A Brisk Jaunt to Supersingular Elliptic Curves

A few prequsites for Elkies' proof of the existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$

Siddharth G

May 15, 2020

1 Preliminaries

Throughout this article, we will have k as our base field. To make life easier, we will assume that $char(k) \neq 2, 3$. We will refer to projective points by $[x : y : z]$.

Definition 1.1. *An **elliptic curve** E/k is a smooth projective curve of genus one with a distinguished $k-$rational point.*

Concretely, this boils down to the following (projective) equation:

$$y^2 z = x^3 + Axz^2 + Bz^3$$

or equivalently we have the following affine equation (known as the Weierstrass form):

$$y^2 = x^3 + Ax + B$$

where $A^3 + 27B^2 \neq 0$ to ensure smoothness.
Here $[0 : 1 : 0]$ is the point at infinity and the distinguished point.

We can in fact make E into an abelian variety by giving it a group structure where the distinguished point acts as the identity element, 0. The group operation can (informally) be described by:

Any three points on a line sum to zero. We may need to double or triple count tangent points appropriately.

While it is easy to see that the binary operation thus defined is commutative, proving associativity requires some work. Using the above description, one can derive an explicit formula for the sum in terms of rational functions of the two points, however, there will be some casework involved.

2 Isogenies

We now proceed to define isogenies, which are "morphisms" of elliptic curves.

Definition 2.1. *An isogeny $\phi : E1 \to E2$ of elliptic curves is a surjective morphism of curves that induces a group homomorphism $E1(\bar{k}) \to E2(\bar{k})$.*

We will now try to expand a bit on the above definition and give a more concrete description of isogenies.

Definition 2.2. *Let C/k be a plane projective curve give by a homogeneous, non-constant $f(x, y, z)$ which is irreducible in $\bar{k}[x, y, z]$. Then the* ***function field*** *$k(C)$ is the set of equivalence classes of g/h where g, h are homogeneous polynomials of the same degree with $h \notin (f)$ and the equivalence relation $g_1/h_1 \; g_2/h_2$ if $g_1h_2 - g_2h_1 \in (f)$*

The elements of $k(C)$ act as functions on projective points as long as the denominator does not evaluate to 0. However, note that even if $h(P) = 0$, there could exist other elements in the equivalence class of g/h such that the denominator does not evaluate to 0 at P.

Definition 2.3. *Let C_1 and C_2 be plane projective curves given by f_1 and f_2 respectively. Then, a* ***rational map*** *$\phi : C_1 \to C_2$ is a triple of homogeneous polynomials $\psi_x, \psi_y, \psi_z \in k[x, y, z]$ of the same degree such that at least one of them is not in (f_1) and $f_2(\psi_1, \psi_2, \psi_3) \in (f_1)$. The rational map ϕ is defined at P if not all ψ's are zero and in this case, $[\psi_1(P) : \psi_2(P) : \psi_3(P)] \in C_2(k)$.*

A *morphism* is a rational map defined at every point P. Luckily for us, for smooth curves, every rational map is a morphism and in fact, every morphism is either surjective or constant. This sheds more light into the definition of an isogeny. In addition, if the rational map preserves the distinguished point, it automatically becomes a group homomorphism.

So, an isogeny is a non-constant rational map which preserves the distinguished point.

Example 2.4. *$P \mapsto -P$ is an isogeny*

Example 2.5. *$P \mapsto P + P \ldots + P = nP$ is an isogeny*

Example 2.6. *If $char(k) = p$, then the Frobenius map $\pi_E : [x, y, z] \mapsto [x^p : y^p : z^p]$ is an isogeny*

While we have somewhat simplified the notion of an isogeny, one can do even better and give a much simpler form using the Weierstrass form for Elliptic curves. We will call this the *standard form* of an isogeny.

Theorem 2.7. *Let $E_1 : y^2 = f_1(x), E_2 : y^2 = f_2(x) and \alpha : E_1 \to E_2$ be an isogeny. Then we can represent it using rational functions of the form:*

$$\alpha(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)} y \right)$$

where $u, v, s, t \in k[x]$ and u and v are coprime and so are s and t. Additionally, $v^3 | t^2$ and $t^2 | v^3 f_1$. In particular, v and t have the same roots.

The last two lines are important, and are essential in proving the following corollaries:

Corollary 2.8. *$[x : y : 1]$ is in the kernel of α iff $v(x) = 0$. The only other element in the kernel is 0.*

Corollary 2.9. *$ker(\alpha)$ is a finite subgroup of $E_1(k)$*

We now move on to define two invariants of isogenies which will serve us well in the future.

