Supersingular Elliptic Curves

Travis Scholl

April 23, 2015

Abstract

The goal of this is to define supersingular elliptic curves and say some basic stuff about them.

1 Elliptic Curves Over Fields

Definition 1.1 ([Sil09, III.3, p 59])**.** An *elliptic curve* is a smooth curve (projective variety of dimension 1) of genus 1 together together with a point on the curve.

We will slowly go through each word in the definition to see what it means.

1.1 Variety

1.1.1 Affine

An *affine algebraic set* V is the vanishing set of some polynomials in $\overline{K}[X]$. We will identify $\mathbb{A}^n$ with $\overline{K}^n$. We will denote K^n will be denoted by $\mathbb{A}^n(K)$. An algebraic set V is defined over K if it is the vanishing set of polynomials in $K[X]$. This is denoted by V/K. Let $V(K)$ denote $V \cap \mathbb{A}^n(K)$. The corresponding ideal $I(V)$ lives in $\overline{K}[X]$ and $I(V/K)$ lives in $K[X]$ (it is just $I(V) \cap K[X]$). An *affine variety* is an *irreducible* algebraic set. That means that either the ideal of vanishing polynomials $I(V)$ is prime in $\overline{K}[X]$ or the set cannot be written as a union of two closed subsets.

Remark 1.2. $x^2 - 2y^2$ is prime in $\mathbb{Q}[x, y]$ but not in $\overline{\mathbb{Q}}[x, y]$ because $x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y)$. So it is not enough to check $I(V/K)$ is prime but really $I(V) = I(V/K)\overline{K}[X]$ is prime.

1.1.2 Projective

The word projective means we take the analogous definitions in projective space $\mathbb{P}^n$, represented by homogeneous coordinates from $\mathbb{A}^{n+1}$. A *projective algebraic set* is the vanishing set of homogenous polynomials, which makes sense in $\mathbb{P}^n$. A *projective variety* is an irreducible projective algebraic set. The definitions of irreducible are more or less the same. For example, we could use that the homogeneous ideal $I(V)$ is prime in $\overline{K}[X]$.

Remark 1.3. We can also define $V(K)$ as $\{P \in V : P^\sigma = P \ \forall \ \sigma \in G_{\overline{K}/K}\}$. Here the action is on the coordinates of P in the obvious way. The same holds for projective varieties since the action will respect the equivalence relation.

Remark 1.4. For the case of $\mathbb{P}^n(\mathbb{Q})$ note that any homogeneous coordinate has a representative of the form $(x_1, \ldots, x_n)$ for relatively prime integers. So to find rational solutions to homogeneous polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$, it is sufficient to check for solutions that are relatively prime integers. In particular, to describe $V(\mathbb{Q})$, it is enough to describe the relatively prime integer solutions to the polynomials generating $I(V/\mathbb{Q})$.

1.2 Dimension

1.2.1 Affine

Let V be an affine-variety. *The dimension of* V is given by the transendence degree of the function field $\overline{K}(V)$ over the ground field $\overline{K}$. Here $L[V] = L[X]/I(V/L)$ and $L(V)$ is the fraction field of $L[V]$. Again here we are using algebraically closed fields.

Alternatively, it is the Krull dimension of the affine coordinate ring. Here we can use the ground field directly. If V is defined over K, then $\dim V = \dim K[X]/I(V/K)$.

1.2.2 Projective

Let V be a projective variety. Fix an embedding $\mathbb{A}^n \to \mathbb{P}^n$ such that $V \cap \mathbb{A}^n \neq \varnothing$. Then define $\dim V = \dim V \cap \mathbb{A}^n$. Proposition 2.6 in Chapter I says that $V \cap \mathbb{A}^n$ is an affine variety.

1.3 Smooth

1.3.1 Affine

Let V be an affine-variety of $\mathbb{A}^n$ and $I(V)$ be the corresponding ideal in the coordinate ring $\overline{K}[X_1, \ldots, X_n]$. By Hilbert Basis Theorem this ring is noetherian so $I(V)$ is finitely generated say by $f_1, \ldots, f_m$. Then V is *non-singular or smooth* at a point $P \in \mathbb{A}^n$ if the matrix

$$\left[\frac{\partial f_i}{\partial X_j}(P)\right]$$

has rank $n - \dim V$.

