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:

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

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 it is isomorphic to $\mathbb{Q}$, an imaginary quadratic field, or a quaternion algebra. In this lecture we will show that $\operatorname{End}^0(E)$ is a quaternion algebra if and only if 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 prime 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 $(x : y : z) \mapsto (x^p : y^p : z^p)$.
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 $\# \ker \alpha = \deg_s \alpha$.
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.
6. A sum of separable isogenies need not be separable.
7. The sum of a separable and an inseparable isogeny is separable.
8. A composition of separable (inseparable) isogenies is separable (inseparable).
9. The multiplication-by-n is inseparable if and only if $p|n$.

Before analyzing the situation over finite fields, let us first note that the property of being ordinary or supersingular is an isogeny invariant.

Theorem 14.1. *Let $\phi \colon E_1 \to E_2$ be an isogeny. 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 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

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

We now note that E_i is supersingular if and only if $\deg_s(p_i) = 1$; the theorem follows. $\square$

14.1 Ordinary/supersingular elliptic curves over finite fields

Theorem 14.2. *An elliptic curve $E/\mathbb{F}_q$ is supersingular if and only if* $\operatorname{tr}\pi_E \equiv 0 \bmod p$.

Proof. Let $q = p^n$. If E is supersingular then $E[p] = \ker[p] = \ker \pi\hat{\pi}$ is trivial; therefore $\ker\hat{\pi}$ is trivial and $\hat{\pi}$ is inseparable. The isogeny $\hat{\pi}^n = \widehat{\pi^n} = \hat{\pi}_E$ is also inseparable, as is $\pi_E = \pi^n$, so $\operatorname{tr}\pi_E = \pi_E + \hat{\pi}_E$ is a sum of inseparable endomorphisms, hence inseparable, therefore $\operatorname{tr}\pi_E \equiv 0 \bmod p$, since $\operatorname{tr}\pi \in \mathbb{Z} \subseteq \operatorname{End}(E)$ is an integer ($[n]$ is inseparable iff $p|n$).

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, so $\ker\hat{\pi}$ must be trivial, since $\deg\hat{\pi} = p$ is prime. The kernel of π is also trivial, so $E[p] = \ker\hat{\pi}\pi$ is trivial and E is supersingular. $\square$

Corollary 14.3. *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, $|\operatorname{tr}\pi_E| \leq 2\sqrt{p}$, and $2\sqrt{p} < p$ for $p > 3$. $\square$

Warning 14.4. Corollary 14.3 is *not* true when p is 2 or 3.

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

Theorem 14.5. *If $E/\mathbb{F}_q$ is an ordinary elliptic curve then $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E)$ is an imaginary quadratic field.*

Proof. Let $q = p^n$. If $\pi_E \in \mathbb{Z} \subseteq \operatorname{End}(E)$ then $q = \deg\pi_E = \deg[r] = r^2$ for some $r \in \mathbb{Z}$, which implies that n is even and $r = \pm p^{n/2}$. But then $\operatorname{tr}\pi_E = 2r \equiv 0 \bmod p$ and E is supersingular, by Theorem 14.2, a contradiction. So $\pi_E \notin \mathbb{Z}$, and, $\pi_E \notin \mathbb{Q}$, because π_E is an algebraic integer.

Claim: For all $m \geq 1$ we have $\pi_E^m = a\pi_E + b$, for some $a \not\equiv 0 \bmod p$ and $b \equiv 0 \bmod p$.

Proof of claim: We proceed by induction on m. The base case holds with $a = 1$ and $b = 0$. For the inductive step:

$$\begin{aligned}
\pi_E^{m+1} &= \pi_E\pi_E^m = \pi_E(a\pi_E + b) && \text{(inductive hypothesis)}\\
&= b\pi_E + a((\operatorname{tr}\pi_E)\pi_E - q) && (\text{since } \pi_E^2 - (\operatorname{tr}\pi_E)\pi_E + q = 0)\\
&= (a(\operatorname{tr}\pi_E) + b)\pi_E - aq\\
&= c\pi_E + d,
\end{aligned}$$

where $c = a(\operatorname{tr}\pi_E) + b \not\equiv 0 \bmod p$, since $a\operatorname{tr}\pi_E \not\equiv 0 \bmod p$ and $b \equiv 0 \bmod p$, and we have $d = -aq \equiv 0 \bmod p$, as desired.

