Math 8430 Final Exam: The Semi-Stable Reduction Theorem for Elliptic Curves

James Stankewicz

University of Georgia

Dec 13, 2007

According to class on September 19th, an elliptic curve E over a field K is defined to be a nonsingular projective plane algebraic curve defined by an affine *Weierstrass Equation*

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

According to class on September 19th, an elliptic curve E over a field K is defined to be a nonsingular projective plane algebraic curve defined by an affine *Weierstrass Equation*

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

We shall in this talk consider Elliptic Curves to be a point at infinity plus the set of zeros in K^2 of a Weierstrass equation as above, unique up to a change of coordinates

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t,$$

We will find u, r, s and t in K, $u \neq 0$ and we further must have the discriminant

$$\Delta(E) = \Delta(a_1, a_2, a_3, a_4, a_6) \neq 0.$$

Equivalence of the two definitions is found in [AEC] as Theorem III.3.1, but that requires The Riemann-Roch Theorem, an equivalence of categories proven in Hartshorne and other heavy machinery. Since we don't use the fact that a Weierstrass equation in fact defines a "curve" in this talk or really anything besides the affine geometry of a Weierstrass Equation, it will go unproven here.

Our concern will be curves defined over fields with a given discrete valuation v.

Definition

A *Discrete Valuation* v on a field K is for us, a group homomorphism

$$v : K^{\times} \twoheadrightarrow \mathbb{Z}$$

such that $v(a+b) \geq \min\{v(a), v(b)\}$.

Our valuation v gives us the set

$$R = \{r \in K^\times : v(r) \geq 0\} \cup \{0\},$$

which we call the valuation ring, the set

$$\mathfrak{p} = \{r \in K^\times : v(r) > 0\} \cup \{0\},$$

which we call the valuation ideal and the residue field $k = R/\mathfrak{p}$. For the sake of being direct, we will refer to reducing an elliptic curve at v although it is equivalent to reducing at $\mathfrak{p}$ as Silverman does.

Since R is a PID, we can write each a_i in reduced form with respect to $(\pi) = \mathfrak{p}$ and have a well-defined LCM. Thus we make the change of coordinates $x = u^2x'$, $y = u^3y'$ with $u = LCM(n_1, \ldots, n_6)$ where n_i is the numerator of a_i, so we can assume each $a_i \in R$. Therefore the reduction map $R \to R/(\pi)$ gives us an elliptic curve over $R/(\pi)$ defined by the Weierstrass equation where a_i is replaced by the class of a_i mod π as long as $v(\Delta) = 0$.

As discussed in class, though, there is some ambiguity in this reduction map from the class of elliptic curves over K to the class of elliptic curves over $R/(\pi)$, so the map must be refined to be defined using only a *minimal* Weierstrass equation.

Definition

A *minimal Weierstrass equation* is a Weierstrass equation for an elliptic curve where $v(\Delta(E))$ is minimal in $\mathbb{Z}$ and $a_i \in R$. This equation is unique up to the standard change of coordinates

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t,$$

Where $u \in R^\times$ and $r, s, t \in R$.

To understand what an Elliptic Curve can reduce to, we consider Weierstrass equations over a general field k. If $\Delta(E) = 0$, we will say that the set of solutions to the Weierstrass equation $(x, y) \in k^2$ together with the point at infinity is a *Singular Curve*.

This terminology makes sense when we consider the definition of a *singular point* (x_0, y_0) of a plane curve $f(x, y) = 0$ to be a point where $\partial f/\partial x(x_0, y_0) = \partial f/\partial y(x_0, y_0) = 0$. It turns out that $\Delta(E) = 0$ if and only if we get a singular point among our solutions to the Weierstrass equation(with one small exception in characteristic 2).

