Elliptic Curves

Elliptic Curves

Definition (Weiestrass form of an Elliptic Curve)

Let K be a field of characteristic > 3. Then an **elliptic curve** E/K is a curve defined by a polynomial of the form

$$Y^2 = X^3 + aX + b$$

where $a, b \in K$ and $4a^3 + 27b^2 \neq 0$, along with a singular "point at infinity".

Elliptic Curves

Definition (Weiestrass form of an Elliptic Curve)

Let K be a field of characteristic > 3. Then an **elliptic curve** E/K is a curve defined by a polynomial of the form

$$Y^2 = X^3 + aX + b$$

where $a, b \in K$ and $4a^3 + 27b^2 \neq 0$, along with a singular "point at infinity".

Remark

Formally, an elliptic curve E/K is a projective algebraic variety of genus 1 with points in $\mathbb{P}^2_K$. Here, we have restricted the definition to nonsingular curves over finite fields.

Elliptic Curves

Definition

The set of points (x, y) on the curve such that $x, y \in K$ is denoted by $E(K)$.

Elliptic Curves

Definition

The set of points (x, y) on the curve such that $x, y \in K$ is denoted by $E(K)$.

For any field extension $\overline{K}/K$, we have that $E(\overline{K})$ forms an abelian group with the point at infinity as the identity.

Elliptic Curves

Definition

The set of points (x, y) on the curve such that $x, y \in K$ is denoted by $E(K)$.

For any field extension $\overline{K}/K$, we have that $E(\overline{K})$ forms an abelian group with the point at infinity as the identity.

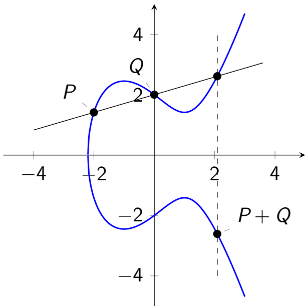


Figure: Elliptic Curve Group Law

Structure of Elliptic Curves

Let $K = \mathbb{F}_q$ where $q = p^k$ for some prime p.

Theorem

$E(\mathbb{F}_q)$ is either cyclic, or $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ with $n_1 | n_2$.

Isomorphisms Between Curves

- Over K, two curves $y^2 = x^3 + ax + b$ and $y^2 = x^3 + a'x + b'$ are isomorphic if and only if $a' = u^4 a$ and $b' = u^6 b$ for some u.

Isomorphisms Between Curves

- Over K, two curves $y^2 = x^3 + ax + b$ and $y^2 = x^3 + a'x + b'$ are isomorphic if and only if $a' = u^4 a$ and $b' = u^6 b$ for some u.

Definition (J-invariant)

We define the j-invariant as

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- The j-invariant determines the isomorphism class of E over $\overline{K}$

Isomorphisms Between Curves

- Over K, two curves $y^2 = x^3 + ax + b$ and $y^2 = x^3 + a'x + b'$ are isomorphic if and only if $a' = u^4 a$ and $b' = u^6 b$ for some u.

Definition (J-invariant)

We define the j-invariant as

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- The j-invariant determines the isomorphism class of E over $\overline{K}$
- Two curves not isomorphic over K but isomorphic over $\overline{K}$ are said to be *twists*

Isomorphisms Between Curves

Example

Let $E_1 : y^2 = x^3 - 25x$ and $E_2 : y^2 = x^3 - 4x$ over $\mathbb{Q}$. These two are not isomorphic over $\mathbb{Q}$, but over $\mathbb{Q}(\sqrt{10})$, we have the isomorphism

$$(x, y) \mapsto \left(\frac{10}{4}x, \frac{10\sqrt{10}}{8}y \right)$$

Isomorphisms Between Curves

Example

Let $E_1 : y^2 = x^3 - 25x$ and $E_2 : y^2 = x^3 - 4x$ over $\mathbb{Q}$. These two are not isomorphic over $\mathbb{Q}$, but over $\mathbb{Q}(\sqrt{10})$, we have the isomorphism

$$(x, y) \mapsto \left(\frac{10}{4}x, \frac{10\sqrt{10}}{8}y \right)$$

Note that $j(E_1) = 1728$ and $j(E_2) = 1728$. Curves with j-invariant 0 or 1728 are special: they have extra automorphisms.

Isogenies

Definition (Isogeny)

An **isogeny** from E_1 to E_2 is a homomorphism between the two curves

$$\phi : E_1(K) \to E_2(K)$$

given by rational functions

$$(x, y) \mapsto (R_1(x, y), R_2(x, y))$$

Isogenies

Definition (Isogeny)

An **isogeny** from E_1 to E_2 is a homomorphism between the two curves

$$\phi : E_1(K) \to E_2(K)$$

given by rational functions

$$(x, y) \mapsto (R_1(x, y), R_2(x, y))$$

- Every isogeny also induces a surjective group morphism from $E_1(\overline{K}) \to E_2(\overline{K})$.

