14 Ordinary and supersingular elliptic curves

Let E/k be an elliptic curve over a field of positive characteristic p. In Lecture 7 we proved that for any nonzero integer n, the multiplication-by-n map $[n]$ is separable if and only if n is not divisible by p. This implies that the separable degree of the multiplication-by-p map cannot be $p^2 = \deg[p]$, it must be either p or 1, meaning that its kernel $E[p]$ is either cyclic of order p or trivial. The terms *ordinary* and *supersingular* distinguish these two cases:

$$\begin{aligned} E \text{ is ordinary} \quad &\Longleftrightarrow \quad E[p] \simeq \mathbb{Z}/p\mathbb{Z}.\\ E \text{ is supersingular} \quad &\Longleftrightarrow \quad E[p] = \{0\}.\end{aligned}$$

We now want to explore this distinction further, and relate it to our classification of endomorphism algebras. In the previous lecture we showed that $\operatorname{End}^0(E) := \operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ has dimension $1, 2$, or 4 as a $\mathbb{Q}$-vector space, depending on whether $\operatorname{End}^0(E)$ is isomorphic to $\mathbb{Q}$, an imaginary quadratic field, or a quaternion algebra. In this lecture we will show that over fields of positive characteristic we never have$\operatorname{End}^0(E) \simeq \mathbb{Q}$, and that we can only have $\operatorname{End}^0(E)$ isomorphism to a quaternion algebra when E is supersingular.

Before we begin, let us recall some facts about isogenies proved in Lectures 6 and 7. We assume throughout that we are working in a field k of positive characteristic p.

1. Any isogeny α can be decomposed as $\alpha = \alpha_{\text{sep}} \circ \pi^n$, where α_{sep} is separable, and π is the (purely inseparable) p-power Frobenius map $\pi\colon (x : y : z) \mapsto (x^p : y^p : z^p)$.
2. If $\alpha = \alpha_{\text{sep}} \circ \pi^n$ then $\deg_s \alpha := \deg \alpha_{\text{sep}}$, $\deg_i \alpha := p^n$, and $\deg \alpha = (\deg_s \alpha)(\deg_i \alpha)$.
3. We have $\#\ker \alpha = \deg_s \alpha$ (so E is supersingular if and only if $\deg_s[p] = 1$).
4. We have $\deg(\alpha \circ \beta) = (\deg \alpha)(\deg \beta)$, and similarly for $\deg_s$ and $\deg_i$.
5. A sum of inseparable isogenies is inseparable and the sum of a separable and an inseparable isogeny is separable (a sum of separable isogenies need not be separable).
6. The multiplication-by-n map $[n]$ is inseparable if and only if $p|n$.

Recall that an isogeny α is purely inseparable when $\deg_s \alpha = 1$, equivalently, when $\ker \alpha = \{0\}$. Thus an elliptic curve is supersingular if and only if the multiplication-by-p map $[p]$ is purely inseparable. This makes it clear that the property of being ordinary or supersingular is invariant under base change: if E/k is an elliptic curve over k and L/k is any field extension, the separable degree of $[p]$ on E_L does not depend on L.

Warning 14.1. As noted in the previous lecture, in this course the ring $\operatorname{End}(E)$ consists of endomorphisms defined over k; if we wish to refer to endomorphisms defined over $\bar{k}$ we will write $\operatorname{End}(E_{\bar{k}})$ or refer to the *geometric* endomorphism ring (or algebra). Many authors use $\operatorname{End}(E)$ to denote $\operatorname{End}(E_{\bar{k}})$, but this distinction is important.[1]

The property of being ordinary or supersingular is an isogeny invariant.

Theorem 14.2. *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).*

[1] For example, there are algorithms that apply to any elliptic curve $E/\mathbb{F}_q$ for which $\operatorname{End}(E)$ is an imaginary quadratic field, but one often finds them written under the strictly stronger assumption that E is ordinary.

