The University of Arizona, Tucson
College of Science
Department of Mathematics

The Weil Conjectures for Elliptic Curves

Math 596G - Research Tutorial Group - Fall 2020

Author: Gaurish Korpal *Advisor:* Brandon Levin

Abstract

In this report we discuss the proof of the Weil conjectures for elliptic curves [Sil09, §V.2]. We assume the knowledge of Galois theory [DF04, §14.9], commutative algebra [AM69, Chapter 9], algebraic number theory [Neu99, §I.8,12 and §IV.1,2], and algebraic varieties [Sha77, §III.5.6].

Contents

Notations

K	a perfect field, like $\mathbb{Q}, \mathbb{R}, \mathbb{Q}_p, \mathbb{F}_q$.
$\bar{K}$	a fixed algebraic closure of K, like $\mathbb{A}, \mathbb{C}, \mathbb{C}_p, \bigcup_{d\geq 1} \mathbb{F}_{q^d}$.
$G_{\bar{K}/K}$	the infinite Galois group of $\bar{K}/K$ given by $\varprojlim_L \mathrm{Gal}(L/K)$.
V	a projective variety[1], i.e. a projective algebraic set whose homogeneous ideal is a prime ideal in $\bar{K}[X_0, X_1, \ldots, X_n]$.
$V(K)$	the set of K-rational points of V, also described as the set $\{P \in V \ : \ \sigma(P) = P \ \forall \ \sigma \in G_{\bar{K}/K}\}$.
V/K	V is defined over K, i.e. the ideal of V is generated by polynomials in $K[X_0, X_1, \ldots, X_n]$.
$\bar{K}(V)$	the function field of V, i.e. the field of fractions corresponding to the coordinate ring of affine subvariety $V \cap \mathbb{A}^n$.

[1]We will write some inhomogeneous equations to describe V, with the understanding that V is the projective closure of the indicated affine variety.

$K(V)$	the function field of V/K.
$\bar{K}[V]_P$	the local ring of V at P.
$\mathfrak{m}_P$	the maximal ideal of $\bar{K}[V]_P$.
C	a curve, i.e. a projective variety of dimension one.
$\mathrm{ord}_P(f)$	valuation on $f \in \bar{K}[C]_P$ at a smooth point $P \in C$. It is defined as $\sup\{d \in \mathbb{Z} : f \in \mathfrak{m}_P^d\}$. We can extend it to $\bar{K}(C)$ by using $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$.
$\deg(\phi)$	degree of a rational map $\phi : C_1 \to C_2$ defined over K. If ϕ is constant then $\deg(\phi) = 0$, otherwise we have $\deg(\phi) = [K(C_1) : \phi^* K(C_2)] < \infty$ with $\phi^* : K(C_2) \to K(C_1)$ defined as $\phi^* f = f \circ \phi$.
$\deg_s(\phi)$	separable degree of extension of $K(C_1)/\phi^* K(C_2)$.
$\deg_i(f)$	inseparable degree of extension of $K(C_1)/\phi^* K(C_2)$.
$e_\phi(P)$	ramification index of a nonconstant rational map $\phi : C_1 \to C_2$ of smooth curves at point $P \in C_1$. If $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$ then $e_\phi(P) = \mathrm{ord}_P\left(\phi^* t_{\phi(P)}\right)$.
$\mathrm{Div}(C)$	divisor group of C, i.e. a free abelian group generated by points of C.
$\mathrm{Div}^0(C)$	subgroup of divisors of degree 0. It is defined as the set $\{D = \sum_{P \in C} n_P P \in \mathrm{Div}(C) \ : \ \sum_{P \in C} n_P = 0\}$.
$\mathrm{div}(f)$	the divisor associated to $f \in \bar{K}(C)^*$ when C is smooth. It is defined as $\sum_{P \in C} \mathrm{ord}_P(f) P$.
$\mathrm{Pic}^0(C)$	degree 0 part of the divisor class group of C. It is defined as the quotient of $\mathrm{Div}^0(C)$ by the subgroup of divisors of the form $\mathrm{div}(f)$ for some $f \in \bar{K}(C)^*$.
ℓ	a prime number different from $p = \mathrm{char}(K)$.
$\boldsymbol{\mu}_n$	the group of n^{th} roots of unity in $\bar{K}^*$
$T_\ell(\boldsymbol{\mu})$	the Tate module of the multiplicative group $\bar{K}^*$ defined as $\varprojlim_d \boldsymbol{\mu}_{\ell^d}$. As abstract group, it is isomorphic to $\mathbb{Z}_\ell$.

