Weil Conjectures for Elliptic Curves

Tianyang WANG

Sorbonne Université

12 juin 2024

Table des matières

Riemann Hypothesis

Conjecture (Riemann Hypothesis)

The Riemann zeta function is defined as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Then, the non-trivial zeros of the Riemann zeta function all have a real part equal to 1/2.

Zeta Function for Projective Varieties

Definition (Zeta Function for Projective Varieties)

Let V be a projective variety over $\mathbb{F}_q$. The zeta function of V is the formal series

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty}(\#V(\mathbb{F}_{q^n}))\frac{T^n}{n}\right) \in \mathbb{Q}[[T]],$$

where $\exp(F(T))$ denotes the formal series $\sum_{i=0}^{\infty} F(T)^i/i!$ for a formal series without a constant term.

Weil Conjecture

Taking a change of variable $T = q^{-s}$, we define the zeta function as:

$$\zeta(s) = Z(E/\mathbb{F}_q; q^{-s}).$$

Theorem (Weil Conjecture (Part))

(Deligne 1973) Let V be a smooth projective variety over $\mathbb{F}_q$ of dimension n. The Riemann hypothesis holds for the zeta function. That is, the zeros of the zeta function all have a real part equal to $1/2$.

Main Theorem

GOAL: Weil Conjectures for Elliptic Curves, in other words:

Theorem (Main Theorem)

(Hasse) Let E be an elliptic curve over $\mathbb{F}_q$. Then there exists $a \in \mathbb{Z}$ such that

$$Z(E/\mathbb{F}_q; T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} \text{ (Rationality)},$$

$$Z(E/\mathbb{F}_q; \frac{1}{qT}) = Z(E/\mathbb{F}_q; T) \text{ (Functional Equation)},$$

and

$$1 - aT + qT^2 = (1-\alpha T)(1-\beta T) \text{ with } |\alpha| = |\beta| = \sqrt{q} \text{ (Riemann Hypothesis)}.$$

Table des matières

Projective Curve

Definition (Projective Curve)

Let the projective plane $\mathbb{P}^2(k)$ be the quotient $(k^3\backslash\{0\})/k^\times$. The class of a point $\tilde{P} = (x_0, x_1, x_2) \in \mathbb{A}^3$ is denoted $P := [x_0, x_1, x_2]$ in $\mathbb{P}^2(k)$. A projective curve is a closed subvariety of a projective plane. It can be written as

$$V(f) := \{[x_0, x_1, x_2] \in \mathbb{P}^2 : f([x_0, x_1, x_2]) = 0\}$$

where f is a homogeneous polynomial in $k[T_0, T_1, T_2]$.

Why projective?

Example (Weierstrass Equation)

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Anti-Equivalence

Theorem

There is an anti-equivalence between the two categories:

$$\left[\begin{array}{cc} \textit{Objects:} & \textit{extensions of } k \\ & \textit{of finite type and} \\ & \textit{of transcendence} \\ & \textit{degree 1} \\ \textit{Morphisms:} & \textit{field extensions} \end{array}\right] \leftrightsquigarrow \left[\begin{array}{cc} \textit{Objects:} & \textit{smooth} \\ & \textit{projective} \\ & \textit{curves} \\ \textit{Morphisms:} & \textit{dominant} \\ & \textit{morphisms} \end{array}\right]$$

Anti-Equivalence

Démonstration.

(Idea)

- $\rightsquigarrow$: Just take the function field.
- $\leftarrow$: for K/k, a finite type extension of transcendence degree 1, suppose

$$C_K := \{\text{valuation of } K/k \ v : K^\times \twoheadrightarrow \mathbb{Z}\}$$

  endowed with the cofinite topology. We can give a sheaf structure on C_K and verify that it is indeed a smooth projective curve.

$\square$

Elliptic Curve

Definition (Elliptic Curve)

An elliptic curve over k is a pair (E,O) where E is a smooth projective curve of genus 1 defined over k and O is a k-rational point.

