Mixba'al Rev. Met. de Mat.
Nº 1, Vol. I, Junio 2010. 89 – 102

Las conjeturas de Weil para curvas elípticas

Marco Antonio Sánchez Mirafuentes

Resumen

En este trabajo se presentan las conjeturas de *Weil* y se da una demostración en el caso de una curva elíptica. Estas conjeturas tienen antecedentes en los trabajos de Gauss, concretamente en las *Disquisitiones* Art. 358, donde se da el número de soluciones de congruencias de las forma $ax^3 - by^3 \equiv 1 (\mathrm{mod}\, p)$, con p un número primo de la forma $p = 3n+1$. Tiempo después en los trabajos de *Artin* y *Hasse* se formula la conjetura de Riemann para campos de funciones, demostrada por Hasse en el caso elíptico y por Weil en el caso de una curva arbitraria. En la demostración que se presenta a continuación son importantes las nociones de morfismo *separable*, el morfismo de *Frobenius* y el apareamiento de *Weil*.

Palabras clave: variedad proyectiva, función zeta, curva algebraica, curva elíptica, diferenciales, morfismo de Frobenius, isogenia, apareamiento de Weil, módulo de Tate, cohomología ℓ-ádica.

Clasificación de la AMS: 14H52, 11G20

1. Funciones zeta y las conjeturas de Weil

Denotaremos la cardinalidad de un conjunto C por $N(C)$. Si k es un campo finito con q elementos, que también denotaremos por $\mathbb{F}_q$, se tiene el lema siguiente

Lema 1.1. *Sea k un campo finito con q elementos, entonces la cardinalidad de $\mathbb{P}^n(k)$ es $1 + q + \ldots + q^n$.*

Demostración. Definiendo $\varphi : k^{n+1} - \{0\} \to \mathbb{P}^n(k)$ como

$$\varphi(x_0, \ldots x_n) = [x_0, \ldots x_n],$$

se tiene que φ es suprayectiva, y dado un punto cualquiera $[x_0, \dots x_n]$ en $\mathbb{P}^n(k)$ observe que

$$\varphi^{-1}[x_0, \dots x_n] = \{(\lambda x_0, \dots \lambda x_n) : \lambda \in k - \{0\}\}.$$

ya que si $(x'_0, \dots x'_n) \in \varphi^{-1}[x_0, \dots x_n]$ entonces existe un $\lambda \neq 0$ en k tal que $x'_i = \lambda x_i$ para cada i; así el conjunto $\varphi^{-1}[x_0, \dots x_n]$ tiene $q-1$ elementos. Puesto que φ es suprayectiva y $N(k^{n+1} - \{0\}) = q^n - 1$, se tiene que $q^{n+1} - 1 = (q-1)N(\mathbb{P}^n(k))$, es decir, $N(\mathbb{P}^n(k)) = 1 + q + \dots + q^n$. □

Recuerde ahora que si k es un campo finito, con q elementos, para cada $s \in \mathbb{N}$ existe un campo k_s, y sólo uno, tal que $k \subseteq k_s$ y $N(k_s) = q^s$.

Ahora sea X una variedad proyectiva en $\mathbb{P}^n(k)$. Como los polinomios homogéneos que definen a X pertenecen a

$$k[x_0, \dots, x_n] \subseteq k_s[x_0, \dots, x_n],$$

podemos pensar a X como una variedad proyectiva en $\mathbb{P}^n(k_s)$ y por lo tanto tiene sentido considerar el número $N_s = N(X)$ de puntos de la variedad X vista en $\mathbb{P}^n(k_s)$.

Definición 1.2. *Si k es un campo finito con q elementos, la función zeta de la variedad proyectiva $X \subseteq \mathbb{P}^n(k)$ es la serie:*

$$Z_X(u) = \exp\Big(\sum_{s=1}^{\infty} \frac{N_s u^s}{s}\Big),$$

donde $\exp(u) = \sum_{s=0}^{\infty} \frac{u^s}{s!}$. *La variable u toma valores en $\mathbb{C}$, por lo tanto podemos pensar a Z_X como una serie formal de potencias o, utilizando la desigualdad siguiente (que se obtiene del lema 1.1)*

$$N_s \leq \frac{q^{s(n+1)} - 1}{q^s - 1} \leq (n+1)q^{sn},$$

vemos que $f(u) = \sum_{s=1}^{\infty} \frac{N_s u^s}{s}$ *se puede comparar con la serie* $g(u) = \sum_{s=1}^{\infty} \frac{(q^n u)^s}{s}$, *y concluir que Z_X es holomorfa en alguna vecindad del 0.*

Las conjeturas de Weil. Sea X una variedad proyectiva lisa de dimensión n definida sobre $k = \mathbb{F}_q$, y sea $Z_X(u)$ la función zeta de X.

