18.783 Elliptic Curves **Spring 2013**
Lecture #15 **04/04/2013**

15.1 Ordinary and supersingular curves

Let E/k be an elliptic curve over a field of positive characteristic p. In Lecture 7 we proved that the p-torsion subgroup of E is either cyclic of order p, or it is trivial, and we used this dichotomy to define the terms *ordinary* and *supersingular*:

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

We now explore this distinction further, focusing on the case that k is a finite field $\mathbb{F}_q$. We first recall some facts about separable and inseparable isogenies that were either proved in Lectures 6 and 7, or follow from Lemma 14.4, which states that the degree map is multiplicative.

1. A isogeny is separable if and only if the size of its kernel is equal to its degree.
2. The sum of a separable and an inseparable isogeny is separable.
3. Any sum or composition of inseparable isogenies is inseparable.
4. Any composition of separable isogenies is separable.

Note that a sum of separable isogenies need not be separable.

Theorem 15.1. *Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field, and let π_E be the Frobenius endomorphism of E. Then E is supersingular if and only if $\operatorname{tr}\pi_E \equiv 0 \bmod p$.*

Proof. Let $q = p^n$ and let π be the p-power Frobenius map $\pi(x, y) = (x^p, y^p)$ (note that π is an isogeny, but not necessarily an endomorphism, since E need not be defined over $\mathbb{F}_p$). We have $\hat\pi\pi = [p]$, where $[p]$ denotes the multiplication-by-p endomorphism on E.

We first suppose that E is supersingular. The kernel of $\hat\pi$ must then be trivial, since the kernel of $[p]$ is trivial, and $\hat\pi$ is therefore inseparable, since it has degree $p > 1$. The map $\hat\pi^n = \widehat{\pi^n} = \hat\pi_E$ is also inseparable, as is π_E, so $\operatorname{tr}\pi_E = \pi_E + \hat\pi_E$ is a sum of inseparable endomorphisms. Thus the endomorphism $[\operatorname{tr}\pi_E]$ is inseparable, which means that p divides $\operatorname{tr}\pi_E$, since $[m]$ is separable $\Leftrightarrow p \nmid m$, by Theorem 6.9. So $\operatorname{tr}\pi_E \equiv 0 \bmod p$.

Conversely, if $\operatorname{tr}\pi_E \equiv 0 \bmod p$, then $[\operatorname{tr}\pi_E]$ is inseparable, and $\hat\pi_E = \operatorname{tr}\pi_E - \pi_E$ is a sum of inseparable isogenies and therefore inseparable. This means that $\hat\pi^n$ and therefore $\hat\pi$ is inseparable. Therefore $\hat\pi$ must have trivial kernel, since its degree is prime, and the same is true of π. So the kernel of $[p] = \hat\pi\pi$ is trivial and E is supersingular. □

Corollary 15.2. *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 $\#E(\mathbb{F}_p) = p + 1$).*[1]

Proof. By Hasse's theorem, $|\operatorname{tr}(\pi_E)| \le 2\sqrt{p}$, which is smaller than p for all $p > 3$. □

[1] Corollary 15.2 is *not* true when p is 2 or 3.

This should convince you that supersingular curves over $\mathbb{F}_p$ are rare: there are $\Theta(\sqrt{p})$ 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 $\widetilde{\Theta}(1/\sqrt{p})$.[2] 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 §15.3. Thus the proportion of supersingular curves over $\mathbb{F}_{p^n}$ declines exponentially with n.

Theorem 15.3. *Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field. Then the endomorphism-algebra $\operatorname{End}^0(E)$ is either an imaginary quadratic field or a quaternion algebra. The latter occurs if and only if E is supersingular.*

Proof. We will just prove that $E/\mathbb{F}_q$ is ordinary if and only if $\operatorname{End}^0(E)$ is an imaginary quadratic field. For the supersingular case, see [1, V.3.1].

So let $E/\mathbb{F}_q$ be an ordinary elliptic curve, with $q = p^n$, and let π_E be the Frobenius endomorphism of E. Suppose $\pi_E \in \mathbb{Z} \subseteq \operatorname{End}^0(E)$. We have $N\pi_E = q^2$, and the only such integers in $\operatorname{End}^0(E)$ are $\pm q$, and therefore $\operatorname{tr}\pi_E = \pm 2q \equiv 0 \bmod p$. But this is a contradiction, since $\operatorname{tr}(\pi_E) \not\equiv 0 \bmod p$, by Theorem 15.1, so $\pi_E \notin \mathbb{Z}$, and $\operatorname{End}(E)$ must be either an imaginary quadratic field or a quaternion algebra, by Theorem 14.12.

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

Proof of claim: We proceed by induction. The base case holds with $a = 1$ and $b = 0$. We then have

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

where $c \not\equiv 0 \bmod p$, since $\operatorname{tr}(\pi_E) \not\equiv 0 \bmod p$, and clearly $d = -aq \equiv 0 \bmod p$.