Proof

If the characteristic of k is not 2, then if we permit ourselves to stray from Weierstrass form for a moment, we can complete the square on

$$y^2 + a_1xy + a_3y$$

by replacing y with $1/2(y - a_1x - a_3)$ so that $y^2 + a_1xy + a_3$ becomes

$$1/4(y^2 - (a_1x + a_3)^2),$$

so that the solutions to our Weierstrass equations are exactly the solutions(under the shift of y) to

$$\begin{aligned} y^2 &= 4(x^3 + a_2x^2 + a_4x + a_6) + (a_1x + a_3)^2 \\ &= 4x^3 + b_2x^2 + 2b_4x + b_6 =: g(x) \end{aligned}$$

Therefore we have a singular point if and only if there is a point (x_0, y_0) where

$$\partial f/\partial y(x_0, y_0) = 2y_0 = 0$$

and

$$g'(x) = \partial f/\partial x = -(12x_0^2 + 2b_2x_0 + 2b_4) = 0$$

where $f(x, y) = y^2 - g(x)$. Thus $y_0 = 0$ and x_0 is a common root of g and g'. However, we know that the discriminant of g is the resultant of g and g', so we have a singular point if and only if the discriminant of g is zero. Then by a simple calculation, the discriminant of g is $\Delta(E)/16$.

If the characteristic of k is 2, then $j = c_4^3/\Delta(E)$ but $c_4 = b_2^2 - 24b_4 = b_2^2$ and $b_2 = a_1^2 + 4a_2 = a_1^2$ so $j = a_1^{12}/\Delta(E)$. We proceed by cases: If $j \neq 0$ then a_1 is invertible, so we can make the change of coordinates

$$x = a_1^2 x'^2 + a_3/a_1, \qquad y = a_1^3 y' + (a_1^2 a_4)/a_1^3$$

giving the form

$$y^2 + xy = x^3 + a_2 x^2 + a_6$$

where $\Delta(E) = a_6$. We then note that we have a singular point if and only if $x = 0$ and $y - 3x^2 = y = 0$ and the point $(0, 0)$ is on the curve if and only if $a_6 = \Delta(E) = 0$.

If $j = 0$ then we make the coordinate change $x = x' + a_2$ and $y = y'$ giving

$$y^2 + a_3 y = x^3 + a_4 x + a_6 \qquad \Delta(E) = a_3^4$$

so we get a singular point if and only if $a_3 = 0$, $3x^2 + a_4 = x^2 - a_4 = 0$, and $y^2 = a_4^{3/2} + a_4^{3/2} + a_6 = a_6$. In the cases that Silverman considers (k perfect) we then have a singularity if and only if $\Delta(E) = 0$, but if a_4 or a_6 is not a square in k, the curve will not be singular even if $\Delta(E) = 0$.

Note further that in each of these cases, we have at most one singular point when $\Delta(E) = 0$. If the characteristic is not 2, since $0 = 16\Delta(E) = \Delta(g)$, g has a double root, but since g is cubic, there can be at most one double root. If the characteristic is 2 and $j \neq 0$ then $(0, 0)$ is the only possible singular point and if $j = 0$ then the singular point is $(\sqrt{a_4}, \sqrt{a_6})$ (if these square roots exist).

We now explore the types of singularities that can occur at the one given point. At a nonsingular point, at least one of $\partial f/\partial x$ or $\partial f/\partial y$ is nonzero, so at the nonsingular point (x_0, y_0) we have the well-defined tangent line

$$\partial f/\partial x(x_0, y_0)(x - x_0) + \partial f/\partial y(x_0, y_0)(y - y_0) = 0.$$

If (x_0, y_0) is a singular point, both partials are zero and the equation is simply $0 = 0$, which does not define a line. We will nonetheless have a pair of lines which get arbitrarily close to our singular curve. When these two lines coincide, we will call that singularity a *cusp* and when they do not coincide we will call that singularity a *node*.

Theorem (AEC III.1.4)

A singular point (x_0, y_0) is a node if $c_4 \neq 0$ and a cusp if $c_4 = 0$.

First, for ease of calculation, a Lemma whose proof is computational.

Lemma

Two invariants of a Weierstrass equation, Δ and $c_4 = b_2^2 - 24b_4$ become Δ/u^{12} and c_4/u^4 under the standard coordinate change(and are thus unchanged by translation).

With this in mind, we shift the singular point (x_0, y_0) over to $(0, 0)$ without changing c_4. We can now see clearly that $a_6 = a_4 = a_3 = 0$ because $a_6 = f(0, 0)$, $a_4 = \partial f/\partial x(0, 0)$ and $a_3 = \partial f/\partial y(0, 0)$. Then $c_4 = b_2^2 = (a_1^2 + 4a_2)^2$ because $b_4 = 0$.