(1) **La racionalidad de la función zeta.** Z_X es una función racional, es decir, es un cociente de polinomios con coeficientes racionales.

(2) **Ecuación funcional.** Sea E el número de autointersección de la diagonal Δ de $X \times X$. Entonces Z_X satisface la ecuación funcional siguiente:

$$Z_X\Big(\frac{1}{q^n u}\Big) = \pm q^{n\frac{E}{2}} u^E Z_X(u).$$

(3) **Analogía con la hipótesis de Riemann.** Es posible escribir

$$Z_X(U) = \frac{P_1(u)P_3(u)\dots P_{2n-1}(u)}{P_0(u)P_2(u)\dots P_{2n}(u)},$$

donde $P_0(u) = 1 - u$; $P_{2n} = 1 - q^n u$; y para cada $1 \leq i \leq 2n-1$, $P_i(u)$ es un polinomio con coeficientes enteros que se puede escribir de la forma siguiente:

$$P_i(u) = \prod(1 - \alpha_{ij} u),$$

donde los α_{ij} son enteros algebraicos con $|\alpha_{ij}| = q^{\frac{1}{2}}$.

Estas conjeturas aparecen por primera vez en el artículo de *A. Weil*, Number of solutions of equations over finite fields, Bull. Amer. Math. Soc. 55 (1949), 497 - 508; el artículo en cuestión empieza tratando el caso de variedades algebraicas de la forma $V(a_0 X_0^n + \ldots + a_r X_r^n)$ donda cada $a_i \in k$; de aquí obtiene la racionalidad de la función zeta asociada a tal variedad y después enuncia las conjeturas en el caso general. Cabe señalar que *A. Weil* probó sus conjeturas en el caso de curvas, es decir, variedades algebraicas de dimensión 1.

Ejemplo 1.3.

Calculamos la función zeta de $\mathbb{P}^n$ usando el lema 1.1. En efecto, como el resultado es independiente del campo finito usado, esto significa que $N_s = 1 + q^s + \ldots + q^{sn}$, por lo que:

$$\sum_{s=1}^{\infty} \frac{(1 + q^s + \ldots + q^{sn})u^s}{s} = \sum_{s=1}^{\infty} \frac{u^s}{s} + \sum_{s=1}^{\infty} \frac{(uq)^s}{s} + \ldots \sum_{s=1}^{\infty} \frac{(uq^n)^s}{s}.$$

Y recordando que $-\log(1-u) = \sum_{s=1}^{\infty} \frac{u^s}{s}$ obtenemos:

$$Z_{\mathbb{P}^n}(u) = \frac{1}{(1-u)(1-qu)\dots(1-q^n u)}.$$

En particular esto muestra que $Z_{\mathbb{P}^n}$ es una función racional, en concordancia con la conjetura de Weil correspondiente.

2. Curvas algebraicas

Por una *curva* o *curva algebraica* entenderemos una variedad *proyectiva* (irreducible) de dimensión 1. No sólo nos interesamos por las variedades proyectivas sino también por los morfismos entre ellas y en este sentido se tiene el teorema siguiente.

Teorema 2.1. *Si $\phi : C_1 \to C_2$ es un morfismo de curvas, entonces ϕ es constante o suprayectivo.*

Demostración. Como $\phi : C_1 \to C_2$ es regular sabemos que $\phi(C_1)$ es un subconjunto algebraico de C_2. Si $\phi(C_1)$ es finito, entonces sólo puede tener un punto, ya que en caso contrario como ϕ es continua, podríamos escribir a C_1 como unión disjunta de conjuntos algebraicos, contradiciendo que C_1 es irreducible y, en este caso, ϕ es constante.