Definition 2.10. *Let $\alpha(x, y) = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$ be an isogeny in standard form. The **degree** of α is deg $\alpha := max(deg\ u, deg\ v)$. α is called **separable** if the derivative of $\frac{u(x)}{v(x)} \neq 0$ and otherwise we say that is **inseparable**.*

To justify why this nomenclature is warranted, we see that this definition of degree and separability coincide with the degree and separability of the field extension $\alpha^* : k(E_2) \to k(E_1)$.
It is easy to see that when $char(k) = 0$ every isogeny is separable. So, the inseparability occurs only in characteristic p, and in fact, it arises solely due to the Frobenius isogeny. This leads us to the following lemma:

Lemma 2.11. *In characteristic $p > 0$, every isogeny can be split into the following form*

$$\alpha = \alpha_{sep} \circ \pi^n$$

where α_{sep} is a separable isogeny. This gives us that deg α=p^ndeg α_{sep}.

We call the degree of α_{sep} the separable degree of α and denote it by $deg_s\ \alpha$ and we call the p^n the inseparable degree and denote it by $deg_i\ \alpha$.

Theorem 2.12. *The order of the kernel of an isogeny is equal to its separable degree.*

This immediately leads to a couple of corollaries:

Corollary 2.13. *Every purely inseparably extension has trivial kernel*

Corollary 2.14. *(Separable/Inseparable) degrees are multiplicative.*

Of course, this follows from vanilla field theory as well.
When $\alpha : P \mapsto nP$ then the kernel of α is called the *n-torsion subgroup* $E[n]$ and we denote α by $[n]$. This is going to be crucial in the definition of a supersingular elliptic curve.

Theorem 2.15. *Let $char(k) = p$, then, for each prime l, we have*

$$E[l^e] = \left\{ \begin{array}{ll} \mathbb{Z}/l^e\mathbb{Z} \oplus \mathbb{Z}/l^e\mathbb{Z}, & if\ l \neq p \\ \mathbb{Z}/l^e\mathbb{Z}\ or\ 0, & if\ l = p \end{array} \right\}$$

3 The Endomorphism Algebra

We define $Hom(E_1, E_2)$ to be the union of isogenies and the zero morphism. This makes $Hom(E_1, E_2)$ into a group under point-wise addition. For $\alpha \in Hom(E_1, E_2)$, we also have that $[n] \circ \alpha = \alpha \circ [n]$ and this indicates that this would impose a ring structure on $Hom(E, E) = End(E)$ and indeed, it does. Also, $\mathbb{Z}$ sits inside it as $[n]$. In fact, if we are in *char* $p > 0$ situation, then $\mathbb{Z}[\pi_E]$ lies in the center of $End(E)$ since $p(x_1^r, \ldots, x_n^r) = p(x_1, \ldots, x_n)^r$ and hence $\pi_E \circ \alpha = \alpha \circ \pi_E$ for any endomorphism α. Additionally, $End(E)$ has no zero divisors by virtue of **Corollary 2.9**

For any isogeny $\alpha : E_1 \to E_2$ we have the dual isogeny $\hat{\alpha} : \hat{E_2} = E_2 \to E_1 = \hat{E_1}$. This has the unique property that $\hat{\alpha} \circ \alpha = [deg\ \alpha] = [deg\ \hat{\alpha}]$. We have that $[\hat{n}] = [n] =$.

Lemma 3.1. $\hat{}: End(E) \to End(E)$ *is an involution (an anti-homomorphism of order 2).*

Lemma 3.2. *Let* $\alpha \in End(E)$. *Then* α *and* $\hat{\alpha}$ *are solutions to the characteristic equation*

$$x^2 - (tr\ \alpha)x + \deg\ \alpha$$

where $tr\ \alpha := \alpha + \hat{\alpha}$.

We now come to the question of reducing endomorphism to the torsion subgroups. This is useful invariant which helps us with differentiating endomorphisms.
Since $\alpha \in End(E)$ commutes with $[n]$, α preserves $E[n]$ and thus restricts to group endomorphism of $E[n]$ which we denote by α_n. With appropriate basis for $E[n]$ and n coprime to p, we can view α_n as a 2×2 matrix, by virtue of **Theorem 2.15**.

Theorem 3.3. *Let* n *be coprime to* $char(k)$. *Then,*

$$tr\ \alpha \equiv tr\ \alpha_n\ mod\ n$$

$$deg\ \alpha \equiv det\ \alpha_n\ mod\ n$$

This theorem is powerful enough to prove Hasse's Theorem ($\#E(\mathbb{F}_q) = q + 1 - t$).

