Reducing points mod p

Idea: $E: y^2 = x^3 + ax + b$ an elliptic curve / $\mathbb{Q}$. $\Delta = \mathrm{disc}\, E = 2(4a^3 + 27b^2)$

Let p be a prime such that • a, b have no 'p' in denominators
• $p \nmid \Delta$.

Then we can reduce a, b mod p (call reds $\bar{a}, \bar{b} \in \mathbb{F}_p$),

& get an EC $\bar{E}: y^2 = x^3 + \bar{a}x + \bar{b}$ over $\mathbb{F}_p$.

Moreover, we can reduce points. Let $(x_0 : y_0 : z_0) \in E(\mathbb{Q})$

Then choose representative (x_0', y_0', z_0') such that:

• x_0', y_0', z_0' have no p in denom;
• p doesn't divide all 3 of them

} ex: always possible

Then can again reduce mod p, getting $(\bar{x}_0, \bar{y}_0, \bar{z}_0)$

Ex: • The point $(\bar{x}_0 : \bar{y}_0 : \bar{z}_0)$ is on $\bar{E}(\mathbb{F}_p)$
• The pt is indep of choices.

This defines a map of sets $E(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p)$.

In fact, it is even a group homomorphism. Idea: lines reduce to lines. More formal proof later.

In general, $E(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p)$ is neither injective nor surjective.

Amazing fact: $E(\mathbb{Q})_{\text{tors}} \to \bar{E}(\mathbb{F}_p)$ is injective. Pf in 3 weeks?

reached end of lecture

(24) Aims for now (towards pf of fact, & later MW):

- Generalise 'reduction mod p' to larger class of fields 'fraction fields of DVRs'.
- Introduce $\mathbb{Q}_p$: - $\mathbb{Q} \subseteq \mathbb{Q}_p$
  - $E(\mathbb{Q}_p) \to E(\mathbb{F}_p)$ is surjective.
- Hasse principal,
- Pf that $E(\mathbb{Q})_{tors} \hookrightarrow E(\mathbb{F}_p)$ (in particular, finite!) Will give algorithm to find torsion pts.

Discrete valuation rings (DVRs)

Let K be a field. A discrete valuation on K is a function

$v: K \to \mathbb{Z} \cup \{\infty\}$ s.t.

- $v(x \cdot y) = v(x) + v(y)$
- $v(x+y) \geq \min\{v(x), v(y)\}$
- $v(x) = \infty \iff x = 0$

(here $\infty +$ anything $= \infty$, & $\infty >$ everything else).

- Is called trivial if only takes values $0, \infty$.
  normalised if surjective.

Eg: $K = \mathbb{Q}$, p prime. $v(p^j \frac{a}{b}) = j$, where $a, b \in \mathbb{Z}$, $p \nmid ab$.

- Clearly $v(xy) = v(x) + v(y)$. $v = v_p = \text{ord}_p$
- others ex.

Eg: k field, $K = k(t)$,

$v(f)$ = exponent of lowest degree term

$v(a_n t^n + a_{n+1} t^{n+1} + \cdots) = n$ if $a_n \neq 0$.

Given a field K with disc. val. v, we define the integers

$$\mathcal{O}_K = \mathcal{O}_{K,v} = \{x \in K \mid v(x) \geq 0\}.$$

Ex: $\mathcal{O}_K$ is a subring of K.

eg: $K = \mathbb{Q}$, $v = v_p$, then $\mathcal{O}_{\mathbb{Q},p} = \left\{x \in \mathbb{Q} \;\middle|\; \begin{array}{c}\text{can write} \\ x = \frac{a}{b} \text{ with } p \nmid b\end{array}\right\}$.

Def: A DVR is a ring R s.t. $\exists$ a (non-trivial, discrete) valuation $v : \mathrm{Frac}\, R \to \mathbb{Z} \cup \{\infty\}$ s.t. $R = \{x \in \mathrm{Frac}\, R \mid v(x) \geq 0\}$.

Ex: Let R a DVR. Then $\exists!$ normalized valuation $v : \mathrm{Frac}\, R \to \mathbb{Z} \cup \{\infty\}$ s.t. $R = \{x \mid v(x) \geq 0\}$.

From now on, use this unless otherwise stated.

(other facts needed here)

- $\mathfrak{m} := \{x \in R \mid v(x) > 0\}$. This is an ideal, in fact it is the maximal ideal of R; (eg. $p \cdot \mathcal{O}_{\mathbb{Q},p}$)
- $R/\mathfrak{m} := k$, the residue field of R (eg $\mathbb{F}_p$)

- Let $\pi \in R$ such that $v(\pi) = 1$ (such a π is called a uniformiser).
  Then $\mathfrak{m} = \pi \cdot R$ (ex).

Reduction over DVRs

For this section, fix a DVR R, $K = \mathrm{Frac}\, R$, $v: K \to \mathbb{Z} \cup \{\infty\}$ normalized, m, k.
Let (E, o) be an E Curve K. $E: y^2 = f(x) = x^3 + ax^2 + bx + c$.

Assume: • $v(a) \geq 0$ & $v(b) \geq 0$ & $v(c) \geq 0$;

• $v(\Delta_E) = 0$.