Alternatively, a point $P \in V$ is non-singular if and only if

$$\dim_{\overline{K}} M_P/M_P^2 = \dim V$$

where M_P is the maximal ideal in $\overline{K}[X]$ corresponding to P.

1.3.2 Projective

Let V be a projective variety. Fix an embedding $\mathbb{A}^n \to \mathbb{P}^n$ such that $P \in \mathbb{A}^n$. Note that $V \cap \mathbb{A}^n \neq \varnothing$. Then define $\dim V = \dim V \cap \mathbb{A}^n$.

1.4 Genus

1.4.1 Divisors

Let C be a curve. The *divisor group* $\operatorname{Div} C$ of a curve C is the free abelian group generated by the points of C. The *degree of a divisor* $D = \sum_{P \in C} n_P P$ is given by $\deg D = \sum n_P$. Let $\operatorname{Div}^0 C$ be the subgroup of divisors of degree 0.

Note that the Galois group acts on divisors in an obvious way, $D^\sigma = \sum n_P P^\sigma$. A divisor is *defined over* K if $D^\sigma = D$ for all $\sigma \in \operatorname{Gal}_{\overline{K}/K}$.

Let C be a smooth curve. Then by Proposition II.1.2 (finite number of poles/zeros) we can define $\operatorname{div}(f) = \sum \operatorname{ord}_P(f) P$ (see II.1). Here $\operatorname{ord}_P(f)$ is the maximum integer $d \geqslant 0$ such that $f \in M_P^d$ for polynomial f. It is basically the order of the 0 at P. It is extended to rational functions by $\operatorname{ord}_P(f/g) = \operatorname{ord}_P(f) - \operatorname{ord}_P(g)$.

Define $l(D) = \dim \mathscr{L}(D)$ where $\mathscr{L}(D) = \{f \in \overline{K}(C) \backslash \{0\} \colon \operatorname{div}(f) \geqslant -D\} \cup \{0\}$. We can think of $\mathscr{L}(D)$ to be the space of rational functions on C whose poles at every point are not worse than the corresponding coefficient in D.

Theorem 1.5 (Riemann-Roch, [Sil09, II.5.4])**.** *There exists an integer $g \geqslant 0$ called the genus of C, such that for every divisor $D \in \operatorname{Div} C$,*

$$l(D) - l(K_C - D) = \deg D - g + 1$$

where K_C is a canonical divisor on C (see [Sil09, II.4.4]).

Problem 1.6. *Show that $\mathscr{L}(D)$ is finite dimensional.*

Proof. We will show $l(D) \leqslant \deg D + 1$ whenever $\deg D \geqslant 0$ by induction on $\deg D$.

Base: If $\deg D = 0$ then show only constant functions work. Suppose a function had a root. Then it also has a pole somewhere.

Induction: Use the following fact:

$$\operatorname{div}(f) = \operatorname{div}(g) \Rightarrow f = cg \ , \quad \text{some constant } c.$$

□

1.5 Group Law

There are two equivalent ways of defining the group law on an elliptic curve. There is the geometrical way of intersecting lines and the following using the Picard group.

Definition 1.7. Let $(E/K, O)$ be an elliptic curve. Let $\mathrm{Div}^0(E)$ be the subgroup of $\mathrm{Div}(E)$ given by divisors of degree 0. We say a divisor D is *principle* if $D = \mathrm{div}(f)$ for some $f \in \overline{K}(E)^*$. Two divisors D_1, D_2 (denoted $D_1 \sim D_2$) are *linearly equivalent* if $D_1 - D_2$ is principle. Then define $\mathrm{Pic}^0(E)$ to be the quotient of Div^0 by the principle divisors. We also define $\mathrm{Pic}^0_K(E)$ to be the subgroup of $\mathrm{Pic}^0(E)$ fixed by $G_{\overline{K}/K}$.

Note that a map ϕ between curves induces a homomorphism on the group of divisors which takes degree 0 to degree 0. Moreover it takes principle divisors to principle divisors ($\mathrm{div}(f) \mapsto \mathrm{div}(\phi^* f)$) so it induces a group homomorphism on Pic^0, hence the naturality.