Our Weierstrass equation is then

$$f(x,y) = y^2 + a_1xy - a_2x^2 - x^3 = 0.$$

We then consider that perhaps in the splitting field of $h(y) = y^2 + a_1y - a_2$,

$$y^2 + a_1xy - a_2x^2 = (y - \alpha x)(y - \beta x)$$

where α and β are roots of h. The lines $y = \alpha x$ and $y = \beta x$ are the lines to which we refer because if $|x| < \varepsilon$, then the points $(x, \alpha x)$ and $(x, \beta x)$ are such that $|f(x, \alpha x)| < \varepsilon^3$ and likewise for β.

The question has now been reduced to: When is $\alpha = \beta$? If the characteristic of k is not 2, the quadratic formula tells us that

$$\alpha = \frac{-a_1 + \sqrt{a_1^2 + 4a_2}}{2}, \beta = \frac{-a_1 - \sqrt{a_1^2 + 4a_2}}{2}.$$

Therefore we have a cusp if and only if $0 = a_1^2 + 4a_2 = b_2$, or as the book prefers, $c_4 = 0$.
If the characteristic is 2, we note that $b_2 = a_1^2 + 4a_2 = a_1^2$. But when we consider that
$h(y) = (y - \alpha)(y - \beta) = y^2 - (\alpha + \beta)y + \alpha\beta$ we see that

$$\alpha = \beta \iff \alpha + \beta = 0 \iff a_1 = 0 \iff b_2 = 0 \iff c_4 = 0.$$

Since we have defined bad reduction to be when an elliptic curve E/K reduces to a singular curve, it makes sense to say E/K has *good reduction* at a discrete valuation v when $\tilde{E}/k$ is everywhere nonsingular (k is the residue field of v).

When $\tilde{E}$ has a node, we will say that E/K has *semi-stable reduction* at v and when $\tilde{E}$ has a cusp, we will say that E/K has *unstable reduction* at v.

We now collect our results as follows:

Corollary

If v is a discrete valuation on K with valuation ring R and valuation ideal π, then if E is an elliptic curve defined over K,

- *E has good reduction at v if $v(\Delta) = 0$*
- *E has semi-stable reduction at v if $v(\Delta) > 0$ but $v(c_4) = 0$*
- *E has unstable reduction at v if $v(\Delta), v(c_4) > 0$.*

We have now developed enough terminology where we can state our Theorem:

Theorem (The Semi-Stable Reduction Theorem)

If E/K is an elliptic curve and v a discrete valuation on K, then there is a finite extension K'/K and a discrete valuation v' lying over v so that if we let E'/K' be an elliptic curve over K' defined by the same Weierstrass equation as E, then E' has either good or semi-stable reduction.

Our main tool for proving this will be to use special normal forms defined over extensions of K, *Legendre Normal Form* and *Deuring Normal Form*.

Theorem

If K is a field of characteristic not equal 2, any Elliptic Curve E/K is isomorphic over $\overline{K}$ to some

$$E_\lambda : y^2 = x(x-1)(x-\lambda),$$

where $\lambda \in \overline{K}$.

As in the classification of singularities, since the characteristic is not 2, E/K can be shifted to

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = g(x)$$

and then back to a Weierstrass equation by the substitution $(x, y) \mapsto (x, 2y)$ giving us $y^2 = (1/4)g(x)$.

Since $(1/4)g(x)$ is monic, in a splitting field L,

$$(1/4)g(x) = (x - e_1)(x - e_2)(x - e_3).$$

We know that they are all distinct because $\Delta(E) = 16\Delta(g) \neq 0$. This is important because we will define $\lambda = \frac{e_3 - e_1}{e_2 - e_1}$, and if $\lambda = 0$ or 1 then our curve is singular.
Extending to $L(\sqrt{e_2 - e_1})$, we make the substitution

$$x = (e_2 - e_1)x' + e_1, \;\; y = (e_2 - e_1)^{3/2}y',$$

Which completes our proof. Note here that we could in fact find a finite, separable extension over which they were isomorphic, rather than going all the way up to $\overline{K}$.

Theorem

If the characteristic of K is not 3, we can put E in what is called Deuring Normal Form, i.e.

$$y^2 + \alpha xy + y = x^3$$

where $\alpha \in \overline{K}$ and $\alpha^3 \neq 27$ (we are forced into this last condition because the discriminant here is $\alpha^3 - 27$).