1 Introduction

1.1 Weil Conjectures

Let $\mathbb{F}_q$ be a finite field consisting q elements, such that q is a power of some prime interger p.

Definition 1.1 (Zeta function)**.** The zeta function of $V/\mathbb{F}_q$ is defined as

$$Z_{V/\mathbb{F}_q}(t) = \exp\left(\sum_{n=1}^{\infty} \left(\#V(\mathbb{F}_{q^n})\right) \frac{t^n}{n}\right)$$

where $\#V(\mathbb{F}_{q^n})$ is the number of points in V over $\mathbb{F}_{q^n}$.

Remark 1.1. By setting $t = q^{-s}$ we get

$$\zeta_{V/\mathbb{F}_q}(s) = \exp\left(\sum_{n=1}^{\infty} \left(\#V(\mathbb{F}_{q^n})\right) \frac{q^{-ns}}{n}\right)$$

Then, for example, when $V = \mathbb{P}^N$ we get the familiar looking zeta function

$$\zeta_{\mathbb{P}^N/\mathbb{F}_q}(s) = \prod_{j=0}^{N} \frac{1}{1 - q^{-(s-j)}}$$

Theorem 1.1 (Weil conjectures)**.** *Let $V/\mathbb{F}_q$ be a nonsingular[2] (or smooth) projectve variety of dimension N. Then its zeta function satisfies the following properties:*

1. *Rationality: $Z_{V/\mathbb{F}_q}(t) \in \mathbb{Q}(t)$ such that*

$$Z_{V/\mathbb{F}_q}(t) = \frac{p_1(t)p_3(t)\cdots p_{2N-1}(t)}{p_0(t)p_2(t)\cdots p_{2N}(t)}$$

   with each $p_j \in \mathbb{Z}[t]$, and $p_0(t) = 1 - t$, $p_{2N}(t) = 1 - q^N t$.

2. *Riemann hypothesis: For every $0 \le j \le 2N$, the polynomial $p_j(t)$ factors over $\mathbb{C}$ as*

$$p_j(t) = \prod_{i=1}^{b_j}(1 - \alpha_{ij}t)$$

   such that $|\alpha_{ij}| = q^{j/2}$.

3. *Functional equation:*

$$Z_{V/\mathbb{F}_q}\left(\frac{1}{q^N t}\right) = \pm q^{\frac{\chi(V)N}{2}} t^{\chi(V)} Z_{V/\mathbb{F}_q}(t)$$

   where $\chi(V)$ is the Euler characteristic[3] of V.

4. *Betti numbers: If $V/\mathbb{F}_q$ is the "good reduction" of a smooth projective variety $\tilde{V}$ defined over a number field embedded in $\mathbb{C}$, then the j^{th} Betti number[4] of the topological space $\tilde{V}(\mathbb{C})$ (complex points of $\tilde{V}$) equals the degree b_j of each p_j.*

1.2 Elliptic Curves

Definition 1.2 (Elliptic curve)**.** An elliptic curve is a pair (E, O), where E is a nonsingular curve of genus one and base point $O \in E$. Moreover, the elliptic curve E is defined over K, written E/K, if E is defined over K as a curve and $O \in E(K)$.

Remark 1.2. We generally denote the elliptic curve by E, the point O being understood.

