# 18.783 Elliptic Curves
# Lecture 13

Andrew Sutherland

March 14, 2022

# Ordinary and supersingular elliptic curves

**Definition**

Let $E/k$ be an elliptic curve of positive characteristic $p$.
If $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ then $E$ is ordinary, otherwise $E$ is supersingular.

We proved the following in previous lectures:

- Any isogeny $\alpha$ can be decomposed as $\alpha = \alpha_{\mathrm{sep}} \circ \pi^n$, where $\alpha_{\mathrm{sep}}$ is separable.
- $\deg_s \alpha := \deg \alpha_{\mathrm{sep}}$, $\deg_i \alpha := p^n$, and $\deg \alpha = (\deg_s \alpha)(\deg_i \alpha)$.
- We have $\# \ker \alpha = \deg_s \alpha$ (so $E$ is supersingular if and only if $\deg_s[p] = 1$).
- We have $\deg(\alpha \circ \beta) = (\deg \alpha)(\deg \beta)$, and similarly for $\deg_s$ and $\deg_i$.
- A sum of inseparable isogenies is inseparable.
- The sum of a separable and an inseparable isogeny is separable.
- The multiplication-by-$n$ map $[n]$ is inseparable if and only if $p|n$.
- Supersingularity is invariant under base change: $E[p] = \{Q \in E(\bar{k}) : pQ = 0\}$.

# Supersingularity is an isogeny invariant

**Theorem**

*Let $\phi\colon E_1 \to E_2$ be an isogeny of elliptic curves. Then $E_1$ is supersingular if and only if $E_2$ is supersingular (and $E_1$ is ordinary if and only if $E_2$ is ordinary).*

**Proof**: Let $p_1 \in \operatorname{End}(E_1)$ and $p_2 \in \operatorname{End}(E_2)$ denote multiplication-by-$p$ maps.
We have $p_2 \circ \phi = \phi + \cdots + \phi = \phi \circ p_1$, thus

$$\begin{aligned} p_2 \circ \phi &= \phi \circ p_1 \\ \deg_s(p_2 \circ \phi) &= \deg_s(\phi \circ p_1) \\ \deg_s(p_2)\deg_s(\phi) &= \deg_s(\phi)\deg_s(p_1) \\ \deg_s(p_2) &= \deg_s(p_1). \end{aligned}$$

The elliptic curve $E_i$ is supersingular if and only if $\deg_s(p_i) = 1$; the theorem follows.

# Criteria for supersingularity

Assume $p > 3$, so that $E\colon y^2 = x^3 + Ax + B$, and $E^{(p)}\colon y^2 = x^3 + A^p x + B^p$, so that $\pi\colon E \to E^{(p)}$. We also define $E^{(q)}\colon y^2 = x^3 + A^q x + B^q$ for any $q = p^n$.

Note that $[p] = \pi\hat{\pi}$, so $E$ is supersingular if and only if $\hat{\pi}\colon E^{(p)} \to E$ is inseparable.

### Theorem

*An elliptic curve $E/\mathbb{F}_q$ with $q = p^n$ is supersingular if and only if $\operatorname{tr}\pi_E \equiv 0 \bmod p$.*

**Proof**: If $E$ is supersingular then $[p] = \pi\hat{\pi}$ is purely inseparable, in which case $\hat{\pi}$ is inseparable, as are $\hat{\pi}^n = \widehat{\pi^n} = \hat{\pi}_E$ and $\pi_E = \pi^n$.

Their sum $[\operatorname{tr}\pi_E] = \pi_E + \hat{\pi}_E$ is inseparable, so $p$ must divide $\operatorname{tr}\pi_E$.
Equivalently, $\operatorname{tr}\pi_E \equiv 0 \bmod p$.

Conversely, if $\operatorname{tr}\pi_E \equiv 0 \bmod p$, then $[\operatorname{tr}\pi_E]$ is inseparable, as is $\hat{\pi}_E = [\operatorname{tr}\pi_E] - \pi_E$.
This means that $\hat{\pi}^n$ and $\hat{\pi}$ are inseparable which implies that $E$ is supersingular.

