre él, pues entonces conoceremos los polos de $L(V^{\otimes 2k}, T)$. Como la imagen de π_1^{geom} en $Sp = \mathrm{Aut}(V, \langle , \rangle)$ es Zariski densa (por el teorema de Kazhdan-Margoulis), sus covariantes son los mismos:

$$(V^{\otimes 2k})_{\pi_1^{\mathrm{geom}}} \simeq (V^{\otimes 2k})_{Sp}$$

Los covariantes tensoriales del grupo simpléctico, o más bien su dual, son bien conocidos de la teoría clásica de invariantes. Por la definición de covariantes, las formas lineales sobre $(V^{\otimes 2k})_{Sp}$ son lo mismo que las formas $2k$-lineales en V, y estas son todas sumas de "contracciones completas": para cada partición del conjunto $\{1, \ldots, 2k\}$ en dos conjuntos ordenados $\{a_1, \ldots, a_k, b_1, \ldots, b_k\}$, la contracción completa correspondiente es la forma $2k$-lineal sobre V

$$(v_1, \ldots, v_{2k}) \mapsto \prod_{i=1}^{k} \langle v_{a_i}, v_{b_i} \rangle$$

Si recordamos la acción de π_1^{arit}, entonces la forma de intersección $\langle , \rangle$ sobre V toma valores en $\mathbb{Q}_\ell(1-2n)$, y vemos que el producto $\prod_{i=1}^k \langle v_{a_i}, v_{b_i} \rangle$ está en $\mathbb{Q}_\ell(k(1-2n))$. Así que si escogemos un conjunto de contracciones completas linealmente independientes maximal, obtenemos un isomorfismo

$$(V^{\otimes 2k})_{Sp} \simeq \oplus \mathbb{Q}_\ell(k(1-2n));$$

un espacio en el que F actúa como multiplicación por $q^{k(2n-1)}$.

Volviendo al teorema de Grothendieck, el *denominador* de $L(V^{\otimes 2k}, T)$ viene dado en el peor de los casos por

$$\det(\mathrm{Id} - qTF | \oplus \mathbb{Q}_\ell(k(1-2n))) = \text{una potencia de } (1 - q^{1+k(2n-1)}T).$$

Por tanto la serie $L(V^{\otimes 2k}, T)$ converge arquimedianamente para $|T| < q^{1+k(2n-1)}$.

El argumento de positividad entonces muestra que cada factor $\dfrac{1}{\det(\mathrm{Id} - T^{\deg x} F_x | V^{\otimes 2k})}$ converge arquimedianamente para $|T| < 1/q^{1+k(2n-1)}$.

Ahora supóngase que $\alpha(x)$ es un autovalor de F_x en V. Debemos probar que $|\alpha(x)| \leq 1/\sqrt{q^{\deg x}}^{2n-1}$. Pero $\alpha(x)^{2k}$ será un autovalor de F_x sobre $V^{\otimes 2k}$, y por tanto $1/\det(\mathrm{Id} - T^{\deg x} F_x | V^{\otimes 2k})$ tendrá un *polo* en $T = 1/\alpha(x)^{2k/\deg x}$. Pero como esta serie *converge* para $|T| < 1/^{1+k(2n-1)}$, debemos tener la desigualdad

$$|1/\alpha(x)^{2k/\deg x}| \geq 1/q^{1+k(2n-1)}$$

o equivalentemente

$$|\alpha(x)^{2k/\deg x}| \geq q^{1+k(2n-1)}$$

o equivalentemente

$$|\alpha(x)| \geq \sqrt{q^{\deg x}}^{(2n-1+1/k)}$$

Haciendo que k tienda a $+\infty$, obtenemos

$$|\alpha(x)| \leq \sqrt{q^{\deg x}}^{2n-1}.$$

Observación. La expresión cohomológica para $L(V^{\otimes 2k+1}, T)$ junto con el hecho de que el grupo simpléctico *no* tiene covariantes en ninguna potencia tensorial *impar* de su representación estándar muestra que de hecho cada serie $L(V^{\otimes 2k+1}, T)$ es un *polinomio*, así que tiene radio de convergencia *infinito*. Pero es sólo para las potencias tensoriales *pares* $V^{\otimes 2k}$ que sabemos que cada factor local $1/\det(\mathrm{Id} - T^{\deg x} F_x | V^{\otimes 2k})$ tiene coeficientes *positivos*.

