9 Elliptic curves over local fields

In this section, we will discuss the (good) reduction of elliptic curves, and ultimately use this to understand rational points of elliptic curves. Our treatment of reduction is admittedly somewhat ad hoc, but will be sufficient for the purposes at hand.

9.1 Warmup

Question 9.1. *We can define a map*

$$\mathbb{P}^2(\mathbb{Q}) \longrightarrow \mathbb{P}^2(\mathbb{F}_p)$$

as follows:

a. *Suppose $P \in \mathbb{P}^2(\mathbb{Q})$. Show that P has a representative*

$$P = [a, b, c]$$

where $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$.

b. *Use this to define $P \mapsto [\overline{a}, \overline{b}, \overline{c}] \in \mathbb{P}^2(\mathbb{F}_p)$, where $a \mapsto \overline{a}$ is the reduce mod p map $\mathbb{Z} \to \mathbb{Z}/p$.*

c. *Does this map induce a map $\mathbb{A}^2(\mathbb{Q}) \to \mathbb{A}^2(\mathbb{F}_p)$? Explain.*

9.2 Good reduction of varieties

Let A be a local ring, with field of fractions K, maximal ideal $\mathfrak{p}$ and residue field $\kappa = A/\mathfrak{p}$. (Example: $(A, K, \kappa) = (\mathbb{Z}_{(p)}, \mathbb{Q}, \mathbb{F}_p)$ or $(A, K, \kappa) = (\mathbb{Z}_p, \mathbb{Q}_p, \mathbb{F}_p)$.) We often denote the "reduce mod $\mathfrak{p}$" map by $a \mapsto \overline{a}$.

An affine variety over A is given by a collection of polynomials $f_1, \cdots, f_r \in A[x_1, \cdots, x_n]$. Let $\mathcal{V}$ be such a variety. Using the inclusion $A \subset K$, we obtain an affine variety $V = \mathcal{V}_K$ over K; simply view each of the polynomials as "actually" having coefficients in K. We also get a variety $\overline{V} = \mathcal{V}_\kappa$ over κ; apply $a \mapsto \overline{a}$ to each coefficient of each polynomial. We will say that $\mathcal{V}$ has good reduction if V if is smooth over K: $\overline{V}$ is smooth over κ; and $\dim V = \dim \overline{V}$.

(There is also an analogous definition of a projective variety over A, and of good reduction...)

Question 9.2. *Let $E/\mathbb{Q}$ be an elliptic curve, given by an equation*

$$y^2 = f(x)$$

where $f(x) \in \mathbb{Z}[x]$ is a monic cubic with integer coefficients. Then for each prime p, we can view E as a variety $\mathcal{E}/\mathbb{Z}_{(p)}$.

Let Δ be the discriminant of f, and let p be any prime such that $p \nmid 2\Delta$. Show that $\mathcal{E}$ has good reduction at p.

Often, we *start* with a variety over K, pick equations for it, and then reduce those equations mod $\mathfrak{p}$ in order to try to compute the (sic) reduction of that variety. Unfortunately, this process is somewhat sensitive to the choice of equations.

Question 9.3. *Consider the varieties*

$$\mathcal{E}_1 : y^2 = x^3 - 81x$$
$$\mathcal{E}_2 : v^2 = u^3 - u$$

as curves over $\mathbb{Z}_{(3)}$.

a. *Show that* $\mathcal{E}_2$ *has good reduction at* 3, *but* $\mathcal{E}_1$ *does not.*

b. *Let* $E_i = \mathcal{E}_{i,\mathbb{Q}}$. *Show that* $E_1 \cong E_2$. *(*HINT: Let $u = \frac{x}{3}$.*)*

Thus, we are forced to make the following definition: A variety X/K has good reduction at $\mathfrak{p}$ if there is some variety $\mathcal{X}/A$ such that $\mathcal{X}_K \cong X$.

For example, even though the discriminant of $x^3 - 81x$ is $2^2 3^{12}$, the curve $y^2 = x^3 - 81x$ has good reduction at 3.

Question 9.4. *Consider a projective line* $L/\mathbb{Q}$, *say with (projective) equation* $aX + bY + cZ = 0$. *Show that, for each* p, L *has good reduction at* p. *(*HINT: Use the strategy of Question 9.1.*)*

Question 9.5. *Let* E/K *be a curve with (short) Weierstrass equation*

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Assume $\mathrm{char}(\kappa) \neq 2, 3$.

a. *Suppose* u *in*K. *Show that the change of coordinates*

$$(x, y) \longmapsto \left(\frac{x}{u^2}, \frac{y}{u^3}\right)$$

leads to a new equation

$$y^2 = f_u(x) = x^3 + au^2x^2 + bu^4x + cu^6.$$

for E.

b. *What is the relation between the discriminants* $\Delta(f(x))$ *and* $\Delta(f_u(x))$*?*

c. *Show that one can always choose a* u *such that each* $a_i \in A$ *and*

$$0 \leq \mathrm{ord}_p(\Delta(f_u(x)) < 12.$$

Such an equation is called a minimal model, or equation, for E. The curve has good reduction if and only if $\mathrm{ord}_p(\Delta(f_u(x))) = 0$.

9.3 Reduction maps

We now work with some elliptic curve E with good reduction at $\mathfrak{p}$, and assume a minimal model has been chosen.

Question 9.6. *a. Explain why there is a map (of sets)*

$$E(K) \xrightarrow{r} E(\kappa)$$

$$P \longmapsto \overline{P}$$

b. Suppose $P \in E(K)$. Show that $P \in \ker r \iff$ P has a representative $P = [x, y, z]$, where $x, z \in \mathfrak{p}$, $y \notin \mathfrak{p}$.