Lecture by Andrew Sutherland

Proof. Let $p_1 \in \operatorname{End}(E_1)$ and $p_2 \in \operatorname{End}(E_2)$ denote the multiplication-by-p maps on E_1 and E_2, respectively. 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. □

In what follows we will often want to refer to the image of E under the p-power Frobenius isogeny $(x : y : z) \mapsto (x^p : y^p : z^p)$ which will shall denote $E^{(p)}$. When E is defined over $\mathbb{F}_p$ we will have $E^{(p)} = E$ and π will be the Frobenius endomorphism π_E, but in general $E^{(p)}$ is the elliptic curve obtained by taking an equation for E and raising each coefficient to the pth power (it does not matter which equation we pick, the curve $E^{(p)}$ is well-defined up to isomorphism). We similarly define $E^{(q)}$ to be the image of the q-power Frobenius isogeny. Note that $[p] = \pi\hat{\pi}$ is purely inseparable if and only if $\hat{\pi}$ is purely inseparable (since π is always purely inseparable), thus E is supersingular if and only if $\hat{\pi}$ is purely inseparable.

In order to simplify the presentation we will often assume $p > 3$ and use short Weierstrass equations $y^2 = x^3 + Ax + B$ to define our elliptic curves, but except for where explicitly noted otherwise, all results in this lecture also hold in characteristic 2 and 3. An advantage of using short Weierstrass equations is that it allows us to put isogenies in our standard form $\left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$, with $u, v, s, t \in k[x]$ chosen so that $u \perp v$ and $s \perp t$.

We also note that $[p] = \pi\hat{\pi}$, where $\hat{\pi}$ is the dual of the p-power Frobenius isogeny π. The multiplicativity of separable degrees implies that $[p]$ is purely inseparable if and only if $\hat{\pi}$ is (since π is always purely inseparable) and $\deg \hat{\pi} = p$ is prime, so $\hat{\pi}$ is purely inseparable if and only if it is inseparable. Thus E is supersingular if and only if $\hat{\pi}$ is inseparable, a fact we will use to shorten the proofs that follow.

14.1 Ordinary/supersingular elliptic curves over finite fields

Theorem 14.3. *An elliptic curve $E/\mathbb{F}_q$ 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 then 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 therefore $\hat{\pi}$ is inseparable which implies that E is supersingular. □

Corollary 14.4. *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, if and only if $\#E(\mathbb{F}_p) = p + 1$.*

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

Warning 14.5. Corollary 14.4 does not hold for $p \le 3$; there are supersingular curves over $\mathbb{F}_2$ and $\mathbb{F}_3$ with nonzero Frobenius traces.

This should convince you that supersingular curves over $\mathbb{F}_p$ are rare: there are $\approx 4\sqrt{p}$ possible values for $\operatorname{tr}\pi_E$, all but one of which correspond to ordinary curves.

Theorem 14.6. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and suppose $\pi_E \not\in \mathbb{Z}$. Then $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E) \simeq \mathbb{Q}(\sqrt{D})$ is an imaginary quadratic field with $D = (\operatorname{tr}\pi_E)^2 - 4q$. This applies in particular whenever q is prime, and also whenever E is ordinary.*

Proof. The Frobenius endomorphism π_E is a root of its characteristic polynomial

$$x^2 - (\operatorname{tr}\pi_E)x + \deg \pi_E,$$

with discriminant $D = (\operatorname{tr}\pi_E)^2 - 4\deg\pi = (\operatorname{tr}\pi_E)^2 - 4q$, so $\mathbb{Q}(\pi_E) \simeq \mathbb{Q}(\sqrt{D})$. The assumption $\pi_E \not\in \mathbb{Z}$ implies $\pi_E \not\in \mathbb{Q}$, since π_E is an algebraic integer, and that $\operatorname{tr}(\pi_E)^2 \neq 4q$, so $D < 0$ (by the Hasse bound) and $\mathbb{Q}(\pi_E)$ is an imaginary quadratic field.

