Last time: Reduction of $E/\mathbb{Q}$. The groups one gets in each case

- Good reduction: an elliptic curve
- Multiplicative split: $\mathbb{G}_m : R \mapsto \mathbb{G}_m(R) = R^\times$
- Multiplicative non-split, $U(1)$, the 1-units in $\mathbb{F}_{p^2}$ with $x^{p+1} = 1$. What would the points of a general R be for R an algebra over $\mathbb{F}_{p^2}$.
- Additive case, $\mathbb{G}_a : R \mapsto R^+$ (viewed as an additive group).

We want to understand reductions over $\overline{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$). Let $\overline{\mathbb{Z}}$ be the algebraic integers.

If we have a maximal ideal $\subseteq \overline{\mathbb{Z}}$ then $\cap\,\mathbb{Z} = p\mathbb{Z}$ for some p prime.

We can think of

$$\overline{\mathbb{Q}} = \bigcup_{K/\mathbb{Q} \text{ finite alg}} K.$$

For each K we have $\mathcal{O}_K$ the ring of integers of K, and play this same game (here $\overline{\mathbb{Z}} \cap K = \mathcal{O}_K$).

We can consider what $p\mathcal{O}_K$ is for p a prime. Then

$$p\mathcal{O}_K = \prod_{j=1}^{g_K} {}_{K,j}^{e_j},$$

where ${}_{K,j}$ are prime ideals in $\mathcal{O}_K$ and $e_i \in \mathbb{N}$. These will be maximal, so $\mathcal{O}_K/{}_{K,j}$ is a field (a finite extension of $\mathbb{F}_p$). It is customary to say

$$f_i = [\mathcal{O}_K/{}_{K,j} : \mathbb{F}_p].$$

Then we actually have

$$[K : \mathbb{Q}] = \sum_{j=1}^{g_K} e_j f_j.$$

An alternate way to view this, we have a map $\mathbb{Z} \to \mathcal{O}_K$ and so a map $\operatorname{Spec} \mathcal{O}_K \to \operatorname{Spec} \mathbb{Z}$, and this is counting the degree at $p\mathbb{Z}$ in two different ways (degree defined appropriately)

Remark .0.1

Neukirch "Algebraic Number Theory" and also Cassels and Frohlich are good references for algebraic number theory.

If we have then $\subseteq \overline{\mathbb{Z}}$ then we can write it as

$$= \bigcup_{K/\mathbb{Q}} {}_K$$

such that for K'/K we have $\mathfrak{p}_{K'} \cap \mathcal{O}_K = {}_K$. Then in fact

$$\overline{\mathbb{Z}}_{(\overline{\mathfrak{p}})} = \{x/y \mid y \notin \overline{\mathfrak{p}}\}$$
$$\overline{\mathbb{Z}}_{(\overline{\mathfrak{p}})}/\overline{\mathfrak{p}} = \overline{\mathbb{Z}}/\overline{\mathfrak{p}} = \overline{\mathbb{F}_p}.$$

Lemma .0.1

If we have $\subseteq \overline{\mathbb{Z}}$ a maximal ideal and $\alpha \in \overline{\mathbb{Q}}$ then α or $1/\alpha$ lies in $\overline{\mathbb{Z}}_{()}$.

Proof. Fix α. Then $\alpha \in K/\mathbb{Q}$ for some finite extension $K/\mathbb{Q}$. Thus it suffices to show α or $1/\alpha$ lies in $\mathcal{O}_{K_{(K)}}$. This is in fact easy since $\mathcal{O}_{K_{(K)}}$ is a discrete valuation ring.

For the unitiated (including the current writer of the notes, check back with the future writer),this is a valuation map from the ring to $\mathbb{Z} \cup \{\infty\}$. Then $v_{_K} = -v_{_K}(1/\alpha)$. Furthermore $v_{_K}^{-1}(\mathbb{Z}_{\geq 0}) = \mathcal{O}_{K_{(K)}}$, so one of these lies in the set.

