

open.michigan

**Author(s):** Andrew Snowden

**License:** Unless otherwise noted, this material is made available under the terms of the **Creative Commons Attribution 3.0 License**: <http://creativecommons.org/licenses/by/3.0/>


**We have reviewed this material** in accordance with U.S. Copyright Law **and have tried to maximize your ability to use, share, and adapt it.** The citation key on the following slide provides information about how you may share and adapt this material.

Copyright holders of content included in this material should contact [open.michigan@umich.edu](mailto:open.michigan@umich.edu) with any questions, corrections, or clarification regarding the use of content.

For more information about **how to cite** these materials visit <http://open.umich.edu/education/about/terms-of-use>.

Any **medical information** in this material is intended to inform and educate and is **not a tool for self-diagnosis** or a replacement for medical evaluation, advice, diagnosis or treatment by a healthcare professional. Please speak to your physician if you have questions about your medical condition.

**Viewer discretion is advised:** Some medical content is graphic and may not be suitable for all viewers.

 UNIVERSITY OF MICHIGAN



# Attribution Key

for more information see: <http://open.umich.edu/wiki/AttributionPolicy>

## Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

-  **Public Domain – Government:** Works that are produced by the U.S. Government. (17 USC § 105)
-  **Public Domain – Expired:** Works that are no longer protected due to an expired copyright term.
-  **Public Domain – Self Dedicated:** Works that a copyright holder has dedicated to the public domain.
-  **Creative Commons – Zero Waiver**
-  **Creative Commons – Attribution License**
-  **Creative Commons – Attribution Share Alike License**
-  **Creative Commons – Attribution Noncommercial License**
-  **Creative Commons – Attribution Noncommercial Share Alike License**
-  **GNU – Free Documentation License**

## Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

-  **Public Domain – Ineligible:** Works that are ineligible for copyright protection in the U.S. (17 USC § 102(b)) \*laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

-  **Fair Use:** Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (17 USC § 107) \*laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

## Lecture 8: Elliptic curves over DVRs

This lecture is devoted to the behavior of elliptic curves over DVRs. The various types of reduction (good, multiplicative, additive) are defined, and their behavior under extension is studied. Then the behavior of torsion points under reduction is discussed. Finally, I prove the Néron–Ogg–Shafarevich theorem.

A good reference for this lecture is Chapter VII of Silvermans “The arithmetic of elliptic curves” ([MR0817210](#)).

Let  $R$  be a complete DVR,  $\mathfrak{p}$  its maximal ideal,  $K$  its field of fractions,  $k$  its residue field, and  $v$  the valuation with  $v(\pi) = 1$ , for  $\pi$  a uniformizer. We are going to study elliptic curves over  $K$ , and their reduction modulo  $\mathfrak{p}$ . We assume throughout that  $k$  does not have characteristic 2 or 3.

### 1 Minimal Weierstrass equations

Let  $E/K$  be an elliptic curve given by a Weierstrass equation  $y^2 = x^3 + ax + b$ . Recall that the discriminant  $\Delta = -16(4a^3 + 27b^2)$  is non-zero. A Weierstrass equation for  $E$  is not unique: one can replace  $y$  with  $u^3y$  and  $x$  with  $u^2x$ , for  $u \in K^\times$ , which has the effect of changing  $a$  to  $u^{-4}a$  and  $b$  to  $u^{-6}b$ . We say that a Weierstrass equation is minimal if  $a$  and  $b$  belong to  $R$  and  $v(a) < 4$  or  $v(b) < 6$  (this is equivalent to asking that  $v(\Delta)$  be minimal). A minimal Weierstrass equation is unique up to a change of variables as above with  $u$  a unit. We let  $\mathcal{E}$  be the projective scheme over  $R$  defined by a minimal Weierstrass equation. We call this the minimal Weierstrass model for  $E$ . It is independent of the choice of minimal Weierstrass equation, up to isomorphism (since  $u$  must be a unit in any change of variables).