We can write any $\alpha \in \operatorname{End}^0(E)$ as $\alpha = s\phi$ with $s \in \mathbb{Q}$ and $\phi \in \operatorname{End}(E)$. Writing ϕ as $\phi(x,y) = (r_1(x), r_2(x)y)$ in standard form, we have

$$(\phi\pi_E)(x,y) = (r_1(x^q), r_2(x^q)y^q) = (r_1(x)^q, r_2(x)^q y^q) = (\pi_E\phi)(x,y),$$

thus ϕ, and therefore α, commutes with π_E. Therefore $\alpha \in \mathbb{Q}(\pi_E)$, by Lemma 13.18, so $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E)$ as claimed. □

Corollary 14.7. *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 if q is a square and $\operatorname{tr}\pi_E$ is a multiple of p, in which case n is even and E is supersingular. The corollary then follows from Theorem 14.6. □

If $E/\mathbb{F}_q$ is an ordinary elliptic curve, or more generally, whenever $\pi_E \not\in \mathbb{Z}$, the subring $\mathbb{Z}[\pi_E]$ of $\operatorname{End}(E)$ generated by π_E is a lattice of rank 2. It follows that $\mathbb{Z}[\pi_E]$ is an order in the imaginary quadratic field $K := \operatorname{End}^0(E)$, and is therefore contained in the maximal order $\mathcal{O}_K$ (the ring of integers of K). The endomorphism ring $\operatorname{End}(E)$ need not equal $\mathbb{Z}[\pi]$, but the fact that it contains $\mathbb{Z}[\pi]$ and is contained in $\mathcal{O}_K$ constrains $\operatorname{End}(E)$ to a finite set of possibilities. Recall from Theorem 13.27 that every order $\mathcal{O}$ in K is characterized by its *conductor* $[\mathcal{O} : \mathcal{O}_K]$.

Theorem 14.8. *Let $E/\mathbb{F}_q$ be an elliptic curve for which $\operatorname{End}^0(E)$ is an imaginary quadratic field K with ring of integers $\mathcal{O}_K$. Then*

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

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

Proof. Immediate from the discussion above. □

Remark 14.9. Theorem 14.8 implies that once we know $\operatorname{tr}\pi$ (which we can compute in polynomial time using Schoof's algorithm), which determines $\operatorname{End}^0(E) \simeq K = \mathbb{Q}(\sqrt{D})$ and the orders $\mathcal{O}_K$ and $\mathbb{Z}[\pi_E]$, we can constrain $\operatorname{End}(E)$ to a finite set of possibilities distinguished by the conductor $f := [\mathcal{O}_K : \operatorname{End}(E)]$. No polynomial-time algorithm is known for computing the integer f, but there is a Las Vegas algorithm that has a heuristically subexponential expected running time [1]. This makes it feasible to compute f even when q is of cryptographic size (say $q \approx 2^{256}$).

Remark 14.10. It will often be convenient to identify $\mathrm{End}^0(E)$ with K and $\mathrm{End}(E)$ with an order $\mathcal{O}$ in K. But we should remember that we are actually speaking of isomorphisms. In the case of an imaginary quadratic field, there are two distinct choices for this isomorphism. This choice can be made canonically, see [3, Thm. II.1.1], however this is not particularly relevant to us, as we are going to be working in finite fields where we cannot distinguish the square roots of D in any case. We thus accept the fact that we are making an arbitrary choice when we fix an isomorphism of $\mathrm{End}^0(E)$ with K by identifying π_E with, say, $(t+\sqrt{D})/2$ (as opposed to $(t-\sqrt{D})/2$).

Before leaving the topic of of ordinary and supersingular curves, we want to prove a remarkable fact: while over any algebraically closed field there are always infinitely many non-isomorphic elliptic curves, only a finite number can be supersingular. To prove this we first introduce the j-invariant, which will play a critical role in the lectures to come.

14.2 The j-invariant of an elliptic curve

As usual, we shall assume we are working over a field k whose characteristic is not 2 or 3, so that we can put our elliptic curves E/k in short Weierstrass form $y^2 = x^3 + Ax + B$.

Definition 14.11. 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 the denominator of $j(E)$ is nonzero, since it is the discriminant of the cubic $x^3 + Ax + B$, which has no repeated roots. There are two special cases worth noting: if $A = 0$ then $j(A,B) = 0$, and if $B = 0$ then $j(A,B) = 1728$ (note that A and B cannot both be zero). The j-invariant can also be defined for elliptic curves in general Weierstrass form, which is necessary to address fields of characteristic 2 and 3; see [2, III.1].[2]

The key property of the j-invariant $j(E)$ is that it characterizes E up to isomorphism over $\bar{k}$. Before proving this we first note that every element of the field k is the j-invariant of an elliptic curve defined over k.

