18.783 Elliptic Curves **Spring 2015**
Lecture #14 **03/31/2015**

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 mulitplication-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 explore this distinction further, focusing on the case that k is a finite field $\mathbb{F}_q$ of characterstic p. For an elliptic curve $E/\mathbb{F}_q$ we use π_E to denote the q-power Frobenius endomorphism of E and $\pi\colon (x,y) \mapsto (x^p, y^p)$ to denote the p-power Frobenius map from $E\colon y^2 = x^3 + Ax + B$ to $E^{(p)}\colon y^2 = x^3 + A^px + B^p$. The map π is an isogeny but not necessarily an endomorphism. Let us recall some standard facts about isogenies that we proved in Lectures 6 and 7.

1. A isogeny is separable if and only if the size of its kernel is equal to its degree.
2. Any isogeny α can be decomposed as $\alpha = \alpha_{\rm sep} \circ \pi^n$, where $\alpha_{\rm sep}$ is separable.
3. If $\alpha = \alpha_{\rm sep} \circ \pi^n$ then $\deg \alpha = \deg_s \alpha \deg_i \alpha$ with $\deg_s \alpha := \deg \alpha_{\rm sep}$ and $\deg_i \alpha := p^n$.
4. We have $\deg(\alpha \circ \beta) = (\deg \alpha)(\deg \beta)$, and similarly for $\deg_s$ and $\deg_i$.
5. A sum of a separable and an inseparable isogeny is separable.
6. A sum or composition of inseparable isogenies is inseparable.
7. A composition of separable isogenies is separable.

Note that a sum of separable isogenies may be separable or inseparable.

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. The isogeny ϕ is a group homomorphism, so we have

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

Thus E_1 is supersingular if and only if $\deg_i(p_1) = 1 = \deg_i(p_2)$ if and only E_2 is supersingular; this also implies that E_1 is ordinary if and only if E_2 is ordinary. □

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. We first suppose that E is supersingular and assume $q = p^n$ so that $\pi_E = \pi^n$. Then $\ker[p] = \ker \pi\hat{\pi}$ is trivial, and therefore $\ker\hat{\pi}$ is trivial. Thus $\hat{\pi}$ is inseparable, since it has degree $p > 1$. The isogeny $\hat{\pi}^n = \widehat{\pi^n} = \hat{\pi}_E$ is also inseparable, as is π_E, so $\operatorname{tr}\pi_E = \pi_E + \hat{\pi}_E$ is a sum of inseparable endomorphisms, hence inseparable (here we are viewing the integer $\operatorname{tr}\pi$ as an endomorphism). Therefore $\deg(\operatorname{tr}_E \pi) = (\operatorname{tr}_E \pi)^2$ is divisible by p, so $\operatorname{tr}\pi_E \equiv 0 \bmod p$.

Conversely, if $\operatorname{tr}\pi_E \equiv 0 \bmod p$, then p divides $\deg(\operatorname{tr}\pi_E) = (\operatorname{tr}\pi_E)^2$ and $\operatorname{tr}\pi_E$ 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 $\ker\hat{\pi}$ is trivial, since it has prime degree p, and the same is true of π. Thus the kernel of $[p] = \hat{\pi}\pi$ is trivial and E is supersingular. □

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, $|\operatorname{tr}\pi_E| \le 2\sqrt{p} < p$ for $p > 3$. □

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. In fact, the probability that a randomly chosen elliptic curve over $\mathbb{F}_p$ is supersingular is $\widetilde{\Theta}(1/\sqrt{p})$.[1] A similar proportion of supersingular curves arise over $\mathbb{F}_{p^2}$: the probability that a random elliptic curve $E/\mathbb{F}_{p^2}$ is supersingular is $\Theta(1/p)$. Remarkably, this trend does not continue. Up to isomorphism, *every* supersingular elliptic curve over a field of characteristic p can be defined over $\mathbb{F}_{p^2}$, as we will prove in §14.3.

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. Suppose $\pi_E \in \mathbb{Z} \subseteq \operatorname{End}(E)$. We have $\deg\pi_E = q^2$, and the only integers in $\operatorname{End}(E)$ with degree q^2 are $\pm q$. But then $\operatorname{tr}\pi_E = \pm 2q \equiv 0 \bmod p$ and E is supersingular, a contradiction. So $\pi_E \notin \mathbb{Z}$, and this implies $\pi_E \notin \mathbb{Q} \subseteq \operatorname{End}^0(E)$, since π_E is an algebraic integer. Thus either $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E)$ is an imaginary quadratic field, or $\operatorname{End}^0(E)$ is a quaternion algebra, in which case it contains some β that does not commute with π_E. We must show that the latter case does not occur.

Claim: For all $m \ge 1$ 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. In 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.

[1] The "soft" $\widetilde{O}$-notation ignores logarithmic factors.

The claim implies $\pi_E^m \notin \mathbb{Q}$ for any $m \geq 1$, since $\pi_E^m = a\pi_E + b$ with $a \neq 0$. 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 $\bar{\mathbb{F}}_q$, 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 13.16 proved in the previous lecture that $\alpha \in \mathbb{Q}(\pi_E^m) \subseteq \mathbb{Q}(\pi_E)$. Thus $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E)$ as claimed. □

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 $\operatorname{End}^0(E)$ 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 $\operatorname{End}^0(E)$ is an imaginary quadratic field, it tells us exactly which quadratic field $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E)$ is.