We will accomplish this via a suitable change of coordinates. We will first divide the problem up into cases. If char(k) is 2 and $j \neq 0$, we first change to the form $y^2 + xy = x^3 + a_2x^2 + a_6$, if $j = 0$ we can switch first to $y^2 + a_3y = x^3 + a_4x + a_6$, and if the characteristic is neither 2 nor 3 we switch to short Weierstrass form $y^2 = x^3 + Ax + B$.

Once we have made our initial change of coordinates for $j \neq 0$ (so we must have $a_1 = 1$ and $a_6 \neq 0$) we let u be a solution to $u^{12} + u^9 + a_6 = 0$, then $r = u^3$, s a solution to $s^2 + s + a_2 + u^3$ and $t = u^3 s + u^6$. In this case our $\alpha = 1/u$.

If $j = 0$ after our inital coordinate change, we see that $a_3 \neq 0$ because $\Delta = a_3^4$. Then we have u a cube root of a_3, s a root of $s^4 + a_3 s + a_4 = 0$, $r = s^2$ and t a root of $t^2 + a_3 t + a_6 + s^2 a_4 = 0$. In this case, $\alpha = 0$.

Finally if the characteristic is not 2 or 3 we first switch to short Weierstrass form and our coordinate change is predetermined. We must have $s = 0$, $r = \sqrt{-A}/3$, $t = \sqrt{B + A\sqrt{-A}/3 - A\sqrt{-A}/27}$ and $u = \sqrt[3]{2\sqrt{B + A\sqrt{-A}/3 - A\sqrt{-A}/27}}$.

Note that in all these cases, the extensions are finite(clearly) and separable by computing the gcd of each defining polynomial with its derivative.

We now have all the machinery in place to complete a proof of Semi-Stable Reduction. We begin with a Lemma

Lemma

If K'/K is a finite extension and E/K is an elliptic curve with E' the corresponding curve over K' then if E has good reduction, so does E'. Likewise, if E has semistable reduction, so does E'.

To prove this we must first recall that since the way we categorized reduction types depends entirely upon a valuation, we must define v' on K' "lying over" v. Our first step will be to look at R', the integral closure of R in K'. Since R' is the integral closure of a PID(we only need a Dedekind Domain) in a finite separable extension of K, it is a Dedekind Domain and so has unique factorization of ideals.

Then with unique factorization of ideals, we can look at

$$\pi R' = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

We will get a valuation lying over v if we localize R' at any of these prime ideals lying over π and then build a valuation v' as we build the p-adic valuation in $\mathbb{Z}$ or $\mathbb{Z}_p$(because $R'_{\mathfrak{P}}$ is a local PID). A good way to characterize v' coming from $\mathfrak{P}_i$ as "lying over" (π) is by noting that $v'|_K = e_i v$.
With this in mind, we take a minimal Weierstrass equation for E over K and then for E'/K' we make a coordinate change to a Weierstrass equation minimal over K'. As we mentioned earlier, Δ becomes Δ/u^{12} and c_4 becomes c_4/u^4 under any standard change of coordinates.

We consider then that

$$0 \leq v'(\Delta') = -12v'(u) + v'(\Delta)$$

and

$$0 \leq v'(c_4') = -4v'(u) + v'(c_4).$$

And therefore

$$v'(u) \leq \min\{(e_i/12)v(\Delta), (e_i/4)v(c_4)\},$$

a quantity which is zero if E has good or semi-stable reduction.

Therefore $v'(u) = 0$ so that

$$v'(\Delta') = v'(\Delta) = e_i v(\Delta) \ \& \ v'(c_4') = v'(c_4) = e_i v(c_4).$$

Thus $v(\Delta) = 0$ if and only if $v'(\Delta) = 0$ and likewise for c_4. So E' retains good reduction and likewise for semistable reduction. With these tools, we will now prove the Semi-Stable Reduction Theorem.

If the characteristic of k is not 2, we can put E/K into Legendre Normal form

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

in some finite separable extension L/K. Our key quantities are then

$$\Delta = 16\lambda^2(\lambda-1)^2, \;\; c_4 = 16(\lambda^2-\lambda+1).$$

Therefore if $\lambda \in R'$, the valuation ring for v' with valuation ideal (π') and $\lambda \neq 0, 1$ in $R/(\pi')$ then E_λ has good reduction at v' because $v(2) = 0$ (because otherwise, $2 \equiv 0 \bmod \pi$)
If $\lambda \in R'$ and $\lambda \equiv 0, 1 \bmod \pi'$ then E_λ has semistable reduction at v' because $v'(c_4) = 0$.(and note the equation is minimal in this case because if we lower the valuation of Δ, we bring $v'(c_4) < 0$).