Theorem 14.12. *For every $j_0 \in k$ there is an elliptic curve E/k with j-invariant $j(E) = j_0$.*

Proof. We assume $\mathrm{char}(k) \neq 2,3$; see [2, III.1.4.c] for a general proof. If j_0 is 0 or 1728 we may take E to be $y^2 = x^3+1$ or $y^2 = x^3+x$, respectively. Otherwise, let E/k be the elliptic curve defined by $y^2 = x^3 + Ax + B$ where

$$\begin{aligned} A &= 3j_0(1728-j_0),\\ B &= 2j_0(1728-j_0)^2. \end{aligned}$$

We claim that $j(A,B) = j_0$. We have

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

□

[2] As noted in the errata, there is a typo on p. 42 of [2]; the equation $b_2 = a_1^2 - 4a_4$ should read $b_2 = a_1^2 - 4a_2$.

We now give a necessary and sufficient condition for two elliptic curves to be isomorphic. An isomorphism ϕ of elliptic curves is an invertible isogeny, equivalently, an isogeny of degree 1 (the dual isogeny gives an inverse isomorphism, since $\phi\hat{\phi} = \hat{\phi}\phi = 1$). Recall from Lecture 5 that an isogeny between elliptic curves that are defined over k is assumed to be defined over k (hence representable by rational functions with coefficients in k), and we say that two elliptic curves are isogenous over an extension L of k to indicate that the isogeny is defined over L (strictly speaking, it is an isogeny between the base changes of the elliptic curves to L). As we saw in problem 3 of Problem Set 1, elliptic curves that are isomorphic over $\bar{k}$ need not be isomorphic over k.

Theorem 14.13. *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. Let $\phi\colon E \to E'$ be an isomorphism in standard form $\phi(x, y) = (r_1(x), r_2(x)y)$ with $r_1, r_2 \in k(x)$. Since ϕ is an isomorphism, its kernel is trivial, so r_1 and r_2 must be polynomials, by Lemma 5.26 and Corollary 5.27. Thus $r_1(x) = ax + b$ for some $a, b \in k$ with $a \neq 0$. Substituting into the curve equation for E', we have

$$r_2(x)^2 y^2 = (ax + b)^3 + A'(ax + b) + B'$$
$$r_2(x)^2 (x^3 + Ax + B) = (ax + b)^3 + A'(ax + b) + B'.$$

By comparing the degrees of the polynomials on both sides, we see that $r_2(x)$ must be constant, say $r_2(x) = c$. Comparing coefficients of x^2 shows that $b = 0$, and comparing coefficients of x^3 shows that $c^2 = a^3$; thus $a = (c/a)^2$ and $c = (c/a)^3$. If we let $\mu = c/a \in k^\times$ then we have

$$\mu^6(x^3 + Ax + B) = \mu^6 x^3 + A'(\mu^2 x) + B',$$

and it follows that $A' = \mu^4 A$ and $B' = \mu^6 B$ as claimed.

Conversely, if $A' = \mu^4 A$ and $B' = \mu^6 B$ for some $\mu \in k^*$, then the map $\phi\colon E \to E'$ defined by $\phi(x, y) = (\mu^2 x, \mu^3 y)$ is an isomorphism, since it is an isogeny of degree 1. □

We are now ready to prove the theorem stated at the beginning of this section.

Theorem 14.14. *Let E and E' be elliptic curves over k. Then E and E' are isomorphic over $\bar{k}$ if and only if $j(E) = j(E')$. If $j(E) = j(E')$ and the characteristic of k is not 2 or 3 then there is a field extension K/k of degree at most 6, 4, or 2, depending on whether $j(E) = 0$, $j(E) = 1728$, or $j(E) \neq 0, 1728$, such that E and E' are isomorphic over K.*

Remark 14.15. The first statement is true in characteristic 2 and 3 (see [2, III.1.4.b]), 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.

