Weil Conjectures for Elliptic Curves

Chol Park

Dec. 15th. 2008

1 Introduction

In 1949, Andre Weil made a series of very general conjectures concerning the number of points on varieties defined over finite fields. In this paper we will state Weil conjectures and prove them for elliptic curves. Let K be a field with q elements and for each integer $n \geq 1$. let K_n be the extension of K of degree n, so $\#K_n = q^n$. Let V be a projective variety defined over K (I.e. $I(V) \cap K[V]$ generates $I(V)$), denoted V/K, so V is the set of zeros

$$f_1(x_0, ...x_N) = ... = f_m(x_0, ..., x_N) = 0$$

of a collection of homogeneous polynomials with coefficients in K. Then $V(K_n)$ is the set of points of V with coordinates in K_n. We code the number of such points into a generating function.

Definition 1.1. The zeta function of V/K is the power series

$$Z(V/K;T) = \exp(\sum_{n=1}^{\infty}(\#V(K_n))\frac{T^n}{n}).$$

Example 1.2. Let $V = \mathbb{P}^N$. Then a point of $V(K_n)$ is given by homogeneous coordinates $[x_0, ..., x_N]$ with $x_i \in K_n$ not all zero. Two sets of coordinates give the same point if they differ by multiplication by an element of K_n^*. Hence

$$\#V(K_n) = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni},$$

so

$$\sum_{n=1}^{\infty}(\#V(K_n))\frac{T^n}{n}) = \sum_{n=1}^{\infty}(\sum_{i=0}^{N} q^{ni})\frac{T^n}{n} = \sum_{i=0}^{N} -log(1 - q^iT).$$

Thus

$$Z(\mathbb{P}^N/K;T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^NT)}.$$

Theorem 1.3. (Weil Conjectures) Let K be a field with q elements and V/K a projective variety of dimension N.

(a) (Rationality)

$$Z(V/K;T) \in \mathbb{Q}(T).$$

(b) (Functional Equation) There is an integer ε(the Euler characteristic of V) so that

$$Z(V/K; \frac{1}{q^N T}) = \pm q^{\frac{N\varepsilon}{2}} T^{\varepsilon} Z(V/K; T).$$

(c) (Riemann Hypothesis) There is a factorization

$$Z(V/K; T) = \frac{P_1(T)P_3(T)\cdots P_{2N-1}(T)}{P_0(T)P_2(T)\cdots P_{2N}(T)}$$

with each $P_i(T) \in \mathbb{Z}(T)$. Further $P_0(T) = 1 - T$, $P_{2N}(T) = 1 - q^N T$, and for each $1 \leq i \leq 2N - 1$, $P_i(T)$ factors over $\mathbb{C}$ as

$$P_i(T) = \prod_j (1 - \alpha_{ij} T) \text{ with } |\alpha_{ij}| = q^{\frac{i}{2}}.$$

This conjectures was proposed by Weil in 1949, and proven by him for curves and abelian varieties. The rationality of the zeta function in general was established by Dwork in 1960 using techniques of p-adic functional analysis. Soon thereafter the l-adic cohomology theory developed by M. Artin, Grothendieck, and others gave another proof of the rationality and the functional equation. Then in 1973 Deligne proved the Riemann hypothesis.

2 Riemann-Roch Theorem

In this section, we introduce some basic properties of irreducible projective curves without proof. *By curve, we always mean an irreducible projective curve.* The *divisor group of a curve* C, denoted $Div(C)$, is the free abelian group generated by the points of C. Thus a divisor $D \in Div(C)$ is a formal sum

$$D = \sum_{P \in C} n_P(P)$$

with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. The degree of D is defined by

$$degD = \sum_{P \in C} n_P.$$

The divisors of degree 0 form a subgroup of $Div(C)$, which we denote by

$$Div^0(C) = \{D \in Div(C) : degD = 0\}.$$

Assume now that the curve C is smooth, and let $f \in \overline{K}(C)^*$. Then we can associate to f the divisor $div(f)$ given by

$$div(f) = \sum_{P \in C} ord_P(f)(P).$$

Since each ord_P is a valuation, we see that the map

$$div : \overline{K}(C)^* \to Div(C)$$

is a homomorphism of abelian groups. It is analogous to the map which sends an element of a number field to the corresponding fractional ideal. This prompts the following definitions.

Definition 2.1. A divisor $D \in Div(C)$ is *principal* if it has the form $D = div(f)$ for some $f \in \overline{K}(C)^*$. Two divisors D_1, D_2 are *linearly equivalent*, denoted $D_1 \ D_2$ if $D_1 - D_2$ is principal. The *divisor class group* (or *Picard group*) *of* C, denoted $Pic(C)$, is the quotient of $Div(C)$ by the subgroup of the principal divisors.