Isogenies

Definition (Isogeny)

An **isogeny** from E_1 to E_2 is a homomorphism between the two curves

$$\phi : E_1(K) \to E_2(K)$$

given by rational functions

$$(x, y) \mapsto (R_1(x, y), R_2(x, y))$$

- Every isogeny also induces a surjective group morphism from $E_1(\overline{K}) \to E_2(\overline{K})$.
- If there exists a nonzero isogeny $E_1 \to E_2$, we say E_1 and E_2 are isogenous.

Isogenies

Definition (Isogeny)

An **isogeny** from E_1 to E_2 is a homomorphism between the two curves

$$\phi : E_1(K) \to E_2(K)$$

given by rational functions

$$(x, y) \mapsto (R_1(x, y), R_2(x, y))$$

- Every isogeny also induces a surjective group morphism from $E_1(\overline{K}) \to E_2(\overline{K})$.
- If there exists a nonzero isogeny $E_1 \to E_2$, we say E_1 and E_2 are isogenous.
- Note that we can rewrite the map as $(r_1(x), y \cdot r_2(x))$

Isogenies

Definition (Degree)

The degree of an isogeny is defined as the degree of the rational map $r_1(x)$, or

$$\max\{\deg p(x), \deg q(x)\}$$

where $r_1 = p/q$.

Isogenies

Definition (Degree)

The degree of an isogeny is defined as the degree of the rational map $r_1(x)$, or

$$\max \{\deg p(x), \deg q(x)\}$$

where $r_1 = p/q$.

Definition (Separable)

If the derivative $r_1'(x) \neq 0$, then we say the isogeny is **separable**.

Isogenies

Example

The multiplication by n map $[n] : E \to E$ defined by

$$P \mapsto nP = P + P + \cdots + P$$

is an isogeny from E to itself.

Isogenies

Example

The multiplication by n map $[n] : E \to E$ defined by

$$P \mapsto nP = P + P + \cdots + P$$

is an isogeny from E to itself.

Example

Let $E : y^2 = x^3 - x$ and $E' : y^2 + x^3 + 4x$. Then E and E' are isogenous by the map

$$(x, y) \mapsto (y^2/x^2, y(1 - x^2)/x^2)$$

Isogenies

Theorem

Let α be a separable isogeny. Then

$$\deg \alpha = \# \operatorname{Ker}(\alpha)$$

Isogenies

Theorem

Let α be a separable isogeny. Then

$$\deg \alpha = \#\,\mathrm{Ker}(\alpha)$$

Theorem

Given a finite subgroup $G \subseteq E_1(\overline{\mathbb{F}_q})$ there exists a unique separable isogeny $\alpha : E_1 \to E_2$ with kernel G. Moreover, it is efficient to compute such isogeny.

Isogenies

Theorem

For every $\alpha : E_1 \to E_2$*, there exists a dual isogeny* $\hat{\alpha} : E_2 \to E_1$ *such that*

$$\alpha \circ \hat{\alpha} = [\deg \alpha]$$

Isogenies

Theorem

For every $\alpha : E_1 \to E_2$, there exists a dual isogeny $\hat{\alpha} : E_2 \to E_1$ such that

$$\alpha \circ \hat{\alpha} = [\deg \alpha]$$

- $\hat{\hat{\alpha}} = \alpha$
- $\widehat{[n]} = [n]$
- For any α, β we have $\widehat{(\alpha + \beta)} = \hat{\alpha} + \hat{\beta}$

Torsion

Definition (n-torsion Subgroup)

The kernel of the multiplication by n map $[n] : E \to E$ is the *n-torsion subgroup*

$$E[n] = \left\{ P \in E(\overline{K}) : [n]P = 0 \right\}$$

Torsion

Definition (n-torsion Subgroup)

The kernel of the multiplication by n map $[n] : E \to E$ is the *n-torsion subgroup*

$$E[n] = \left\{ P \in E(\overline{K}) : [n]P = 0 \right\}$$

Theorem

If char K *does not divide* n*, then*

$$E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$$

If char $K \mid n$*, write* $n = p^r n'$ *with* $p \nmid n'$*. Then* $E[n] \cong \mathbb{Z}_{n'} \times \mathbb{Z}_{n'}$ *or* $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_{n'}$*.*

Torsion

Definition (n-torsion Subgroup)

The kernel of the multiplication by n map $[n] : E \to E$ is the *n-torsion subgroup*

$$E[n] = \{P \in E(\overline{K}) : [n]P = 0\}$$

Theorem

If char K *does not divide* n, *then*

$$E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$$

If char $K \mid n$, *write* $n = p^r n'$ *with* $p \nmid n'$. *Then* $E[n] \cong \mathbb{Z}_{n'} \times \mathbb{Z}_{n'}$ *or* $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_{n'}$.