If $\lambda \notin R'$ then $v'(\lambda) = -m < 0$. But then $v'(\pi'^m \lambda) = 0$. Now if we extend up to $L(\sqrt{\pi'})$ then we can make the coordinate change where $u = \sqrt{\pi'}^m$ and $r = s = t = 0$ to get an integral equation

$$E'_\lambda : y^2 = x(x - \pi'^m)(x - \pi'^m \lambda)$$

with

$$\Delta' = 16(\pi'^m \lambda)^2(\pi'^{2m})(\pi'^m \lambda - \pi'^m)^2, \quad c'_4 = 16(\pi'^{2m} - \pi'^{2m}\lambda + (\pi'^m \lambda)^2)$$

So $v'(\Delta') = 2m$ but $v'(c'_4) = 0$, and thus E'_λ has semistable reduction.

If the characteristic of k is 2, we proceed in about the same fashion using Deuring Normal form, where $\Delta = \alpha^3 - 27 \equiv \alpha^3 + 1 \bmod \pi$ and $c_4 \equiv \alpha^4 \bmod \pi$.

If $\alpha \in R'$, $v'(\alpha^3 - 27) = 0$ then we have good reduction. If $\alpha \in R'$ but $v'(\alpha^3 - 27) > 0$ then $\alpha^3 = 1 + \pi' r$ for some $r \in R'$ and so $3v'(\alpha) = v'(1 + \pi' r) = 0$ so $v'(c_4) = 4v'(\alpha) = 0$ and we have semi-stable reduction.

Then if $\alpha \notin R'$ then we pick the substitution where $u = \pi'^m$ if $v(\alpha) = -m$ and $r = s = t = 0$. This gives us the equation

$$y^2 + \pi'^m \alpha xy + \pi'^{3m} y = x^3$$

with $\Delta' = \pi'^{9m}(\pi'^m \alpha + \pi'^{3m})$ and $c_4' = (\pi'^m \alpha)^4$.
Therefore $v'(\Delta') = 9m$ and $v'(c_4') = 4v'(\pi'^m \alpha) = 0$ and we have semi-stable reduction, completing our proof.

A related topic to semi-stable reduction is that of *Potential Good Reduction*. In the VIGRE seminar we defined an Elliptic curve to have potential good reduction when it had an integral j-Invariant. The definition in Silverman however is that E/K has potential good reduction if there is a finite (and for us, separable) extension K' such that E'/K' has good reduction. The important fact that we wish to prove here is that these two definitions are equivalent. Moreover, our method of proof will be the same (Legendre and Deuring Normal Forms)

If $j(E)$ is integral and char$(k) \neq 2$, we find $\lambda \in L/K$ such that $E_\lambda = E$ via a change of coordinates. By computing the j-Invariant of E_λ (which is just $j(E)$ since the j-Invariant doesn't change under changes of coordinates), we find

$$(1 - \lambda(1 - \lambda))^3 - j(E)\lambda^2(1 - \lambda)^2 = 0.$$

Since $j(E)$ is integral, so is λ by the above relation. Moreover, if we reduce this equation mod π' we see that $v(\lambda) = 0$ and $v(1 - \lambda) = 0$ (or else $1 \equiv 0 \bmod \pi'$) and thus E_λ has good reduction at v'.

Now on the other hand if E/K has potential good reduction, then let E'/K' have good reduction. By definition $v'(\Delta') = 0$, telling us that $\Delta' \in R'^{\times}$. Therefore

$$j(E) = j(E') = \frac{c_4'^3}{\Delta'}$$

and we are done if the characteristic is not 2.

If $j(E)$ is integral and char$(k) = 2$, then we can find an extension L/K in which E has a Deuring Normal Form. Then we have the relation

$$\alpha^3(\alpha^3 - 24) - (\alpha^3 - 27)j(E) = 0$$

This immediately tells us that α is integral and that $v(\alpha^3 - 27) = 0$ because otherwise $\alpha^3 \equiv 27 \bmod \pi'$, which leads us to a contradiction unless the characteristic of k is 3. Since $\Delta' = \alpha^3 - 27$ we have good reduction at v'.
Meanwhile our converse argument from characteristic not 2 holds just as well, completing the proof and the lecture.