Theorem 1.2. *Let E/K be an elliptic curve.*

1. *There exist functions $x, y \in K(E)$ such that the map*

$$\begin{aligned} \phi : E &\to \mathbb{P}^2 \\ P &\mapsto [x(P) : y(P) : 1] \end{aligned}$$

   gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

   with coefficients $a_1, \ldots, a_6 \in K$ and satisfying $\phi(O) = [0 : 1 : 0]$. The functions x and y are called Weierstrass coordinates for the elliptic curve E.

[2] That is, $\dim_{\bar{K}} \mathfrak{m}_P/\mathfrak{m}_P^2 = \dim(V)$ for every point $P \in V$.
[3] It is the intersection number of the diagonal with itself in the product $V \times V$ [Mil13, §II.26].
[4] It is defined using étale cohomology [Mil13, §I.1].

2. *Conversly, every smooth cubic curve C given by a Weierstrass equation (as above) is an elliptic curve defined over K with base points $O = [0 : 1 : 0]$.*

Proposition 1.1 (Geometric group law)**.** *Let $E \subset \mathbb{P}^2$ be an elliptic curve given by a Weierstrass equation. Then, we define addition $P \oplus Q$ of two points $P, Q \in E$ as follows:*

Let $L \subset \mathbb{P}^2$ be the line through P and Q (if $P = Q$, let L be the tangent line to E at P), and R be the third point of intersection of L with E. Then, let $L' \subset \mathbb{P}^2$ be the line through R and O. Then L' intersects E at R, O, and a third point denoted by $P \oplus Q$.

Then the following properties hold:

1. *The addition law makes E into an abelain group with identity element O.*

2. *Suppose E is defined over K. Then*

$$E(K) = \{(a, b) \in K^2 \ : \ b^2 + a_1ab + a_3b = a^3 + a_2a^2 + a_4a + a_6\} \cup \{O\}$$

is a subgroup of E.

Theorem 1.3 (Algebraic group law)**.** *Let (E, O) be an elliptic curve.*

1. *For every $D \in \mathrm{Div}^0(E)$ there exists a unique point $P \in E$ such that D and $P - O$ belong to the same divisor class of $\mathrm{Pic}^0(E)$.*

2. *There exists a surjective map $\sigma : \mathrm{Div}^0(E) \to E$ which maps each degree-0 divisor D to its associated point P.*

3. *σ induces a bijection of sets $\tilde{\sigma} : \mathrm{Pic}^0(E) \to E$.*

4. *If E is given by a Weierstrass equation, then the "geometric group law" on E described above and the "algebraic group law" induced from $\mathrm{Pic}^0(E)$ using σ are the same.*

Corollary 1.1. *Then E be an elliptic curve and $D = \sum n_P P \in \mathrm{Div}(E)$. Then D is a principal divisor if and only if $\sum n_P = 0 \in \mathbb{Z}$ and $\sum [n_P]P = O \in E$.*

2 The Proof

2.1 Preliminary Results

Definition 2.1 (Isogeny)**.** Let E_1 and E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ satisfying $\phi(O_{E_1}) = O_{E_2}$.

Theorem 2.1. *Every isogeny is a group homomorphism.*

Definition 2.2 (Homomorphism group of isogenies)**.** The set of isogenies $\mathrm{Hom}(E_1, E_2)$ from E_1 to E_2 form a group under addition where the sum of two isogenies is defined by $(\phi + \psi)(P) = \phi(P) \oplus \psi(P)$.

Proposition 2.1. $\mathrm{Hom}(E_1, E_2)$ *is a torsion-free $\mathbb{Z}$-module.*

Proposition 2.2. *The degree map* $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ *is a positive definite quadratic form.*

Definition 2.3 (Endomorphism ring of E)**.** If $E_1 = E_2 = E$, then $\mathrm{Hom}(E_1, E_2) = \mathrm{End}(E)$ is a ring whose multiplication is given by composition defined as $(\phi\psi)(P) = \phi(\psi(P))$.