Degree

Definition (Degree, Algebraic Side)

Let $\varphi : C \to C'$ be a dominant morphism. We define its degree $deg(\varphi) := [k(C) : k(C')]$, and its separable degree $deg_s(\varphi) := [k(C)_{sep} : k(C')] = [k(C) : k(C')]_s$.

Lemma (Geometric Side)

Let $\varphi : C \to C'$ be a morphism between two smooth projective curves, then for any $Q \in C'$,

$$deg(\varphi) = \sum_{P \in \varphi^{-1}(Q)} e_P(\varphi)$$

Table des matières

Proposition

Proposition

Let $\mathbb{F}_{q^n}$ denote the extension of $\mathbb{F}_q$ of degree n, and $E(\mathbb{F}_{q^n})$ the $\mathbb{F}_{q^n}$-rational points of E. We have

$$\#E(\mathbb{F}_{q^n}) = 1 - \alpha^n - \beta^n + q^n$$

where α, $\beta \in \mathbb{C}$ are two complex conjugate numbers with ordinary norm $\sqrt{q}$ in $\mathbb{C}$.

Proof of the Main Theorem Assuming the Previous Proposition.

$$\log Z(E/\mathbb{F}_q; T) = \sum_{n=1}^{\infty}(1-\alpha^n-\beta^n+q^n)\frac{T^n}{n}$$
$$= -\log(1-T)+\log(1-\alpha T)+\log(1-\beta T)$$
$$-\log(1-qT).$$

This implies that

$$Z(E/\mathbb{F}_q; T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

where α, $\beta \in \mathbb{C}$ are two complex conjugate numbers with ordinary norm $\sqrt{q}$ in $\mathbb{C}$ and

$$a := \alpha+\beta = Tr(\phi_\lambda) = 1+q-\deg(1-\phi) \in \mathbb{Z}.$$

We can verify that it is the desired form. $\square$

Weierstrass Equation

Lemma

Let (E,O) be an elliptic curve over k. There exists an embedding $\iota : E \hookrightarrow \mathbb{P}^2$ defined over k whose image is the curve defined by a Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Problems

- **Problem 1**: Is the morphism $id - \phi^n$ unramified?
  Solution: Use differentials.
- **Problem 2**: Write any elliptic curve in Weierstrass form.
  Solution: Use the Riemann-Roch theorem.
- **Problem 3**: Compute the degree.
  Solution: Use the Tate module.

Table des matières

Kähler Differential

Definition

Let $A \to B$ be a morphism of rings. We define the B-module $\Omega_{B/A}$ of Kähler differentials as the quotient of the B-module generated by the symbols dx, $x \in B$ by the relations $d(x+y) = dx + dy$, $d(xy) = xdy + ydx$, $dx = 0$ if $x \in A$. It is thus equipped with an A-linear map $x \mapsto dx$. We can also define it as:

$$\Omega_{B/A} := I/I^2, \text{where } I := \ker(B \otimes_A B \overset{mult}{\to} B),$$

in which case, $dx = (x \otimes 1 - 1 \otimes x) \mod I^2$.

We have the universal property: for any B-module M, we have the isomorphism

$$\mathrm{Hom}_B(\Omega_{B/A}, M) \overset{\simeq}{\to} \mathrm{Der}_A(B, M),$$

where an A-linear derivation on B is an A-module morphism $d : B \to M$ satisfying the Leibniz rule $d(fg) = fdg + gdf$.

Properties of Differential Modules

Lemma

We have the following properties for the module of differentials.