The claim implies $\pi_E^m \notin \mathbb{Q}$ for $m \geq 1$, since $\pi_E^m = a\pi_E + b$ with $a \neq 0$, and $\pi_E \notin \mathbb{Q}$. Now consider any $\alpha \in \operatorname{End}^0(E)$. We can write α as $\alpha = s\phi$ with $s \in \mathbb{Q}$ and $\phi \in \operatorname{End}(E)$. The endomorphism ϕ is defined over $\overline{\mathbb{F}}_q$, hence over $\mathbb{F}_{q^m}$ for some m. Writing ϕ as $\phi(x, y) = (r_1(x), r_2(x)y)$, we have

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

thus ϕ, and therefore α, commutes with π_E^m. It then follows from Lemma 13.17 proved in the previous lecture that $\alpha \in \mathbb{Q}(\pi_E^m) \subseteq \mathbb{Q}(\pi_E)$. Therefore $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E)$ as claimed. $\square$

Remark 14.6. In the proof above we used the fact that every endomorphism commutes with some power of the Frobenius endomorphism π_E to prove that when E is ordinary $\mathrm{End}^0(E)$ is an imaginary quadratic field. When E is supersingular it is still true that every endomorphism commutes with a power of π_E, but this power of π_E may lie in $\mathbb{Z}$.

In the case that $E/\mathbb{F}_q$ is ordinary, the proof above not only shows that $\mathrm{End}^0(E)$ is an imaginary quadratic field, it tells us exactly which quadratic field $\mathrm{End}^0(E) = \mathbb{Q}(\pi_E)$ is.

Corollary 14.7. *If $E/\mathbb{F}_q$ is an ordinary elliptic curve then $\mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{D})$, where $D = t^2 - 4q < 0$, with $t = \operatorname{tr} \pi_E$.*

Proof. By Theorem 14.5, $\mathrm{End}^0(E) = \mathbb{Q}(\pi_E)$, and $D = t^2 - 4q$ is the discriminant of the quadratic equation $x^2 - tx + q = 0$ satisfied by π_E, so $\mathbb{Q}(\pi_E) = \mathbb{Q}(\sqrt{D})$. We must have $D < 0$, since $\mathbb{Q}(\pi_E)$ is imaginary quadratic. $\square$

If $E/\mathbb{F}_q$ is an ordinary elliptic curve, then its Frobenius endomorphism π_E is not an integer, thus the subring $\mathbb{Z}[\pi_E]$ of $\mathrm{End}(E)$ 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 $K = \mathrm{End}^0(E)$, and is therefore contained in the maximal order $\mathcal{O}_K$, the ring of integers of K. The endomorphism ring $\mathrm{End}(E)$ need not equal $\mathbb{Z}[\pi]$, but the fact that it contains $\mathbb{Z}[\pi]$ and is contained in $\mathcal{O}_K$ constrains $\mathrm{End}(E)$ to a finite set of possibilities. Recall from Theorem 13.27 that every order $\mathcal{O}$ in K is uniquely characterized by its *conductor*, which is equal to $[\mathcal{O} : \mathcal{O}_K]$.

Theorem 14.8. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $\mathrm{End}^0(E) \simeq K = \mathbb{Q}(\sqrt{D})$ as above. Then*

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

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

Proof. Immediate from the discussion above. $\square$

Remark 14.9. Theorem 14.8 implies that once we know $t = \operatorname{tr} \pi$ (which we can compute in polynomial time using Schoof's algorithm), which determines $\mathrm{End}^0(E) \simeq K = \mathbb{Q}(\sqrt{D})$ and the orders $\mathcal{O}_K$ and $\mathbb{Z}[\pi_E]$, we can constrain $\mathrm{End}(E)$ to a finite set of possibilities distinguished by the conductor $f = [\mathcal{O}_K : \mathrm{End}(E)]$. 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. Thus we 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 about supersingular curves: they are all defined over $\mathbb{F}_{p^2}$. 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].[1]

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 $\operatorname{char}(k) \neq 2, 3$; 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

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

∎

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 $\mu \in k^\times$.*

[1] 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 $b_2 = a_1^2 - 4a_2$.

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 5.22 and Corollary 5.23. 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

$$\begin{aligned} r_2(x)^2y^2 &= (ax+b)^3 + A'(ax+b) + B' \\ r_2(x)^2(x^3+Ax+B) &= (ax+b)^3 + A'(ax+b) + B'. \end{aligned}$$

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

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

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

Conversely, if $A' = \mu^4A$ and $B' = \mu^6B$ for some $\mu \in k^*$, then the map $\phi\colon E \to E'$ defined by $\phi(x,y) = (\mu^2x, \mu^3y)$ 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 $A' = \mu^4A$ and $B' = \mu^6B$, by Theorem 14.13. We then have