Write $\bar{\ }: R \to R/m = k$ for the quotient map.

• Define $\bar{E}$ by $y^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}$, an E Curve k.

• Given $p \in E(K)$, choose a representative

(x_p, y_p, z_p) such that

• $v(x_p), v(y_p) \geq 0$ & $v(z_p) \geq 0$

• at least one of $v(x_p), v(z_p) = 0$

(ex: always possible).

Define $\bar{p} = (\bar{x}_p : \bar{y}_p : \bar{z}_p)$. Since the equation

$z_p y_p^2 = f(x_p)$ holds in R, it's clear that

$\bar{z}_p \bar{y}_p^2 = \bar{f}(\bar{x}_p)$ holds in k, so $\bar{p} \in \bar{E}(k)$.

Check • the map $E(K) \to \bar{E}(k)$ is indep. of choices.

$p \longmapsto \bar{p}$

Prop: The map $\tilde{\ }: E(K) \to \tilde{E}(k)$ is a group hom.

Pf: · Clearly sends $(0:1:0)$ to $(0:1:0)$. (id to id).

· Could approach this via: if P, Q, R lie on line $L: \alpha x+\beta y+\delta z=0$ then $\tilde{P}, \tilde{Q}, \tilde{R}$ lie on line $\tilde{L}: \tilde{\alpha} x+\tilde{\beta} y+\tilde{\delta} z=0$.
However, get problems when need to take into account higher intersection multiplicities.

However, is immediately obvious from formulae for group law.

□

p-adic numbers

- For us, these will be the most important eg. of DVRs.
- Recall $E(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_q)$ not surj. in gen. The p-adics will "fix this"
- Also super-useful in lots of contexts;
- cf Eyang's local fields course.
- key in proving $E(\mathbb{Q})_{tors} \hookrightarrow \tilde{E}(\mathbb{F}_p)$ & $E(\mathbb{Q})$ fin. gen.

- Recall $\mathbb{R} = \frac{\{\text{cauchy seq. in } \mathbb{Q} \text{ wrt } |\cdot|\}}{\{\text{null seq in } \mathbb{Q} \text{ wrt } |\cdot|\}}$.

- Idea: replace $|\cdot|$ with $|\cdot|_p$ (as in hwork), then apply same construction

Recall (from Hw): • $|p^r \frac{a}{b}|_p = p^{-r}$ if $p \nmid a,b$.

• $|\cdot|_p$ is an absolute value (Sometimes write $\|\cdot\|_p$).

So cauchy & null seq. wrt $|\cdot|_p$ make sense.

Def: $\mathbb{Q}_p := \frac{\{\text{cauchy seq. in } \mathbb{Q} \text{ wrt } |\cdot|_p\}}{\{\text{null} \quad \text{---}''\text{---} \quad \}}$.

Basic properties:

- $\mathbb{Q}_p$ inherits a field structure from $\mathbb{Q}$, with component-wise addition & multiplication of elts. Pf: same as for $\mathbb{R}$. □

Prop: Let $(a_n)_n \not\to 0$ be a cauchy seq. in $\mathbb{Q}$ wrt $|\cdot|_p$. Then $\exists N \in \mathbb{N}$ s.t. $|a_n|_p = |a_m|_p \ \forall m,n > N$.

Pf: $(a_n)_n$ cauchy means: $\forall \varepsilon > 0 \exists N_\varepsilon$ s.t. $\forall m,n > N_\varepsilon$, $|a_m - a_n|_p < \varepsilon$.

$(a_n)_n \not\to 0$ means $\exists \varepsilon_0$ s.t. $\forall N \in \mathbb{N} \ \exists n_0 > N$ s.t. $|a_{n_0}|_p > \varepsilon_0$.

Ok, ~~then take that~~ such an ε_0, N_{ε_0}. Then if $m > N_{\varepsilon_0}$ then

$$|a_m|_p = |a_m - a_{n_0} + a_{n_0}|_p \leq \max\{\underbrace{|a_m - a_{n_0}|_p}_{<\varepsilon_0}, |a_{n_0}|_p\}$$
$$\therefore |a_{n_0}|_p \qquad \square$$

Cor: We can define an abs value $|-|_p$ on $\mathbb{Q}_p$ by

$$|0|_p = 0, \qquad |(a_n)_n|_p = \lim_{n\to\infty} |a_n|_p, \text{ which stabilizes, so lim exists!}$$

- check that this is actually an abs value (easy).
- Clearly, image of $|-|_p : \mathbb{Q}_p \to \mathbb{R}$ equals image of $H_p : \mathbb{Q} \to \mathbb{R}$. ⊛

Recall: $v : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ ⇝ $|-|_p : \mathbb{Q} \to \mathbb{R}$

$p^r \frac{a}{b} \longmapsto r$ $\qquad x \longmapsto p^{-v(x)}$

We can reverse this to get a discrete valuation on $\mathbb{Q}_p$:

$ord_p = v : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$.

$$x \longmapsto -\log_p(|x|_p)$$

- well-def'd because $|-|_p$ has by ⊛
- check it's a disc. valuation (easy).

Ok, so have a field $\mathbb{Q}_p$ with a disc. val. (normalized) dvr. val.
Same get a DVR:

Def: $\mathbb{Z}_p := \mathcal{O}_{\mathbb{Q}_p} = \{x \in \mathbb{Q}_p \mid ord_p(x) \geq 0\}$.