Ahora si $\phi(C_1)$ no fuera finito entonces $\dim(\phi(C_1)) > 0$ además $\dim(\phi(C_1)) \leq \dim(C_2) = 1$ por lo tanto $\dim(\phi(C_1)) = \dim(C_2)$, y como $\phi(C_1) \subseteq C_2$ se tiene que, ([1] capítulo I ejercicio 1.10), $\phi(C_1) = C_2$ en particular, ϕ es suprayectiva. □

Ahora supongamos que tenemos curvas C_1/k y C_2/k y $\phi : C_1 \to C_2$ un morfismo no constante definido sobre k. Entonces ϕ induce una función $\phi^* : k(C_2) \to k(C_1)$ entre los campos de funciones $k(C_2)$ y $k(C_1)$ mediante $\phi^*(f) = f \circ \phi$.

Puesto que ϕ no es constante, por el teorema 2.1, ϕ es suprayectiva, por lo que ϕ^* es inyectiva. Además, ϕ^* es un morfismo de campos que deja fijo al campo k. Por lo anterior ya podemos suponer que $k(C_1)$ es una extensión de $\phi^* k(C_2)$, y el teorema siguiente nos da una caracterización de tal extensión.

Teorema 2.2. *Sean C_1/k y C_2/k dos curvas y $\phi : C_1 \to C_2$ un morfismo de curvas no constante. Entonces $k(C_1)$ es una extensión finita de $\phi^* k(C_2)$.*

Demostración. Usando ϕ^* podemos pensar que se tiene la inclusión de campos $k(C_2) \subseteq k(C_1)$. Ambos campos son extensiones finitamente generadas y de grado de trascendencia 1 sobre k. De la torre de campos siguiente

$$\begin{array}{c} k(C_1) \\ | \\ k(C_2) \\ | \\ k \end{array}$$

se sigue que $\operatorname{gr}\operatorname{tr}(k(C_1)/k) = \operatorname{gr}\operatorname{tr}(k(C_2)/k) + \operatorname{gr}\operatorname{tr}(k(C_1)/k(C_2))$ y, ya que $\operatorname{gr}\operatorname{tr}(k(C_1)/k) = \operatorname{gr}\operatorname{tr}(k(C_2)/k) = 1$, se tiene que $\operatorname{gr}\operatorname{tr}(k(C_1)/k(C_2)) = 0$. Por lo tanto la extensión es algebraica y, puesto que las extensiones son finitamente generadas sobre k, se tiene que $k(C_1)/k(C_2)$ es finita. □

Con base en los Teoremas 2.1 y 2.2 se tiene la definición siguiente.

Definición 2.3. *Sea $\phi : C_1 \to C_2$ un morfismo de curvas definidas sobre k. Si ϕ es constante se define el grado de ϕ, que denotaremos por $\operatorname{gr}(\phi)$, igual a 0. Si ϕ no es constante diremos que ϕ es finito y se define el grado de ϕ como:*

$$\operatorname{gr}(\phi) = [k(C_1) : \phi^* k(C_2)]$$

Decimos que ϕ es separable si $k(C_1)/\phi^* k(C_2)$ es separable, y el grado de separabilidad de ϕ, denotado por $\operatorname{gr}_s \phi$, es el grado de separabilidad de $k(C_1)/\phi^* k(C_2)$.

Definición 2.4. *Sea C una curva. El espacio de formas diferenciales (meromorfas) en C, denotado por Ω_C, es el $\overline{k}(C)$-espacio vectorial generado por los símbolos de la forma dx para $x \in \overline{k}(C)$, donde $\overline{k}$ es una cerradura algebraica de k, que satisfacen las relaciones siguientes:*

(1) $d(x+y) = dx + dy$ para todo $x, y \in \overline{k}(C)$.

(2) $d(xy) = xdy + ydx$ para todo $x, y \in \overline{k}(C)$.

(3) $da = 0$ para cada $a \in \overline{k}$.

Sean C_1 y C_2 dos curvas y $\varphi : C_1 \to C_2$ un morfismo no constante. Entonces la función natural $\varphi^* : \overline{k}(C_2) \to \overline{k}(C_1)$ induce una función $\varphi^* : \Omega_{C_2} \to \Omega_{C_1}$ dada por:

$$\varphi^*\Big(\sum f_i\, dx_i\Big) = \sum (\varphi^* f_i)\, d(\varphi^* x_i). \qquad (*)$$

El teorema siguiente, cuya demostración puede verse en [3] capítulo II proposición 4.2, enuncia algunas propiedades del espacio de formas diferenciales sobre una curva C.