7. Aplicaciones. La consecuencia aritmética más chocante es la conjetura de Ramanujan-Peterson sobre el orden de magnitud de los coeficientes de las formas cuspidales de peso mayor o igual que 2 en subgrupos de congruencia de $SL_2(\mathbb{Z})$. (Deligne y Serre también han probado la conjetura para formas de peso uno (inédito)), pero la demostración no depende de la Hipótesis de Riemann.

Otra aplicación aritmética es la estimación de sumas exponenciales en varias variables. Aunque difícil técnicamente, la idea procede de Weil [56], quien mostró cómo la Hipótesis de Riemann para *curvas* sobre cuerpos finitos daba la estimación "buena" para sumas exponenciales en *una* variable.

En cuanto a aplicaciones geométricas, ya hemos mencionado el teorema de Lefschetz fuerte. Tambien hay toda una cadena de ideas construida alrededor del "yoga de pesos", la frase gancho de Grothendieck para deducir resultados en la cohomología de variedades arbitrarias asumiendo la Hipótesis de Riemann para variedades proyectivas no singulares sobre cuerpos finitos (cf., [7]). Toda la "teoría de Hodge mixta" de Deligne para variedades algebraicas complejas ([8], [9]), desarrollada antes de su demostración de la Hipótesis de Riemann, tiene como intención *demostrar* resultados sobre la cohomología de estas variedades que se siguen de la Hipótesis de Riemann y de la aplicación sistemática de la resolución de singularidades de Hironaka. El trabajo reciente de Deligne, Griffiths, Morgan y Sullivan sobre el tipo de homotopía racional de variedades algebraicas complejas también queda considerablemente aclarado por el uso de la Hipótesis de Riemann.

8. Algunas cuestiones abiertas.

8.1. Independencia de ℓ. Sea X una variedad arbitraria sobre un cuerpo algebraicamente cerrado k. Para cada número primo ℓ distinto de la característica de k, los grupos de cohomología ℓ-ádica $H^i(X, \mathbb{Q}_\ell)$ y los grupos ℓ-ádicos "con soporte compacto" $H^i_c(X, \mathbb{Q}_\ell)$ son finito-dimensionales ([10]) sobre $\mathbb{Q}_\ell$. Denotaremos por $b^c_{i,\ell}(X)$ sus dimensiones. No se sabe si estos números son independientes de ℓ, excepto en algunos casos particulares, como sigue.

Cuando el cuerpo k es de característica cero, el "teorema de comparación" [2] afirma que si "escogemos" una inmersión de k en el cuerpo $\mathbb{C}$, y denotamos por $X(\mathbb{C})$ el espacio analítico sobre $\mathbb{C}$ correspondiente con su topología usual, entonces tenemos isomorfismos

$$H^i(X, \mathbb{Q}_\ell) \simeq H^i_{\text{sing}}(X(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_\ell$$
$$H^i_c(X, \mathbb{Q}_\ell) \simeq H^i_{c,\text{sing}}(X(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_\ell$$

donde H^i_{sing} (resp. $H^i_{c,\text{sing}}$) denota cohomología singular clásica (resp. con soporte compacto) de espacios topológicos usuales.

Cuando el cuerpo k es de característica p, un argumento sencillo de especialización nos lleva al caso en que k es el cierre algebraico de un cuerpo finito $\mathbb{F}_q$, y X/k procede por extensión de escalares de una variedad $X_0/\mathbb{F}_q$.

En caso de que X/k es completa y lisa, entonces $b_{i,\ell}(X) = b^c_{i,\ell}(X)$, simplemente porque X ya es "compacta", y podemos usar la Hipótesis de Riemann para $X_0/\mathbb{F}_q$ (extendida por Deligne al caso completo y liso en [6]) para interpretar $b_{i,\ell}(X)$ como el número de ceros complejos (si i es impar) o polos (si i es par) de la función zeta $Z(X_0/\mathbb{F}_q, T)$ que están en el círculo $|T| = q^{-i/2}$. Como la propia función zeta es independiente de ℓ, esto muestra que el entero $b_{i,\ell}(X)$ es independiente de ℓ, y que el polinomio (a priori) ℓ-ádico $\det(\text{Id} - TF|H^i(X, \mathbb{Q}_\ell))$ tiene coeficientes en $\mathbb{Q}$ que son independientes de ℓ.