Proposition 2.3. $\mathrm{End}(E)$ *is a ring of characteristic zero with no zero divisors.*

Definition 2.4 (Frobenius endomorphism)**.** Let K be a field of characteristic $p > 0$ and $q = p^r$. If E/K is an elliptic curve given by a Weierstrass equation, then $E^{(q)}/K$ is the elliptic curve defined by raising the coefficients of the equation for E to the q^{th} power. Then the Frobenius morphism ρ is defined by

$$\begin{aligned} \rho : E &\to E^{(q)} \\ (a, b) &\mapsto (a^q, b^q) \end{aligned}$$

ρ is called Frobenius endomorphism when $K = \mathbb{F}_q$ since then $E^{(q)} = E$.

Theorem 2.2. *Let $E/\mathbb{F}_q$ be an elliptic curve and $\rho : E \to E$ be the Frobenius endomorphism.*

1. $\rho^* \mathbb{F}_q(E) = \mathbb{F}_q(E)^q = \{f^q \ : \ f \in \mathbb{F}_q(E)\}$
2. *ρ is purely inseparable*
3. $\deg(\rho) = q$
4. *If $m, n \in \mathbb{Z}$ then the map $[m] + [n]\rho : E \to E$ is separable if and only if $p \nmid m$, where $p = \mathrm{char}(\mathbb{F}_q)$. In particular, the map $1 - \rho$ is separable.*

Definition 2.5 (Translation-by-Q map)**.** Let E/K be an elliptic curve and $Q \in E$. Then we define a translation-by-Q map as the morphism

$$\begin{aligned} \tau_Q : E &\to E \\ P &\mapsto P \oplus Q \end{aligned}$$

Remark 2.1. The map τ_Q is an isomorphism with τ_{-Q} as the inverse. However, τ_Q is an isogeny iff $Q = O$.

Theorem 2.3. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny.*

1. *For every $Q \in E_2$, we have $\#\phi^{-1}(Q) = \deg_s(\phi)$. Moreover, for every $P \in E_1$, $e_\phi(P) = \deg_i(\phi)$.*
2. *The map*

$$\begin{aligned} \Psi : \ker(\phi) &\to \mathrm{Aut}(\bar{K}(E_1)/\phi^* \bar{K}(E_2)) \\ Q &\mapsto \tau_Q^* \end{aligned}$$

   is an isomorphism. Here τ_Q^* is the automorphism that the translation-by-Q map $\tau_Q : E_1 \to E_1$ induces on $\bar{K}(E_1)$.

3. *If ϕ is separable, then ϕ is unramified with $\#\ker(\phi) = \deg(\phi)$. Moreover, $\bar{K}(E_1)$ is a Galois extension of $\phi^* \bar{K}(E_2)$.*

Definition 2.6 (Multiplication-by-m isogeny)**.** For each $m \in \mathbb{Z}$ we define the multiplication-by-m isogeny as

$$\begin{aligned} [m] : E &\to E \\ P &\mapsto \begin{cases} \underbrace{P \oplus P \oplus \cdots \oplus P}_{m \text{ times}} & \text{if } m > 0 \\ O & \text{if } m = 0 \\ [-m](-P) & \text{if } m < 0 \end{cases} \end{aligned}$$

Proposition 2.4. *Let E/K be an elliptic curve and $m \in \mathbb{Z}$ with $m \neq 0$. Then $[m] : E \to E$ is nonconstant (surjective) on $E(\bar{K})$.*

Theorem 2.4 (Dual isogeny)**.** *Let $\phi : E_1 \to E_2$ be a nonconstant isogeny such that $\deg(\phi) = m$. Then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ satisfying $\hat{\phi} \circ \phi = [m]$.*

Remark 2.2. The $\hat{\phi}$ obtained above is called the dual isogeny to ϕ. This assumes that $\phi \neq [0]$. If $\phi = [0]$ then we set $\hat{\phi} = [0]$.