We can now introduce most of the objects we will be interested in:

- We let  $\overline{E}$  be  $\mathcal{E}_k$ , the special fiber of  $\mathcal{E}$ . We call this the reduction of  $E$  modulo  $\mathfrak{p}$ . This is an irreducible projective curve over  $k$ , though possibly singular.
- We let  $\overline{E}_{\text{sm}}$  be the smooth locus of  $\overline{E}$ . A basic fact is that  $\overline{E}_{\text{sm}}$  is a group variety: the group law can be defined using the secant line construction, as on an elliptic curve.
- Since  $\mathcal{E}$  is projective,  $\mathcal{E}(R) = \mathcal{E}(K) = E(K)$ . We therefore have a well-defined map  $E(K) \rightarrow \overline{E}(k)$ , which we call the reduction map.
- We let  $E_0(K)$  be the subset of  $E(K)$  which reduces into  $\overline{E}_{\text{sm}}(k)$ . Then  $E_0(K)$  is a subgroup of  $E(K)$ , and the reduction map  $E_0(K) \rightarrow \overline{E}_{\text{sm}}(k)$  is a group homomorphism. In fact, it is surjective by Hensel’s lemma.
- We let  $E_1(K)$  be the kernel of the reduction map  $E_0(K) \rightarrow \overline{E}_{\text{sm}}(k)$ .

### 2 Types of reduction

The curve  $\overline{E}$  is defined by the equation  $y^2 = x^3 + \overline{a}x + \overline{b}$ , where  $\overline{a}$  and  $\overline{b}$  are the images of  $a$  and  $b$  in  $k$ . This curve is an elliptic curve if and only if  $\overline{\Delta} \neq 0$ , which is equivalent to asking that  $\Delta$  be a unit of  $R$ . If  $\overline{E}$  is an elliptic curve, we say that  $E$  has good reduction. In this case,  $\mathcal{E}$  is a smooth scheme over  $R$  and is naturally a group object in the category of schemes over  $R$ .

---

These are notes for Math 679, taught in the Fall 2013 semester at the University of Michigan by Andrew Snowden.

Now suppose  $\overline{E}$  is singular, i.e.,  $\overline{\Delta} = 0$ . We then say that  $E$  has bad reduction. There are two possibilities. If  $\overline{a} = \overline{b} = 0$  then  $\overline{E}$  has a single singularity, at  $(0, 0)$ , and it is a cusp. The smooth locus  $\overline{E}_{\text{sm}}$  is isomorphic to  $\mathbf{G}_a$ , as a group variety. We therefore say that  $E$  has additive reduction. If  $\overline{a}$  or  $\overline{b}$  is non-zero then both are non-zero (since  $\overline{\Delta} = 0$ ), and  $E$  has a single singularity, at  $(-3b/2a, 0)$ , and it is a node. The smooth locus  $\overline{E}_{\text{sm}}$  is isomorphic (over  $\overline{k}$ ) to  $\mathbf{G}_m$ , as a group variety. We therefore say that  $E$  has multiplicative reduction.

We say that  $E$  has semi-stable reduction if it has either good or multiplicative reduction.

To summarize:

- $E$  has good reduction if and only if  $\Delta$  is a unit of  $R$ .
- $E$  has multiplicative reduction if and only if  $\Delta \in \mathfrak{p}$  but  $a$  and  $b$  are units of  $R$ .
- $E$  has additive reduction if and only if  $a$  and  $b$  are both in  $\mathfrak{p}$ .
- $E$  has semi-stable reduction if and only if one of  $a$  or  $b$  is a unit of  $R$ .

### 3 Behavior of reduction type under extensions

**Proposition 1.** *Let  $K'/K$  be a finite extension. Suppose that either  $K'/K$  is unramified or  $E$  has semi-stable reduction over  $K$ . Then a minimal Weierstrass equation for  $E$  over  $K$  is still minimal over  $K'$ . It follows that the reduction type of  $E$  over  $K$  is the same as that over  $K'$ .*