Definition 3.4. *The* ***endomorphism algebra*** *of* E, $End^0(E) := End(E) \otimes \mathbb{Q}$

Since we are tensoring with $\mathbb{Q}$, every element can be written as pure tensor. $End^0(E)$ is a $\mathbb{Q}$-algebra, and like $End(E)$, it has no zero divisors. We denote $\alpha \otimes r$ by $r\alpha$. We would like to extend the notions for $End(E)$ to $End^0(E)$, in particular the dual, and thus we define it to be $\hat{r\alpha} = r\hat{\alpha}$. Note that this is constant on $\mathbb{Q}$.

Definition 3.5. *The reduced norm* $N\alpha := \alpha\hat{\alpha}$ *and the reduced trace* $T\alpha := \alpha + \hat{\alpha}$

The trace is a $\mathbb{Q}$-linear map and positive definite. The norm is multiplicative and respects duality and is positive definite. This shows that $End^0(E)$ is a division algebra.

Before we move on to a big theorem, we will need a definition:

Definition 3.6. *A* ***quaternion algebra*** *over k is a $k-$algebra that has a basis of the form $\{1, a, b, ab\}$ with $a^2, b^2 \in k^*$ and $ab = -ba$.*

And finally, what all of this has been leading up to:

Theorem 3.7 (Classification of Endomorphism Algebras)**.**
Let E/k be an elliptic curve. Then $End^0(E)$ is isomorphic to one of:

- $\mathbb{Q}$
- *an imaginary quadratic field $\mathbb{Q}(a)$ with $a^2 < 0$.*
- *a quaternion algebra $\mathbb{Q}(a, b)$ with $a^2, b^2 < 0$.*

Given this, one can prove that $End(E)$ is a free $\mathbb{Z}$-module of rank $1, 2$ or 4 respectively. In the second or third case, E is said to have *complex multiplication.*

If $char(k) = 0$, then only the first two cases can occur. If $char(k) > 0$, then only the last two case can occur. This can be proves using the facts in the following section.

4 Supersingular Elliptic Curves

For this section we will let $char(k) = p > 0$. From **Theorem 2.15**, recall that $E[p]$ is either $\mathbb{Z}/p\mathbb{Z}$ or 0. In the first case, E is called *ordinary* and in the second case, E is called *supersingular* as they are quite rare. We will try to give some characterizations of supersingular curves in this section.

Theorem 4.1. *If $\alpha : E_1 \to E_2$ is an isogeny, then E_1 is supersingular iff E_2 is.*

Theorem 4.2. *$E/\mathbb{F}_q$ is supersingular iff $tr\ \pi_E \equiv 0\ mod\ p$*

Using the above theorem and Hasse's theorem, one can see that out of the $4\sqrt{p}$ possibilities for $tr\ \pi_E$, only one of them corresponds to supersigular curves, which makes them quite rare.

We have already seen the j-invariant for modular forms, so lets work with the analagous j-invariant for elliptic curves.

Definition 4.3. *The j-invariant of an elliptic curve $E : y^2 = x^3 + Ax + B$ is*

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

As it will turn out, the j-invariant is a powerful invariant of elliptic curves.

Theorem 4.4. *For every $j_0 \in k$, there is an elliptic curve E/k such that $j(E) = j_0$.*

We now give a strong and surprising! (to me, at least) condition to check if two elliptic curves are isomorphic.

Theorem 4.5. *Elliptic curves E_1 and E_2 over k are isomorphic iff $A_1 = \mu^4 A_2$ and $B_1 = \mu^6 B_2$ for some $\mu \in k^*$.*

Coming back to the j-invariant, note that if $A = 0$, then $j(A, B) = 0$ and if $B = 0$, then $j(A, B) = 1728$. All of this leads to the following:

Theorem 4.6. *Let E_1 and E_2 be elliptic curves over k. They are isomorphic over $\bar{k}$ iff $j(E_1) = j(E_2)$. Furthermore, $j(E_1) = j(E_2)$ implies that there is a field extension K/k of degree $6, 4$ or 2 (in the cases $j(E_1) = 0, 1728$ or neither respectively) such that E_1 and E_2 are isomorphic over K.*

Note that elliptic curves being isomorphic over $\bar{k}$ is a weaker condition than being isomorphic over $\bar{k}$.

Lemma 4.7. *$j(E)$ is in $\mathbb{F}_{p^2}$*

Finally, here are some equivalent conditions for supersingular curves -

Theorem 4.8. *The following are equivalent*

- *E is supersingular.*
- *The dual of the Frobenius map is purely inseparable.*
- *$tr\ \pi_E \equiv 0\ mod\ p$*
- *$End(E_{\bar{\mathbb{F}}_q})$ is a quaternion algebra.*

Of course, if any of the above conditions is false, then E is ordinary.