Ex: $\mathbb{Q}_p \cap \mathbb{Q} \cap \mathbb{Z}_p = \{p^r \frac{a}{b} \in \mathbb{Z}\mathbb{Q} \mid r \geq 0\}$.

- max. ideal is $m_p = \{x \in \mathbb{Q}_p \mid ord_p(x) > 0\}$
- $v(p) = 1$, so $m_p = p\mathbb{Z}_p$.

Prop: $\mathbb{Z}_p / p\mathbb{Z}_p = \mathbb{F}_p$ (residue field) — canonical

Pf: Let $\alpha \in \mathbb{Z}_p$, and let $(a_n)_n$ be cauchy seq rep α. Then $\mathrm{ord}_p(\alpha) \geq 0$ so $\exists N \in \mathbb{N}$ s.t. $\forall n \geq N$, $\mathrm{ord}_p(a_n) \geq 0$. (this was massmail as pass)

Since (a_n) cauchy we know $\exists M \in \mathbb{N}$ s.t. $\forall m, n \geq M$, $|a_m - a_n| < 1$, ie. $\mathrm{ord}_p(a_n - a_m) > 0$. (this was massmail as pass)

Write $a_n = \frac{b_n}{c_n}$, coprime integers, so $p \nmid c_n$ if $n \geq N$. $\overline{b_n}$ = image of b_n in $\mathbb{F}_p = \mathbb{Z}/p$ etc

Define $\varphi: \mathbb{Z}_p \to \mathbb{F}_p$ by:
- first choose $r \geq \max(M, N)$.

$$\varphi(\alpha) = \overline{c_r}^{-1} \cdot \overline{b_r}$$

Then: φ indep of choice of b_r, c_r (easy check);

- $\overline{c_r} \neq 0$ because $\mathrm{ord}_p(a_r) \geq 0$;
- Indep of r because if we chose $r' > r$ instead then

$\mathrm{ord}_p(a_r - a_{r'}) > 0$, so

$$p \mid b_r c_{r'} - b_{r'} c_r, \text{ so } \frac{\overline{b_r}}{\overline{c_r}} = \frac{\overline{b_{r'}}}{\overline{c_{r'}}}.$$

So φ is well defined. Clearly surjective, as $\mathbb{Z} \subseteq \mathbb{Z}_p$, & map restricts to $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

Kernel is exactly α s.t. $\mathrm{ord}_p \alpha > 0$, $= p\mathbb{Z}_p$. □

Prop: $\mathbb{Z}_p / p^n \mathbb{Z}_p = \mathbb{Z}/p^n\mathbb{Z}$ $\forall n \geq 1$

Pf: Similar, omitted. (□)

Expansions of p-adic numbers

Prop: Let $\alpha \in \mathbb{Z}_p$. Then $\exists\ a_0, a_1, \ldots$ in $\{0, 1, \ldots, p-1\}$ such that $\alpha = \sum_{i=0}^{\infty} a_i p^i$, & moreover the a_i are unique.

Also, $a_0 = 0 \iff \alpha \in p\mathbb{Z}_p$.

Pf: Let $\varphi : \mathbb{Z}_p \xrightarrow{\sim} \mathbb{F}_p$ as before. Choose a_0 s.t. $\varphi(\alpha) = \bar{a}_0$.

(so clearly $a_0 = 0 \iff \alpha \in p\mathbb{Z}_p$).

Now $\mathrm{ord}_p(\alpha - a_0) > 0$, ie $\alpha - a_0 \in p\mathbb{Z}_p$.

Let $\alpha_1 \in \mathbb{Z}_p$ be s.t. $\alpha - a_0 = p\alpha_1$. Choose a_1 s.t. $\varphi(\alpha_1) = \bar{a}_1$.

Then $\alpha_1 - a_1 \in p\mathbb{Z}_p$, so $\alpha_1 - a_1 = p\alpha_2$ some $\alpha_2 \in \mathbb{Z}_p$.

Induction, construct a_i for all i,

Then $\sum_{i=0}^{\infty} a_i p^i$ - converges (partial sums cauchy wrt $|\cdot|_p$)

$- \alpha - \sum_{i=0}^{\infty} a_i p^i = 0$ - check converges to 0.

- if $\sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{\infty} b_i p^i$, then similar argument shows $a_i = b_i\ \forall i$. □

Cor Let $\alpha \in \mathbb{Q}_p$. Then α can be written as $\sum_{i=-N}^{\infty} a_i p^i$, some $N \geq 0$, $a_i \in \{0, 1, \ldots, p-1\}$, with a_i unique.

Pf: $p^{-\mathrm{ord}_p \alpha} \alpha \in \mathbb{Z}_p$, apply above prop. □

Aside: The Hasse Principal

Let $C \subseteq \mathbb{P}^n_{\mathbb{Q}}$ a variety. We have $\mathbb{Q} \subset \mathbb{Q}_p$ $\forall p$ & $\mathbb{Q} \subset \mathbb{R}$,

so if $C(\mathbb{Q}) \neq \emptyset$ then $C(\mathbb{Q}_p) \neq \emptyset$ & $C(\mathbb{R}) \neq \emptyset$!