*Proof.* Let  $v'$  be the valuation on  $K'$ . First suppose that  $K'/K$  is unramified. Then for  $x \in K$  we have  $v(x) = v'(x)$ . Thus if  $v(a) < 4$  or  $v(b) < 6$  then  $v'(a) < 4$  or  $v'(b) < 6$ . Now suppose that  $E$  has semi-stable reduction. Then either  $v(a) = 0$  or  $v(b) = 0$ , and so  $v'(a) = 0$  or  $v'(b) = 0$ , which shows that the equation is minimal over  $K'$ .  $\square$

**Theorem 2** (Semi-stable reduction theorem). *There exists a finite extension  $K'/K$  such that  $E$  has semi-stable reduction over  $K'$ .*

*Proof.* Recall that we can make a change of variables to replace  $(a, b)$  with  $(a', b') = (u^{-4}a, u^{-6}b)$ . First suppose that  $3v(a) \leq 2v(b)$ . Taking  $u = a^{1/4}$ , we find that  $a' = 1$  is a unit and  $b'$  is integral, so the new equation is minimal and has semi-stable reduction. Thus  $E$  has semi-stable reduction over  $K' = K(u)$ . Now suppose that  $3v(a) \geq 2v(b)$ . Taking  $u = b^{1/6}$ , we find that  $a'$  is integral and  $b' = 1$  is a unit, so the new equation is minimal and has semi-stable reduction. Thus  $E$  has semi-stable reduction over  $K' = K(u)$ .  $\square$

**Remark 3.** The proof shows that the extension  $K'/K$  can always be taken to have degree at most 6.  $\square$

Combining the above two results, we see that for all sufficiently large extensions  $K'/K$ , the curve  $E_{K'}$  has either good or multiplicative reduction (independent of  $K'$ ). We say that  $E$  has potentially good or potentially multiplicative reduction accordingly. There is a simple test to determine which, in terms of the equation for  $E$ :

**Proposition 4.**  *$E$  has potentially good reduction if and only if  $j(E) = -1728(4a)^3/\Delta$  is integral.*

*Proof.* Since the  $j$ -invariant is independent of the model, we may as well assume that we have passed to an extension where  $E$  is semi-stable and we are working with the minimal model. If  $E$  has good reduction then  $\Delta$  is a unit, and  $j(E)$  is integral. If  $E$  has multiplicative reduction then  $\Delta$  is not a unit but  $a$  is, and so  $j(E)$  is not integral.  $\square$

**Example 5.** Suppose  $E$  is the curve over  $\mathbf{Q}_p$  given by  $y^2 = x^3 + p$ . Then  $E$  has additive reduction. We have  $a = 0$  and  $b = p$ , so  $j = 0$  is integral, and so  $E$  has potentially good reduction. Indeed, changing  $y$  to  $p^{1/2}y$  and  $x$  to  $p^{1/3}x$ , we find that  $E$  is isomorphic to  $y^2 = x^3 + 1$  over  $\mathbf{Q}_p(p^{1/6})$ , which is still an elliptic curve mod  $p$  (since  $p \geq 5$ ).  $\square$

## 4 Reduction of torsion points

We assume in this section that  $E$  has good reduction. Since  $\mathcal{E}$  is a proper smooth group over  $R$ , its  $n$ -torsion  $\mathcal{E}[n]$  is a finite flat group scheme over  $R$ , for any  $n$ . We can therefore apply our knowledge of group schemes to its study.

**Proposition 6.** *Let  $G$  be a finite flat group scheme over  $R$  whose order is prime to the residue characteristic. Then the reduction map  $G(\overline{K}) \rightarrow G(\overline{k})$  is an isomorphism of Galois modules. In particular,  $G(\overline{K})$  is an unramified Galois module.*

*Proof.* The reduction map is obviously Galois equivariant, so it suffices to show it's a bijection. To do this, we can assume  $k$  is algebraically closed. Since the order of  $G$  is invertible on the base,  $G$  is étale. Thus, if  $G = \text{Spec}(A)$ , then  $A$  is a product of copies of  $R$ . Clearly then,  $G(\overline{K}) = G(K) = G(k)$ .  $\square$

**Corollary 7.** *Suppose  $E$  has good reduction and  $n$  is prime to the residue characteristic. Then the reduction map  $E[n](\overline{K}) \rightarrow \overline{E}[n](\overline{k})$  is an isomorphism of Galois modules. In particular,  $E[n](\overline{K})$  is an unramified Galois module.*

Using Raynaud's theorem, we can say something about the  $p$ -torsion when the residue characteristic is  $p$ .