Proposition 2.2. Let C be an irreducible and smooth projective curve and $f \in \overline{K}(C)^*$.
(a) $div(f) = 0$ if and only if $f \in \overline{K}^*$.
(b) $deg(dev(f)) = 0$.
Proof) (a) If $div(f) = 0$, then f has no poles, so the corresponding map $f : C \to \mathbb{P}^1$ is not surjective. therefore it is constant, so $f \in \overline{K}^*$. The converse in clear.
(b) [Hartshorne, 2.6.10]

From (2.2b) we see that the principal divisors form a subgroup of $Div^0(C)$.

Definition 2.3. The degree 0 part of the divisor class group of C, which we denote by $Pic^0(C)$, is the quotient of $Div^0(C)$ by the subgroup of principal divisors.

Definition 2.4. Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves, and let $P \in C_1$. The *ramification index of* ϕ *at* P, denoted $e_\phi(P)$, is given by

$$e_\phi(P) = ord_P(\phi^* t_{\phi(P)}),$$

where $t_{\phi(P)} \in \overline{K}(C_2)$ is a uniformizer at $\phi(P)$. Note that $e_\phi(P) \geq 1$. We say that ϕ is *unramified at* P if $e_\phi = 1$; and ϕ is *unramified* if it is unramified at every points of C_1.

Proposition 2.5. Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves.
(a) For every $Q \in C_2$,

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = deg\phi,$$

where $deg\phi = [\overline{K}(C_1) : \phi^* \overline{K}(C_2)]$.
(b) For all but finitely many $Q \in C_2$,

$$\#\phi^{-1}(Q) = deg_s(\phi),$$

where $deg_s\phi = [\overline{K}(C_1) : \phi^* \overline{K}(C_2)]_s$.
(c) Let $\psi : C_2 \to C_3$ be another non-constant map. Then for all $P \in C_1$,

$$e_{\psi \circ \phi}(P) = e_\phi(P) e_\psi(\phi(P)).$$

Proof)(a) [Hartshorne, 2.6.9]
(b) [Hartshorne 2.6.8]
(c) [Silverman, 2.2.6c]

Now let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves. Then ϕ induces map on the function fields of C_1 and C_2,

$$\phi^* : \overline{K}(C_2) \to \overline{K}(C_1).$$

We similarly define maps on the divisor groups as follows.

$$\phi^* : Div(C_2) \to Div(C_1) : (Q) \to \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)$$

and extend $\mathbb{Z}$-linearly to arbitrary divisors.

Definition 2.6. Let C be a curve. The space of (*meromorphic*) *differential forms on* C, denoted Ω_C, is the $\overline{K}(C)$-vector space generated by symbols of the form dx for $x \in \overline{K}(C)$, subject to the usual relations:
(a) $d(x+y) = dx + dy$ for all $x, y \in \overline{K}(C)$;
(b) $d(xy) = xdy + ydx$ for all $x, y \in \overline{K}(C)$;
(c) $da = 0$ for all $a \in \overline{K}$.

Proposition 2.7. Let C be a curve, $P \in C$, and $t \in \overline{K}(C)$ be a uniformizer at P.
(a) Ω_C is a 1-dimensional $\overline{K}(C)$ vector space.
(b) For every $\omega \in \Omega_C$ there exists a unique function $g \in \overline{K}(C)$, depending on ω and t, such that

$$\omega = gdt.$$

We denote g by ω/dt.
(c) Let $f \in \overline{K}(C)$ be regular at P. Then df/dt is also regular at P.
(d) The quantity

$$ord_P(\omega/dt)$$

depends only on ω and P, independent of the choice of uniformizer t. We call this value the order of ω at P, and denote it by $ord_P(\omega)$.
(e) For all but finitely many $P \in C$,

$$ord_P(\omega) = 0.$$

Proof)(a)[Shafarevich 2, 3.4 thm 3]
(b) [Silverman, 2.4.3(a)]
(c) [Silverman, 2.4.3(b)]
(d) [Silverman, 2.4.3(c)]
(e) [Silverman, 2.4.3(e)]

Definition 2.8. Let $\omega \in \Omega_C$. The divisor associated to ω is

$$div(\omega) = \sum_{P \in C} ord_P(\omega)(P) \in Div(C).$$

Definition 2.9. A differential $\omega \in \Omega_C$ is *regular* (or *holomorphic*) if

$$ord_P(\omega) \geq 0 \text{ for all } P \in C.$$

It is *non-vanishing* if

$$ord_P(\omega) \leq 0 \text{ for all } P \in C.$$

If $\omega_1, \omega_2 \in \Omega_C$ are non-zero differentials, then (2.7a) implies that there is a function $f \in \overline{K}(C)^*$ so that $\omega_1 = f\omega_2$. Thus

$$div(\omega_1) = div(f) + div(\omega_2),$$

which shows that the following definition makes sense.

Definition 2.10. The *canonical divisor class on* C is the image in $Pic(C)$ of $div(\omega)$ for any non-zero differential $\omega \in \Omega_C$. Any divisor in this divisor class is called a *canonical divisor*.