Sin embargo, cuando X/k no es completa y lisa, el argumento falla. Para X/k arbitraria, Deligne ha probado (cf., [6]) que para cada $\ell \neq p$, el polinomio $\det(\text{Id} - TF|H^i_c(X, \mathbb{Q}_\ell))$, cuyo grado es $b^c_{i,\ell}(X)$, tiene coeficientes números algebraicos, y que cada uno de sus ceros

recíprocos (los autovalores de F en $H_c^i(X, \mathbb{Q}_\ell)$) es un número algebraico α para el cual existe un entero $j \leq i$ (j dependiente de α) tal que α y todos sus conjugados sobre $\mathbb{Q}$ tienen $|\alpha| = q^{j/2}$. Pero no se sabe si $\det(\mathrm{Id} - TF|H_c^i(X, \mathbb{Q}_\ell))$ tiene coeficientes en $\mathbb{Q}$, y a fortiori si es independiente de ℓ. Es el *mezclado* de autovalores entre los diversos H_c^i lo que nos impide expresar los polinomios $\det(\mathrm{Id} - TF|H_c^i(X, \mathbb{Q}_\ell))$ en términos de $Z(X_0/\mathbb{F}_q, T)$, como podíamos en el caso completo y liso. [Una forma lo bastante fuerte de la resolución de singularidades de Hironaka [27] (por el momento sólo establecida en característica cero) nos permitiría recuperar estos polinomios característicos intrínsecamente en términos de las funciones zeta de las diversas variedades completas y lisas que aparecerían en una compactificación y resolución de X. Pero quizás uno puede apañárselas sin resolución.]

8.2. Una demostración elemental. (cf. [4]) Ahora que *sabemos* que la Hipótesis de Riemann para variedades sobre cuerpos finitos es cierta, ¿podemos dar una demostración elemental contando directamente puntos racionales? Para curvas, esto ha sido hecho recientemente por Bombieri-Stepanov. Una dificultad añadida en el caso de dimensión superior es que para la variedad "típica" de dimensión $d > 1$, la Hipótesis de Riemann no parece ser equivalente a ningún enunciado diofantino; el grupo de cohomología máximo H^{2d} da la contribución dominante al número de puntos racionales, y *todo* el resto de la cohomología es un término de error:

$$N_n = q^{dn} + O\left(q^{n\left(d-\frac{1}{2}\right)}\right).$$

Esta estimación, sin embargo, fue establecida en 1953 por Lang-Weil [33] como consecuencia de la Hipótesis de Riemann para *curvas*. Hay, por supuesto, muchas clases particulares de variedades (por ej. curvas, intersecciones completas, superficies simplemente conexas) para las que la Hipótesis de Riemann *es* equivalente a una estimación diofántica, y una demostración directa de ello sería de gran interés.

8.3. La función zeta de Hasse-Weil. (cf. [59], [61]) Con la demostración de todas las conjeturas de Weil, podríamos mirar la cuestión del número de soluciones de ecuaciones en cuerpos finitos como algo bastante bien comprendido. Lo que no está para nada bien comprendido es la cuestión de soluciones de ecuaciones en números racionales. Se espera que la función zeta de Hasse-Weil juegue un papel importante en esta cuestión. Para fijar ideas, supóngase que X es un esquema proyectivo liso sobre $\mathbb{Z}[1/N]$ (i.e., X es una variedad proyectiva no singular sobre $\mathbb{Q}$ que tiene "buena reducción" en todos los primos p que no dividen a cierto "conductor" N). Entonces para cada primo p que no divide a N, la "reducción mód. p"de X, denotada $X(p)$, es una variedad proyectiva lisa sobre $\mathbb{F}_p$. Para cada entero $0 \leq i \leq \dim(X/\mathbb{Z}[1/N])$, consideramos el i-ésimo polinomio $P_i(X(p)/\mathbb{F}_p, T)$ que aparece en la función zeta de $X(p)/\mathbb{F}_p$. La i-ésima función L de Hasse-Weil se define como la serie de Dirichlet con producto de Euler (sobre primos que no dividen a N)

$$L(i; X, s) = \prod_p \frac{1}{P_i(X(p)/\mathbb{F}_p, p^{-s})}.$$

Es convergente para $\mathrm{Re}(s) > 1 + i/2$ por la Hipótesis de Riemann para las $X(p)$'s. La función zeta de Hasse-Weil es por definición el producto alternado de estas funciones L.