# Trace zero elliptic curves are supersingular

**Corollary**

*Let $E/\mathbb{F}_p$ be an elliptic curve over a field of prime order $p > 3$.*
*Then $E$ is supersingular if and only if $\operatorname{tr}\pi_E = 0$, equivalently, $\#E(\mathbb{F}_p) = p + 1$.*

**Proof**: By Hasse's theorem, $|\operatorname{tr}\pi_E| \le 2\sqrt{p}$, and $2\sqrt{p} < p$ for $p > 3$.

**Warning**: The corollary does not hold for $p = 2, 3$.

The corollary should convince you that supersingular elliptic curves are rare.
Of the $4\sqrt{p}$ possible Frobenius traces for $E/\mathbb{F}_p$, only one yields supersingular curves.

# Endomorphism algebras of ordinary elliptic curves

**Theorem**

*Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$ and suppose $\pi_E \notin \mathbb{Z}$.*
*Then $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E) \simeq \mathbb{Q}(\sqrt{D})$ is an imaginary quadratic field, $D = (\operatorname{tr} \pi_E)^2 - 4q$.*
*This applies in particular whenever $q$ is prime, and also whenever $E$ is ordinary.*

**Proof**: To the blackboard!

**Corollary**

*Let $E$ be an elliptic curve over $\mathbb{F}_q$ with $q = p^n$. If $n$ is odd or $E$ is ordinary, then $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E) \simeq \mathbb{Q}(\sqrt{D})$ is an imaginary quadratic field with $D = (\operatorname{tr} \pi_E)^2 - 4q$.*

**Proof**: If $\pi_E \in \mathbb{Z}$ then $D = (\operatorname{tr} \pi_E)^2 - 4 \deg \pi_E = 0$ and $2\sqrt{q} = \pm \operatorname{tr} \pi_E \in \mathbb{Z}$,
which is possible only when $q$ is a square and $\operatorname{tr} \pi_E$ is a multiple of $p$.
But then $n$ is even and $E$ is supersingular.

# Endomorphism algebras of ordinary elliptic curves

If $E/\mathbb{F}_q$ is an ordinary elliptic curve, or more generally, whenever $\pi_E \notin \mathbb{Z}$, the subring $\mathbb{Z}[\pi_E]$ of $\mathrm{End}(E)$ generated by $\pi_E$ is a lattice of rank 2.

It follows that $\mathbb{Z}[\pi_E]$ is an order in the imaginary quadratic field $K := \mathrm{End}^0(E)$, and is therefore contained in the maximal order $\mathcal{O}_K$ (the ring of integers of $K$).

**Definition**

The conductor of an order $\mathcal{O}$ in a number field $K$ is the positive integer $[\mathcal{O}_K : \mathcal{O}]$.

**Theorem**

*Let $E/\mathbb{F}_q$ be an elliptic curve for which $\mathrm{End}^0(E)$ is an imaginary quadratic field $K$ with ring of integers $\mathcal{O}_K$. Then*

$$\mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K,$$

*and the conductor of $\mathrm{End}(E)$ divides $[\mathcal{O}_K : \mathbb{Z}[\pi_E]]$.*

# The $j$-invariant of an elliptic curve

**Definition**

The $j$-invariant of the elliptic curve $E\colon y^2 = x^3 + Ax + B$ is

$$j(E) := j(A, B) := 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

Note that $\Delta(E) = -16(4A^3 - +27B^2) \neq 0$.