It follows that $\pi_E^k \notin \mathbb{Q}$ for any k: if π_E^k is in $\mathbb{Q}$ then it must be an integer $\pm p^{nk}$ and then $\operatorname{tr}\pi_E^k = \operatorname{tr}(\pm p^{nk}) = \pm 2p^{nk}$ is divisible by p, but $\operatorname{tr}\pi_E^k = \operatorname{tr}(a\pi_E + b) \not\equiv 0 \bmod p$, by the claim. Now consider any $\alpha \in \operatorname{End}^0(E)$. We can write α as $\alpha = s\phi$ for some $s \in \mathbb{Q}$ and some $\phi \in \operatorname{End}(E)$. The endomorphism ϕ is defined over $\bar{\mathbb{F}}_q$, hence over $\mathbb{F}_{q^k}$ for some k. This implies that ϕ, and therefore α, commutes with π_E^k, since if $\phi(x,y) = (r_1(x), r_2(x)y)$ then

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

By Lemma 14.13, this implies that $\alpha \in \mathbb{Q}(\pi_E^k) \subseteq \mathbb{Q}(\pi_E)$. Therefore, $\operatorname{End}^0(E) = \mathbb{Q}(\pi_E)$ is an imaginary quadratic field. □

Remark 15.4. 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 $\mathbb{Z}$, and commuting with an element of $\mathbb{Z}$ tells us nothing about $\operatorname{End}^0(E)$.

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

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 15.5. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π_E. Then $\mathrm{End}^0(E) \simeq \mathbb{Q}(\sqrt{D})$, where $D = t^2 - 4q < 0$, with $t = \operatorname{tr} \pi_E$.*

Proof. The proof of Theorem 15.3 shows that $\mathrm{End}^0(E) = \mathbb{Q}(\pi_E)$, and D is the discriminant of the characteristic quadratic equation $x^2 - tx + q = 0$ satisfied by π_E, thus $\mathbb{Q}(\pi_E) \simeq \mathbb{Q}(\sqrt{D})$. Hasse's theorem implies $t^2 - 4q \le 0$, 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 $\mathrm{End}(E)$ 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 $\mathcal{O}_K$ narrows the possibilities. Recall from Theorem 14.20 that every order $\mathcal{O}$ in K is uniquely characterized by its *conductor*, which is equal to $[\mathcal{O} : \mathcal{O}_K]$, the index of $\mathcal{O}$ in $\mathcal{O}_K$.

Theorem 15.6. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π_E, and let $\mathcal{O}_K$ be the ring of integers of the imaginary quadratic field $K \simeq \mathrm{End}^0(E)$. Then*

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

and the conductor of $\mathrm{End}(E)$ is bounded by $[\mathcal{O}_K : \mathbb{Z}[\pi]]$.

Proof. Immediate from the discussion above. □

Remark 15.7. In Theorem 15.6 (and elsewhere), we 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 [2, Thm. II.1.1], however this is not so relevant to us, as we are going to be working in finite fields where we cannot distinguish the square roots of the discriminant 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 group order.

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 finite fields of degree at most 2, either a prime field $\mathbb{F}_p$, or $\mathbb{F}_{p^2}$. To prove this we first introduce the j-invariant, which will play a critical role in the lectures to come.

15.2 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 assume that elliptic curves E/k are in short Weierstrass form $y^2 = x^3 + Ax + B$.

Definition 15.8. 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 never 0, since we always require $4A^3 + 27B^2 \neq 0$. There are two special cases worth noting: if $A = 0$ then $j(A,B) = 0$, and if $B = 0$ then $j(A,B) = 1728$ (of course 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 [1, III.1].[3]

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 15.9. *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 [1, 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

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

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 (since $\hat{\phi}\phi = 1$). In general, the rational functions that define an isogeny may have coefficients in the algebraic closure $\bar{k}$, but in many situations we may want to distinguish isomorphisms that are actually defined over k, or some finite extenstion of k. For any field extension K/k, we say that two elliptic curves E/k and E'/k are isomorphic over K if there exists an isomorphism $\phi\colon E \to E'$ that is defined over K.

This distinction is important when working over a finite field $\mathbb{F}_q$. For example, two elliptic curves that are isomorphic over $\overline{\mathbb{F}}_q$ need not have the same number of $\mathbb{F}_q$-rational points, but if they are actually isomorphic over $\mathbb{F}_q$, this must be the case.

[3] As noted in the errata, there is a typo on p. 42 of [1]; the equation $b_2 = a_1^2 - 4a_4$ should read $b_2 = a_1^2 - 4a_2$.