Proposition 1.8. *There is a well defined map $\sigma : \mathrm{Div}^0(E) \to E$ which takes a divisor D to a point P which satisfies $D \sim (P) - (O)$.*

There is a bijection of sets $\sigma : \mathrm{Pic}^0(E) \to E$.

If E is given by a Weirstrass equation then the geometric group law coincides with the group law induced by Pic^0.

Proof. Riemann-Roch plus the following clever lemma. □

Lemma 1.9. *Let C be a curve of genus 1 and $P, Q \in C$. Then $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. The reverse direction is trivial.

The Riemann-Roch theorem tells us $l((Q)) - l(K_C - (Q)) = \deg(Q)$. Also $\deg(K_C) = 2g - 2 = 0$. So $\deg K_C - D < 0$ which implies $l(K_C - (Q)) = 0$. This is because any non-constant function either has no roots/poles, or some roots/poles. Thus $\mathrm{div}(f)$ can not be effective (meaning the coefficient at every point is non-negative) unless it is 0. Hence $\mathscr{L}(K_C - (Q)) = 0 \Rightarrow l(K_C - (Q)) = 0$. So we have that $l((Q)) = \deg(Q) = 1$. Note that $\mathscr{L}((Q))$ already contains constant functions because $\mathrm{div}(c) = 0 \geqslant -(Q)$. What this means is that $\mathscr{L}((Q)) = \overline{K}$, i.e. it is only constant functions.

By hypothesis $(P) - (Q)$ is principle so there is some $f \in \overline{K}^*(C)$ such that $\mathrm{div}(f) = (P) - (Q)$. Then in particular $f \in \mathscr{L}$. So by above $f \in \overline{K}$. This implies $\mathrm{div}(f) = 0 \Rightarrow (P) = (Q) \Rightarrow P = Q$. □

2 Reduction

Let K be a local field with a discrete valuation v. Think of finite extensions of $\mathbb{Q}_p$ or formal Laurent series $\mathbb{F}_q((t))$ where q is a power of a prime p. Let R be the valuation ring of K, i.e. $R = \{x \colon v(x) \geqslant 0\}$.

Then R is a local PID. Let $M = (\pi) = \pi R$ be the maximal ideal. We may assume v is normalized so $v(\pi) = 1$. By convention $v(0) = \infty$. Let k be the residue field R/M.

We assume k, K are both perfect (finite extensions are separable).

We can always find a Weierstrass equation for an elliptic curve E/K of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Remark 2.1. The indices on the a_i are because if we replace (x, y) with $(x/u^2, y/u^3)$ (which is an isomorphism of curves) the coefficients become a_iu^i. This allows us to "scale" them so that all coefficients lie in R.

Definition 2.2. A Weierstrass equation is *minimal* if $v(\Delta)$ is minimized with respect to the condition $a_i \in R$.

Remark 2.3. It is easy to see every curve E/K has a minimal Weierstrass model because v is discrete.

One can show the minimal equation is unique up to a certain change of coordinates, see [Sil09, VII.2 Prop. 1.3].

Definition 2.4. Given an elliptic curve E/K and a minimal Weirstrass equation, define a curve $\tilde{E}/k$ to be the *reduction of E modulo π* given by the equation

$$\tilde{E} : \ y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

Here $x \mapsto \tilde{x}$ is the map $R \to R/\pi R$. Again, the equation for $\tilde{E}$ is unique up to a change of coordinates over k (not K) like before.

Remark 2.5. There is a map $E \to \tilde{E}$ which is just the restriction of a reduction map $\mathbb{P}^2(K) \to \mathbb{P}^2(k)$. In general, given any homogeneous coordinate $[x_0, \dots, x_n]$ we can find representatives such that all $x_i \in R$ and one of them is a unit.

To see this, let $n = \max |v(x_i)|$. Then consider $[\pi^n x_0, \dots, \pi^n x_n]$. Because $v(\pi^n x_0) = v(\pi^n) + v(x_0)$ it will be non-negative by construction and one of them will be 0. So all will live in R and one is a unit. Choosing these coordinates defines a reduction map $\mathbb{P}^n(K) \to \mathbb{P}^n(k)$.

As stated, the reduced curve *may not necessarily be an elliptic curve*. Since we have written a nice (Weierstrass) equation for it, $\tilde{E}$ is a curve. Also we have a point $\tilde{O} \in \tilde{E}$, the image of the given point O on E. So the only thing stopping $\tilde{E}$ from being an elliptic curve is smoothness. This suggestions the following definitions.