- *(i) If B is generated as an A-algebra by elements $x_1, \dots, x_n$, then $\Omega_{B/A}$ is generated by the dx_i as a B-module.*
- *(ii) If $B = A[X_1, \dots, X_n]$, then $\Omega_{B/A}$ is free over B with basis $dX_1, \dots, dX_n$.*
- *(iii) For $A \to B \to C$, we have an exact sequence*

$$C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to \Omega_{C/B} \to 0.$$

- *(iv) For L/K a finite type extension of k, the morphism $L \otimes_K \Omega_{K/k} \to \Omega_{L/k}$ is an isomorphism if and only if L/K is a separable extension.*

Examples

Example

- (i) Let $L = \mathbb{F}_p(X)$ and $K = \mathbb{F}_p(X^p)$. Since any $\mathbb{F}_p$-linear derivation of L is zero on K, by the universal property we have $\Omega_{L/K} = \Omega_{L/\mathbb{F}_p} = L \cdot dX$.
- (ii) Let L/K be a separable extension. For any $x \in L$, suppose f is a polynomial that annihilates x such that $f'(x) \neq 0$. Then we have $f(x) = 0$, and hence $0 = df(x) = f'(x)dx$. It follows that $dx = 0$. We conclude that $\Omega_{L/K} = 0$.

Meromorphic Differential on a Smooth Curve

Proposition

Let C be a smooth curve. We denote $\Omega_C := \Omega_{k(C)/k}$, called the space of meromorphic differentials on C.

- *(i) Ω_C is a $k(C)$-vector space of dimension 1.*
- *(ii) Let $\varphi : C \to C'$ be a non-constant morphism of elliptic curves. The extension $\varphi^* : k(C') \to k(C)$ induces a $k(C')$-linear map*

$$\Omega_{C'} \to \Omega_C, \sum f_i dx_i \mapsto \sum (\varphi^* f_i) d(\varphi^* x_i).$$

  This map is non-zero (and thus injective) if and only if φ is separable.

Démonstration.

(Proof of (ii)) We use (iii) and (iv) of the previous lemma. $\square$

Problem 1

Lemma

Let $\varphi : E_1 \to E_2$ be a non-constant morphism of varieties between two elliptic curves. If φ is non-constant, we have:
(i) $deg_i(\varphi) = e_P(\varphi)$ does not depend on P.
(ii) $deg_s(\varphi) = \#\varphi^{-1}(Q)$ for all $Q \in E_2$.

The Riemann-Hurwitz formula can be used to prove this.
Problem 1: Choose a non-zero differential $\omega \in \Omega_{C'}$. Since the Frobenius morphism ϕ is inseparable, we have $(id - \phi)^*\omega = \omega \neq 0$.

Table des matières

Divisor

Definition

Let C be a smooth curve. We denote $Div(C)$ the free abelian group generated by the points of C. If $D = \sum_P a_P[P]$ is a divisor, its degree $deg(D)$ is the integer $\sum_P a_P$. Let D,D' be two divisors, we say $D \leq D'$ if for all points $P \in C$, the coefficient of D is less than or equal to that of D'. We say D is effective if $D \geq 0$. Furthermore, we define a map

$$\text{div} : k(C)^{\times} \to Div(C), f \mapsto \sum_P v_P(f)[P].$$

Let $\ell(D)$ be the dimension of the k-vector space

$$\mathcal{L}(D) := \{f \in k(C) : \text{div}(f) + D \geq 0\}.$$

Example

Let C be a projective curve. If there exists $P \in C$ such that $\ell([P]) = 2$, then $C \simeq \mathbb{P}^1$.

Riemann-Roch Theorem

Theorem

Let C be a (smooth projective) curve. Then for any $D \in Div(C)$, we have

$$\ell(D) - \ell(K_C - D) = \deg(D) + 1 - g(C).$$

Note that $\deg(K_C) = 0$ for an elliptic curve. Using Riemann-Roch, we obtain the relationship between the number $\ell(D)$ of a divisor and its degree $\deg(D)$ as shown in the table below.

$\deg(D)$:	$\cdots$	-2	-1	0	1	2	3	$\cdots$
$\ell(D)$:	$\cdots$	0	0	0 or 1	1	2	3	$\cdots$

That is, $\ell(D)$ is determined by $\deg(D)$ except when $\deg(D) = 0$. But when $\deg(D) = 0$, $\ell(D) = 1$ if D is principal, and $\ell(D) = 0$ otherwise.

Weierstrass Equation

Démonstration.