Thm [Legendre]: Let $C \subseteq \mathbb{P}^2_{\mathbb{Q}}$ a smooth curve of degree 2. Then

$$C(\mathbb{Q}) \neq \emptyset \iff \left\{ C(\mathbb{R}) \neq \emptyset \;\&\; \forall p,\ C(\mathbb{Q}_p) \neq \emptyset \right\}$$

We say degree 2 curves satisfy the Hasse principal.

Thm [Selmer]: The curve in $\mathbb{P}^2_{\mathbb{Q}}$ given by $3x^3 + 4y^3 + 5z^3 = 0$ has $C(\mathbb{R}) \neq \emptyset$ & $C(\mathbb{Q}_p) \neq \emptyset$, but $C(\mathbb{Q}) = \emptyset$ so Hasse principal fails for this curve

- studying which (classes of) varieties HP hold for is big subject!

End lecture

lemma: Let $\{f_1, \dots, f_r\} \subseteq \mathbb{Z}_p[x_1, \dots, x_k]$ and set of polys. Then

$$\left(\text{The } f_i \text{ have a common soln in } \mathbb{Z}_p^k\right) \iff \left(\forall n,\ \text{the } f_i \text{ have a common soln in } \left(\mathbb{Z}_p / p^n \mathbb{Z}_p\right)^k \cong \left(\mathbb{Z}/p^n\mathbb{Z}\right)^k\right).$$

Pf: $\Rightarrow$ easy.

$\Leftarrow$: Let $S(n) = \left\{ (x_1, \dots, x_k) \in \left(\mathbb{Z}/p^n\mathbb{Z}\right)^k \;\middle|\; f_i(x_1, \dots, x_k) \underset{\bmod p^n}{\equiv} 0 \ \forall i \right\}$.

Have red'n mod p^n maps $\dots \to S(n+2) \to S(n+1) \to S(n)$.

Let $\tilde{S}(n) = \left\{ x \in S(n) \;\middle|\; \begin{array}{l} \text{there exist infinitely many } y \in \bigcup_{m>n} S(m) \\ \text{such that } y \equiv x \bmod p^n \text{ (i.e. } y \text{ maps to } x \text{ under above maps.} \end{array} \right\}$

~~Note $\hat{S}(m) \neq \emptyset$ since $\prod_{n\geq 1} S(n)$ is infinite and $S(n)$ is infinite.~~

Pick x_1 in $S(1)$ s.t. $\{ y \in \bigcup_{m>1} S(m) \mid y \equiv x_1 \bmod p \text{ infinite} \}$.

Pick x_2 in $S(2)$ s.t. $x_1 \equiv x_2 \bmod p$

$\{ y \in \bigcup_{m>2} S(m) \mid y \equiv x_2 \bmod p^2 \text{ infinite} \}$

$\rightsquigarrow (x_1, x_2, \ldots), \quad x_n \in \mathbb{Z}/p^n$.

- Choose lifts $\tilde{x}_i$ of x_i to $\mathbb{Z}_p$.
- By construction, the sequence $(\tilde{x}_i)_i$ is cauchy, so converges to something in $\mathbb{Z}_p$, call it $\underline{x}$.

Wts $f_j(\underline{x}) = 0 \ \forall j$. For this, use that polynomials define cts fcns in p-adic topology. Then

$$f_i(\underline{x}) = f_i(\lim_i \tilde{x}_i) \overset{\text{fcts}}{=} \lim_i f(\tilde{x}_i) = 0.$$

(Can remove all choices if desired) $\square$

(34)

Hensel's lemma

This lemma is why p-adics are useful!

lemma (Hensel): Let $f \in \mathbb{Z}_p[x_1, \dots, x_n]$, & let $\underline{a} \in \mathbb{Z}_p^n$ be s.t. for some $m \geq 0$:

- $f(\underline{a}) \equiv 0 \mod p^{2m+1}$
- $\exists i$ s.t. $\left.\frac{\partial f}{\partial x_i}\right|_{\underline{a}} \not\equiv 0 \mod p^{m+1}$.

(i.e. $|f(\underline{a})|_p < \left|\left(\frac{\partial f}{\partial x_i}\right)|_{\underline{a}}\right|_p^2$ for some i).

Then $\exists\, \underline{b} \in \mathbb{Z}_p^n$ s.t. $\underline{b} \equiv \underline{a} \mod p^{m+1}$ & $f(\underline{b}) = 0$.

"if you have an approximate soln, then you can find an actual soln close to it, assuming a bit of smoothness."

Easily gives $E(\mathbb{Q}_p) \to E(\mathbb{F}_p)$ surjective.

~~Pf.~~

Pf: Assume we're in the setup of the lemma.

Step 1: & Find $\underline{\beta} \in \mathbb{Z}_p^n$ s.t. $\underline{\beta} \equiv \underline{\alpha} \mod p^{m+1}$ & $f(\underline{\beta}) \equiv 0 \mod p^{2m+2}$.

How? Write $\beta_j = \alpha_j + h_j p^{m+1}$, some $h_j \in \mathbb{Z}_p$ to be determined later.

