

les conjectures de Weil pour les courbes elliptiques sur les corps finis

Théorème: Soient k un corps fini à q éléments et E une courbe elliptique sur k . Alors il existe un entier $a \in \mathbb{Z}$ tel que

$$Z(E/k, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$

De plus, le polynôme $1 - aT + qT^2$ est égal à $(1 - \alpha T)(1 - \beta T)$ avec $|\alpha| = |\beta| = \sqrt{q}$

et $Z(E/k, T) = Z(E/k, \frac{1}{qT})$.

La démonstration repose sur les propriétés du module de Tate de E . Soit donc ℓ un nombre premier distinct de $\text{car } k$ et

$$T_\ell(E) = \varprojlim_n E[\ell^n] \simeq \mathbb{Z} \times \mathbb{Z}_\ell$$

le module de Tate ℓ -adique de E . Rappelons que ℓ -on a une injection

$$\begin{aligned} \text{End}(E) &\hookrightarrow \text{End}(T_\ell(E)) \\ \varphi &\longmapsto \varphi_\ell \end{aligned}$$

Proposition: Soit $\varphi \in \text{End}(E)$ une isogénie. Alors

$$\det(\varphi_E) = \deg(\varphi)$$

$$\text{tr}(\varphi_E) = 1 + \deg(\varphi) - \deg(\text{Id} - \varphi)$$

En particulier, les éléments $\det(\varphi_E), \text{tr}(\varphi_E) \in \mathbb{K}_E$ sont dans $\mathbb{Z}$ et indépendants de E .

Preuve: Soit $\{v_1, v_2\}$ une $\mathbb{K}_E$ -base de $T_E(E)$.
La matrice de φ_E dans cette base est $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
On utilise l'acupuncteur de Weil

$$e: T_E(E) \times T_E(E) \rightarrow T_E(\mathbb{P}^1)$$

pour calculer:

$$\begin{aligned} e(v_1, v_2)^{\deg \varphi} &= e([\deg \varphi]v_1, v_2) \\ &= e(\widehat{\varphi}_E \varphi_E v_1, v_2) \\ &= e(\varphi_E v_1, \widehat{\widehat{\varphi}_E} v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad - bc} \\ &= e(v_1, v_2)^{\det(\varphi_E)} \end{aligned}$$

et puisque l'acupuncteur est un dégré, on en déduit $\deg \varphi = \det(\varphi_E)$.

(2)

La dernière égalité suit alors de

$$\begin{aligned}\operatorname{tr}(A) &= 1 + \det(A) - \det(\operatorname{Id} - A) \\ &= 1 + ad - bc - (1-a)(1-d) + bc \\ &= a + d\end{aligned}\quad \square$$

Soit $\varphi_q: E \rightarrow E$ la q -ième puissance du morphisme de Frobenius, de sorte que

$$|E(K_n)| = \deg(1 - \varphi^n) \quad \text{pour tout } n \geq 1$$

D'après le lemme,

$$\begin{aligned}\det(T - \varphi_e) &= T^2 - \operatorname{tr}(\varphi_e)T + \det(\varphi_e) \\ &= (T - \alpha)(T - \beta)\end{aligned}$$

pour des nombres complexes $\alpha, \beta \in \mathbb{C}$ (on utilise que c'est un polynôme à coefficients entiers).

En ailleurs,

$$\det\left(\frac{m}{n}\operatorname{Id} - \varphi_e\right) = \frac{\det(m\operatorname{Id} - n\varphi_e)}{n^2} = \frac{\deg(m\operatorname{Id} - n\varphi_e)}{n^2}$$

est ≥ 0 pour tout $m/n \in \mathbb{Q}$, ce qui veut dire que les racines de $\det(T - \varphi_e)$ sont soit des nombres réels soit des nombres complexes conjugués soit se suivent doublement.

On en déduit $|\alpha| = |\beta|$, puis $\alpha\beta = \det(\varphi_e) = \deg(\varphi_e) = q$
 c'est-à-dire $|\alpha| = |\beta| = \sqrt{q}$.

le polynôme caractéristique de φ^n est

$$\det(T - \varphi^n) = (T - \alpha^n)(T - \beta^n),$$

comme on le voit par exemple en utilisant la forme de Jordan de la matrice de φ .

On a donc :

$$\begin{aligned} |E(K_n)| &= \deg(1 - \varphi^n) \\ &= \det(1 - \varphi^n) \\ &= (1 - \alpha^n)(1 - \beta^n) \\ &= 1 - \alpha^n - \beta^n + \alpha^n \beta^n \end{aligned}$$

Démonstration du Théorème : calculons

$$\begin{aligned} \log Z(E/K, T) &= \sum_{n=1}^{\infty} |E(K_n)| \frac{T^n}{n} \\ &= \sum_{n=1}^{\infty} (1 - \alpha^n - \beta^n + \alpha^n \beta^n) \frac{T^n}{n} \end{aligned}$$

$$\begin{aligned} &= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) \\ &\quad - \log(1-\alpha\beta T) \end{aligned}$$

$$\text{d'où } Z(E/K, T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-\alpha\beta T)}$$

(3)

L'entier $a \in \mathbb{Z}$ dans l'anneau est

$$a = \alpha + \beta = \text{tr}(\varphi_1) = 1 + q - \deg(\text{Id} - \varphi) \in \mathbb{Z}.$$

Enfin, pour l'équation fonctionnelle, on calcule

$$\begin{aligned} Z(E/K, \frac{1}{qT}) &= \frac{(1 - \frac{\alpha}{qT})(1 - \frac{\beta}{qT})}{(1 - \frac{1}{qT})(1 - \frac{q}{qT})} \\ &= \frac{(qT - \alpha)(qT - \beta)}{(qT - 1)(qT - q)} \\ &= \frac{q(qT^2 - (\alpha + \beta)T + 1)}{q(1 - T)(1 - qT)} \\ &= Z(E/K, T) \end{aligned} \quad \square$$

Remarque: avec le changement de variable $T = q^{-s}$, la fonction zêta prend la forme

$$J_{E/K}(s) = \frac{1 - a q^{-s} + q^{1-2s}}{(1 - q^{-s})(1 - q^{1-s})}$$

l'équation fonctionnelle

$$J_{E/K}(1-s) = J_{E/K}(s)$$

et si $J_{E/K}(s) = 0$ alors $|q^s| = \sqrt{q}$, c'est-à-dire

line $\operatorname{Re}(v) = \frac{1}{2}$. C'est l'énoncé de l'hypothèse
de Riemann.