Se conjetura generalmente que cada función $L(i, X, s)$ admite una extensión meromorfa a todo el plano de la s, satisface una ecuación funcional bajo $s \mapsto i + 1 - s$, y tiene todos sus ceros en el semiplano $\mathrm{Re}(s) \leq \frac{i+1}{2}$, con todos los ceros que no son introducidos por los factores Γ en la ecuación funcional contenidos en la recta $\mathrm{Re}(s) = \frac{i+1}{2}$. Esta última conjetura es la "Hipótesis de Riemann generalizada".

Del punto de vista de la geometría algebraica aritmética, una variedad X sobre $\mathbb{Z}[1/N]$ es el análogo de una *familia* de variedades parametrizada por una curva sobre un cuerpo finito. Para tales familias, los análogos de las funciones L de Hasse-Weil son las funciones L asociadas a las diversas representaciones ℓ-ádicas de π_1^{arit} provistas por la cohomología ℓ-ádica; la meromorfía (de hecho, racionalidad como función de p^{-s}) de estas últimas funciones L, y sus ecuaciones funcionales, se deducen de la teoría de Grothendieck de tales funciones L. La localización de sus ceros es una forma generalizada de la Hipótesis de Riemann para variedades sobre cuerpos finitos (que también ha sido probada por Deligne, pero todavía no publicada).

¿Qué ha sido probado sobre las funciones L de Hasse-Weil? La continuación meromórfica y ecuación funcional han sido establecidas sólo para X muy particulares (por ej. curvas elípticas con multiplicación compleja [13], [14], hipersuperficies diagonales [60], curvas uniformizadas por funciones modulares [48], y X de dimensión *cero*). No hay un sólo caso conocido de la Hipótesis de Riemann. En el caso más simple, cuando la variedad X sobre $\mathbb{Z}$ es "un punto"(es decir, $X = \mathrm{Spec}(\mathbb{Z})$), la función zeta de Hasse-Weil $\zeta(X, s)$ se convierte en la función zeta de Riemann.

Bibliografía

[1] N. A'Campo: *Sobre la monodromía de las singularidades aisladas de hipersuperficies complejas.* (1973)

[2] E. Artin: *Cuerpos cuadráticos en el dominio de congruencias superiores* (1924).

[3] M. Artin, A. Grothendieck y J.-L. Verdier: *SGA 4 Teoría de topos y cohomología étale de los esquemas.* (1972).

[4] E. Bombieri: *Contando puntos en curvas sobre cuerpos finitos (según A. Stepanov)* (1973)

[5] P. Deligne: *La conjetura de Weil I.* 1974.

[6] P. Deligne: *La conjetura de Weil II.* 1980.

[7] P. Deligne: *Teoría de Hodge I.* 1971.

[8] P. Deligne: *Teoría de Hodge II.* 1972.

[9] P. Deligne: *Teoría de Hodge III.* Por publicar.

[10] P. Deligne: *Primeros pasos en cohomología étale.* 1974.

[11] P. Deligne: *Formas modulares y representaciones ℓ-ádicas.* 1971.

[12] P. Deligne y N. Katz: *SGA 7, parte II. Grupos de monodromía en geometría algebraica.* 1973.

[13] M. Deuring: *La función zeta de una curva algebraica de género uno.* 1953.

[14] M. Deuring: *Sobre la función zeta de un cuerpo de funciones elíptico con multiplicación compleja.* 1956.

[14bis] M. Deuring: *Teoría aritmética de las correspondencias algebraicas de cuerpos de funciones I.* 1937.

[15] J. Dieudonné: *Curso de Geometría Algebraica I, II.* 1974.

[16] B. Dwork: *Sobre la racionalidad de la función zeta de una variedad algebraica.* 1960.

[17] M. Eichler: *Una generalización de las integrales abelianas.* 1957.

[18] A. Grothendieck: *SGA 7 parte I. Grupos de monodromía en geometría algebraica* 1973.

[19] A. Grothendieck: *Fórmula de Lefschetz y racionalidad de las funciones L* 1966.

[20] A. Grothendieck: *Sobre una nota de Mattuck-Tate* 1958.

[21] G. H. Hardy: *Ramanujan. Doce lecciones sobre materias sugeridas por su vida y obra* 1940.

[22] H. Hasse: *Demostración del análogo de la hipótesis de Riemann para funciones zeta de congruencias de Artin y Schmid en ciertos casos elípticos* 1933.