**Proposition 8.** *Suppose  $K$  is an extension of  $\mathbf{Q}_p$  with  $e < p - 1$ . Let  $G$  be a finite flat group scheme over  $R$ . Then the map  $G(R) \rightarrow G(k)$  is injective.*

*Proof.* Let  $\Gamma$  be the group  $G(R)$ , regarded as a constant group scheme over  $R$ . There is a natural map  $\Gamma \rightarrow G$  of group schemes over  $R$ , inducing the identity on  $R$ -points. Let  $\overline{\Gamma}$  be the scheme-theoretic image of this map in  $G$ , which is a closed subgroup of  $G$ . (One can also describe  $\overline{\Gamma}$  as the scheme-theoretic closure of  $G(K)$  in  $G$ .) Since the map  $\Gamma \rightarrow \overline{\Gamma}$  is an isomorphism on the generic fibers, Raynaud's theorem implies that it is an isomorphism. It follows that  $\Gamma_k \rightarrow G_k$  is injective; since  $\Gamma(R) \rightarrow \Gamma(k)$  is bijective (as  $\Gamma$  is constant), the composite  $G(R) = \Gamma(R) \rightarrow G(k)$  is injective.  $\square$

**Remark 9.** In the above situation, the reduction map need not be surjective. For example, let  $G$  be the Kummer extension of  $\mathbf{Z}/p\mathbf{Z}$  by  $\mu_p$  corresponding to  $a \in R$ . If  $A$  is a connected  $R$ -algebra, then  $G(A)$  is the set of pairs  $(i, z)$ , where  $i \in \mathbf{Z}/p\mathbf{Z}$  and  $z \in A$  satisfies  $z^p = a^i$ . If  $R$  does not contain a primitive  $p$ th root of unity or a  $p$ th root of  $a$  then  $G(R) = 0$ . But if  $k$  is perfect then  $G_k$  is the trivial extension (since  $a$  has a  $p$ th root), so  $G(k) = \mathbf{Z}/p\mathbf{Z}$ .  $\square$

**Remark 10.** Without the assumption on  $e$ , the reduction map need not be injective. For example, take  $G = \mu_p$  and suppose  $K$  contains the  $p$ th roots of unity. Then  $G(R) = \mu_p(K)$  has order  $p$  but  $G(k)$  is the trivial group.  $\square$

**Corollary 11.** *Suppose  $E$  has good reduction and maintain the same assumptions on  $K$ . Then the reduction map  $E[n](K) \rightarrow \overline{E}[n](k)$  is injective.*

## 5 The kernel of reduction

We now study the group  $E_1(K)$ , the kernel of the homomorphism  $E_0(K) \rightarrow \overline{E}_{\text{sm}}(k)$ . Since points on  $E_1(k)$  are  $\mathfrak{p}$ -adically close to the identity, the point at infinity, it makes sense to switch coordinates so that the identity is at  $(0, 0)$ . The projective equation for  $E$  is

$$ZY^2 = X^3 + aZ^2X + bZ^3$$

We usually put  $x = X/Z$  and  $y = Y/Z$ . We now put  $u = X/Y$  and  $v = Z/Y$  to obtain the equation

$$v = u^3 + auv^2 + bv^3.$$

The point at infinity in projective coordinates is  $[0 : 1 : 0]$ , and thus corresponds to  $(u, v) = (0, 0)$ . The set  $E_1(K)$  is given by the set of solutions to the above equation with  $u$  and  $v$  in  $\mathfrak{p}$ .