Taylor expansion:

$$f(\beta_1, \dots, \beta_n) = f(\alpha_1, \dots, \alpha_n) + \sum_{j=1}^{n} \left(\frac{\partial f}{\partial x_j}\right)\Big|_{\underline{a}} h_j p^{m+1} + p^{2m+2}(\text{stuff})$$

Sowewant h_j s.t. $f(a_1, \dots, a_n) + \sum_j \left(\frac{\partial f}{\partial x_j}\right)_{\underline{a}} h_j p^{m+1}$ is divisible by p^{2m+2}.

We know $\exists k \le m$ s.t. $p^k \mid \left(\frac{\partial f}{\partial x_j}\right)_{\underline{a}}$ $\forall j$ & $p^{k+1} \nmid \left(\frac{\partial f}{\partial x_j}\right)_{\underline{a}}$ for some j.

Find $H_j \in \mathbb{Z}_p$ solving

$m \ge 0$: $$\frac{f(a_1, \dots, a_n)}{p^{2m+1}} + \sum_j \left(\frac{\partial f}{\partial x_j}\right)_{\underline{a}} \cdot \frac{1}{p^k} \cdot H_j \equiv 0 \bmod p,$$

Then set $h_j = H_j \cdot p^{m-k}$. Check that $\underline{b}$ does what we want.

Step 1 done.

Rk If $\underline{a}$ satisfies $f(\underline{a}) \equiv 0 \bmod p^{2m+r}$, $r \ge 1$, then step (1) gives us $\underline{\beta} \equiv \underline{a} \bmod p^{m+r}$ s.t. $f(\underline{\beta}) \equiv 0 \bmod p^{2m+r+1}$.

Step 2: let $\underline{a}_{2m+2} \in \mathbb{Z}_p^n$ be s.t. $\underline{a}_{2m+2} \equiv \underline{a} \bmod p^{m+1}$ & $f(\underline{a}_{2m+2}) \equiv 0 \bmod p^{2m+1}$, possible by step (1). Because $\underline{a}_{2m+2} \equiv \underline{a} \bmod p^{m+1}$, we find that $$\left(\frac{\partial f}{\partial x_j}\right)_{\underline{a}_{2m+2}} \equiv \left(\frac{\partial f}{\partial x_j}\right)_{\underline{a}} \bmod p^{m+1},$$

so there exists i s.t. $$\left(\frac{\partial f}{\partial x_i}\right)_{\underline{a}_{2m+2}} \not\equiv 0 \bmod p^{m+1}.$$

Then apply Rk to get $\underline{a}_{2m+3}$ s.t. $\underline{a}_{2m+3} \equiv \underline{a}_{2m+2} \bmod p^{m+2}$ etc,

End up with $\underline{a}$, $\underline{a}_{2m+2}$, $\underline{a}_{2m+3}$, ...

Clearly cauchy, write $\underline{b}$ for the limit in $\mathbb{Z}_p^n$.

f continuous, so

$$f(\underline{b}) = f\left(\lim_r \underline{a}_{2m+r}\right) = \lim_r f(\underline{a}_{2m+r}) = 0$$

□

(36)

Rk In statement of Hensel's lemma, can try replacing $\mathbb{Z}_p$ by a DVR R, and the $\equiv 0 \bmod p^n$ by $v(-) \geq n$.

Sometimes the resulting lemma holds (eg. $R = \mathbb{Z}_p$),

sometimes not (eg. $R = \mathcal{O}_{\mathbb{Q}, v_p}$).

Def We say a DVR R is Henselian if Hensel's lemma holds.
for R - to use later.
(So Hensel's lemma says that $\mathbb{Z}_p$ is Henselian)

Elliptic curves over $\mathbb{Q}_p$

Now things get a bit more fun. If you like, you can check that everything we will do with $\mathbb{Z}_p$ works just as well for an arbitrary Henselian DVR in place of $\mathbb{Z}_p$.

For rest of this section, we fix an elliptic curve

$E: y^2 = x^3 + ax + b$ over $\mathbb{Q}_p$, with $a, b \in \mathbb{Z}_p$ (so $\Delta \in \mathbb{Z}_p$) and $\Delta \not\equiv 0 \bmod p$

By previous §, have a reduction map

$$\text{red}: E(\mathbb{Q}_p) \to \overline{E}(\mathbb{F}_p), \text{ gp hom.}$$

Prop: red is surjective.

Pf:
- red $(0:1:0) = (0:1:0)$, so enough to hit points with z-coordinate 1
- Let $(x_0, y_0) \in \overline{E}(\mathbb{F}_p)$. Let $x_0', y_0' \in \mathbb{Z}_p$ s.t. $x_0' \equiv x_0 \bmod p$, $y_0' \equiv y_0 \bmod p$.

  Set $F = y^2 - (x^3 + ax + b)$, set $m = 0$.

  Then
- $F(x_0', y_0') \equiv 0 \bmod p$
- either $\left.\frac{\partial F}{\partial x}\right|_{x_0', y_0'} \not\equiv 0 \bmod p$ or $\left.\frac{\partial F}{\partial y}\right|_{x_0', y_0'} \not\equiv 0 \bmod p$,

since $\overline{E}$ smooth (as $p \nmid \Delta$).

Then Hensel's lemma gives us $(x_0, y_0) \in \mathbb{Z}_p^2$ s.t.