Proof. We assume $\operatorname{char}(k) \neq 2, 3$. Suppose $E\colon\ y^2 = x^3 + Ax + B$ and $E'\colon\ y^2 = x^3 + A'x + B'$ are isomorphic over $\bar{k}$. For some $\mu \in \bar{k}^*$ we have $A' = \mu^4 A$ and $B' = \mu^6 B$, by Theorem 14.13. We then have

$$j(A', B') = \frac{4(\mu^4 A)^3}{4(\mu^4 A)^3 + 27(\mu^6 B)^2} = \frac{4A^3}{4A^3 + 27B^2} = j(A, B).$$

For the converse, suppose that $j(A, B) = j(A', B') = j_0$. If $j_0 = 0$ then $A = A' = 0$ and we may choose $\mu \in K^\times$, where K/k is an extension of degree at most 6, so that $B' = \mu^6 B$

(and $A' = \mu^4 A = 0$). Similarly, if $j_0 = 1728$ then $B = 0$ and we may choose $\mu \in K^\times$, where K/k is an extension of degree at most 4, so that $A' = \mu^4 A$ (and $B' = \mu^6 B = 0$). We may then apply Theorem 14.13 to show that E and E' are isomorphic over K (by extending the field of definition of E and E' from k to K).

We now assume $j_0 \neq 0, 1728$. Let $A'' = 3j_0(1728 - j_0)$ and $B'' = 2j_0(1728 - j_0)^2$, as in the proof of Theorem 14.12, so that $j(A'', B'') = j_0$. Plugging in $j_0 = 1728 \cdot 4A^3/(4A^3 + 27B^2)$, we have

$$\begin{aligned} A'' &= 3 \cdot 1728 \frac{4A^3}{4A^3+27B^2}\left(1728 - 1728\frac{4A^3}{4A^3+27B^2}\right) \\ &= 3 \cdot 1728^2 \frac{4A^3 \cdot 27B^2}{(4A^3+27B^2)^2} = \left(\frac{2^7 3^5 AB}{4A^3+27B^2}\right)^2 A, \\ B'' &= 2 \cdot 1728 \frac{4A^3}{4A^3+27B^2}\left(1728 - 1728\frac{4A^3}{4A^3+27B^2}\right)^2 \\ &= 2 \cdot 1728^3 \frac{4A^3 \cdot 27^2 B^4}{(4A^3+27B^2)^3} = \left(\frac{2^7 3^5 AB}{4A^3+27B^2}\right)^3 B. \end{aligned}$$

Plugging in $j_0 = 1728 \cdot 4A'^3/(4A'^3 + 27B'^2)$ yields analogous expressions for A'' and B'' in terms of A' and B'. If we let

$$u = \left(\frac{2^7 3^5 AB}{4A^3+27B^2}\right)\left(\frac{4A'^3+27B'^2}{2^7 3^5 A'B'}\right),$$

then $A' = u^2 A$ and $B' = u^3 B$. We now choose $\mu \in K^\times$, where K/k is an extension of degree at most 2, so that we have $\mu^2 = u$. Then $A' = \mu^4 A$ and $B' = \mu^6 B$ and Theorem 14.13 implies that E and E' are isomorphic over K. □

Note that while $j(E) = j(A, B)$ always lies in the minimal field k containing A and B, the converse is not necessarily true. It could be that $j(A, B)$ lies in a proper subfield of k (squares in A can cancel cubes in B, for example). In this case we can construct an elliptic curve E' that is defined over the minimal subfield of k that contains $j(E)$ such that E' is isomorphic to E over $\bar{k}$ (but not necessarily over k).

14.3 Supersingular elliptic curves

Theorem 14.16. *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. Since E is supersingular, $\hat{\pi}$ is purely inseparable, so $\hat{\pi} = \hat{\pi}_{\text{sep}}\pi$ with $\deg \hat{\pi}_{\text{sep}} = 1$. We thus have $[p] = \hat{\pi}\pi = \hat{\pi}_{\text{sep}}\pi^2$, so $\hat{\pi}_{\text{sep}}$ is an isomorphism $E^{(p^2)} \to E$. By Theorem 14.13,

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

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 σ, 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 $\mathbb{F}_{p^2}$. □

Remark 14.17. Note that this theorem applies to any field k of characteristic p, not just finite fields. Thus in any field k of positive characteristic, the number of $\bar{k}$-isomorphism classes of supersingular elliptic curves is finite (it certainly cannot exceed $\#\mathbb{F}_{p^2} = p^2$). In fact, there are at most $\lfloor \frac{p}{12} \rfloor + 11$; see [2, Thm. V.4.1].