Teorema 2.5. *Sea C una curva. Entonces:*

(1) Ω_C es un $\overline{k}(C)$-espacio vectorial de dimensión 1.

(2) Sea $x \in \overline{k}(C)$. Entonces $dx \in \overline{k}(C)$ es una base para Ω_C si y sólo si $\overline{k}(C)/\overline{k}(x)$ es una extensión finita separable. Aquí $\overline{k}(x)$ denota el campo de funciones racionales en x.

Proposición 2.6. *Sean C_1, C_2 curvas y $\phi : C_1 \to C_2$ un morfismo no constante. Entonces ϕ es separable si y sólo si la función $\varphi^* : \Omega_{C_2} \to \Omega_{C_1}$ es inyectiva.*

Demostración. Por el teorema 2.5 se puede escoger un $y \in \overline{k}(C_2)$ tal que $\{dy\}$ es una base del $\overline{k}(C_2)$-espacio vectorial Ω_{C_2} y $\overline{k}(C_2)/\overline{k}(y)$ es separable. Ahora $\phi^* : \overline{k}(C_2) \to \overline{k}(C_1)$ es un $\overline{k}$-monomorfismo, por lo que $\phi^*\overline{k}(C_2)$ es separable sobre $\phi^*\overline{k}(y) = \overline{k}(\phi^* y)$, esta última igualdad por que ϕ^* es un $\overline{k}$-monomorfismo.

Se afirma que $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ es inyectiva si y sólo si $d(\phi^* y) \neq 0$. Para ver esto supongamos que ϕ^* es inyectiva; por $(*)$ se tiene que $\phi^*(dy) = d(\phi^* y)$ y puesto que $dy \neq 0$, ya que ϕ^* inyectiva, se tiene que $d(\phi^* y) \neq 0$. Recíprocamente supongamos que $d(\phi^* y) \neq 0$ y sea $f \in \Omega_{C_2}$ tal que $\phi^*(f) = 0$. Entonces $f = \eta dy$, con $\eta \in \overline{k}(C_2)$, así $\phi^*(f) = \phi^*(\eta) d(\phi^* y)$, por $(*)$. Como ϕ^* es un monomorfismo de campos se sigue que $\eta = 0$ por lo que $f = 0$. Con esto la afirmación queda completamente probada.

Ahora, $d(\phi^* y) \neq 0$ si y sólo si $d(\phi^* y)$ es una base para Ω_{C_1}, por el teorema 2.5 (1), y $d(\phi^* y)$ es base de Ω_{C_1} si y sólo si $\overline{k}(C_1)/\overline{k}(\phi^* y)$ es separable, por el teorema 2.5 (2).

Puesto que $\overline{k}(\phi^* y) \subseteq \phi^*\overline{k}(C_2) \subseteq \overline{k}(C_1)$ y $\phi^*\overline{k}(C_2)/\overline{k}(\phi^* y)$ es separable, entonces $\overline{k}(C_1)/\overline{k}(\phi^* y)$ es separable si y sólo si $\overline{k}(C_1)/\phi^*\overline{k}(C_2)$ es separable. Por lo tanto $\overline{k}(C_1)/\phi^*\overline{k}(C_2)$ es separable si y sólo si ϕ^* es inyectiva. □

3. Curvas elípticas

Una *curva elíptica* sobre un campo k es un par (E, O), donde E es una curva de género 1 definida sobre k, y $O \in E$ es un punto distinguido de E y con coordenadas en k.

Ejemplo 3.1.

Sea K un campo, de característica distinta de 2. La curva

$$y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

donde los α_i son distintos entre sí, es una curva elíptica, ya que por [3] capítulo II ejemplo 5.7, tal curva tiene género 1 (ver la figura siguiente de una curva elíptica en $\mathbb{C}$, aunque solo veamos la parte real de tal curva, aquí $\alpha_1 = -1$, $\alpha_2 = 0$ y $\alpha_3 = 1$.)
Una curva elíptica E se puede identificar con una curva dada por una ecuación de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

con coeficientes en K, ver [3] capítulo III proposición 3.1. Una diferencial importante asociada a tal curva elíptica

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

se le llama *la diferencial invariante* asociada a la ecuación de Weierstrass E.