Definition 2.6. E has *good reduction* at π if $\tilde{E}$ is non-singular. Otherwise E has *bad reduction*.

Proposition 2.7. *E has good reduction at π if and only if* $\min v(\Delta) > 0$ *where the minimum is taken over all models/Weierstrass equations with integer coefficients representing E.*

Proof. Being non-singular is the same as $\Delta \neq 0$ by [Sil09, Prop. III.1.4(a)]. Now use the fact that $x \mapsto \tilde{x}$ is a ring homomorphism and Δ is an algebraic combination of the coefficients. □

So in the case of $\mathbb{Q}$, a curve has good reduction at p if there is a model whose discriminant is not divisible by p, i.e. $p \nmid \Delta$ or $v(\Delta) = 0$.

Example 2.8. Consider the two equations $E_1 : y^2 = x^3 + 16$ and $E_2 : y^2 + y = x^3$. Both define elliptic curves over $\mathbb{Q}$ because the matrices

$$\begin{pmatrix} -3x^2 & 2y \end{pmatrix}, \begin{pmatrix} -3x^2 & 2y+1 \end{pmatrix}$$

have maximal rank (rank 1) at points on the curves. This shows the curves on non-singular. In fact it is easy to see this holds over $\mathbb{F}_p$ for any $p \neq 2, 3$. Actually E_2 also works over $\mathbb{F}_2$, but E_1 does not.

Next we want to see $E_1 \cong E_2$. To see this, just notice

$$\begin{aligned} y^2 + y = x^3 \to \left(y + \frac{1}{2}\right)^2 &= x^3 + \frac{1}{4} \\ \to 64\left(y + \frac{1}{2}\right)^2 &= 64x^3 + 16 \\ \to (8y+4)^2 &= (4x)^3 + 16. \end{aligned}$$

So the inverse change of coordinates $(x, y) \mapsto \left(\frac{x}{4}, \frac{y-4}{8}\right)$ takes E_2 to E_1.

Notice this does *not* work mod 2! These are two forms representing the same abstract variety over $\mathbb{Q}$. The problem is that they don't necessary work well with the same primes. Notice that E_1 has bad reduction at 2 while E_2 has good reduction at 2. In fact, E_2 has good reduction at every prime except 3. E_2 is actually the minimal model so the elliptic curve has good reduction at all primes except 3.

Note that the minimal model is just a model which has good reduction at π if E does. There are lots of models. We choose the minimal because if E does, then the model does also. Note that this model is minimal *with respect to* π. If we wanted to use a different prime we would get a different minimal model.

This makes the next question come naturally: When can I use the same model for more then one prime?

Theorem 2.9. *A number field K has class number 1 if and only if every elliptic curve E/K has a global minimal Weierstrass equation. In particular, this is true for $\mathbb{Q}$.*

3 Supersingular

Definition 3.1. Let K be a perfect field of characteristic p and E/K an elliptic curve. We say E is *supersingular* if one of the following conditions holds [1]:

(i) $E[p^r] = 0$ for one (all) $r \geqslant 1$.

(ii) $\hat{\phi}_r$ (the dual of the p^r-power Frobenius map $\phi_r : E \to E^{(p^r)}$) is (purely) inseparable for one (all) $r \geqslant 1$.

(iii) The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.

(iv) $\mathrm{End}(E)$ is an order in a quaternion algebra.

(v) The formal group $\hat{E}/K$ associated to E has height 2.

(vi) The group scheme of points of order p is connected, see wiki.

(vii) If $K = \mathbb{F}_p$ then E is supersingular if and only if $\#E(\mathbb{F}_p) \equiv 1 \mod p$ (this is counting projective points), see wiki.

(viii) If $p \geqslant 5$, then E is supersingular if and only if $\#E(\mathbb{F}_p) = p + 1$, problem 5.10 silverman.

Remark 3.2. The "one (all)" business is because if $E[p^r]$ is non-trivial, then all r are non-trivial because $E[p^r]$ will be $\mathbb{Z}/p^r\mathbb{Z}$ (theorem) and will contain (and show they are non-trivial) $E[p^s]$ for all $s \leqslant r$. It is contained in $E[p^t]$ for all $t \geqslant r$.