Proposition 2.5. *Let $\phi : E_1 \to E_2$ be an isogeny.*

1. *If $\deg(\phi) = m$ then $\hat{\phi} \circ \phi = [m]$ on E_1 and $\phi \circ \hat{\phi} = [m]$ on E_2.*
2. *If $\lambda : E_2 \to E_3$ is another isogeny then $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.*
3. *If $\phi : E_1 \to E_2$ is another isogeny then $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.*
4. *For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ and $\deg([m]) = m^2$.*
5. $\deg(\hat{\phi}) = \deg(\phi)$
6. $\hat{\hat{\phi}} = \phi$.

Definition 2.7 (m-torsion subgroup of E)**.** Let E be an elliptic curve with $m \in \mathbb{Z}_{\geq 1}$. Then the m-torsion subgroup of E, denoted by $E[m]$, is the set of points of E of order m, i.e.

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

Theorem 2.5. *Let E be an elliptic curve and m be a nonzero integer.*

1. *If $m \neq 0$ in K, i.e. if either $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) \nmid m$, then*

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

   Thus $E[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank two.

2. *If $\mathrm{char}(K) = p > 0$, then one of the following is true:*
   (a) *$E[p^d] = \{O\}$ for all $d = 1, 2, 3, \ldots$*
   (b) *$E[p^d] = \mathbb{Z}/p^d\mathbb{Z}$ for all $d = 1, 2, 3, \ldots$*

Definition 2.8 (ℓ-adic Tate module of E)**.** Let E be an elliptic curve and let $\ell \in \mathbb{Z}$ be a prime. The ℓ-adic Tate module of E is the group

$$T_\ell(E) = \varprojlim_d E[\ell^d]$$

with the inverse limit being taken with respect to the natural maps $[\ell] : E[\ell^{d+1}] \to E[\ell^d]$.

Proposition 2.6. *The Tate module has the following structure:*

1. *$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as a $\mathbb{Z}_\ell$-module if $\ell \neq \mathrm{char}(K)$.*
2. *$T_p(E) \cong \{0\}$ or $\mathbb{Z}_p$ as a $\mathbb{Z}_p$-module if $p = \mathrm{char}(K) > 0$.*

Remark 2.3. Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Then ϕ induces maps $\phi : E_1[\ell^d] \to E_2[\ell^d]$, and hence induces a $\mathbb{Z}_\ell$-linear map $\phi_\ell : T_\ell(E_1) \to T_\ell(E_2)$. In particular, if $a \in \mathbb{Z}_\ell$ then $[a] : T_\ell(E) \to T_\ell(E)$ is the map induced by $a = (a_d)_{d\geq 1}$ such that $[a_d] : E \to E$ is the multiplication-by-a_d isogeny.

Definition 2.9 (Weil e_m-pairing)**.** Let $Q \in E[m]$. Then, by Corollary 1.1, there is $f \in \bar{K}(E)$ satisfying $\operatorname{div}(f) = mQ - mO$. Next, by Proposition 2.4, there is $Q' \in E$ such that $[m]Q' = Q$. Then, again using Corollary 1.1, there is $g \in \bar{K}(E)$ satisfying

$$\operatorname{div}(g) = [m]^*Q - [m]^*O = \sum_{R\in E[m]} \big((Q' \oplus R) - R\big)$$

Now, since $f \circ [m]$ and g^m have the same divisor, by multiplying f with an appropriate constant from $\bar{K}^*$, we may assume that $f \circ [m] = g^m$. Then, for $P \in E[m]$ and $X \in E$ we have

$$g(X \oplus P)^m = f([m]X \oplus [m]P) = f([m]X) = g(X)^m$$

That is, for every X, the function $g(X + P)/g(X)$ is an m^{th} root of unity. This allows us to define the Weil e_m-pairing

$$\begin{aligned} e_m : E[m] \times E[m] &\to \boldsymbol{\mu}_m \\ (P, Q) &\mapsto \frac{g(X \oplus P)}{g(X)} \end{aligned}$$

where $X \in E$ is any point such that $g(X \oplus P)$ and $g(X)$ are both defined and nonzero.

