1 Elliptic Curves Over Finite Fields

1.1 Introduction

Definition 1.1. Elliptic curves can be defined over any field K; the formal definition of an elliptic curve is a non-singular (no cusps, self-intersections, or isolated points) projective algebraic curve over K with genus 1 with a given point defined over K. If the characteristic of K is neither 2 or 3, then every elliptic curve over K can be written in the form

$$y^2 = x^3 - px - q$$

where $p, q \in K$ such that the RHS does not have any double roots. If the characteristic of K is 3, then the most general equation is of the form

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

such that RHS has distinct roots.

In characteristic 2, the most general equation is of the form

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

provided that the variety it defines is non-singular.

Definition 1.2. A rational point is a point whose coordinates lie in K. W denote the set of rational points as $E(K)$ and this set forms a group.

1.2 Isogenies

Definition 1.3. A non-constant morphism $\phi : E_1 \to E_2$ between elliptic curves such that $\phi(O) = O$ is called an isogeny. Let $\phi : E_1 \to E_2$ be an isogeny. Then there is a unique isogeny $\hat{\phi} : E_2 \to E_1$ satisfying $\hat{\phi} \circ \phi = [\deg \phi]$. $\hat{\phi}$ is called the dual of ϕ.

Remark. In the above statement, $[n]$ denotes the isogeny which adds n times.

If E is defined over $\mathbb{F}_q$ and $\pi_{q,E} : E \to E$ is the Frobenius morphism $(x, y) \longmapsto (x^q, y^q)$, then $E(\mathbb{F}_q) = \ker(1 - \pi_{q,E})$.

As we noted, an isogeny has finite kernel.

Lemma 1.1. *Let E_1 and E_2 be isogenous elliptic curves defined over $\mathbb{F}_q$. Then $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.*

Proof. Any isogeny $\phi : E_1 \to E_2$ commutes with the Frobenius map on E_1 and E_2. Now, ϕ is surjective. So we have $y \in E_2(\mathbb{F}_q) \Leftrightarrow \pi_{q,E_2}(\phi(x)) = \phi(x) \Leftrightarrow x \in \ker((1 - \pi_{q,E_2})\phi)$. Now, each $\phi^{-1}(y)$ has $\deg_{\text{sep}} \phi$ elements.
Thus, $\#E_2(\mathbb{F}_q) = \ker((1 - \pi_{q,E_2})\phi)/\deg_{\text{sep}} \phi = \#\ker(\phi(1 - \pi_{q,E_2}))/\deg_{\text{sep}} \phi = \#\ker(\phi(1 - \pi_{q,E_1}))/\deg_{\text{sep}} \phi = \deg_{\text{sep}}(1 - \phi_{q,E_1}) = \#E_1(\mathbb{F}_q)$. □

Recall the following useful facts on degrees and dual maps

(i) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$

(ii) $[\hat{n}] = [n]$

(iii) $\deg[n] = n^2$

(iv) $\deg \hat{\phi} = \deg \phi$

(v) $\hat{\hat{\phi}} = \phi$

(vi) $\deg(-\phi) = \deg(\phi)$

(vii) $d(\phi, \psi) := \deg(\phi + \psi) - \deg \phi - \deg \psi$ is symmetric, bilinear on $\text{Hom}(E_1, E_2)$, where E_i is an elliptic curve.

(viii) $\deg \phi > 0$ for any isogeny ϕ

1.3 Riemann Hypothesis for Elliptic Curves

For an elliptic curve E defined over a finite field $\mathbb{F}_q$, the most obvious parameter is the number of points in $E(\mathbb{F}_q)$.

Theorem 1.1. *(Riemann hypothesis for elliptic curves (Hasse, 1934))*
Let E be an elliptic curve defined over $\mathbb{F}_q$. Then

$$|\#E(F_{q^n}) - 1 - q^n| \leqslant 2q^{n/2} \qquad \forall n \geqslant 1$$

Proof. Choose a Weierstrass equation with coefficients in $\mathbb{F}_q$. Since $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is topologically generated by $x \overset{\pi_q}{\longmapsto} x^q$, a point P of $E(\overline{\mathbb{F}_q})$ lies in $E(\mathbb{F}_q)$ if and only if $\pi_{q,E}(P) = P$. Thus $P \in E(\mathbb{F}_{q^n})$ if and only if $\pi_{q,E}^n(P) = P$, i.e., $E(\mathbb{F}_{q^n}) = \ker(1 - \pi_{q,E}^n)$. Now $1 - \pi_{q,E}^n$ is a separable morphism (since its differential is the identity). Thus, $\#E(\mathbb{F}_{q^n}) = \deg(1 - \pi_{q,E}^n)$. We noted that, for any two elliptic curves over a field, the function $d : \mathrm{Hom}(E_1, E_2) \times \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$, $(\phi, \psi) \longmapsto \deg(\phi + \psi) - \deg\phi - \deg\psi$ is a positive definite bilinear form. By the Cauchy-Schwarz inequality, we get