Definition 2.11. A divisor $D = \Sigma n_P(P) \in Div(C)$ is *positive*, denoted by

$$D \geq 0,$$

if $n_P \geq 0$ for every $P \in C$. similarly, if $D_1, D_2 \in Div(C)$, then we write to indicate that $D_2 - D_1$ is *positive*.

Definition 2.12. Let $D \in Div(C)$. We associate to D the set of functions

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* : div(f) \geq -D\} \cup \{0\}.$$

$\mathcal{L}(D)$ is a finite-dimensional $\overline{K}$-vector space (see below), and we denote its dimension by

$$l(D) = dim_{\overline{K}}\mathcal{L}(D).$$

Proposition 2.13. Let $D \in Div(C)$.
(a) If $degD < 0$, then

$$\mathcal{L}(D) = \{0\} \text{ and } l(D) = 0.$$

(b) $\mathcal{L}(D)$ is a finite-dimensional $\overline{K}$-vector space.
(c) If $D^{'} \in Div(C)$ is linearly equivalent to D, then

$$\mathcal{L}(D) = \mathcal{L}(D^{'}); \text{ and so } l(D) = l(D^{'}).$$

Proof)(a) Let $f \in \mathcal{L}(D)$ with $f \neq 0$. Then

$$0 = deg(div(f)) \geq (-D) = -deg(D),$$

so $degD \geq 0$.
(b) [Hartshorne, 2.5.19]
(c) If $D = D^{'} + div(g)$, then the map

$$\mathcal{L}(D) \to \mathcal{L}(D^{'}) : f \to fg$$

is an isomorphism.

We are now ready to state one of the most fundamental results in the algebraic geometry of curves.

Theorem 2.14. (Riemann-Roch) Let C be a smooth curve and K_C a canonical divisor on C. There is an integer $g \geq 0$, called the genus of C, such that for every divisor $D \in Div(C)$,

$$l(D) - l(K_C - D) = deg(D) - g + 1.$$

Corollary 2.15. (a) $l(K_C) = g$.
(b) $deg(K_C) = 2g - 2$.
(c) If $deg(D) \geq 2g - 2$, then

$$l(D) = deg(D) - g + 1.$$

Proof)(a) Use the Riemann-Roch theorem with $D = 0$. Note that $\mathcal{L}(0) = \overline{K}$, so $l(0) = 1$.
(b) Use (a) and the Riemann-Roch theorem with $D = K_C$.
(c) From (b), $deg(K_C - D) < 0$. Now use the Riemann-Roch theorem and (2.13a). □

3 Elliptic Curves

Elliptic curves are curves of genus 1 having a specified basepoint. In this section, we introduce some basic properties of elliptic curves. Let E be an elliptic curve given by a Weierstrass equation. Remember that $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the equation together with the point $O = [0, 1, 0]$ at infinity. Let $L \subset \mathbb{P}^2$ be a line. Then since the equation has degree three, L intersects E at exactly 3 points, say P, Q, R. Note that if L is tangent to E, then P, Q, R may not be distinct. The fact that $L \cap E$, taken with multiplicities, consists of three points, is a special case of Bezout's theorem.

We define a group law $\oplus$ on E by the following rule.
Group Law Let $P, Q \in E$, L the line connecting P and Q (tangent line to E if $P = Q$), and R the third point of intersection of L with E. Let $L^{'}$ be the line connecting R and O. Then $P \oplus Q$ is the point such that $L^{'}$ intersects E at R, O, and $P \oplus Q$.

Next we use the Riemann-Roch theorem to describe a group law on the points of E. Of course, this will turn to be the same group law already described above when E is given by a Weierstrass equation. We start with a simple lemma, which serves to distinguish $\mathbb{P}^1$ from curves of genus 1.

Lemma 3.1. Let C be a curve of genus 1, and let $P, Q \in C$. Then

$$(P) \sim (Q) \text{ if and only if } P = Q.$$

Proof) Suppose $(P) \sim (Q)$, and choose $f \in \overline{K}(C)$ so that

$$div(f) = (P) - (Q).$$

Then $f \in \mathcal{L}((Q))$, and by Riemann-Roch theorem

$$dim\mathcal{L}((Q)) = 1.$$

But $\mathcal{L}((Q))$ already contains the constant functions, hence $f \in \overline{K}$ and $P = Q$. □