Theorem 3.3.

$$E[p^r](\overline{K}) = \begin{cases} \mathbb{Z}/p^r\mathbb{Z} & or \\ 0. \end{cases}$$

Remark 3.4. Note that supersingular curves are elliptic curves and hence non-singular.

Example 3.5.

- $y^2 + y = x^3 + x + 1$ over $\mathbb{F}_2$. Just checking there is only one point on this curve: $(0 : 1 : 0)$. Hence it is supersingular. The two torsion is trivial (there is one point so the group is trivial).
- The curve $y^2 = x^3 + 1$ over $\mathbb{F}_5$ has 6 points:

  $$(0 : 1 : 0), (0 : 1 : 1), (0 : 4 : 1), (2 : 2 : 1), (2 : 3 : 1), (4 : 0 : 1).$$

  Hence it is supersingular. The group of points is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ (by the "abelian_group" command in sage).
- The curve $y^2 = x^3 + x$ over $\mathbb{F}_7$ has 8 points. The group is isomorphic to $\mathbb{Z}/8\mathbb{Z}$ and hence is supersingular.

[1] `http://en.wikipedia.org/wiki/Supersingular_elliptic_curve`

4 A Short Exact Sequence

Notation: Given a curve (possible singular) E/K, let E_{ns} be the set of non-singular points and $E_{\text{ns}}(K)$ be the set of non-singular points of $E(K)$.

Proposition 4.1. *Suppose a curve is given by a Weierstrass equation. It is non-singular if and only if $\Delta = 0$. If $\Delta \neq 0$ then there is only one singular point.*

Proof. First show the given point O, which is usually given as the point at infinity $[0, 1, 0]$ is non-singular (look at hommogeneous equation).

Now move a singular point to $(0, 0)$. Write down the equation, and notice partials can not vanish else where. □

Proposition 4.2. *The regular composition law turns E_{ns} into an abelian group.*

Proof. Recall that the composition law to add points takes the line between them. If a line intersects the singular point, it is counted twice. Hence that would be a total of 4 intersections (two from the points defining the line and two from the singular point). This is a contradiction (Bezout's Theorem).

Now use some special maps to show inverses work. □

Now in the same notation as in the reduction section, define the following

$$E_0(K) = \{P \in E(K) \colon \tilde{P} \in \tilde{E}_{\text{ns}}(k)\}, \quad E_1(K) = \{P \in E(K) \colon \tilde{P} \in \tilde{O}\}.$$

So in particular E_1 is the kernel of the reduction and E_0 is the points with non-singular reduction. It can be shown (with some geometry) that E_0, E_1 are subgroups of E with $E_0 \subseteq E_1$. See proof of VII.2.1 Silverman.

Proposition 4.3. *There is an exact sequence of abelian groups*

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{\text{ns}}(k) \to 0.$$

Note: The right map is the reduction map.

Proof. We need to show $E_0(K) \to \tilde{E}_{\text{ns}}(k)$ is a group homomorphism and exactness on the right. With this we are done since exactness in the center and left is by definition of E_1 and E_0.

Essentially the homomorphism property holds because the group law is defined by intersecting lines and reduction takes lines to lines. We have to be careful here because this is not true in general, some lines are sent to points.

Surjectivity follows from "Hansel's lemma" which says something about lifting simple roots of reduced functions. □

Next we want to describe E_1.

Proposition 4.4. *Let E/K be given by a minimal Weierstrass equation, let $\hat{E}/R$ be the formal group associated to E ([Sil09, IV.2.2.3]), and let $w(z) \in R[[x]]$ be the power series from [Sil09, IV.1.1]. Then the map*

$$\hat{E}(\mathcal{M}) \to E_1(K), \quad z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$$

is an isomorphism of groups. (We use $z = 0 \mapsto O \in E_1(K)$).

Note that with this, if E has good reduction there is an exact sequence

$$0 \to \hat{E}(\mathcal{M}) \to E(K) \to \tilde{E}(k) \to 0.$$

Lucas will discuss $\hat{E}(\mathcal{M})$.

References

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics. Springer, 2009.

Travis Scholl
Department of Mathematics, University of Washington, Seattle WA 98195
email: tscholl2@uw.edu