$$|\deg(1 - \pi_{q,E}^n) - \deg 1 - \deg \pi_{q,E}^n| \leqslant 2\sqrt{\deg 1 \deg \pi_{q,E}^n}$$

i.e.

$$|\#E(\mathbb{F}_{q^n}) - 1 - q^n| \leqslant 2q^{n/2}$$

□

1.4 The Weil Conjectures

Let $K_n = F_{q^n}$. If V is a projective variety, we want to keep account of $\#V(K_n)$. We can do this by using the zeta function of V and it is defined as the formal power series

$$Z(V/K_1 : T) = \exp\left(\sum_{n=1}^{\infty} \#V(K_n)\frac{T^n}{n}\right)$$

Note that

$$\#V(K_n) = \frac{1}{(n-1)!}\frac{\mathrm{d}^n}{\mathrm{d}T^n}\log Z(V/K_1, T)|_{T=0}$$

The reason for defining the zeta function in this manner is that the series $\sum_{n\geqslant 1} \#V(K_n)\frac{T^n}{n}$ often looks like the log of a rational function of T.

Let V be any smooth projective variety of dimension n, defined over $K_1 = \mathbb{F}_q$. Then:

- **Rationality conjecture**

$$Z(V/K_1; T) \in \mathbb{Q}(T)$$

- **Functional conjecture**

  There exists an integer χ such that

$$Z\left(V/K_1; \frac{1}{q^n T}\right) = \pm q^{n\chi/2} T^{\chi} Z(V/K_1; T)$$

- **Factorization**

  There exists a factorization

$$Z = \frac{P_1(T)P_3(T)\cdots P_{2n-1}(T)}{P_0(T)P_2(T)\cdots P_{2n-2}(T)P_{2n}(T)}$$

with $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$, each $P_i(T) \in \mathbb{Z}[T]$ and

$$P_i\left(\frac{1}{q^n T}\right) = P_{2n-i}(T)\left(\frac{-1}{Tq^{n-i/2}}\right)^{b_i}$$

where $b_i = \deg P_i = \deg P_{2n-i}$

- **Riemann hypothesis**

  Each root of $P_i(T)$ satisfies $|\alpha| = q^{-i/2}$

The conjecture was proven in its entirety by the efforts of Weil, Dwork, M. Artin, Grothendieck, Lubkin, Deligne, Laumon. But the first case for elliptic curves was solved by Hasse in 1934 before the conjectures were formulated in this generality by Weil in 1949. Weil pointed out that if one had a suitable cohomology theory for abstract varieties analogous to the usual cohomology for varieties over $\mathbb{C}$, the standard properties of the cohomology would imply all the conjectures. For instance, the functional equation would follow from Poincaré duality property. Such a cohomology is the étale cohomology.

1.5 Tate Modules and the Weil Pairing

Let E be an elliptic curve defined over $\mathbb{F}_q$. Suppose l is a prime not dividing q. We know that the $l-$division points of E, i.e., $E[l^n] \overset{d}{=} \ker[l^n]$ is $\mathbb{Z}/l^n \times \mathbb{Z}/l^n$.

The inverse limit of the groups $E[l^n]$ with respect to the maps $E[l^{n+1}] \xrightarrow{[l]} E[l^n]$ is the Tate module $T_l(E) = \varprojlim E[l^n]$. Since each $E[l^n]$ is naturally a $\mathbb{Z}/l^n-$module, it can be checked that $T_l(E)$ is a $\mathbb{Z}_l(= \varprojlim \mathbb{Z}/l^n)-$module. It is a free $\mathbb{Z}_l-$module of rank 2.

Any isogeny $\phi : E_1 \to E_2$ induces a $\mathbb{Z}_l-$module homomorphism $\phi_l : T_l(E_1) \to T_l(E_2)$. In particular, we have a representation $\mathrm{End}(E) \to M_2(\mathbb{Z}_l), \phi \longmapsto \phi_l$ if $l \nmid q$.