If char $K = p$ and $E[p] \cong 0$, then E is called supersingular.

Endomorphisms

Definition (Endomorphism)

An endomorphism is an isogeny from E to itself.

Definition (Endomorphism Ring)

We define the endomorphism ring $\mathrm{End}(E)$ as the set of all endomorphisms on E with

- Addition defined as $(\alpha + \beta)(P) = \alpha(P) + \beta(P)$
- Multiplication defined as $\alpha\beta = \alpha \circ \beta$

Endomorphisms

Remark

We see that the map $\mathbb{Z} \to \mathrm{End}(E)$ *defined by*

$$n \mapsto [n]$$

is a ring morphism.

Frobenius Endomorphism

Let $\mathbb{F}_q$ be a finite field. Then define the Frobenius endomorphism $\pi_q : E(F_q) \to E(F_q)$ as

$$(x, y) \mapsto (x^q, y^q)$$

Frobenius Endomorphism

Let $\mathbb{F}_q$ be a finite field. Then define the Frobenius endomorphism $\pi_q : E(F_q) \to E(F_q)$ as

$$(x, y) \mapsto (x^q, y^q)$$

Lemma

Let E be defined over $\mathbb{F}_q$, and let $(x, y) \in E(\overline{\mathbb{F}_q})$. Then $(x, y) \in E(\mathbb{F}_q)$ if and only if $\pi_q(x, y) = (x, y)$.

Frobenius Endomorphism

Let $\mathbb{F}_q$ be a finite field. Then define the Frobenius endomorphism $\pi_q : E(F_q) \to E(F_q)$ as

$$(x, y) \mapsto (x^q, y^q)$$

Lemma

Let E be defined over $\mathbb{F}_q$, and let $(x, y) \in E(\overline{\mathbb{F}_q})$. Then $(x, y) \in E(\mathbb{F}_q)$ if and only if $\pi_q(x, y) = (x, y)$.

Proposition

Let $n > 1$. Then

- $\text{Ker}\left(\pi_q^n - 1\right) = E(\mathbb{F}_{q^n})$
- $\#E(\mathbb{F}_{q^n}) = \deg(\pi_q^n - 1)$

Hasse's Theorem and Frobenius Polynomial

Theorem (Hasse)

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

Furthermore, let $a = q + 1 - \#E(\mathbb{F}_q)$*. Then*

$$\pi_q^2 - a\pi_q + q = 0$$

and a *is the unique integer satisfying this polynomial.*

Trace

Lemma

For any $\alpha \in \mathrm{End}(E)$, *we have that* $\alpha + \hat{\alpha} = 1 + \deg \alpha - \deg(1 - \alpha)$

Trace

Lemma

For any $\alpha \in \text{End}(E)$*, we have that* $\alpha + \hat{\alpha} = 1 + \deg \alpha - \deg(1 - \alpha)$

Definition (Trace)

The trace of an endomorphism α is the integer $\text{tr}\,\alpha = \alpha + \hat{\alpha}$

Theorem

For all $\alpha \in \text{End}(E)$*, both* α *and* $\hat{\alpha}$ *are solutions to*

$$x^2 - (\text{tr}\,\alpha)x + \deg \alpha = 0$$

Restricted Endomorphisms

Definition (Restricted Endomorphism)

For any $\alpha \in \text{End}(E)$, its restriction to $E[n]$ is denoted $\alpha_n \in \text{End}(E[n])$.

Restricted Endomorphisms

Definition (Restricted Endomorphism)

For any $\alpha \in \mathrm{End}(E)$, its restriction to $E[n]$ is denoted $\alpha_n \in \mathrm{End}(E[n])$.

Recall that $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n = \langle P_1, P_2 \rangle$. Then we can view α_n as the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

Restricted Endomorphisms

Definition (Restricted Endomorphism)

For any $\alpha \in \text{End}(E)$, its restriction to $E[n]$ is denoted $\alpha_n \in \text{End}(E[n])$.