Example .0.1

$K = \mathbb{Q}, \mathcal{O}_K = \mathbb{Z}$ and p a prime. Then we write

$$v_p\left(\frac{a}{b}\right) = v_p\left(\frac{a'p^k}{b'p^j}\right) = k - j,$$

where $a = a'p^k, b = b'p^j$ where $p \nmid a', b'$. The points in $\mathbb{Z}_{(p)}$ are exactly those points with nonnegative valuation.

Suppose we have an elliptic curve $E/\overline{\mathbb{Q}}$. Transform the Weierstrass equation so that we have something $\overline{\mathbb{Z}}$-integral. We know $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Z}}$. So we can assume the coefficients of E lie in $\overline{\mathbb{Z}}_{()}$.

Reduce via map $\overline{\mathbb{Z}}_{()} \to \overline{\mathbb{F}}_p$ to get Weierstrass equation. We can then make sense of ordinary, supersingular, multiplicative, and additive cases.

Potentially: Isomorphism classes of elliptic curves over $\overline{\mathbb{Q}}$ are much bigger than those over $\mathbb{Q}$. In fact this happens. Thus when we think about reduction, the situation is slightly different.

Fact: So long as $p \neq 2$ we can change coordinates to the form

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

where $\lambda \notin \{0, 1\}$ and $\lambda \in \overline{\mathbb{Z}}_{()}$. Then one can check that additive reduction is not possible for an equation of this type. The same is true for $p = 2$, but this is not quite the right form.

Definition .0.1

A -minimal Weierstrass equation is one with only good or multiplicative reduction over .

Proposition .0.2

Reduction type is well defined on $\overline{\mathbb{Q}}$-isomorphism classes. That is the reduction type cannot move between good and multiplcative for minimal models like the above.

Proof. There is the number Δ, and there's another number c_4, associated to the elliptic curves. We in fact have

$$\text{additive reduction} \iff \Delta = 0, c_4 = 0 \mod$$

If we do a change of variables, then $u^{12}\Delta' = \Delta$ and $u^4 c_4' = c_4$ for some u (in terms of the change of coordinates).

The case we're frightened of–$\Delta' \in \overline{\mathbb{Z}}_{()}^{\times}$ but $\Delta \in \overline{\mathbb{Z}}$.

If this is the case then $u^{12}, u^4 \in \overline{\mathbb{Z}}_{()}$. Then c_4 will also lie this ideal, which will give us additive reduction (which is impossible with minimal models).

Proposition .0.3

$E/\overline{\mathbb{Q}}$ has good reduction at if and only if $j[E] \in \overline{\mathbb{Z}}_{()}$.

Proof. Remember that the j invariant is $j = c_4^3/\Delta$.

Reducing Points. There is a reduction map

$$\mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{P}^n(\overline{\mathbb{F}}_p)$$
$$[x_0, \dots, x_n] \mapsto [\widetilde{x}_1, \dots, \widetilde{x}_n].$$

Technical point, we have to scale $x_0, \dots, x_n$ so that one of them does not lie in $\overline{\mathbb{Z}}$ and all of them lie in $\overline{\mathbb{Z}}_{()}$.

Hence $E \subseteq \mathbb{P}^2(\overline{\mathbb{Q}})$ can be reduced on points. We want to understand reduction of $E[N]$.

Theorem .0.4

We get a map $E[N] \to \widetilde{E}[N]$ that is surjective.

Proof. Getting the map is clear–equations for N-torsion are algebraic and we can just reduce. When $p \nmid 6N$, then $E[p^n] = \mathbb{Z}/p^n\mathbb{Z}$ or $E[p^n] = 0$. The second obviously works and the first we'll get an isomorphism if we have injectivity... then we stare at the map.

Proposition .0.5

Say $E/\overline{\mathbb{Q}}$ has good reduction at p. Say $C \subseteq E$ is a cyclic subgroup of order p. Then

- E/C has good reduction
- $E, E/C$ have the same reduction type, ordinary versus supersingular.

Proof of second piece. Say $\varphi : E \to E/C = E'$ is the isogeny. Then $\psi : E' \to E$ can be given as the dual isogeny.