Proposition 3.2. Let (E, O) be an elliptic curve.
(a) For every divisor $D \in Div^0(E)$ there exists a unique point $P \in E$ so that

$$D \sim (P) - (O).$$

Let

$$\sigma : Div^0(E) \to E$$

be the map given by this association.
(b) The map σ is surjective.
(c) Let $D_1, D_2 \in Div^0(E)$. Then

$$\sigma(D_1) = \sigma(D_2) \text{ if and only if } D_1 \sim D_2.$$

Thus σ induces a bijection of sets

$$\sigma : Pic^0(E) \backsimeq E.$$

(d) The inverse to σ is the map

$$k : E \backsimeq Pic^0(E) : P \to \text{class of } (P) - (O).$$

(e) It E is given by a Weierstrass equation, then the "geometric group law" on E and the group law induced from $Pic^0(E)$ by using σ are the same.
Proof)(a) Since E has genus 1, the Riemann-Roch Theorem says that

$$dim\mathcal{L}(D + (O)) = 1.$$

Let $f \in \overline{K}(E)$ be a generator for $\mathcal{L}(D + (O))$. Since

$$div(f) \geq -D - (O) \text{ and } deg(div(f)) = 0,$$

it follows that

$$div(f) = -D - (O) + (P)$$

for some $P \in E$. Hence

$$D \sim (P) - (O),$$

which gives the existence of a point with desired property.

Next suppose $P^{'}$ has the same property. Then

$$(P) \sim D + (O) \sim (P^{'}),$$

so $P = P^{'}$ from (3.1). Hence P is unique.
(b) For any $P \in E$,

$$\sigma((P) - (O)).$$

(c) Let $D_1, D_2 \in Div^0(E)$, and set $P_i = \sigma(D_i)$. Then from the definition of σ,

$$(P_1) - (P_2) \sim D_1 - D_2.$$

Hence $P_1 = P_2$ certainly implies $D_1 \sim D_2$. Conversely, if $D_1 \sim D_2$, then $(P_1) \sim (P_2)$, so $P_1 = P_2$ from (3.1).
(d) clear.
(e) Let E be given by a Weierstrass equation, and let $P, Q \in E$. It clearly suffices to show that

$$k(P + Q) = k(P) + k(Q).$$

Let

$$f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$$

give the line L in $\mathbb{P}^2$ going through P and Q, let R be the third point of intersection of L with E, and let

$$f^{'}(X, Y, Z) = \alpha^{'} X + \beta^{'} Y + \gamma^{'} Z = 0$$

be the line $L^{'}$ through R and O. Then from the definition of addition on E and the fact that the line $Z = 0$ intersects E at O with multiplicity 3, we have

$$div(f/Z) = (P) + (Q) + (R) - 3(O)$$

and

$$div(f'/Z) = (R) + (P+Q) - 2(O).$$

Hence

$$(P+Q) - (P) - (Q) + (O) = div(f'/f) \sim 0,$$

so

$$k(P+Q) - k(P) - k(Q) = 0.$$

□

Corollary 3.3. Let E be an elliptic curve and $D = \Sigma n_P(P) \in Div(E)$. Then D is principal if and only if $\Sigma n_P = 0$ and $\Sigma[n_P]P = O$.
Proof) From (2.2b), every principal divisor has degree 0. Assuming now $D \in Div^0(E)$, (3.2a,e) implies

$$D \sim 0 \Leftrightarrow \sigma(D) = O \Leftrightarrow \Sigma[n_P]\sigma((P) - (O)) = O,$$

which is the desired result since $\sigma((P) - (O)) = P$. □

Definition 3.4. Let E_1 and E_2 be elliptic curves. An *isogeny between E_1 and E_2* is a morphism

$$\phi : E_1 \to E_2$$

satisfying $\phi(O) = O$.

Example 3.5. For each $m \in \mathbb{Z}$ we can define an isogeny multiplication by m

$$[m] : E \to E$$

in the natural way. If $m > 0$ then

$$[m](P) = P + P + ... + P(m \text{ terms});$$

if $m < 0$ then $[m](P) = [-m](-P)$. That [m] is an isogeny follows easily by induction since the group law $\oplus : E \times E \to E$ is a morphism. Notice that if E is defined over K, then $[m]$ is defined over K.

An isogeny is a morphism between elliptic curves which sends O to O. Since an elliptic curve is a group, it might seem more natural to focus on those isogenies which are group homomorphisms. In fact, it turns out that every isogeny has this property.

Theorem 3.6. Let

$$\phi : E_1 \to E_2$$

be an isogeny. Then

$$\phi(P+Q) = \phi(P) + \phi(Q) \text{ for all } P, Q \in E_1.$$

Proof) [Silverman, 3.4.8]

Theorem 3.7. Let $\phi : E_1 \to E_2$ be a non-constant isogeny.
(a) For every $Q \in E_2$,

$$\#\phi^{-1}(Q) = deg_s\phi.$$

Further, for every $P \in E_1$,

$$e_\phi(P) = deg_i(\phi).$$

(b) The map

$$ker\phi \to Aut[\overline{K}(E_1)/\phi^*\overline{K}(E_2)] : T \to \tau_T^*$$

is an isomorphism. (Here τ_T is the translation-by-T map.)
Proof) [Silverman, 3.4.10]