Recall that $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n = \langle P_1, P_2 \rangle$. Then we can view α_n as the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

Theorem

Let $\alpha \in \text{End}(E)$*, and let* $\text{char}\, K = p \nmid n$*. Then*

$$\text{tr}\, \alpha \equiv \text{tr}\, \alpha_n \pmod{n}$$

$$\deg \alpha \equiv \det \alpha_n \pmod{n}$$

Point Counting

Theorem

Let $\#E(\mathbb{F}_q) = q + 1 - a$. *We can then write* $x^2 - ax + q = (x - \alpha)(x - \beta)$. *Then*

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

Point Counting

Theorem

Let $\#E(\mathbb{F}_q) = q + 1 - a$*. We can then write* $x^2 - ax + q = (x - \alpha)(x - \beta)$*. Then*

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

Proof.

Let $f(x) = (x^n - \alpha^n)(x^n - \beta^n) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n$.

Point Counting

Theorem

Let $\#E(\mathbb{F}_q) = q + 1 - a$. *We can then write* $x^2 - ax + q = (x - \alpha)(x - \beta)$. *Then*

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

Proof.

Let $f(x) = (x^n - \alpha^n)(x^n - \beta^n) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n$.
Clearly $x^2 - ax + q$ divides $f(x)$.

Point Counting

Theorem

Let $\#E(\mathbb{F}_q) = q + 1 - a$. *We can then write* $x^2 - ax + q = (x - \alpha)(x - \beta)$. *Then*

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

Proof.

Let $f(x) = (x^n - \alpha^n)(x^n - \beta^n) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n$.
Clearly $x^2 - ax + q$ divides $f(x)$.Therefore, $f(\pi_q) = 0$. We then see that

$$(\pi_q^n)^2 - (\alpha^n + \beta^n)(\pi_q^n) + q^n = 0$$

Point Counting

Theorem

Let $\#E(\mathbb{F}_q) = q + 1 - a$. *We can then write* $x^2 - ax + q = (x - \alpha)(x - \beta)$. *Then*

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

Proof.

Let $f(x) = (x^n - \alpha^n)(x^n - \beta^n) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n$.
Clearly $x^2 - ax + q$ divides $f(x)$.Therefore, $f(\pi_q) = 0$. We then see that

$$(\pi_q^n)^2 - (\alpha^n + \beta^n)(\pi_q^n) + q^n = 0$$

Note that $\pi_q^n = \pi_{q^n}$.

Point Counting

Theorem

Let $\#E(\mathbb{F}_q) = q + 1 - a$. *We can then write* $x^2 - ax + q = (x - \alpha)(x - \beta)$. *Then*

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

Proof.

Let $f(x) = (x^n - \alpha^n)(x^n - \beta^n) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n$.
Clearly $x^2 - ax + q$ divides $f(x)$.Therefore, $f(\pi_q) = 0$. We then see that

$$(\pi_q^n)^2 - (\alpha^n + \beta^n)(\pi_q^n) + q^n = 0$$

Note that $\pi_q^n = \pi_{q^n}$.Since the value k such that $\pi_{q^n}^2 - k\pi_{q^n} + q^n = 0$ must be unique, we have

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

Supersingularity

Supersingular curves behave differently from ordinary curves. They have more "symmetry", or more endomorphisms, and are also very rare.

Theorem

Let $q = p^k$ where p is prime, and let E be an elliptic curve over $\mathbb{F}_q$. Then E is supersingular ($E[p] \cong 0$) if and only if $\operatorname{tr} \pi_q \equiv 0 \pmod{p}$.

Supersingularity

Supersingular curves behave differently from ordinary curves. They have more “symmetry”, or more endomorphisms, and are also very rare.

Theorem

Let $q = p^k$ where p is prime, and let E be an elliptic curve over $\mathbb{F}_q$. Then E is supersingular ($E[p] \cong 0$) if and only if $\operatorname{tr} \pi_q \equiv 0 \pmod{p}$.

Theorem

Let $p \geq 5$ be prime and $E(\mathbb{F}_p)$ supersingular. Then some power of π_p is an integer.

Supersingularity

Supersingular curves behave differently from ordinary curves. They have more "symmetry", or more endomorphisms, and are also very rare.

Theorem

Let $q = p^k$ where p is prime, and let E be an elliptic curve over $\mathbb{F}_q$. Then E is supersingular ($E[p] \cong 0$) if and only if $\operatorname{tr} \pi_q \equiv 0 \pmod{p}$.

Theorem

Let $p \geq 5$ be prime and $E(\mathbb{F}_p)$ supersingular. Then some power of π_p is an integer.

Supersingularity

Proof.