**Theorem**

*For every $j_0 \in k$ there is an elliptic curve $E/k$ with $j$-invariant $j(E) = j_0$.*

**Proof**: We assume $\mathrm{char}(k) \neq 2, 3$. If $j_0 = 0$ take $A = 0, B = 1$ and if $j_0 = 1728$ take $A = 1, B = 0$. Otherwise, let $A = 3j_0(1728 - j_0)$ and $B = 2j_0(1728 - j_0)^2$ so that

$$j(A, B) = 1728 \frac{4A^3}{4A^3 + 27B^2} = 1728 \frac{4 \cdot 3^3 j_0^3 (1728 - j_0)^3}{4 \cdot 3^3 j_0^3 (1728 - j_0)^3 + 27 \cdot 2^2 j_0^2 (1728 - j_0)^4} = j_0.$$

# The $j$-invariant is a $\bar{k}$-isomorphism invariant

**Theorem**

*Elliptic curves $E\colon\ y^2 = x^3 + Ax + B$ and $E'\colon\ y^2 = x^3 + A'x + B'$ defined over $k$ are isomorphic (over $k$) if and only if $A' = \mu^4 A$ and $B' = \mu^6 B$, for some $\mu \in k^\times$.*

**Proof**: To the blackboard!

**Theorem**

*Let $E$ and $E'$ be elliptic curves over $k$. Then $E_{\bar{k}} \simeq E'_{\bar{k}}$ if and only if $j(E) = j(E')$. If $j(E) = j(E')$ and $char(k) \neq 2, 3$ then there is a field extension $K/k$ of degree at most $6$, $4$, or $2$, for $j(E) = 0$, $j(E) = 1728$, or $j(E) \neq 0, 1728$, such that $E_K \simeq E'_K$.*

**Proof**: See notes.

The first statement is true in characteristic 2 and 3, but the second statement is not; one may need to take $K/k$ of degree up to $12$ when $k$ has characteristic 2 or 3.

# Supersingular elliptic curves

### Theorem

*Let $E$ be a supersingular elliptic curve over a field $k$ of characteristic $p > 0$. Then $j(E)$ lies in $\mathbb{F}_{p^2}$ (and possibly in $\mathbb{F}_p$).*

**Proof**: $E$ is supersingular, so $\hat{\pi}$ is purely inseparable and $\hat{\pi} = \hat{\pi}_{\mathrm{sep}}\pi$ with $\deg \hat{\pi}_{\mathrm{sep}} = 1$.
We thus have $[p] = \hat{\pi}\pi = \hat{\pi}_{\mathrm{sep}}\pi^2$, so $\hat{\pi}_{\mathrm{sep}}$ is an isomorphism $E^{(p^2)} \to E$.
By our theorem on $j$-invariants

$$j(E) = j(E^{(p^2)}) = j(A^{p^2}, B^{p^2}) = j(A, B)^{p^2} = j(E)^{p^2}.$$

Thus $j(E)$ is fixed by the $p^2$-power Frobenius automorphism $\sigma\colon x \mapsto x^{p^2}$ of $k$.

It follows that $j(E)$ lies in the subfield of $k$ fixed by $\sigma$, which is either $\mathbb{F}_{p^2}$ or $\mathbb{F}_p$, depending on whether $k$ contains a quadratic extension of its prime field or not.
In either case, $j(E)$ lies in $\mathbb{F}_{p^2}$.

# Endomorphism algebras of supersingular elliptic curves

Let $E/k$ be an elliptic curve over a field $k$ of characteristic $p > 0$.

**Theorem**

*If $E$ is supersingular if and only if $\mathrm{End}^0(E_{\bar{k}})$ is a quaternion algebra.*

**Proof**: To the blackboard!

**Corollary**

*Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic $p$.*
*Either $E$ is supersingular, $\operatorname{tr}\pi_E \equiv 0 \bmod p$, and $\mathrm{End}^0(E_{\overline{\mathbb{F}}_q})$ is a quaternion algebra,*
*or $E$ is ordinary, $\operatorname{tr}\pi_E \not\equiv 0 \bmod p$, and $\mathrm{End}^0(E_{\overline{\mathbb{F}}_q})$ is an imaginary quadratic field.*

When $E/\mathbb{F}_q$ is ordinary we always have $\mathrm{End}^0(E) = \mathrm{End}^0(E_{\overline{\mathbb{F}}_q})$.

But when $E$ is supersingular this need not hold. In particular, if $q = p^n$ with $n$ odd then $\mathrm{End}^0(E)$ is an imaginary quadratic field, while $\mathrm{End}^0(E_{\overline{\mathbb{F}}_q})$ is a quaternion algebra.