Definition 2.10 (ℓ-adic Weil pairing)**.** Let ℓ be a prime number different from $\operatorname{char}(K)$. The ℓ-adic Weil pairing on the Tate module is the morphism of inverse limits

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

such that the diagram

$$\begin{array}{ccc} E[\ell^{d+1}] \times E[\ell^{d+1}] & \xrightarrow{e_{\ell^{d+1}}} & \boldsymbol{\mu}_{\ell^{d+1}} \\ \big\downarrow{\scriptstyle [\ell]} & & \big\downarrow{\scriptstyle \omega\mapsto\omega^\ell} \\ E[\ell^d] \times E[\ell^d] & \xrightarrow{e_{\ell^d}} & \boldsymbol{\mu}_{\ell^d} \end{array}$$

commutes. That is, $e_{\ell^{d+1}}(P, Q)^\ell = e_{\ell^d}([\ell]P, [\ell]Q)$ for all $P, Q \in E[\ell^{d+1}]$.

Theorem 2.6. *The ℓ-adic Weil pairing has the following properties:*

1. *Bilinear:*

$$\begin{aligned} e(P \oplus_\ell P', Q) &= e(P, Q)e(P', Q) \\ e(P, Q \oplus_\ell Q') &= e(P, Q)e(P, Q') \end{aligned}$$

   where the input elements are of the form $P = (P_d)_{d\in\mathbb{Z}^+} \in \prod_d E[\ell^d]$ such that $[\ell](P_{d+1}) = P_d$ and[5] *$P \oplus_\ell P' = (P_d \oplus P'_d)_{d\geq 1}$.*

2. *Alternating: $e(Q, Q) = 1$. In particular, $e(P, Q) = e(Q, P)^{-1}$.*

3. *Nondegenerate: if $e(P, Q) = 1$ for all $P \in T_\ell(E)$, then $Q = O$, where $O = (O, O, \ldots)$.*

4. *Galois invariant: $\sigma\left(e(P, Q)\right) = e(\sigma(P), \sigma(Q))$ for all $\sigma \in G_{\bar{K}/K}$.*

5. *Dual isogeny is adjoint: if $\phi : E_1 \to E_2$ is an isogeny, then ϕ and its dual $\hat{\phi}$ are disjoints for the pairing, i.e. $e(\phi_\ell P, Q) = e(P, \hat{\phi}_\ell Q)$.*

[5] In this notation, when clear from the context, $[a]P = \left([a_d]P_d\right)_{d\geq 1}$.

2.2 Final Steps

Lemma 2.1. *Let $\phi \in \mathrm{End}(E)$, and $\phi_\ell : T_\ell(E) \to T_\ell(E)$ be the map induced by ϕ on the Tate module of E. Next, by Proposition 2.6, we can choose a $\mathbb{Z}_\ell$-basis $\{P, Q\}$ for $T_\ell(E)$ and write $\phi_\ell(P) = [a]P \oplus_\ell [b]Q$ and $\phi_\ell(Q) = [c]P \oplus_\ell [d]Q$ so that the 2×2 matrix[6] of ϕ_ℓ relative to this basis is*

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

Then we have

$$\det(\phi_\ell) = \deg(\phi) \qquad \text{and} \qquad \mathrm{tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1 - \phi)$$

where, as in Theorem 2.2, $1 - \phi = [1] + [-1]\phi \in \mathrm{End}(E)$. In particular, $\det(\phi_\ell)$ and $\mathrm{tr}(\phi_\ell)$ are in $\mathbb{Z} \subset \mathbb{Z}_\ell$ and are independent of ℓ.