We have that $\operatorname{tr} \pi_p \equiv 0$. By Hasse's theorem, we see that $\operatorname{tr} \pi_p = 0$. Since

$$\pi_p^2 - a\pi_p + p = 0$$

we see that

$$\pi_p^2 = -p$$

□

Supersingularity

Proof.

We have that $\operatorname{tr} \pi_p \equiv 0$. By Hasse's theorem, we see that $\operatorname{tr} \pi_p = 0$. Since

$$\pi_p^2 - a\pi_p + p = 0$$

we see that

$$\pi_p^2 = -p$$

□

Remark

The previous theorem also holds for $p = 2, 3$, and can be proved case by case for both (Hasse's theorem gives a small list of possibilities for both).

Supersingularity

With Elliptic curves over $\mathbb{F}_q$, we have

- Endomorphisms corresponding to integers (multiplication)
- Endomorphisms from the Frobenius map
- Sometimes, we also get additional symmetries from extension fields – supersingular!

Isogeny Graphs

Definition (ℓ-isogeny graph)

Given $\mathbb{F}_q$ and a set S of isomorphism classes (j-invariants) of elliptic curves defined over $\mathbb{F}_q$, define the following graph:

- The set of vertices is S
- There exists an edge between $j, j' \in S$ if and only if there exists an ℓ-isogeny between curves with j invariants j, j'.

Endomorphism Rings

- Let $K = \mathbb{Q}(\sqrt{-D})$ (an imaginary quadratic field). Then an order $\mathcal{O} \subseteq K$ is a subring of K such that it is a finitely generated abelian group.

Endomorphism Rings

- Let $K = \mathbb{Q}(\sqrt{-D})$ (an imaginary quadratic field). Then an order $\mathcal{O} \subseteq K$ is a subring of K such that it is a finitely generated abelian group.

Theorem

If E is an elliptic curve over $\mathbb{F}_q$ which is ordinary, then $\mathrm{End}(E) \cong \mathcal{O}$ for some order in an imaginary quadratic field. If E is supersingular, then it corresponds to a larger ring (specifically an order in a quaternion algebra).

Ordinary Isogeny Graphs: Volcanoes

Definition (Directed Isogenies)

Let E, E' be curves with endomorphism rings $\mathcal{O}$, $\mathcal{O}'$. Let $\alpha : E \to E'$ be an isogeny of degree ℓ, then

- If $\mathcal{O} = \mathcal{O}'$, α is horizontal
- If $[\mathcal{O}' : \mathcal{O}] = \ell$, α is ascending
- If $[\mathcal{O} : \mathcal{O}'] = \ell$, α is descending

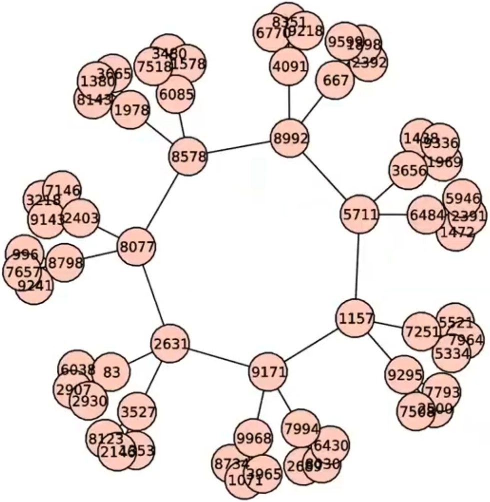
Ordinary Isogeny Graphs: Volcanoes

Definition (Directed Isogenies)

Let E, E' be curves with endomorphism rings $\mathcal{O}$, $\mathcal{O}'$. Let $\alpha : E \to E'$ be an isogeny of degree ℓ, then

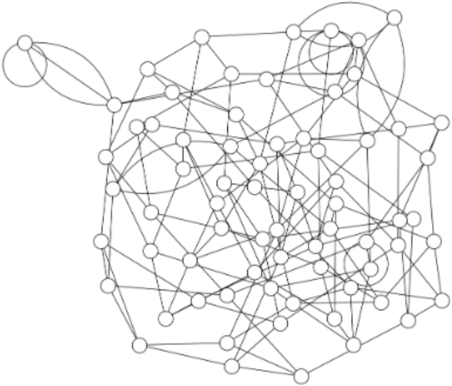
- If $\mathcal{O} = \mathcal{O}'$, α is horizontal
- If $[\mathcal{O}' : \mathcal{O}] = \ell$, α is ascending
- If $[\mathcal{O} : \mathcal{O}'] = \ell$, α is descending

Ordinary Isogeny Graphs: Volcanoes



(Credit: Dustin Moody, NIST)

Supersingular Isogeny Graphs



(Credit: Luca De Feo)