Let  $F(u, v)$  be the right side of the above equation, so that the equation reads  $v = F(u, v)$ . We can then plug this expression for  $v$  into the right side to find  $v = F(u, F(u, v))$ . Continuing in this way, we find  $v = \phi(u)$ , where  $\phi(u)$  is the iterate  $F(u, F(u, F(u, \dots)))$ . It is not difficult to see that  $\phi(u)$  is a power series in  $u$  with coefficients in  $R$ . Note that, because  $R$  is complete, if  $u$  is an element of  $\mathfrak{p}$  then  $\phi(u)$  is a well-defined element of  $R$ , and in fact  $\mathfrak{p}$  since  $\phi(0) = 0$ . It is now an easy exercise to show:

**Proposition 12.** *The map  $\mathfrak{p} \rightarrow E_1(K)$  sending  $u$  to  $(u, \phi(u))$  is a bijection of sets taking 0 to the identity element of  $E_1(K)$ .*

Using this bijection, we can transfer the group structure on  $E_1(K)$  to a group structure on  $\mathfrak{p}$ , which we denote by  $\oplus$ . It is not hard to show that  $\oplus$  is given by a power series over  $R$ , i.e., there exists a power series  $G \in R[[s, t]]$  such that  $s \oplus t = G(s, t)$ . Since 0 is the identity element, we have  $G(s, 0) = G(0, s) = s$ , and so  $G(s, t) = s + t + \dots$ , where  $\dots$  are higher order terms. It follows that  $\mathfrak{p}^n$  is a subgroup of  $\mathfrak{p}$  under  $\oplus$ . Let  $E_n(K)$  be the corresponding subgroup of  $E_1(K)$ . Clearly then, we have an isomorphism

$$E_n(K)/E_{n+1}(K) = \mathfrak{p}^n/\mathfrak{p}^{n+1} = k.$$

We have thus proved:

**Proposition 13.** *The group  $E_1(K)$  has a decreasing filtration  $\{E_n(K)\}_{n \geq 1}$  such that  $E_n(K)/E_{n+1}(K)$  is isomorphic to  $k$ .*

**Corollary 14.** *Suppose  $n$  is prime to the residue characteristic. Then the map  $E_0(K)[n] \rightarrow E_{\text{sm}}(k)[n]$  is injective.*

*Proof.* The kernel is a subgroup of  $E_1(K)$  killed by  $n$ , and therefore 0. □

**Corollary 15.** *Suppose  $k$  is finite of characteristic  $p$ . Then  $E_1(K)$  is a pro- $p$  group.*

## 6 The group $E(K)/E_0(K)$

We have the following important result:

**Theorem 16.** *(a) The group  $E(K)/E_0(K)$  is finite. (b) If  $E$  has split multiplicative reduction (i.e.,  $\overline{E}_{\text{sm}}$  is isomorphic to  $\mathbf{G}_m$  over  $k$ ) then this group is cyclic of order  $-v(j)$ . (c) If  $E$  does not have split multiplicative reduction, the group has cardinality at most 4.*

We will not prove this theorem. Some remarks:

- Part (a) follows immediately from the existence of Néron models. Parts (b) and (c) follow from the classification of Néron models. We will discuss these topics in the next lecture.
- If  $k$  is finite then part (a), for  $E(K)$  is then a compact group and  $E_0(K)$  is an open subgroup; thus  $E(K)/E_0(K)$  is both discrete and compact, and thus finite.
- One can prove the entire theorem without Néron models through a case-by-case analysis. For instance, suppose  $v(a) = 1$  and  $v(b) \geq 2$ . If  $P = (x, y)$  is a point of  $E(K)$  then

$$x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}.$$

Thus if  $(x, y)$  reduces to the singular point  $(0, 0)$ , i.e.,  $v(x) \geq 1$ , then the valuation of the numerator is equal to 2, while the valuation of the denominator is at least 2; thus  $v(x(2P)) \leq 0$ , and so  $2p$  does not reduce to the singular point. This shows that  $E(K)/E_0(K)$  is killed by 2. In fact, one can show that the sum of any two points reducing to the singular point does not reduce to the singular point, and so  $E(K)/E_0(K) = \mathbf{Z}/2\mathbf{Z}$ .

## 7 The Néron–Ogg–Shafarevich criterion

Let  $G_K$  be the absolute Galois group of  $K$  and  $I_K$  the inertia subgroup.