Proof. Using the properties of the Weil pairing stated in Theorem 2.6, we compute

$$\begin{aligned}
e(P,Q)^{\deg(\phi)} &= e\left([\deg(\phi)]P, Q\right) && \text{(bilinearity of } e\text{)} \\
&= e\left(\hat{\phi}_\ell \phi_\ell P, Q\right) && \text{(Theorem 2.4)} \\
&= e\left(\phi_\ell P, \phi_\ell Q\right) && \text{(adjoint dual and Proposition 2.5)} \\
&= e\left([a]P \oplus_\ell [b]Q, [c]P \oplus_\ell [d]Q\right) \\
&= e\left(P,Q\right)^{ad-bc} && \text{(bilinear and alternating } e\text{)} \\
&= e(P,Q)^{\det(\phi_\ell)}
\end{aligned}$$

Since e is nondegenerate, we conclude that $\deg(\phi) = \det(\phi_\ell)$. Finally, the other result follows from the fact that for any 2×2 matrix A, we have $\mathrm{tr}(A) = 1 + \det(A) - \det(\mathrm{Id} - A)$. □

Proposition 2.7. *Let $E/\mathbb{F}_q$ be an elliptic curve, $\rho : E \to E$ be the q^{th}-power Frobenius endomorphism and $a = q + 1 - \#E(\mathbb{F}_q)$. If $\alpha, \beta \in \mathbb{C}$ are the roots of the polynoimal $c(t) = t^2 - at + q$. Then α and β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$, and for every $n \geq 1$ we have*

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

Proof. Since the Galois group $G_{\bar{\mathbb{F}}_q/\mathbb{F}_q}$ is generated by the q^{th} power map on $\bar{\mathbb{F}}_q$, for every point $P \in E(\bar{\mathbb{F}}_q)$ we have $P \in E(\mathbb{F}_q)$ iff $\rho(P) = P$. Thus, $E(\mathbb{F}_q) = \ker(1 - \rho)$. Moreover, from Theorem 2.2 we know that $1 - \rho$ is separable. Hence, we can use Theorem 2.3 to get

$$\boxed{\#E(\mathbb{F}_q) = \#\ker(1 - \rho) = \deg(1 - \rho)}$$

Also, using Lemma 2.1 we get that

$$\begin{aligned}
&\det(\rho_\ell) = \deg(\rho) = q && \text{(Theorem 2.2)} \\
&\boxed{\mathrm{tr}(\rho_\ell) = 1 + \deg(\rho) - \deg(1 - \rho) = 1 + q - \#E(\mathbb{F}_q) = a}
\end{aligned}$$

Hence the characteristic polynomial of ρ_ℓ is

$$\det(t - \rho_\ell) = t^2 - \mathrm{tr}(\rho_\ell)t + \det(\rho_\ell) = t^2 - at + q = c(t)$$

[6]Note that most of the facts that we learn about matrices corresponding to linear transformations between finite dimensional vector spaces over fields also hold for the matrices corresponding to linear maps between finite rank modules over integral domains (eg: integer matrices). Also, here we define the scalar multiplication as $a \cdot P = [a]P$.

Since the characteristic polynomial of ρ_ℓ belongs to $\mathbb{Z}[t]$, we can factor it over $\mathbb{C}$ as

$$\det(t - \rho_\ell) = t^2 - at + q = (t - \alpha)(t - \beta)$$

Moreover, $c(t)$ is a nonnegative quadratic polynomial over $\mathbb{R}$ since for any $a/b \in \mathbb{Q}$ we have

$$\det\left(\frac{a}{b} - \rho_\ell\right) = \frac{\det(a - b\rho_\ell)}{b^2} = \frac{\deg(a - b\rho)}{b^2} \geq 0$$

Therefore, α and β are either complex conjugates or equal to each other. In either case, we have $|\alpha| = |\beta|$. Furthermore, since $\alpha\beta = q$, we get that $|\alpha| = |\beta| = \sqrt{q}$.