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

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 $B' = \mu^6B$ (and $A' = \mu^4A = 0$). Similarly, if $j_0 = 1728$ than $B = 0$ and we may choose $\mu \in K^\times$, where K/k is an extension of degree at most 4, so that $A' = \mu^4A$ (and $B' = \mu^6B = 0$). 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

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

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 $A' = u^2A$ and $B' = u^3B$. 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 $j(E) = (A, B)$ 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. We assume E is defined by $y^2 = x^3 + Ax + B$ and for any prime power q of p, let $E^{(q)}$ denote the elliptic curve $y^2 = x^3 + A^q x + B^q$ (one uses a general Weierstrass equation in characteristic 2 or 3). Let π be the p-power Frobenius isogeny from E to $E^{(p)}$. The endomorphism $[p] = \hat{\pi}\pi$ has trivial kernel, since E is supersingular, so the isogeny $\hat{\pi}\colon E^{(p)} \to E$ has trivial kernel and must have inseparable degree p. By Corollary 6.4, we can decompose $\hat{\pi}$ as $\hat{\pi} = \hat{\pi}_{\rm sep} \circ \pi$, where the separable isogeny $\hat{\pi}_{\rm sep}$ must have degree 1 and is therefore an isomorphism.

We thus have

$$[p] = \hat{\pi}\pi = \hat{\pi}_{\rm sep}\pi^2,$$

and it follows that $\hat{\pi}_{\rm sep}$ is an isomorphism from $E^{(p^2)}$ to E. By Theorem 14.13 we have

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

Thus $j(E)$ is fixed by the 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. It implies that no matter what k is, the number of $\bar{k}$-isomorphism classes of supersingular elltipic curves is finite; there certainly cannot be more than $p^2 = \#\mathbb{F}_{p^2}$. In fact, there are at most $12p + 1$; see [2, Thm. V.4.1].

We can now characterize the endomorphism algebra of a supersingular elliptic curve.

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

Proof. Suppose not. Then $\operatorname{End}(E)$ is isomorphic to $\mathbb{Z}$ or an order in or an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$, where we may assume $D < 0$ is squarefree. We claim that in either case there are infinitely many odd primes ℓ with the property that $\operatorname{End}(E)$ contains no elements of degree ℓ. This is obvious when $\operatorname{End}(E) \simeq \mathbb{Z}$, since every integer endomorphism has square degree, so let us consider the case $\operatorname{End}^0(E) \simeq \mathbb{Q}(\sqrt{D})$. For any $\phi \in \operatorname{End}(E)$ the discriminant of the characteristic polynomial $x^2 + (\operatorname{tr}\phi)x + \deg\phi$ of ϕ is an integer that must be a square in $\operatorname{End}(E)$, since it has ϕ as a root. If $\deg\phi = \ell$ then we must have

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

for some integer v, and this implies that D is a square modulo ℓ. By quadratic reciprocity, whether D is a square modulo ℓ or not depends only on the residue class of ℓ modulo $4D$. For at least one of these residue classes, D is not a square modulo ℓ, and Dirichlet's theorem on primes in arithmetic progressions implies that there are infinitely many primes for which D is not a square modulo ℓ.

So let $\ell_1, \ell_2, \ldots$ be an infinite sequence of primes different from $p = \operatorname{char}(k)$ for which $\operatorname{End}(E)$ contains no elements of degree ℓ_i. 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 6.14). The elliptic curves E_i are all supersingular, by Theorem 14.1, and Theorem 14.18 implies that only finitely many of them have distinct j-invariants. By Theorem 14.14, over $\bar{k}$ we must have an isomorphism $\alpha\colon E_i \xrightarrow{\sim} E_j$ for some distinct i and j. Let us now consider the endomorphism $\phi := \hat{\phi}_j \circ \alpha \circ \phi_i \in \operatorname{End}(E)$ of degree $\ell_i\ell_j$. Since $\ell_i\ell_j$ is not a square we cannot have $\operatorname{End}(E) \simeq \mathbb{Z}$, so $\operatorname{End}(E)$ is an order in $\mathbb{Q}(\sqrt{D})$. The discriminant $(\operatorname{tr}\phi)^2 - 4\ell_i\ell_j$ is a square, and this implies that D must be a square modulo ℓ_i (and ℓ_j), which is a contradiction. □

When k is a finite field, the converse of the Theorem 14.18 is implied by Theorem 14.5. In fact the converse holds for any field k, but we won't prove this. For finite fields we have the following dichotomy.

Corollary 14.19. *The endomorphism algebra of an elliptic curve E over a finite field is either an imaginary quadratic field or a quaternion algebra, depending on whether E is ordinary or supersingular (respectively).*

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.