In fact, one can show:

Proposition The map r in Question 9.6 is a group homomorphism.

Here is a special case:

Question 9.7. *Suppose $P, Q, R \in E(K)$ are distinct points, and in fact that $\overline{P}$, $\overline{Q}$, and $\overline{R}$ are all distinct. Suppose further that*

$$P + Q + R = \mathcal{O} \text{ (on } E).$$

Show that

$$\overline{P} + \overline{Q} + \overline{R} = \overline{\mathcal{O}} \text{ (on } \overline{E})$$

*(*HINT: Remember, $P + Q + R = \mathcal{O}$ if and only if there is a line passing through all three points.*)*

If we now assume that K is *complete*, we can say even more about the reduction map.

Question 9.8. *Suppose that $E/\mathbb{Q}_p$ has good reduction. Show that*

$$E(\mathbb{Q}_p) \xrightarrow{r} \overline{E}(\mathbb{F}_p)$$

*is surjective. (*HINT: Hensel's lemma!*)*

9.4 The kernel of reduction

In this section, we will work our way up to the proof of:

Theorem If $p \nmid m$, then the reduction map on m-torsion,

$$E[m](\mathbb{Q}_p) \longrightarrow E[m](\mathbb{F}_p)$$

is injective.

At some point, you will have to read Question 9.11 to make progress.

We will define a *filtration* on $E(\mathbb{Q}_p)$, as follows. Set

$$\begin{aligned} E^1(\mathbb{Q}_p) &= \ker r \\ &= \{P \text{has a representative } [x,y,z] : p|x, p|z, p \nmid y\} \end{aligned}$$

and, for $n \geq 1$,

$$E^n(\mathbb{Q}_p) = \{P \in E^1(\mathbb{Q}_p) : \frac{x(P)}{y(P)} \in p^n\mathbb{Z}_p\}.$$

(Note that if $P \in E^1(\mathbb{Q}_p)$, then $y(P) \neq 0$ for any representative; and the function $x(P)/y(P)$ is well-defined, independent of the choice of representative.)

Question 9.9. *a. Suppose $P = (x,y) = [x,y,1] \in E^1(\mathbb{Q}_p)$. Show there is some number n such that*

$$\begin{aligned} \text{ord}_p(x) &= 2n \\ \text{ord}_p(y) &= 3n \end{aligned}$$

*(*HINT: Write $x = p^e x_0$, $y = p^f y_0$ with $x_0, y_0 \in \mathbb{Z}_p^\times$. Remember that $f < 0$ (why?), and then use the Weierstrass equation for E.*)*

b. Suppose $P = [x,y,z] \in E^n(\mathbb{Q}_p) \smallsetminus E^{n+1}(\mathbb{Q}_p)$ for some $n \geq 1$. Show that

$$P = [p^n x_0, y_0, p^{3n} z_0] \tag{1}$$

with $y_0 \in \mathbb{Z}_p^\times$, $x_0, y_0 \in \mathbb{Z}_p$.

c. For P as in (1)*, show that*

$$\overline{P}_0 := [\overline{x}_0, \overline{y}_0, \overline{z}_0]$$

lies on the cuspidal cubic $\overline{C}(\mathbb{F}_p)$.

Given this, one can show:

Lemma The map of sets

$$E^n(\mathbb{Q}_p) \longrightarrow \overline{C}_0(\mathbb{F}_p) \cong \mathbb{F}_p$$

$$P \longmapsto \overline{P}_0$$

is a surjective group homomorphism, with kernel $E^{n+1}(\mathbb{Q}_p)$.

Sketch It is a group homomorphism, since the group law on both sides is given by "collinear points sum to zero". It is surjective by Hensel's lemma; and it is easy to see that the kernel is exactly $E^{n+1}(\mathbb{Q}_p)$. □

Question 9.10. *Suppose $p \nmid m$.*

a. *Suppose $P \in E^n(\mathbb{Q}_p) \smallsetminus E^{n+1}(\mathbb{Q}_p)$ is nonzero. Show that $mP \neq \mathcal{O}$. (*HINT: $\mathbb{F}_p$ has no nontrivial m-torsion.*)*

b. *Show that the natural map*

$$E(\mathbb{Q}_p)[m] \longrightarrow E[m](\mathbb{F}_p)$$

is an inclusion.

9.5 Cuspidal cubic

Let C be the projective curve with affine equation $y^2 = x^3$, i.e., with homogeneous equation.

$$C : Y^2Z = X^3.$$

It is singular at $S = [0, 0, 1]$, and smooth elsewhere.

Question 9.11. a. *Show that $C \cap \{Y = 0\} = S$, so that if we dehomogenize on Y, we have the affine equation*

$$v = u^3$$

for the affine curve $C_0 := C \smallsetminus S$.

b. *Consider an (affine) line $L_0 : v = ax + b$, and suppose that*

$$(L_0 \cap C_0)(\overline{K}) = \{(u_1, v_1), (u_2, v_2), (u_3, v_3)\}.$$

*(Why must there be three points?) Show that $u_1 + u_2 + u_3 = 0$. (*HINT: Look at the coefficient of u^2 in the equation for $L_0 \cap C_0$.*)*

One can use this to show that $C_0(K)$ has a group law in which three points sum to zero if and only if they are collinear, and that

$$E_0(K) \longrightarrow (K, +)$$

$$P \longmapsto x(P)$$

is an isomorphism of groups.