Proposition 3.8. Let $char(K) = p > 0$, let E be defined over $\mathbb{F}_q$, let $\phi : E \to E$ be the q^{th}-power Frobenius endomorphism, and $m, n \in \mathbb{Z}$. Then the map

$$m + n\phi : E \to E$$

is separable if and only if $p \nmid m$. In particular, the map

$$1 - \phi$$

is separable.
Proof) [Silverman, 3.5.5]

Theorem 3.9. Let $\phi : E_1 \to E_2$ be a non-constant isogeny of degree m. Then there exists a unique isogeny

$$\widehat{\phi} : E_2 \to E_1$$

satisfying

$$\widehat{\phi} \circ \phi = [m].$$

Such a $\widehat{\phi}$ is called the *dual isogeny to* ϕ.
Proof) [Silverman, 3.6.2a]

4 Tate Modules

Let E/K be an elliptic curve and $m \geq 2$ an integer (prime to char(K) if char$(K) > 0$.) As we have seen in the class,

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

the isomorphism being one between abstract groups. However, the group $E[m]$ comes equipped with considerably more structure. Namely, each element of the Galois group $G(\overline{K}|K)$ acts on $E[m]$, since if $[m]P = O$, then $[m](P^\sigma) = ([m]P)^\sigma = O$. We thus obtain a representation

$$G(\overline{K}|K) \longrightarrow Aut(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z}),$$

where the latter isomorphism involves choosing a basis for $E[m]$. Individually, for each m, these representations are not completely satisfactory, because it is generally easiest to deal with representations whose matrices have coefficients in a ring having characteristic 0. What we will do is to fit them together for varying m so as to achieve this end, the motivating example being the inverse limit construction of the l-adic integers $\mathbb{Z}_l$ from the finite groups $\mathbb{Z}/l^n\mathbb{Z}$.

Definition 4.1. Let E be an elliptic curve and $l \in \mathbb{Z}$ a prime. The (l-*adic*) *Tate module of* E is the group

$$T_l(E) = \lim_{\overleftarrow{n}} E[l^n],$$

the inverse limit being taken with respect to the natural maps

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n].$$

Since each $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module, we see that the Tate module has a natural structure as a Z_l-module.

Proposition 4.2. As a $\mathbb{Z}_l$-module, the Tate module has the following structure. If $l \neq \text{char}(K)$, then

$$T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l.$$

Now the action of $G(\overline{K}|K)$ on each $E[l^n]$ commutes with the multiplication by l maps used to form the inverse limit, so $G(\overline{K}|K)$ also acts on $T_l(E)$. Further since the pro-finite group $G(\overline{K}|K)$ acts continuously on each finite group $E[l^n]$, the resulting action on $T_l(E)$ is also continuous.

Definition 4.3. The *l-adic representation of* $G(\overline{K}|K)$ *on* E, denoted ρ_l, is the map

$$\rho_l : G(\overline{K}|K) \longrightarrow Aut(T_l(E))$$

giving the action of $G(\overline{K}|K)$ on $T_l(E)$ as described above.

The above construction is analogous to the following one, which may be more familiar. Let

$$\mu_{l^n} \subset \overline{K}^*$$

be the group of $(l^n)^{th}$ roots of unity. Then raising to the l^{th}-power gives maps

$$\mu_{l^{n+1}} \xrightarrow{l} \mu_{l^n},$$

and we can take the inverse limit as above to form the Tate module of K

$$T_l(\mu) = \lim_{\overleftarrow{n}} \mu_{l^n}.$$

As an abstract group,

$$T_l(\mu) \cong \mathbb{Z}_l.$$

Further $G(\overline{K}|K)$ acts on each μ_{l^n}, so we obtain a 1-dimensional representation

$$G(\overline{K}|K) \longrightarrow Aut(T_l(\mu)) \cong \mathbb{Z}_l^*.$$

The Tate module is also a useful tool for studying isogenies. If

$$\phi : E_1 \longrightarrow E_2$$

is an isogeny of elliptic curves, then ϕ gives maps

$$\phi : E_1[l^n] \longrightarrow E_2[l^n],$$

and so it induces a $\mathbb{Z}_l$-linear map

$$\phi_l : T_l(E_1) \longrightarrow T_l(E_2).$$

We thus obtain a homomorphism

$$Hom(E_1, E_2) \longrightarrow Hom(T_l(E_1), T_l(E_2)).$$

Notice that if $E_1 = E_2 = E$, then the map

$$End(E) \longrightarrow End(T_l(E))$$

is even a homomorphism of rings. It is not hard to show that the above homomorphism is injective.

5 Weil Pairing

Let E/K be an elliptic curve. For this section we fix an integer $m \geq 2$, prime to $p = char(K)$ if $p > 0$. We will make frequent use of (3.3), which says that $\Sigma n_i(P_i)$ is the divisor of a function if and only if $\Sigma n_i = 0$ and $\Sigma[n_i]P_i = O$.