Note that $\mathrm{End}(E) \hookrightarrow \mathrm{End}(T_l(E))$ is injective because if $\phi_l = 0$ then ϕ is 0 on $E[l^n]$ for large n, i.e., $\phi = O$.

Finally, let us recall the Weil pairing. This is a non-degenerate, bilinear, alternating pairing

$$e : T_l(E) \times T_l(E) \to T_l(\mu) \overset{d}{=} \varprojlim \mu_{l^n} \cong \mathbb{Z}_l$$

It has the important property that $e(\phi x, y) = e(x, \hat{\phi} y)$.

Remark. For any general curves C, D, and a nonconstant morphism $\phi : C \to D$, recall that $\phi^* : \mathrm{Div}(D) \to \mathrm{Div}(C)$ is a homomorphism defined by

$$(P) \longmapsto \sum_{Q \in \phi^{-1}(P)} e_\phi(Q)(Q)$$

where $e_\phi(Q)$ is the ramification index at Q.

For $C = D$ an elliptic curve, all the $e_\phi(Q) = \deg_{\text{insep}} \phi$.

For a general C and D, $\mathrm{ord}_P(f \circ \phi) = e_\phi(Q)\,\mathrm{ord}_{\phi(P)}(f)$ for every nonconstant rational function on D.

1.6 Weil Conjectures for Elliptic Curves

Lemma 1.2. *Let $\phi \in \mathrm{End}(E)$ and $l \nmid q$ be a prime. Then,*

$$\det \phi_l = \deg \phi$$

$$\mathrm{trace}\, \phi_l = 1 + \deg \phi - \deg(1 - \phi)$$

In particular, $\det \phi_l, \mathrm{trace}\, \phi_l$ *are independent of l, and are integers.*

Proof. Let (v_1, v_2) be a $\mathbb{Z}_l-$ basis of $T_l(E)$ and write

$$\phi_l = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix}$$

with respect to this basis. We now use the Weil pairing e which is bilinear and alternating

$$\begin{aligned} e(v_1,v_2)^{\deg\phi} &= e(\deg(\phi)v_1,v_2) \\ &= e((\hat{\phi})_l(\phi)_l)v_1,v_2) \\ &= e(\phi_l v_1,\phi_l v_2) \\ &= e(av_1+cv_2,bv_1+dv_2) \\ &= e(v_1,v_2)^{ad-bc} \\ &= e(v_1,v_2)^{\det\phi_l} \end{aligned}$$

Since e is nondegenerate, we have that $\deg\phi = \deg\phi_l$.
Finally,

$$\begin{aligned} \operatorname{trace}\phi_l &= 1 + det\phi_l - \det(\mathrm{Id}-\phi_l) \\ &= 1+\deg\phi - \deg(1-\phi) \end{aligned}$$

□

To prove the Weil conjectures for E, we have to compute $\#E(K_n)$, where $K_n = \mathbb{F}_{q^n}$. Now $\#E(K_n) = \deg(1-\phi^n)$ where $\phi = \pi_{q,E}$ is the Frobenius isogeny.
A consequence of the lemma is the fact that the characteristic polynomial of ϕ_l has coefficients in $\mathbb{Z}$ when $l \neq \mathrm{char}\mathbb{F}_q$. Write $\det(\mathrm{Id}\cdot T-\phi_l) = (T-\alpha)(T-\beta)$ for $\alpha,\beta\in\mathbb{C}$. Moreover, for all $\frac{m}{n}\in\mathbb{Q}$, we get

$$\det\left(\frac{m}{n}\mathrm{Id}-\phi_l\right) = \frac{1}{n^2}\det(m\mathrm{Id}-n\phi_l) = \deg(m-n\phi)\frac{1}{n^2} > 0$$

This implies $\alpha = \overline{\beta}$. Note by triangularizing, that $\det\mathrm{Id}\cdot T-\phi_l^n) = (T-\alpha^n)(T-\beta^n)$, we get

Theorem 1.2. *For all $n \geqslant 1$, $\#E(K_n) = 1-\alpha^n-\overline{\alpha}^n+q^n$ where $|\alpha| = q^{1/2}$. In particular,*

$$Z(E/K_1;T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$$

where $a\in\mathbb{Z}$ and $1-aT+qT^2 = (1-\alpha T)(1-\overline{\alpha}T)$. Further, $Z(E/K_1;\frac{1}{qT}) = Z(E/K_1;T)$.