We know $\psi \circ \varphi = [p]_E$ and $\varphi \circ \psi = [p]_{E'}$. Then if we look at the reduced isogenies

$$\widetilde{\varphi} \circ \widetilde{\psi} \circ \widetilde{\varphi} = \widetilde{\varphi} \circ [p]_{\widetilde{E}'}$$
$$= [p]_{\widetilde{E}} \circ \widetilde{\varphi}.$$

This in fact tells us that

$$\deg_{\text{sep}}[p]_{\widetilde{E}} = \deg_{\text{sep}}[p]_{\widetilde{E}'}.$$

Reduction for more general Curves. Specifically, we want modular curves.

Definition .0.2

Suppose C is a nonsingular affine curve over $\mathbb{Q}$ cut out by equations $\varphi_1, \dots, \varphi_m \in \mathbb{Z}_{(p)}[X_1, \dots, X_n]$. We'll say C has good reduction at p provided that

(1) $I = \langle \varphi_1, \dots, \varphi_m \rangle \subseteq \mathbb{Z}_{(p)}[X_1, \dots, X_N]$ is prime

(2) $\widetilde{I} = \langle \widetilde{\varphi}_1, \dots, \widetilde{\varphi}_m \rangle \subseteq \mathbb{F}_p[X_1, \dots, X_N]$ defines a nonsingular affine algebraic curve.

What is Condition 1 doing? Lets see what it rules out

Non-Example .0.2

Let $I = \langle p(py-1), (y-x^2)(py-1)\rangle$. Inside $\mathbb{Q}$ we have $I_{\mathbb{Q}} \subseteq \mathbb{Q}[x,y]$ just defines the curve $y = 1/p$. However this is not prime in $\mathbb{Z}_{(p)}[x,y]$ since we cannot scale by $1/p$.

The reduction is $\widetilde{I} \subseteq \mathbb{F}_p[x,y]$ is $y = x^2$.

For elliptic curves Condition 1 is automatic, as Weierstrass equations are very simple.

For projective curves we'll homogenize the affine case.

Definition .0.3

Suppose we have some $I_{(0)} \subseteq \mathbb{Z}_{(p)}[X_1, \dots, X_n]$ prime with homogenization $I \subseteq \mathbb{Z}_{(p)}[X_0, \dots, X_n]$.

Say this gives a projective curve C_{hom}. We say C_{hom} has good reduction at p if for all i either C_i (unhomogenizing at x_i) has good reduction at p or $\widetilde{I}_{(i)} = \mathbb{F}_p[X_1, \dots, \widehat{X}_i, \dots, X_N]$ (empty reduction).

We can let $\widetilde{C}_{\text{hom}}$ be the reduced curve given by $(\widetilde{I}_{(0)})_{\text{hom}}$.

Note: Some commutative algebra tells us that if $I_{(0)}$ is prime, I is prime, and this implies $I_{(i)}$ is prime.

Recalling that $\mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{P}^n(\overline{\mathbb{F}}_p)$ gives us a map on points for reducing projective curves.

Theorem .0.6

If C is nonsingular, projective, of good reduction at p, then the reduction map $C \to \widetilde{C}$ is surjective.

Fact we won't state: You can also reduce morphisms! The idea is to reduce the algebraic equations defining the maps, which gives you something rational, and then extend by nonsingularity.

One would really like to have a commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{h} & C' \\ \downarrow & & \downarrow \\ \widetilde{C} & \xrightarrow[\widetilde{h}]{} & \widetilde{C}' \end{array}$$

But in fact this only holds if $g(C') > 0$.

Theorem .0.7

If $g(C') > 0$ and $h : C \to C'$ over $\mathbb{Q}$ where these have good reduction then

$$\begin{array}{ccc} C & \xrightarrow{h} & C' \\ \downarrow & & \downarrow \\ \widetilde{C} & \overset{\widetilde{h}}{\dashrightarrow} & \widetilde{C}' \end{array}$$

and this $\widetilde{h}$ is unique.