Theorem 14.18. *Let E/k be a supersingular elliptic curve. Then $\operatorname{End}^0(E_{\bar{k}})$ is a quaternion algebra.*

Proof. Without loss of generality we can assume $k = \bar{k}$, so that $\operatorname{End}(E_{\bar{k}}) = \operatorname{End}(E)$. Let us suppose for the sake of contradiction that $\operatorname{End}^0(E)$ is not a quaternion algebra. Then $\operatorname{End}(E)$ is isomorphic to $\mathbb{Z}$ or an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$, where we may assume $D < 0$ is squarefree. Suppose that ℓ is an odd prime equal to the degree of some $\phi \in \operatorname{End}(E)$; this cannot occur if $\operatorname{End}(E) \simeq \mathbb{Z}$, since integers have square degree, and the polynomial $x^2 - (\operatorname{tr}\phi)x + \ell$ must have a root in $\operatorname{End}^0(E) \simeq \mathbb{Q}(\sqrt{D})$, which implies that

$$\operatorname{tr}(\phi)^2 - 4\ell = v^2 D$$

for some integer v, and D must be a square modulo ℓ. There are infinitely many primes $\ell \neq p$ for which this is not true (these are the primes that do not split in the quadratic field $\mathbb{Q}(\sqrt{D})$, so there are infinitely many primes $\ell \neq p$ that are not the degree of any endomorphism of E. Let $\ell_1, \ell_2, \ldots$ be these primes (or all primes $\ell \neq p$ in the case $\operatorname{End}(E) \simeq \mathbb{Z}$).

For each ℓ_i we may construct a separable isogeny $\phi_i \colon E \to E_i$ of degree ℓ_i defined over $\bar{k}$ whose kernel is a cyclic subgroup of order ℓ_i contained in $E[\ell_i]$ using Vélu's formulas (see Theorem 6.15). The elliptic curves E_i are all supersingular, by Theorem 14.2, and Theorem 14.16 implies that only finitely many of them have distinct j-invariants. By Theorem 14.14, over $\bar{k}$ we must have an isomorphism $\iota \colon E_i \xrightarrow{\sim} E_j$ for some distinct i and j. Let us now consider the endomorphism $\phi := \hat{\phi}_j \circ \iota \circ \phi_i \in \operatorname{End}(E)$ of degree $\ell_i \ell_j$. The degree of this endomorphism is not a square, so $\operatorname{End}(E) \not\simeq \mathbb{Z}$ and we have $\operatorname{End}^0(E) \simeq \mathbb{Q}(\sqrt{D})$. As above we must have

$$\operatorname{tr}(\phi)^2 - 4\ell_i\ell_j = v^2 D,$$

for some integer v, which implies that D is a square modulo ℓ_i (and ℓ_j), a contradiction. □

When k is a finite field, the converse of the Theorem 14.18 is implied by Theorem 14.6. In fact the converse holds in all cases, but we won't prove this. For finite fields we have the following dichotomy.

Corollary 14.19. *Let E be an elliptic curve over a finite field of characteristic p. Either E is supersingular, $\operatorname{tr}\pi_E \equiv 0 \bmod p$, and $\operatorname{End}^0(E_{\overline{\mathbb{F}}_q})$ is a quaternion algebra, or E is ordinary, $\operatorname{tr}\pi_E \neq 0$, and $\operatorname{End}^0(E_{\overline{\mathbb{F}}_q})$ is an imaginary quadratic field.*

Warning 14.20. Corollary 14.19 does not hold if we replace $\operatorname{End}^0(E_{\overline{\mathbb{F}}_q})$ with $\operatorname{End}^0(E)$.

References

[1] G. Bisson and A.V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, Journal of Number Theory **131** (2011), 815–831.

[2] J.H. Silverman, *The arithmetic of elliptic curves*, second edition, Springer 2009.

[3] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer, 1994.