$F(x_0, y_0) = 0$ and $x_0 \equiv x_0' \bmod p$, $y_0 \equiv y_0' \bmod p$,

so red $(x_0 : y_0 : 1) = (x_0 : y_0 : 1)$. □

Def: Set $E^1(\mathbb{Q}_p) = \ker\left(E(\mathbb{Q}_p) \xrightarrow{\sim} \tilde{E}(\mathbb{F}_p)\right)$.

Clearly a subgp.

Next, will define a filtration:

$$E(\mathbb{Q}_p) = E^0(\mathbb{Q}_p) \supseteq E^1(\mathbb{Q}_p) \supseteq E^2(\mathbb{Q}_p) \supseteq \cdots$$

This filtration & its quotients will allow us to prove lots of fun things, such as $E(\mathbb{Q})_{\text{tors},p} \hookrightarrow \tilde{E}(\mathbb{F}_p)$, MW.

Prop: Let $P \in E^0(\mathbb{Q}_p)$. TFAE:

1) $P \in E^1(\mathbb{Q}_p)$
2) $P = (x:y:z)$ with $\operatorname{ord}_p(x) \geq 0$, $\operatorname{ord}_p(y) = 0$, $\operatorname{ord}_p(z) > 0$.

Pf: 2 $\Rightarrow$ 1: clearly such $(x:y:z)$ reduces to $(0:1:0)$ mod p.
1 $\Rightarrow$ 2: similar, ex. □

Def: Given $n \geq 2$, set

$$E^n(\mathbb{Q}_p) = \left\{ (x:y:z) \in E^1(\mathbb{Q}_p) \;\middle|\; \operatorname{ord}_p(x) - \operatorname{ord}_p(y) \geq n \right\}$$

- indep. of rep. of $=$ class.
- low, $\frac{x}{y} \in \mathfrak{p}^n \mathbb{Z}_p$.

Thm 1) $\forall n \geq 1$, $E^n(\mathbb{Q}_p)$ is a subgp of $E(\mathbb{Q}_p)$, and

the map $Q \longmapsto p^{-n}\frac{x(Q)}{y(Q)}$ is an isomorphism of gps

$$E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{F}_p$$

2) $\bigcap_n E^n(\mathbb{Q}_p) = \{O\}$.

Pf Part I: Induction on n; assume $E^n(\mathbb{Q}_p)$ subgp of $E(\mathbb{Q}_p)$.

If $Q = (x:y:1) \in E^1(\mathbb{Q}_p)$ then $y \notin \mathbb{Z}_p$.

Set $x = p^{-m} x_0$, $y = p^{-m'} y_0$, with $\mathrm{ord}_p(x_0) = \mathrm{ord}_p(y_0) = 0$, & $m' \geq 1$ (ie $x_0, y_0 \in \mathbb{Z}_p^\times$).

Then $p^{-2m'} y_0^2 = p^{-3m} x_0^3 + a p^{-m} x_0 + b$.

Taking ord_p on both sides, find $2m' = 3m$.

Set $n = m' - m \geq 1$, so $m = 2n$, $m' = 3n$.

Thus if $Q = (x:y:z) \in E^n(\mathbb{Q}_p) / E^{n+1}(\mathbb{Q}_p)$ and $n \geq 1$, then

$\mathrm{ord}_p(x) = \mathrm{ord}_p(z) - 2n$

& $\mathrm{ord}_p(y) = \mathrm{ord}_p(z) - 3n$.

Hence, can write

$$Q = (p^n x_0 : y_0 : p^{3n} z_0) \text{ with } y_0 \in \mathbb{Z}_p^\times,\ x_0, z_0 \in \mathbb{Z}_p.$$

Since $Q \in E(\mathbb{Q}_p)$, find

$$p^{3n} y_0^2 z_0 = p^{3n} x_0^3 + a p^{2n} x_0 z_0^2 + b p^{3n} z_0^3,$$

and so $Q_0 := (\bar{x}_0 : \bar{y}_0 : \bar{z}_0)$ is a pt on the curve

$E_0 : y^2 z = x^3$ over $\mathbb{F}_p$.

Note: · E_0 not smooth, so not EC (pt $(0:0:1)$ singular)

· $\bar{y}_0 \neq 0$, so Q_0 is not sing. pt.

It turns out (ex?) that 1) the formulae for the gp law turn $E_0(\mathbb{F}_p)\setminus\{(0:0:1)\}$ into an abelian gp;

2) using the same formulae, one checks that

$$E^n(\mathbb{Q}_p) \longrightarrow E_0(\mathbb{F}_p)\setminus\{(0:0:1)\}$$
$$Q \longmapsto Q_0$$

is a gp hom, even surjective.

3) The function

$$E_0(\mathbb{F}_p)\setminus\{(0:0:1)\} \longrightarrow \mathbb{F}_p$$
$$(x:y:z) \longmapsto \frac{x}{y}$$

is a gp. isom (same gp law on left, $+$ on right),

4) the kernel of $E^n(\mathbb{Q}_p) \longrightarrow E_0(\mathbb{F}_p)\setminus\{0,1\}$

$$Q \longmapsto Q_0$$

is exactly $E^{n+1}(\mathbb{Q}_p)$.