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

Proof. The proof of Theorem 14.5 shows that $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E)$, and D is the discriminant of the characteristic equation $x^2 - tx + q = 0$ satisfied by π_E, thus $\mathbb{Q}(\pi_E) \simeq \mathbb{Q}(\sqrt{D})$. Hasse's theorem implies $t^2 - 4q \leq 0$, and $t^2 \neq 4q$ because t is not divisible by p. □

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 $\operatorname{End}(E)$ 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 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 $\operatorname{End}^0(E) \simeq K = \mathbb{Q}(\sqrt{D})$ as above. Then*

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

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

Proof. Immediate from the discussion above. □

Remark 14.9. Theorem 14.8 implies that once we know $t = \operatorname{tr}\pi$ (which we can compute in polynomial time with 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 $\operatorname{End}^0(E)$ with K and $\operatorname{End}(E)$ 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 $(t-\sqrt{D})/2$).

In Problem Set 2 we saw how to use Cornacchia's algorithm to solve the equation $m = x^2 + dy^2$, where m and d are positive integers. Applying this to the case $m = 4q$ and $d = -D$, we can attempt to compute a solution to $4q = t^2 - v^2 D$. If it exists, the solution is unique up to the signs of t and v, thus if we know D we can determine t up to a sign. Conversely, given $D = t^2 - 4q < 0$, we will see in later lectures how to construct an elliptic curve with $\mathrm{End}^0(E) = \mathbb{Q}(\sqrt{D})$. Such an elliptic curve necessarily has trace $\pm t$. A preliminary example of this procedure appears on Problem Set 7. This is known as the *CM method*, and it will eventually allows us to construct elliptic curves over finite fields with any desired number of rational points.

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].[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 $j(E) = j_0$.*

This theorem is also true in characteristic 2 and 3; see [2, III.1.4.c].

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

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

[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 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, and when $k = \mathbb{F}_q$ is a finite field, elliptic curves that are isomorphic over $\overline{\mathbb{F}}_q$ need not have the same number of $\mathbb{F}_q$-rational points.

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 (if either had a non-constant denominator, the denominator would have a root in $\bar{k}$ which would be the x-coordinate of a non-trivial element of $\ker\phi$; see Lemma 5.22 and Corollary 5.23). Thus we must have $r_1(x) = ax+b$ for some $a, b \in k$, with $a \neq 0$. Substituting into the curve equation for E', we have

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

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

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

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 shall assume the characteristic of k is not 2 or 3. Suppose $E\colon y^2 = x^3 + Ax + B$ and $E'\colon y^2 = x^3 + A'x + B'$ are isomorphic over $\bar{k}$. then for some $\mu \in \bar{k}^*$ we have $A' = \mu^4 A$ and $B' = \mu^6 B$, by Theorem 14.13. Then

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

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 $j_0 = 1728$ than $B = 0$ and we may choose $\mu \in K^\times$, where K/k is an extension of degree at most 4, so that $A' = \mu A$ (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 $j(E) = (A, B)$ 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 $y^2 = x^3 + A^q x + B^q$. 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 is therefore purely inseparable of degree p. By Corollary 6.4, we can decompose $\hat{\pi}$ as $\hat{\pi} = \hat{\pi}_{\mathrm{sep}} \circ \pi$, where the separable isogeny $\hat{\pi}_{\mathrm{sep}}$ must have degree 1 (since $\hat{\pi}$ is purely inseparable) and is thus an isomorphism.

We therefore have

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

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

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

Thus $j(E)$ is fixed by the field 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* $\mathrm{End}^0(E)$ *is a quaternion algebra.*

Proof. Suppose not. Then $\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O}$ in either $\mathbb{Q}$ 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 primes ℓ with the property that $\mathrm{End}(E)$ contains no elements of degree ℓ. This is obvious when $\mathrm{End}(E) \simeq \mathbb{Z}$, since every integer endomorphism has square degree, so let us consider the case $\mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{d})$. For any $\phi \in \mathrm{End}(E)$ the discriminant of the characteristic polynomial $x^2 + (\mathrm{tr}\,\phi)x + \deg\phi$ of ϕ is an integer that is the square of an element of $\mathcal{O}$, since it has ϕ as a root. If $\deg\phi = \ell$ then we must have

$$(\mathrm{tr}\,\phi)^2 - 4\ell = v^2 d$$

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 $p = \mathrm{char}(k)$ for which $\mathrm{End}(E)$ 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 $E[\ell_i]$ (see Theorem 6.8). The elliptic curves E_i are all supersingular, by Theorem 14.1, so only finitely many of them are non-isomorphic. Thus 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 $\phi := \hat{\phi}_j \circ \alpha \circ \phi_i \in \mathrm{End}(E)$ of degree $\ell_i\ell_j$. Since $\ell_i\ell_j$ is not a square we cannot have $\mathrm{End}(E) \simeq \mathbb{Z}$, so $\mathcal{O}$ is an order in $\mathbb{Q}(\sqrt{D})$. The discriminant $(\mathrm{tr}\,\phi)^2 - 4\ell_i\ell_j$ is a square in $\mathcal{O}$, 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.