La estructura de grupo. Sea E una curva elíptica con un punto base O, dos puntos $P, Q \in E$ y L la recta que une a P y Q si $P \neq Q$ y si $P = Q$, entonces L es la recta tangente a E en P. Sea R el tercer punto de intersección de L con E, que existe por el teorema de Bezout. Sea $\tilde{L}$ la recta que une a O con R. Entonces $R' = P \oplus Q$ es el tercer punto dado por la intersección de $\tilde{L}$ con E, que existe gracias al teorema de Bezout (ver la figura (1)). Se demuestra que, bajo esta operación, E es un grupo abeliano, ver, por ejemplo, [3] capítulo III proposición 2.2.

Definición 3.2. *Sean E_1 y E_2 curvas elípticas. Una isogenia entre E_1 y E_2 es un morfimo de curvas $\phi : E_1 \to E_2$ tal que $\phi(O_1) = O_2$, donde O_1 y O_2 son los puntos distinguidos de E_1 y E_2, respectivamente. Diremos que E_1 y E_2 son isógenas si existe una isogenia $\phi : E_1 \to E_2$ tal que $\phi(E_1) \neq O$, y así, por el teorema 2.1, ϕ es suprayectiva.*

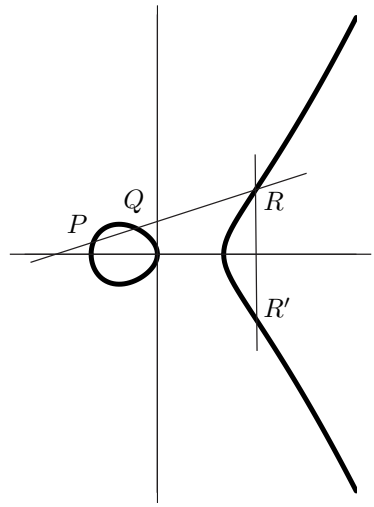

Figura 1: La operación de grupo en una curva elíptica

Ejemplo 3.3.

Sea $m \in \mathbb{Z}$ y E una curva elíptica. Se define la isogenia *multiplicación* por m, $[m] : E \to E$ de la manera siguiente:

$$[m](P) = P + \ldots + P \,(m\text{-veces}).$$

Ejemplo 3.4.

El morfismo de Frobenius. Sea K un campo de característica $p > 0$ y $q = p^r$, r un número natural. Si E/K es una curva elíptica dada por una ecuación de Weierstrass C, $E^{(q)}/K$ es la curva definida por el ideal $I(E^{(q)})$ generado por

$$\{f^{(q)} \mid f \in I(C)\}$$

donde $f(q)$ es el polinomio cuyos coeficientes son los coeficientes de f elevados a la potencia q-ésima y el *morfismo de Frobenius*, $\phi_q : E \to E^{(q)}$, es el dado por

$$(x, y) \mapsto (x^q, y^q)$$

Aquí $E^{(q)}$ está dada por una ecuación de Weierstrass y se puede probar, ver [3] capítulo III ejemplo 4.6, que $E^{(q)}$ es una curva elíptica. En particular si $K = \mathbb{F}_q$, entonces el morfismo potencia q-ésima es la identidad por lo que $E^{(q)} = E$ y ϕ_q es un endomorfismo de E, llamado

el *endomorfismo de Frobenius*. Nótese que los puntos fijos del endomorfismo de Frobenius son los puntos de E con coordenadas en K, es decir, el núcleo del morfismo $1 - \phi_q : E \to E$ consiste de tales puntos y sólo ellos.
Puede mostrarse, ver por ejemplo [3] capítulo III teorema 4.8, que si E es una curva elíptica y $\phi : E \to E$ es una isogenia, entonces ϕ define un morfismo (endomorfismo) del grupo abeliano E en sí mismo. El teorema siguiente nos da información sobre la cardinalidad de las fibras de ϕ.