Proof. We have that

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

and $|\alpha| = \sqrt{q}$. Hence

$$\begin{aligned} \log Z(E/K_1;T) &= \sum_{n\geqslant 1}(1-\alpha^n-\overline{\alpha}^n+q^n)\frac{T^n}{n} \\ &= \sum\frac{T^n}{n} - \sum\frac{(\alpha T)^n}{n} - \sum\frac{(\overline{\alpha}T)^n}{n} + \sum\frac{(qT)^n}{n} \\ &= \log\frac{(1-\alpha T)(1-\overline{\alpha}T)}{(1-T)(1-qT)} \end{aligned}$$

The functional equation is obvious from the expression. The factorization $Z = \frac{P_1}{P_0P_2}$ is with $P_1(T) = 1-aT+qT^2$, so $P_1\left(\frac{1}{qT}\right) = \frac{P_1(T)}{(-1/T\sqrt{q})^2}$ □

Remark. Putting $\zeta_{E/\mathbb{F}_q}(s) = Z(E/K_1; q^{-s})$, one has

$$\zeta_{E/\mathbb{F}_q}(s) = \frac{1 - aq^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})} = \zeta_{E/\mathbb{F}_q}(1-s)$$

Note that the Riemann hypothesis for $Z(E/K_1;T)$ is equivalent to the fact that the zeros of $\zeta_{E/\mathbb{F}_q}(s)$ are on the line $\mathrm{Re}(s) = \frac{1}{2}$.

1.7 Supersingularity

Supersingular curves are a special class of elliptic curves which arise naturally. One of the most useful properties they have, as we shall prove, is that their definition forces them to be defines over a small finite field and, over any field, there are only finitely many elliptic curves isogenous to a supersingular one.
Before defining supersingularity, let us recall that an elliptic curve E is said to have complex multiplication if $\mathrm{End}(E) \neq \mathbb{Z}$. Let us recall the following result on $\mathrm{End}(E)$

Proposition 1.1. *(i)* $\mathrm{End}(E)$ *has no zero divisors.*

(ii) $\mathrm{End}(E)$ *is torsion free.*

(iii) $\mathrm{End}(E)$ *is either* $\mathbb{Z}$*, or an order in an imaginary quadratic field, or an order in a quaternion division algebra over* $\mathbb{Q}$.

Definition 1.4. An elliptic curve E defined over a field of characteristic $p > 0$ is said to be supersingular if $E[p] = O$.

The following characterization of supersingular elliptic curves is very useful

Proposition 1.2. *Let K be a perfect field of characteristic $p > 0$. Then the following statements are equivalent:*

(a) *E is singular*

(b) *$[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$*

(c) *$E[p^r] = O$ for some $r \geqslant 1$*

(d) *$E[p^r] = O$ for all $r \geqslant 1$*

(e) $\mathrm{End}_{\overline{K}}(E)$ *is an order in a quaternion division algebra over* $\mathbb{Q}$.

Remark. By the above proposition, up to isomorphism, there are only finitely many elliptic curves isogenous to a supersingular curve. For $p = 2$, $Y^2 + Y = X^3$ is the unique supersingular curve. For $p > 2$, we have the following theorem:

1.8 Structure of $E(\mathbb{F}_q)$

Theorem 1.3. *A group G of order $N = q + 1 - m$ is isomorphic to $E(\mathbb{F}_q)$ for some elliptic curve E over $\mathbb{F}_q$ if one of the following holds:*

(i) *$(q,m) = 1$, $|m| \leqslant 2\sqrt{q}$, and $G \cong \mathbb{Z}/A \times \mathbb{Z}/B$ where $B|(A, m-2)$*

(ii) *q is a square, $m = \pm 2\sqrt{q}$, and $G \cong (\mathbb{Z}/A)^2$ where $A = \sqrt{q} \mp 1$*

(iii) *q is a square, $p \equiv 1 \bmod 3$, $m = \pm\sqrt{q}$, and G is cyclic*

(iv) *q is not a square, $p = 2$ or 3, $m = \pm\sqrt{pq}$, and G is cyclic*

(v) *q is not a square, $p \not\equiv 3 \bmod 4$, $m = 0$, and G is cyclic*
or q is a square, $p \not\equiv 1 \bmod 4$, $m = 0$, and G is cyclic

(vi) *q is not a square, $p \equiv 3 \bmod 4$, $m = 0$, and G is either cyclic or $G \cong \mathbb{Z}/M \times \mathbb{Z}/2$ where $M = \frac{q+1}{2}$*