We will not write out details of these calcs. here.

In summary the map

$$E^n(\mathbb{Q}_p) \longrightarrow \mathbb{F}_p$$
$$(x:y:z) \longmapsto p^{-n}\frac{x}{y}$$

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

This proves part 1 of the thm.

Part 2 (easier!): Let $Q \in \bigcap E^n(\mathbb{Q}_p)$. Then $x(Q) = 0$ & $y(Q) \neq 0$.

Hence either $z(Q) = 0$ ($\Leftrightarrow Q = 0$) or

$y^2(Q) = b\, z(Q)^{2k}$, but this contradicts $Q \in E^1(\mathbb{Q}_p)$ □

Cor: Fix $m \in \mathbb{Z}_{>0}$ s.t. $p \nmid m$. Then

$$E^1(\mathbb{Q}_p) \longrightarrow E^1(\mathbb{Q}_p)$$
$$Q \longmapsto mQ$$

is a bijection.

Pf. Injectivity is easy: Let $Q \in E^1(\mathbb{Q}_p)$ s.t. $mQ = 0$. If $Q \neq 0$, then $Q \in E^n(\mathbb{Q}_p) \setminus E^{n+1}(\mathbb{Q}_p)$ for some n. Note $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \cong \mathbb{F}_p$. The image of Q in $\mathbb{F}_p$ is non-zero, hence so is the image of mQ. Hence $mQ \neq 0$, so map is injective.

Surjectivity: Fix $Q \in E^1(\mathbb{Q}_p)$. Will construct R s.t. $mR = Q$.

First, $E^1(\mathbb{Q}_p)/E^2(\mathbb{Q}_p) \cong \mathbb{F}_p$ & $p \nmid m$, so $\exists\, R_1 \in E^1(\mathbb{Q}_p)$ s.t. $mR_1 = Q \bmod E^2(\mathbb{Q}_p)$

Similarly $\exists\, R_2 \in E^2(\mathbb{Q}_p)$ s.t. $(Q - mR_1) \equiv mR_2 \bmod E^3(\mathbb{Q}_p)$ etc.

In this way, obtain sequence $R_1, R_2, \ldots$ s.t. $\forall i$, $R_i \in E^i(\mathbb{Q}_p)$ & $Q - m\sum_{j=1}^{i} R_j \in E^{i+1}(\mathbb{Q}_p)$.

~~Suppose we could find a subsequence of $\left(\sum_{j=1}^{i} R_j\right)_i$ which converged in the sense that~~

Idea: ~~Compactness of $\mathbb{Q}_p$ implies we can find a convergent~~

Idea: construct a convergent subsequence of the sequence of partial sums $\left(\sum_{j=1}^{i} R_j\right)_i$, then set R = limit. Then since $\bigcap E^i(\mathbb{Q}_p) = \{0\}$, we find $Q - mR = 0$.

(42) How to find such a subsequence? Compactness! (cool mixture of tools!)

More precisely:

1) Put a metric on $\mathbb{Z}_p$ by $d_p(a,b) = |a-b|_p$;

2) $\mathbb{Z}_p$ w.r.t. this metric, $\mathbb{Z}_p$ is complete; ~~(check this ... complete ...)~~

~~3)~~ 3) $\mathbb{Z}_p$ also totally bounded as metric space

$\forall \varepsilon > 0$ $\exists$ finite cover of $\mathbb{Z}_p$ by balls of radius $< \varepsilon$

Pf: Choose n s.t. $p^n > \frac{1}{\varepsilon}$, note that $\frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p} = \frac{\mathbb{Z}}{p^n\mathbb{Z}}$ is finite □

4) Hence, $\mathbb{Z}_p$ is compact

5) Note $\mathbb{Z}_p^\times = \text{units} = \mathbb{Z}_p \setminus p\mathbb{Z}_p = \{x \in \mathbb{Z}_p \mid \text{ord}_p x = 0\}$ is closed in $\mathbb{Z}_p$, since

- $\text{red}_p : \mathbb{Z}_p \to \mathbb{F}_p$ cts if $\mathbb{F}_p$ given discrete top,
- $\mathbb{Z}_p^\times = \text{red}_p^{-1}\{\mathbb{F}_p \setminus \{0\}\}$, ← closed subset!

6) Put eg sup-metric on $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p^\times$, ⇒ product top, ⇒ also cpct.

7) Define Maps $\psi_0 : \mathbb{Z}_p^\times \times \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{P}^2(\mathbb{Q}_p)$

$$x, y, z \longmapsto (x : y : z)$$

$$\psi_1 : \mathbb{Z}_p \times \mathbb{Z}_p^\times \times \mathbb{Z}_p \to \mathbb{P}^2(\mathbb{Q}_p)$$

$$(x, y, z) \longmapsto (x, y, z)$$

ψ_2 similar

8) Check that $\mathrm{Im}(\psi_0) \cup \mathrm{Im}(\psi_1) \cup \mathrm{Im}(\psi_2) = \mathbb{P}^2(\mathbb{Q}_p)$.

9) Let $S_i = \sum_{j=1}^{i} R_j$ (to simplify notation).