**Theorem 17.** *Let  $\ell$  be a prime different from the residue characteristic. Then:*

- *$E$  has good reduction if and only if  $I_K$  acts trivially on  $T_\ell(E)$ .*
- *$E$  has semi-stable reduction if and only if  $I_K$  acts unipotently on  $T_\ell(E)$ .*

*Proof.* First, note that  $I_K$  acts trivially on  $T_\ell(E)$  if and only if it does so on  $E[\ell^n](\overline{K})$  for all  $n$ . Thus, if  $E$  has good reduction then  $I_K$  acts trivially on  $T_\ell(E)$  by what we've already shown. Conversely, suppose  $I_K$  acts trivially on  $T_\ell(E)$ . Thus all  $\ell^n$  torsion points belong to  $E(K^{\text{un}})$ . Let  $d$  be the order of  $E(K^{\text{un}})/E_0(K^{\text{un}})$ , which is finite. Then  $E_0(K^{\text{un}})[\ell^n]$  is the kernel of the map  $E(K^{\text{un}})[\ell^n] \rightarrow E(K^{\text{un}})/E_0(K^{\text{un}})$ , and thus has cardinality at least  $\ell^{2n}/d$ . Since the reduction map  $E_0(K^{\text{un}}) \rightarrow \overline{E}_{\text{sm}}(\overline{k})$  is injective on  $\ell$ -power torsion, it follows that  $\overline{E}_{\text{sm}}(\overline{k})[\ell^n]$  has cardinality at least  $\ell^{2n}/d$ . But this is not true for  $\mathbf{G}_m$  (where the cardinality is  $\ell^n$ ) or  $\mathbf{G}_a$  (where the cardinality is 1), and so  $E$  cannot have multiplicative or additive reduction. Thus  $E$  has good reduction.

Now suppose that  $I_K$  acts unipotently on  $T_\ell(E)$ . It thus fixes some vector in  $T_\ell(E)$ , which implies that  $E(K^{\text{un}})[\ell^n]$  has cardinality at least  $\ell^n$ . Arguing as in the previous paragraph, we see that  $\overline{E}_{\text{sm}}$  cannot be  $\mathbf{G}_a$ , and so  $E$  has semi-stable reduction.

Finally, suppose that  $E$  has semi-stable reduction. The multiplication-by- $\ell^n$  map on the smooth locus  $\mathcal{E}_{\text{sm}}$  of  $\mathcal{E}$  is flat, and so  $\mathcal{E}_{\text{sm}}[\ell^n]$  is a flat group scheme over  $R$ . Let  $G$  be the scheme-theoretic closure in  $\mathcal{E}_{\text{sm}}[\ell^n]$  of the set of  $\overline{K}$ -points which extend to  $\overline{R}$ -points. Then  $G$  is finite and flat, and  $G_k = \overline{E}_{\text{sm}}[\ell^n]$ . Since  $G$  has  $\ell$ -power order, it is étale, and so  $G(K^{\text{un}}) = \overline{E}_{\text{sm}}[\ell^n](\overline{k})$ , which contains  $\mathbf{Z}/\ell^n\mathbf{Z}$  (since  $E$  is semi-stable). Thus  $E[\ell^n](K^{\text{un}})$  contains  $\mathbf{Z}/\ell^n\mathbf{Z}$  for all  $n$ , which shows that  $I_K$  fixes a vector in  $T_\ell(E)$ . Since the determinant of  $T_\ell(E)$  is the  $\ell$ -cyclotomic character, which is trivial on  $I_K$ , the result follows.  $\square$

**Corollary 18.** *If  $I_K$  acts trivially (or unipotently) on one  $T_\ell(E)$  then it does so on all of them.*

**Corollary 19.**  *$E$  has potentially good reduction if and only if  $I_K$  acts through a finite quotient on  $T_\ell(E)$ .*

**Corollary 20.** *Isogenous curves have the same reduction type.*

*Proof.* If  $E$  and  $E'$  are isogenous then  $T_\ell(E)[1/\ell]$  and  $T_\ell(E')[1/\ell]$  are isomorphic  $\mathbf{Q}_\ell$  representations of  $I_K$ . □