Teorema 3.5. *Sean E_1 y E_2 curvas elípticas y $\phi : E_1 \to E_2$ una isogenia entre ellas, no constante. Entonces para todo $Q \in E_2$, excepto un número finito, se tiene que $N(\phi^{-1}(Q)) = \mathrm{gr}_s\, \phi$.*

Una demostración del teorema anterior puede encontrarse en [3] capítulo II proposición 2.6.

Proposición 3.6. *Sean E_1 y E_2 curvas elípticas y $\phi : E_1 \to E_2$ una isogenia entre ellas no constante. Entonces si ϕ es separable se tiene que:*

$$N(\ker(\phi)) = \mathrm{gr}\, \phi.$$

Demostración. Por el teorema 3.5 sabemos que $N(\phi^{-1}(Q)) = \mathrm{gr}_s\, \phi$ excepto para un número finito de puntos Q en E_2, además como ϕ es separable se tiene que $\mathrm{gr}\, \phi = \mathrm{gr}_s\, \phi$. Si P y P_1 son dos puntos de E_2, puesto que ϕ no es constante, por el teorema 2.1 existe un $R \in E_1$ tal que $\phi(R) = P_1 - P$. De esta manera definimos una función $\psi : \phi^{-1}(P) \to \phi^{-1}(P_1)$ como $\psi(S) = S + R$. Obsérvese que $\phi(S) = P$ y $\phi(R) = P_1 - P$. De este modo $\phi(\psi(S)) = \phi(S) + \phi(R) = P$, es decir, ψ está bien definida.

Si $S_1, S_2 \in E_1$ cumplen que $\psi(S_1) = \psi(S_2)$, se tiene que $R + S_1 = R + S_2$ por lo que $S_1 = S_2$ y así ψ es inyectiva. Sea $P_3 \in \phi^{-1}(P_1)$; notemos que $P_3 - R \in \phi^{-1}(P)$ y que $\psi(P_3 - R) = P_3$ por lo que ψ es suprayectiva. Por lo tanto para todo $Q \in E_2$ se tiene que $N(\phi^{-1}(Q)) = \mathrm{gr}_s\, \phi$, en particular $\ker(\phi) = \phi^{-1}(0)$ y con esto termina la demostración. □

Para la demostración del teorema siguiente consultar [3] capítulo III teorema 5.2.

Teorema 3.7. *Sean E y E' curvas elípticas, ω una diferencial invariante de E, y $\phi, \psi : E' \to E$ dos isogenias. Entonces*

$$(\phi + \psi)^*(\omega) = \phi^*(\omega) + \psi^*(\omega)$$

Corolario 3.8. *Sea ω una diferencial invariante de una curva elíptica E y sea m un entero. Entonces*

$$[m]^*(\omega) = m\omega$$

Demostración. El corolario es cierto para $m = 0$ y $m = 1$. Si en el teorema 3.7 ponemos $\phi = [m]$ y $\psi = [1]$ se obtiene que

$$[m+1]^*\omega = [m]^*\omega + \omega$$

así, por inducción, obtenemos el resultado deseado. □

Proposición 3.9. *Sean E una curva elíptica definida sobre $\mathbb{F}_q$, $q = p^l$, $\phi : E \to E$ el morfismo de Frobenius y $m, n \in \mathbb{Z}$. Entonces, el morfismo $m+n\phi : E \to E$ es separable si y sólo si $p \nmid m$. En particular $1 - \phi$ es separable.*

Demostración. Sea ω una diferencial invariante en E. Por la proposición 2.6, un morfismo $\psi : E \to E$ es separable si y sólo si $\psi^*(\omega) \neq 0$, es decir si y sólo si $\psi^* : \Omega_E \to \Omega_E$ es inyectiva. Considere el morfismo $\psi = m + n\phi$. Usando el teorema 3.7 y el corolario 3.8, se obtiene que:

$$(m + n\phi)^*(\omega) = m^*(\omega) + (n\phi)^*(\omega) = m\omega + n\phi^*\omega$$