Then as many S_i must lie in image of at least one ψ_i.
(choose $\tilde{S}_i$ s.t. $\psi_0(\tilde{S}_i) = S_i$).
Say ψ_0, to ease notation. Then since $\mathbb{Z}_p^\times \to \mathbb{Z}_p \to \mathbb{Z}_p$ cpt,
we find a convergent subsequence of the $\tilde{S}_i$!

10) Write $\tilde{S}$ for its limit, set $R = \psi_0(S)$.

Claim (A) $R \in E'(\mathbb{Q}_p)$ and (B) $m R = Q$.
Gives $\mathbb{P}^2(\mathbb{Q}_p)$ quotient top from $\mathbb{Z}_p$, to simplify (check analogy)
(A): $E(\mathbb{Q}_p)$ is cut out by vanishing of some polys which are
p-adically cts, so $E(\mathbb{Q}_p)$ is closed in $\mathbb{P}^2(\mathbb{Q}_p)$,
$\mathbb{P}^1(\mathbb{Q}_p)$
so $R \in E(\mathbb{Q}_p)$;

The composite $E(\mathbb{Q}_p) \xrightarrow{\text{red}} \tilde{E}(\mathbb{F}_p)$ is moreover cts (check),
discrete top
so $E'(\mathbb{Q}_p)$ is closed, so $R \in E'(\mathbb{Q}_p)$. ✓

B) Similarly, can check $E''(\mathbb{Q}_p)$ closed in $E(\mathbb{Q}_p)$.
Reorder R_i s.t. whole seq. converges.
Then set $T_i = Q - m R_i$, so
T_i in $E'(\mathbb{Q}_p)$ $\forall i$,

and $(T_i)_i$ converges (to $T = Q - mR$, since '-' & 'm' cts).

Claim: $T \in \bigcap_i E'(\mathbb{Q}_p)$ $(= \{O\})$

Pf: $E''(\mathbb{Q}_p)$ closed in cpt, so cpt.
This implies that $\forall i$, $T \in E'(\mathbb{Q}_p)$.

□

Torsion points / $\mathbb{Q}$

- finiteness
- algorithm?
- efficiency ...

~~$E/\mathbb{Q}$ elliptic~~

Def: $E/\mathbb{Q}$ elliptic, $E: y^2 = x^3 + ax + b$, p "good prime for E"

(i.e. $a, b \in \mathbb{Z}$ have no pth divisors & $p \nmid \Delta$)

Write $E(\mathbb{Q})_{p'\text{-tors}} = \{ x \in E(\mathbb{Q}) \mid \exists m \in \mathbb{Z}_{\geq 1} \text{ s.t. } p \nmid m \text{ and } mx = 0 \}$

Ex:

Then $E(\mathbb{Q})_{p'\text{-tors}} \xrightarrow{\text{red}} \tilde{E}(\mathbb{F}_p)$ is injective.

[Ex: $E(\mathbb{Q})_{p'\text{-tors}}$ is a subgp of $E(\mathbb{Q})_{\text{tors}}$].

Pf: Let $Q \in E(\mathbb{Q})$ s.t. $\cdot\ mQ = 0$ some $p \nmid m$
$\cdot\ \text{red}(Q) = 0$.

Let $\varphi: E(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}_p)$. Then

$\text{red}(\varphi(Q)) = 0$, so $\varphi(Q) \in E'(\mathbb{Q}_p)$.

Also, $m\varphi(Q) = \varphi(mQ) = \varphi(0) = 0$, so $\varphi(Q) = 0$

by prev. thm, so $Q = 0$. □

Cor: $E(\mathbb{Q})_{\text{tors}}$ is finite.

Pf: Let p_1, p_2 two distinct good primes. Then

$E(\mathbb{Q})_{p_1'\text{-tors}} \times E(\mathbb{Q})_{p_2'\text{-tors}} \longrightarrow E(\mathbb{Q})_{\text{tors}}$ is surjective,

& $\bar{E}^1(\mathbb{F}_{p_1})$ & $\bar{E}^2(\mathbb{F}_{p_2})$ are finite. □

In fact, thm gives explicit bound on $E(\mathbb{Q})_{tors}$ in terms of Δ and denominators of a & b (using bounds on $\#E(\mathbb{F}_p)$).
Also algorithm, but horrible in practice.
Can we do better? Yes:

Thm: $E/\mathbb{Q}$ elliptic, p good. Then

$$E(\mathbb{Q})_{tors} \longrightarrow \bar{E}(\mathbb{F}_p) \text{ is injective.}$$

Pf: omitted, messy, not really hard. (□)

Thm: If $Q = (x:y:1) \in E(\mathbb{Q})_{tors}$, then

$x \in \mathbb{Z}$ & $y \in \mathbb{Z}$ & either $(y=0$ or $y^2 \mid \Delta)$

Pf: omitted, messy, long, not hard. (□)

Neither of these two generalize well to # field.

Also:

Thm (Mazur, '77): $E/\mathbb{Q}$ elliptic. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of:

- $\mathbb{Z}/m\mathbb{Z}$ $\quad m \in \{1, \dots, 10\} \cup \{12\}$
- $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\quad \forall n \in \{2, 4, 6, 8\}$,

& all these occur.

Pf. Omitted. Ridiculously hard, way beyond this course. (□)