[23] H. Hasse: *Sobre las funciones zeta de congruencias* 1934.

[24] H. Hasse: *Sobre las funciones zeta de congruencias* 1934.

[25] H. Hasse: *Sobre la teoría de los cuerpos de funciones elípticos abstractos I, II y III* 1936.

[26] H. Hasse: *Sobre la hipótesis de Riemann en cuerpos de funcones* 1930.

[27] H. Hironaka: *Resolución de singularidades de una variedad algebraica sobre un cuerpo de característica cero, I, II.* 1964.

[28] W. Hodge: *La teoría y aplicaciones de las integrales armónicas* 1941.

[29] Y. Ihara: *Polinomios de Hecke como funciones zeta de congruencias en el caso elíptico modular* 1967.

[30] Kazhdan y Margoulis: *Comunicación personal a P. Deligne* 1971.

[31] S. Kleiman: *Ciclos algebraicos y las conjeturas de Weil* 1968.

[32] M. Kuga y G. Shimura: *Sobre la función zeta de una variedad fibrada cuyas fibras son variedades abelianas* 1965.

[33] S. Lang y A. Weil: *Número de puntos de variedades sobre cuerpos finitos* 1954.

[34] R. Langlands: *Problemas en la teoría de formas automorfas* 1970.

[35] S. Lefschetz: *El analysis situs y la geometría algebraica* 1924.

[36] D. Lehner: *Nota sobre la distribución de la función tau de Ramanujan* 1970.

[37] A. Mattuck y J. Tate: *Sobre la desigualdad de Castelnuovo-Severi* 1958.

[38] D. Mumford: *Variedades Abelianas* 1970.

[39] R. A. Rankin: *Contribuciones a la teoría de la función $\tau(n)$ de Ramanujan y funciones aritméticas similares II* 1939.

[40] F. K. Schmidt: *Teoría de números analítica en cuerpos de característica p* 1931.
[41] J.-P. Serre.: *Haces algebraicos coherentes* 1955.
[42] J.-P. Serre.: *Sobre la topología de variedades algebraicas en característica p* 1956.
[43] J.-P. Serre.: *Algunas propiedades de las variedades abelianas en característica p* 1958.
[44] J.-P. Serre.: *Análogos Kahlerianos de ciertas conjeturas de Weil* 1960.
[45] J.-P. Serre.: *Racionalidad de las funciones ζ de variedades algebraicas (según Bernard Dwork)* 1966.
[46] J.-P. Serre.: *Funciones zeta y L* 1965.
[47] J.-P. Serre.: *Valores propios de los endomorfismos de Frobenius (según P. Deligne)* Por publicar.
[48] G. Shimura: *Correspondencias modulares y funciones ζ de curvas algebraicas* 1958.
[48bis] G. Shimura: *Sobre las integrales asociadas a las formas automorfas* 1959.
[49] G. Shimura y Y. Taniyama: *Multiplicación compleja de variedades abelianas y sus aplicaciones a la teoría de números*. 1961.
[50] J.-L. Verdier: *Independencia con respecto a ℓ de los polinomios característicos de los endomorfismos de Frobenius de la cohomología ℓ-ádica (según P. Deligne)* Por publicar.
[51] A. Weil: *Sobre las funciones algebraicas con cuerpo de constantes finito*. 1940.
[52] A. Weil: *Sobre la hipótesis de Riemann en cuerpos de funciones*. 1941.
[53] A. Weil: *Sobre las funciones algebraicas con cuerpo de constantes finito*. 1940.
[54] A. Weil: *Sobre las curvas algebraicas y las variedades deducidas de ellas*. 1948.
[55] A. Weil: *Variedades abelianas y curvas algebraicas*. 1948.
[56] A. Weil: *Sobre algunas sumas exponenciales*. 1948.
[57] A. Weil: *Número de soluciones de ecuaciones en cuerpos finitos*. 1949.
[58] A. Weil: *Fibrados en geometría algebraica*. 1952.
[59] A. Weil: *Teoría de números y geometría algebraica*. 1952.
[60] A. Weil: *Sumas de Jacobi como Grossencharaktere*. 1952.
[61] A. Weil: *Geometría algebraica abstracta contra clásica*. 1956.
[62] H. Yoshida: *Sobre un análogo de la conjetura de Sato*. 1973.
[63] O. Zariski: *Superficies algebraicas*. 1971.
[64] O. Zariski: *Obras Completas*. 1973.