Theorem 15.10. *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 $\mu \in k^*$*

Proof. Let $\phi\colon E \to E'$ be an isomorphism in standard form $\phi(x, y) = (r_1(x), r_2(x)y)$ with $r_1, r_2 \in k(x)$. The isogeny ϕ must have degree 1, since $\phi \circ \phi^{-1} = 1$. Since ϕ is an isomorphism, its kernel is trivial, so r_1 and r_2 must be polynomials (if they 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 $\ker\phi$, by Corollary 5.12). 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

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

By comparing degrees, we see that $r_2(x)$ must be constant, say $r_2(x) = c$. Then by considering the coefficient of x^2, we see that $b = 0$. The coefficient of x^3 implies that $c^2 = a^3$. Thus the above equations simplify to

$$a^3(x^3 + Ax + B) = a^3x^3 + A'(ax) + B',$$

and we must have $A' = a^2 A$ and $B' = a^3 B$. But $a^3 = c^2$, so $a = (c/a)^2$ is a square in k^*. So let $\mu = c/a \in k^*$, and then $A' = \mu^4 A$ and $B' = \mu^6 B$ as desired.

Conversely, if $A' = \mu^4 A$ and $B' = \mu^6 B$ for some $\mu \in k^*$, then let $\phi\colon E \to E'$ be the isogeny defined by $\phi(x, y) = (\mu^2 x, \mu^3 y)$. If (x_0, y_0) is any affine point on E then

$$y_0^2 = x_0^3 + Ax_0 + B.$$

Multiplying both sides by μ^6 yields

$$(\mu^3 y_0)^2 = (\mu^2 x_0)^3 + \mu^4 A(\mu^2 x_0) + \mu^6 B,$$

thus $\phi(x_0, y_0)$ is a point on $y^2 = x^3 + \mu^4 Ax + \mu^6 B = x^3 + A'x + B'$. It is clear that $\phi\colon E \to E'$ is an isomorphism, since it has an inverse $\phi^{-1}(x, y) = (\mu^{-2}x, \mu^{-3}y)$, and ϕ is defined over k, so E and E' are isomorphic over k. □

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

Theorem 15.11. *Let E and E' be elliptic curves over k. Then E and E' are isomorphic over $\bar{k}$ if and only if $j(E) = j(E')$. More precisely, there is a field extension K/k of degree at most 6, 4, or 2, depending on whether $j_0 = 0$, $j_0 = 1728$, or $j_0 \neq 0, 1728$, such that E and E' are isomorphic over K if and only if $j(E) = j(E')$.*

The first statement is also true in characteristic 2 and 3; see [1, III.1.4.b]

Proof. 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 15.10. 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 $\mu \in K^*$, where K/k is an extension of degree at most 6, so that $B' = \mu^6 B$ (and $A' = \mu^4 A$, trivially). Similarly, if $j_0 = 1728$ than $B = 0$ and we may choose $\mu \in K^*$, where K/k is an extension of degree at most 4, so that $A' = \mu A$ (and $B' = \mu^6 B$, trivially). We may then apply Theorem 15.10 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 15.9, 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 $\mu \in K^*$, 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 15.10 implies that E and E' are isomorphic over K. □

Note that while $j(A, B)$ always lies in the minimal field k containing A and B, the converse is not necessarily true. If A and B are both nonzero, it could be that $j(A, B)$ lies in a proper subfield of k (fourth powers in A can cancel sixth powers in B). But if we then define the curve $E'\colon y^2 = x^3 + A'x + B'$ using coefficients $A' = 3j_0(1728 - j_0)$ and $B' = 2j_0(1728 - j_0)^2$ and take a suitable quadratic twist, we can always obtain a curve that is isomorphic to E over k and is defined over the field $\mathbb{Q}(j(E))$. The j-invariant $j(E)$ determines the *minimal field of definition* of E.

15.3 The minimal field of definition of a supersingular curve

We now prove that every supersingular curve can be defined over $\mathbb{F}_{p^2}$.

Theorem 15.12. *Let $E/\mathbb{F}_{p^n}$ be a supersingular curve over a finite field. Then $j(E)$ lies in $\mathbb{F}_{p^2}$ (and possibly in $\mathbb{F}_p$) if n is even, and $j(E)$ lies in $\mathbb{F}_p$ otherwise.*

Proof. Let π be the p-power Frobenius isogeny from E to $E^{(p)}$ (if E is $y^2 = x^3+Ax+B$ then $E^{(p)}$ is $y^2 = x^3 + A^p x + B^p$), and let $E^{(p^2)}$ be the image of π^2. 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 5.16, we can decompose $\hat{\pi}$ as $\hat{\pi} = \phi \circ \pi$, where π is the p-power Frobenius isogeny from $E^{(p)}$ to $E^{(p^2)}$ and $\phi\colon E^{(p^2)} \to E$ is a separable isogeny of degree 1. The isogeny ϕ must then be an isomorphism, and it follows from Theorem 15.10 that $j(E) = j(E^{p^2}) = j(A^{p^2}, B^{p^2}) = j(E)^{p^2}$. Thus $j(E)$ is fixed by the p^2-power Frobenius map on the field $\mathbb{F}_{p^n}$. If n is even this means that $j(E)$ lies in $\mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^n}$, and otherwise $j(E)$ must lie in $\mathbb{F}_p$, since $\mathbb{F}_{p^2} \not\subseteq \mathbb{F}_{p^n}$ when n is odd. □

References

[1] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, second edition, Springer, 2009.

[2] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994.

18.783 Elliptic Curves
Spring 2013