Let $T \in E[m]$. Then there is a function $f \in \overline{K}(E)$ such that

$$div(f) = m(T) - m(O).$$

letting $Q \in E$ with $[m]Q = T$, there is similarly a function $g \in \overline{K}(E)$ satisfying

$$div(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (Q + R) - (R).$$

Note $\#E[m] = m^2$ and $[m^2]Q = O$. One immediately verifies that the functions $f \circ [m]$ and g^m have the same divisor, so multiplying f by an element of $\overline{K}^*$, we may assume that

$$f \circ [m] = g^m.$$

Now suppose that $S \in E[m]$ is another m-torsion point($S = T$ is allowed). Then for any point $X \in E$,

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

Hence we can define a pairing

$$e_m : E[m] \times E[m] \longrightarrow \mu_m$$

by setting

$$e_m(S, T) = \frac{g(X + S)}{g(X)},$$

where $X \in E$ is any point such that $g(X+S)$ and $g(X)$ are both defined and non-zero. Note that although g is only defined up to multiplication by an element of $\overline{K}^*$, $e_m(S, T)$ does not depend on this choice. This pairing is called the *Weil e_m-pairing*. We begin by giving some of its basic properties.

Proposition 5.1. The Weil e_m-pairing is:
(a) (Bilinear)

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2) :$$

(b) (Alternating)

$$e_m(T, T) = 1,$$

so in particular,

$$e_m(S, T) = e_m(T, S)^{-1} :$$

(c) (Non-degenerate) If $e_m(S, T) = 1$ for all $S \in E[m]$, then $T = O$:
(d) (Galois invariant) For all $\sigma \in G(\overline{K}|K)$,

$$e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma) :$$

(e) (compatible) If $S \in E[mm^{'}]$ and $T \in E[m]$, then

$$e_{mm'}(S, T) = e_m([m^{'}]S, T).$$

Proof)(a) Linearity in the first factor is easy.

$$e_m(S_1 + S_2, T) = \frac{g(X + S_1 + S_2)}{g(X + S_1)} \frac{g(X + S_1)}{g(X)} = e_m(S_2, T)e_m(S_1, T).$$

For the second, let $f_1, f_2, f_3, g_1, g_2, g_3$ be functions as above for T_1, T_2, and $T_3 = T_1 + T_2$. Choose $h \in \overline{K}(E)$ with divisor

$$div(h) = (T_1 + T_2) - (T_1) - (T_2) + (O).$$

Then

$$div(f_3/(f_1f_2)) = m\, div(h),$$

so for some $c \in \overline{K}^*$

$$f_3 = cf_1f_2h^m.$$

Compose with the multiplication by $[m]$ map, use $f_i \circ [m] = g_i^m$, and take m^{th} roots to find

$$g_3 = c^{'} g_1g_2(h \circ [m]).$$

Now

$$\begin{aligned} e_m(S, T_1 + T_2) =& \frac{g_3(X + S)}{g_3(X)} \\ =& \frac{g_1(X + S)g_2(X + S)h([m]X + [m]S)}{g_1(X)g_2(X)h([m]X)} \\ =& e_m(S, T_1)e_m(S, T_2). \end{aligned}$$

(b) From (a) we have

$$e_m(S + T, S + T) = e_m(S, S)e_m(S, T)e_m(T, S)e_m(T, T),$$

so it suffices to show that $e_m(T,T) = 1$ for all $T \in E[m]$. For any $P \in E$, recall that $\tau_P : E \to E$ denotes the translation by P map. Then

$$div(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}) = m\sum_{i=0}^{m-1}([1-i]T) - ([-i]T) = 0.$$

Hence $\Pi_{i=0}^{m-1} f \circ \tau_{[i]T}$ is constant; and if we choose some $Q \in E$ with $[m]Q = T$ then $\Pi_{i=0}^{m-1} g \circ \tau_{[i]T}$ is also constant, because its m^{th} power is the above product of f's. Evaluating the product of g's at X and $X+Q$ yields

$$\prod_{i=0}^{m-1} g(X+[i]Q) = \prod_{i=0}^{m-1} g(X+[i+1]T).$$

Now canceling like terms gives

$$g(X) = g(X+[m]Q) = g(X+T),$$

so

$$e_m(T,T) = g(X+T)/g(X) = 1$$

(c) If $e_m(S,T) = 1$ for all $S \in E[m]$, so $g(X+S) = g(X)$ for all $S \in E[m]$, then $g = h \circ [m]$ for some function $h \in \overline{K}(E)$. But then

$$(h \circ [m])^m = g^m = f \circ [m],$$

so $f = h^m$. Hence

$$m\, div(h) = div(f) = m(T) - m(O),$$

so

$$div(h) = (T) - (O).$$

Therefore $T = O$.
(d) Let $\sigma \in G(\overline{K}|K)$. If f, g are the functions for T as above, then clearly f^σ, g^σ are the corresponding functions for T^σ. Then

$$e_m(S^\sigma, T^\sigma) = \frac{g^\sigma(X^\sigma + S^\sigma)}{g^\sigma(X^\sigma)} = (\frac{g(X+S)}{g(X)})^\sigma = e_m(S,T)^\sigma.$$