Pero $\phi^*(\omega) = 0$, puesto que $\phi^* dx = d(x^q) = qdx^{q-1} = 0$. Entonces;

$$(m + n\phi)^*(\omega) = m\omega$$

Ahora $m\omega = 0$ si y sólo si $p \mid m$, ya que por el teorema 2.5 se tiene que Ω_E es un $\overline{\mathbb{F}_q}(E)$- espacio vectorial, de dimensión 1, además $\overline{\mathbb{F}_q}(E)$ tiene característica q y, ciertamente, $\omega \neq 0$ por lo que ω es una base de Ω_E, de aquí se sigue nuestra afirmación ya que $(m + n\phi)^*(\omega) \neq 0$ si y sólo si $p \nmid m$. □

4. Las conjeturas de Weil

Probaremos ahora las conjeturas de Weil, en el caso de una curva elíptica. Para empezar sea ℓ un número primo distinto de $\mathrm{car}(K)$, donde K es un campo finito. Se recuerda que se tiene una representación $\mathrm{End}(E) \to \mathrm{End}(T_\ell(E))$ (donde T_ℓ es el *módulo de Tate* de E) dada por

$$\psi \mapsto \psi_\ell$$

ver [3] capítulo III sección 7 y, en esta misma sección proposición 7.1, se tiene que $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ como $\mathbb{Z}_\ell$-módulo. Así es posible escribir a ψ_ℓ como una matriz 2×2, con coeficientes en $\mathbb{Z}_\ell$ y se tiene que

$$\det(\psi_\ell), \mathrm{Tr}\,(\psi_\ell) \in \mathbb{Z}_\ell.$$

En la proposición siguiente aparece el *módulo de Tate* de K, $T_\ell(\mu)$, cuya definición puede verse en [3], p.91.

Proposición 4.1. *Si $\psi \in \mathrm{End}(E)$, entonces*

$$\det(\psi_\ell) = \mathrm{gr}(\psi) \text{ y } \mathrm{Tr}\,(\psi_\ell) = 1 + \mathrm{gr}(\varphi) - \mathrm{gr}(1-\varphi)$$

En particular, $\det(\psi_\ell)$ *y* $\mathrm{Tr}\,(\psi_\ell)$ *son enteros e independientes de ℓ.*

Demostración. Sea v_1, v_2 una $\mathbb{Z}_\ell$-base para $T_l(E)$, y escribamos la matriz de ψ_ℓ para esta base

$$\psi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Usando el apareamiento de Weil, alternante, no degenerado, (ver [3] capítulo III proposición 8.3)

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$$

se tiene que

$$\begin{aligned} e(v_1, v_2)^{\mathrm{gr}(\psi)} &= e((\mathrm{gr}(\psi))v_1, v_2) \\ &= e(\widehat{\psi}_l \psi_l v_1, v_2) \qquad (1) \\ &= e(\psi_\ell v_1, \psi_\ell v_2) \qquad (2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} \\ &= e(v_1, v_2)^{\det(\psi_\ell)} \end{aligned}$$

la igualdad (1) es por [3] capítulo III proposición 6.1(a) y la igualdad (2) es por [3] capítulo III proposición 8.3 y proposición 6.2(f). Puesto que e es no degenerado, se sigue que $\mathrm{gr}(\psi) = \det(\psi_\ell)$. Finalmente para una matriz A de tamaño 2×2, se tiene que:

$$\mathrm{Tr}\,(A) = 1 + \det(A) - \det(1 - A).$$

y de aquí se sigue la última afirmación.[1] □

[1] donde 1 en $\det(1 - A)$ denota la matriz identidad.

Considere ahora el morfismo de Frobenius $\phi : E \to E$. Por el ejemplo 3.4 y las proposiciones 3.6 y 3.9

$$N(E(K)) = \mathrm{gr}(1 - \phi).$$

De modo análogo, para cada $n \geq 1$ tenemos que:

$$N(E(K_n)) = \mathrm{gr}(1 - \phi^n).$$

De la proposición 4.1, el polinomio característico de ϕ_ℓ tiene coeficientes enteros, y este polinomio se puede factorizar sobre los complejos, es decir:

$$\det(T - \phi_\ell) = T^2 - \mathrm{Tr}\,(\phi_\ell)T + \det(\phi_\ell) = (T - \alpha)(T - \beta)$$