Similarly, for each integer $n \geq 1$, the $(q^n)^{th}$-power Frobenius endomorphism satisfies

$$\boxed{\#E(\mathbb{F}_{q^n}) = \deg(1 - \rho^n)}$$

Now, since the Jordan normal form of ρ_ℓ is an upper triangular matrix with α and β along the diagonal [FIS97, §7.1], it follows that the characteristic polynomial of ρ_ℓ^n is given by

$$\det(t - \rho_\ell^n) = (t - \alpha^n)(t - \beta^n)$$

In particular, we have

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

□

Theorem 2.7 (Weil conjectures for elliptic curves)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then we have*

1. *Rationality: $Z_{E/\mathbb{F}_q}(t) \in \mathbb{Q}(t)$ such that*

$$Z_{E/\mathbb{F}_q}(t) = \frac{1 - at + qt^2}{(1 - t)(1 - qt)}$$

   where $a = q + 1 - \#E(\mathbb{F}_q)$ is the trace of Frobenius.

2. *Riemann hypothesis: We have*

$$1 - at + qt^2 = (1 - \alpha t)(1 - \beta t) \in \mathbb{C}(t)$$

   with $|\alpha| = |\beta| = q^{1/2}$.

3. *Functional equation:*

$$Z_{E/\mathbb{F}_q}\left(\frac{1}{qt}\right) = Z_{E/\mathbb{F}_q}(t)$$

4. *Betti numbers: $E(\mathbb{C})$ has the Betti numbers $b_0 = 1, b_1 = 2$, and $b_2 = 1$*

Proof. The second statement follows directly from Proposition 2.7. Therefore, we will prove the other three statements.

1. We take log of both sides of the zeta function and simplify:

$$\begin{aligned}\log\left(Z_{E/\mathbb{F}_q}(t)\right) &= \sum_{n=1}^{\infty}\left(\#E(\mathbb{F}_{q^n})\frac{t^n}{n}\right)\\ &= \sum_{n=1}^{\infty}(1-\alpha^n-\beta^n+q^n)\frac{t^n}{n} && \text{(Proposition 2.7)}\\ &= -\log(1-t)+\log(1+\alpha t)+\log(1-\beta t)-\log(1-qt)\end{aligned}$$

   Therefore, we have

$$\begin{aligned}Z_{E/\mathbb{F}_q}(t) &= \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)}\\ &= \frac{1-at+qt^2}{(1-t)(1-qt)} && \text{(Proposition 2.7)}\end{aligned}$$

3. From the rational function it is clear that this functional equation holds true. Moreover, the Euler characteristic of elliptic curves is 0 since they are genus 1 curves [Sha77, §VII.3.3].

4. It follows from the fact that any elliptic curve over $\mathbb{C}$ can be represented by as torus [Sil09, §VI.5].

□

Remark 2.4. To see why the third statement is called Riemann hypothesis, note that

$$\zeta_{E/\mathbb{F}_q}(s) = \frac{\left(1-\alpha q^{-s}\right)\left(1-\beta q^{-s}\right)}{\left(1-q^{-s}\right)\left(1-q^{-(s-1)}\right)}$$

Therefore, if $\zeta_{E/\mathbb{F}_q}(s)=0$ then $|\alpha|=|\beta|=|q^s|=q^{1/2}$, which is equivalent to $\mathrm{Re}(s)=\frac{1}{2}$.

References

[AM69] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison Wesley Publishing Company, 1st edition, 1969.

[DF04] D. S. Dummit and R. M. Foote. *Abstract Algebra*. John Wiley, 3rd edition, 2004.

[FIS97] S. H. Friedberg, A. J. Insel, and L. E. Spence. *Linear Algebra*. Prentice Hall Inc., 3rd edition, 1997 (Corrected at 2nd printing 1999).

[Mil13] J. S. Milne. *Lectures on Étale Cohomology*, v2.21, 2013. `https://www.jmilne.org/math/CourseNotes/LEC.pdf`

[Neu99] J. Neukirch (Translated from the German by N. Schappacher). *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin-Heidelberg, 1st edition, 1999.

[Sha77] I. R. Shafarevich (Translated from the Russian by K. A. Hirsch). *Basic Algberaic Geometry*, volume 213 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin-Heidelberg, 1st edition, 1977.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, New York, 2nd edition, 2009 (Corrected at 2nd printing 2016).