(e) Taking f, g as above, we have

$$div(f^{m'}) = mm'(T) - mm'(O)$$

and

$$(g \circ [m'])^{mm'} = (f \circ [mm'])^{m'}.$$

Then from the definition of $e_{mm'}$ and e_m,

$$e_{mm'}(S,T) = \frac{g \circ [m'](X+S)}{g \circ [m'](X)} = \frac{g(Y+[m']S)}{g(Y)} = e_m([m']S, T).$$

□

Recall that if E_1 and E_2 are elliptic curves and $\phi : E_1 \to E_2$ is an isogeny connecting them, then there is a dual isogeny $\widehat{\phi} : E_2 \to E_1$ going in the other direction. The following proposition says that ϕ and $\widehat{\phi}$ are dual (or adjoint) with respect to the Weil pairing.

Proposition 5.2. Let $S \in E_1[m]$, $T \in E_2[m]$, and $\phi : E_1 \to E_2$ an isogeny. Then

$$e_m(S, \widehat{\phi}(T)) = e_m(\phi(S), T).$$

Proof) Let

$$div(f) = m(T) - m(O) \text{ and } f \circ [m] = g^m$$

be as above. Then

$$e_m(\phi S, T) = \frac{g(X + \phi S)}{g(X)}.$$

Choose a function $h \in \overline{K}(E_1)$ so that

$$\phi^*((T)) - \phi^*((O)) = (\widehat{\phi}T) - (O) + div(h).$$

Such an h exists because $\widehat{\phi}T$ is precisely the sum of the points of the divisor on the left hand side of this equality. Now

$$div(\frac{f \circ \phi}{h^m}) = \phi^* div(f) - m\, div(h) = m(\widehat{\phi}T) - m(O),$$

and

$$(\frac{g \circ \phi}{h \circ [m]})^m = \frac{f \circ [m] \circ \phi}{(h \circ [m])^m} = (\frac{f \circ \phi}{h^m}) \circ [m].$$

Thus from the definition of the e_m-pairing,

$$\begin{aligned} e_m(S, \widehat{\phi}T) =& \frac{\frac{g \circ \phi}{h \circ [m]}(X + S)}{\frac{g \circ \phi}{h \circ [m]}(X)} \\ =& \frac{g(\phi X + \phi S)}{g(\phi X)} \frac{h([m]X)}{h([m]X + [m]S)} \\ =& e_m(\phi S, T) \end{aligned}$$

□

Let l be a prime number different from $char(K)$. We would like to fit together the pairings

$$e_{l^n} : E[l^n] \times E[l^n] \to \mu_{l^n}$$

for all $n = 1, 2, 3, ...$ to give an l-adic Weil pairing on the Tate module

$$e : T_l(E) \times T_l(E) \to T_l(\mu).$$

Recall that the inverse limits for $T_l(E)$ and $T_l(\mu)$ are formed using the maps

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n] \text{ and } \mu_{l^{n+1}} \xrightarrow{l} \mu_{l^n}.$$

Thus to show that the e_{l^n}-pairings are compatible with taking the inverse limit, we must show that for any $S, T \in E[l^{n+1}]$,

$$e_{l^{n+1}}(S, T)^l = e_{l^n}([l]S, [l]T).$$

But by linearity,

$$e_{l^{n+1}}(S,T)^l = e_{l^{n+1}}(S,[l]T);$$

and then the desired result follows by applying compatibility to $e_{l^{n+1}}(S,[l]T)$ with $m = l^n$ and $m' = l$. This proves that e is well-defined, and it inherits all of the properties from (5.1) and (5.2), which completes the proof of the following.

Proposition 5.3. There exists a bilinear, alternating, non-degenerate, Galois invariant pairing

$$e : T_l(E) \times T_l(E) \to T_l(\mu).$$

Further, if $\phi : E_1 \to E_2$ is an isogeny, then ϕ and its dual isogeny $\widehat{\phi}$ are adjoint for the pairing.