Since O is a k-rational point, the divisor $3[O]$ is defined over k. By the corollary of Riemann-Roch, we have $\ell(2[O]) = 2$, $\ell(3[O]) = 3$. We can find $x \in \mathcal{L}(2[O]) \backslash \mathcal{L}([O])$, and $y \in \mathcal{L}(3[O]) \backslash \mathcal{L}(2[O])$. Then $\{1, x, y\}$ forms a k-basis of $\mathcal{L}(3[O])$ which provides an embedding $\iota : E \to \mathbb{P}^2$. To compute an equation, note that the family of 7 functions $\{y^2, x^3, yx, x^2, y, x, 1\}$ lives in $\mathcal{L}(6[O])$ whose dimension is 6. It follows that the family is k-linearly dependent. Moreover, note that the orders of pole at O of these functions are respectively 6,6,5,4,3,2,0, the families obtained by removing y^2 or x^3 are independent. Therefore, both terms must appear in the equation. After a reasonable multiplication, we can arrange the equation in the form where the coefficients of y^2 and x^3 are 1. Thus, $\iota(E)$ is included in a Weierstrass equation C. $\square$

Table des matières

Torsion Subgroup

Definition

Let E be an elliptic curve and $m \in \mathbb{Z}^{\times}$. We define the m-torsion subgroup

$$E[m] := \{P \in E : [m]P = 0\}.$$

Proposition

Let E be an elliptic curve and $m \in \mathbb{Z}^{\times}$ such that $\gcd(m, \mathrm{char}(k)) = 1$. Then we have

$$E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Tate Module

Definition (Tate Module)

Let E be an elliptic curve and λ a prime number. We have a projective system

$$\cdots \to E[\lambda^{n+1}] \xrightarrow{[\lambda]} E[\lambda^n] \to \cdots \to E[\lambda].$$

The (λ-adic) Tate module is the projective limit of this system

$$T_\lambda(E) := \varprojlim_n E[\lambda^n]$$

which is naturally a $\mathbb{Z}_\lambda$-module.

Structure of the Tate Module

Proposition

If $\lambda \neq \mathrm{char}(k)$, *we have*

$$T_\lambda(E) \simeq \mathbb{Z}_\lambda \times \mathbb{Z}_\lambda.$$

Démonstration.

We take the projective limit in the previous proposition. $\square$

Isogenies and Tate Modules

Let $\varphi : E_1 \to E_2$ be an isogeny between two elliptic curves, then φ induces a map $E_1[\lambda^n] \to E_2[\lambda^n]$, hence a ($\mathbb{Z}_\lambda$-linear) map between Tate modules

$$T_\lambda(E_1) \to T_\lambda(E_2).$$

We obtain a map

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_\lambda(E_1), T_\lambda(E_2))$$

and in particular for any elliptic curve,

$$\mathrm{End}(E) \to \mathrm{End}(T_\lambda(E)), \psi \mapsto \psi_\lambda$$

which is indeed a ring homomorphism. After choosing a $\mathbb{Z}_\lambda$-basis for $T_\lambda(E)$, we can write ψ_λ as a 2×2 matrix in $GL_2(\mathbb{Q}_\lambda)$.

Completion of the Proof

Proposition

Let E be an elliptic curve, $\psi \in \mathrm{End}(E)$ an endomorphism. Recall that we have a Tate module endomorphism $\psi_\lambda \in \mathrm{End}(T_\lambda(E))$. Then we have

$$\det(\psi_\lambda) = \deg(\psi)$$

and

$$\mathrm{Tr}(\psi_\lambda) = 1 + \deg(\psi) - \deg(1 - \psi).$$

In particular, $\det(\psi_\lambda)$ *and* $\mathrm{Tr}(\psi_\lambda)$ *do not depend on the choice of* λ.

Completion of the proof.
An example.

Bibliography

Jean-François Dat, *Variétés algébriques*, Link to document

Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer 2009.

Jean-François Dat, *Introduction aux courbes elliptiques*, Link to document