Además, puesto que para cada número racional $\frac{m}{n}$ se tiene que:

$$\det\left(\frac{m}{n} - \phi_\ell\right) = \frac{\det(m - n\phi_\ell)}{n^2} = \frac{\mathrm{gr}(m - n\phi)}{n^2} \geq 0$$

se sigue que el polinomio cuadrático $\det(T - \phi_\ell)$ tiene una raíz doble o raíces complejas conjugadas. De esto se sigue que $|\alpha| = |\beta|$, y ya que

$$\alpha\beta = \det(\phi_\ell) = gr(\phi) = q$$

se concluye que $|\alpha| = |\beta| = \sqrt{q}$ y así el polinomio característico de ϕ_ℓ^n esta dado por:

$$\det(T - \phi_\ell^n) = (T - \alpha^n)(T - \beta^n).$$

De aquí se sigue que:

$$\begin{aligned} N(E(K_n)) &= \mathrm{gr}(1 - \phi^n) \\ &= \det(1 - \phi_\ell^n) \\ &= 1 - \alpha^n - \beta^n + q^n. \end{aligned}$$

El resultado principal es:

Teorema 4.2 (Conjeturas de Weil para curvas elípticas)**.** *Sea K un campo con q elementos E/K una curva elíptica. Entonces existe un número entero a tal que*

$$Z_{E/K}(T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}.$$

Además

$$Z_{E/K}(\frac{1}{q}T) = Z_{E/K}(T)$$

y

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$$

con $\mid \alpha \mid = \mid \beta \mid = \sqrt{q}$.

Demostración. Calculamos la serie:

$$\begin{aligned}\log Z_{E/K}(T) &= \sum N(E(K_n))T^n/n \\ &= \sum (1 - \alpha^n - \beta^n + q^n)T^n/n \\ &= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) \\ &\quad - \log(1-qT).\end{aligned}$$

Por lo tanto

$$Z_{E/K}(T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}.$$

Así la función $Z_{E/K}$ tiene la forma deseada, ya que por las observaciones anteriores al teorema, vemos que α y β son complejos conjugados, con valor absoluto $\sqrt{q}$, además

$$a = \alpha + \beta = \mathrm{Tr}\,(\phi_\ell) = 1 + q - \mathrm{gr}(1 - \phi) \in \mathbb{Z}.$$

□

Notemos que $\mathrm{gr}(1-\phi) = N(E(K))$, es decir, para obtener a hay que contar el número de soluciones de la curva elíptica sobre el campo K.

Observaciones finales. Para el caso general de una variedad proyectiva lisa sobre un campo finito, las conjeturas de Weil fueron demostradas por los matemáticos siguientes:

- La racionalidad de la función zeta fue demostrada por B. Dwork en 1960 usando métodos de análisis p-ádico. Una demostración más acorde con lo conjeturado por Weil es la de Grothendieck de 1965 y que usa la cohomología étale de un esquema. Así los fundamentos para la geometría algebraica, propuestos por Grothendieck, son un marco de referencia más adecuado para establecer

y probar tales conjeturas, pues permitió generalizar métodos de la topología algebraica en la geometría algebraica, por ejemplo una generalización del teorema de punto fijo de Lefschetz, usando cohomología ℓ-ádica, a pesar de que en una variedad abstracta no se tenga una topología fina, como en el caso complejo. Para el caso de una curva de género arbitrario, generalizando el ejemplo de una curva elíptica, puede verse la tesis de maestría del autor [2].

- La existencia de la ecuación funcional, para cuya demostración se requirió la existencia de un teorema de dualidad de Poincaré para variedades algebraicas no singulares, en esta parte se usa no sólo la cohomología étale sino también la cohomología ℓ-ádica

- La parte más difícil de las conjeturas de Weil, el análogo de la hipótesis de Riemann, fue demostrado para una curva arbitraria por Weil y el caso general, fue demostrado por Pierre Deligne en 1974 completando el programa iniciado por Grothendieck.

Referencias

[1] Hartshorne, R., *Algebraic Geometry*. Springer-Verlag, New York, 1977.

[2] Sánchez Mirafuentes, M., *Racionalidad de la función zeta de una curva*. Tesis de Maestría en Ciencias. Universidad Autónoma Metropolitana-I., México, D. F., 2009.

[3] Silverman J. H., *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

Dirección del autor
Marco Antonio Sánchez Mirafuentes
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Av. San Rafael Atlixco 186, Col. Vicentina
Del. Iztapalapa, C.P. 09340 México, D.F.