6 Weil Conjectures for Elliptic Curves

We now prove the Weil conjectures for elliptic curves. Let l be a prime different from $char(K)$. Recall that we have a representation

$$End(E) \longrightarrow End(T_l(E)) : \psi \longrightarrow \psi_l.$$

If we choose a $\mathbb{Z}_l$-basis for $T_l(E)$, then we can write ψ_l as a 2×2 matrix, and in particular can compute

$$det(\psi_l), tr(\psi_l).$$

Proposition 6.1. Let $\psi \in End(E)$. Then

$$det(\psi_l) = deg(\psi) \text{ and } tr(\psi_l) = 1 + deg(\psi) - deg(1 - \psi).$$

In particular, $det(\psi_l)$ and $tr(\psi_l)$ are in $\mathbb{Z}$ and are independent of l.
Proof) Let v_1 and v_2 be a $\mathbb{Z}_l$-basis for $T_l(E)$, and write the matrix of ψ_l for this basis as

$$\psi_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Recall that there is a non-degenerate, bilinear, alternating pairing

$$e : T_l(E) \times T_l(E) \longrightarrow T_l(\mu).$$

We compute

$$\begin{aligned} e(v_1,v_2)^{deg(\psi)} &= e([deg(\psi)]v_1, v_2) \\ &= e(\widehat{\psi_l}\psi_l v_1, v_2) \\ &= e(\psi_l v_1, \psi_l v_2) \\ &= e(av_1 + bv_2, cv_1 + dv_2) \\ &= e(v_1,v_2)^{ad-bc} \\ &= e(v_1,v_2)^{det(\psi_l)}. \end{aligned}$$

Since e is non degenerate, we conclude that $deg(\psi) = det(\psi_l)$. Finally, for any 2×2 matrix A, a trivial calculation yields

$$tr(A) = 1 + det(A) - det(1 - A).$$

□

Now let

$$\phi : E \longrightarrow E$$

be the q^{th}-power Frobenius endomorphism. Since the Galois group $G(\overline{K}|K)$ is topologically generated by the q^{th}-power map on $\overline{K}$, we see that for a point $P \in E(\overline{K})$,

$$P \in E(K) \text{ if and only if } \phi(P) = P.$$

Thus

$$E(K) = ker(1 - \phi),$$

so

$$\begin{aligned} \#E(K) =& \#ker(1 - \phi) \\ =& deg(1 - \phi). \end{aligned}$$

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

$$\#E(K_n) = deg(1 - \phi^n).$$

The characteristic polynomial of ϕ_l has coefficients in $\mathbb{Z}$, so we can factor it over $\mathbb{C}$ as (say)

$$det(T - \phi_l) = T^2 - tr(\phi_l)T + det(\phi_l) = (T - \alpha)(T - \beta).$$

Further, since for every rational number $m/n \in \mathbb{Q}$,

$$det((m/n) - \phi_l) = det(m - n\phi_l)/n^2 = deg(m - n\phi)/n^2 \geq 0,$$

it follows that the quadratic polynomial $det(T - \phi_l)$ has complex conjugate roots or a double root. Thus $|\alpha| = |\beta|$, so from

$$\alpha\beta = det(\phi_l) = deg(\phi) = q,$$

we conclude that

$$|\alpha| = |\beta| = \sqrt{q}.$$

Finally we note that the characteristic polynomial of ϕ_l^n is given by

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

To compute this, we may put ϕ_l in Jordan normal form, so it is upper triangular with α and β on the diagonal. In particular,

$$\begin{aligned} \#E(K_n) =& \#ker(1 - \phi^n) \\ =& deg(1 - \phi_l^n) \\ =& 1 - \alpha^n - \beta^n + q^n. \end{aligned}$$

where $\alpha, \beta \in \mathbb{C}$ are complex conjugates of absolute value $\sqrt{q}$. From this expression it is easy to verify the Weil conjectures for elliptic curves as follows.

Theorem 6.2. Let K be a field with q elements and E/K an elliptic curve. Then there is an $a \in \mathbb{Z}$ so that

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

Further

$$Z(E/K;\frac{1}{qT}) = Z(E/K;T),$$

and

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

Proof) We compute

$$\begin{aligned}\sum_{n=1}^{\infty}(\#E(K_n))\frac{T^n}{n} &= \sum_{n=1}^{\infty}\frac{(1-\alpha^n-\beta^n+q^n)T^n}{n} \\ &= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) - \log(1-qT).\end{aligned}$$

Hence

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

which has the desired form, since from above α and β are complex conjugates of absolute value $\sqrt{q}$, and

$$a = \alpha + \beta = tr(\phi_l) = 1 + q - deg(1-\phi) \in \mathbb{Z}.$$

The functional equation is immediate with $\varepsilon = 0$. □

Remark 6.3. To see why (1.3c) is called the Riemann hypothesis, we make a change of variable and let $T = q^{-s}$. Thus for an elliptic curve we define

$$\zeta_{E/K}(s) = Z(E/K;q^{-s}) = \frac{1 - aq^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}.$$

Now the functional equation reads

$$\zeta_{E/K}(1-s) = \zeta_{E/K}(s),$$

which certainly looks familiar. Further, the Riemann hypothesis for $Z(E/K;T)$ proved above says that if $\zeta_{E/K}(s) = 0$, then $|q^s| = \sqrt{q}$, so $Re(s) = 1$.

References

[1] Joseph Silverman/The Arithmetic of Elliptic Curves
[2] Robin Hartshorne/Algebraic Geometry
[3] Shafarevich /Basic Algebraic Geometry 2