Elliptic curves over local fields

Conventions (*) discrete valuation, $\mathcal{O}_K$ integers, π uniformizer. $k = \frac{\mathcal{O}_K}{\pi}$

K local field. v

$p = \mathrm{char}(k)$ K, k perfect (no function fields)

(*) local means complete wrt v discrete, and locally compact.

Minimal Weierstrass Equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

$(x,y) \longmapsto (u^{-2}x, u^{-3}y)$ changes $a_i \longmapsto u^i a_i$

so we can clear denominators and take $a_i \in \mathcal{O}_K$

$v(\Delta) \geq 0$

Def. A minimal Weierstrass equation is one where $v(\Delta)$ is minimal

Prop. They exist

pf. $v(\Delta)$: $\{\text{elliptic curves}/R\} \longrightarrow \mathbb{N}$, image is discrete.

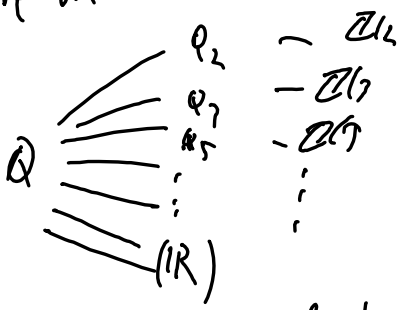
Unique up to change of coordinates

$$x = u^2 x' + r$$
$$y = u^3 y' + u^2 s x' + t$$

$u \in \mathcal{O}_K^\times$, $r, s, t \in \mathcal{O}_K$

Reduction mod $\mathfrak{p}$

Why are we here?



Understood by passing to local, where to reduce.

E: Elliptic curve minimal Weierstrass equation.

Then $\bar{f} \in k[x,y]$ defines $\bar{E}$ in $\mathbb{P}^2(k)$

$$\mathbb{P}^2(K) \longrightarrow \mathbb{P}^2(k)$$

$$[x:y:z] = [a:b:c] \longmapsto [\bar{a}:\bar{b}:\bar{c}]$$

in $\mathcal{O}_K$, at least one in $\mathcal{O}_K^\times$

$$\mathbb{P}^n(K) \overset{?}{\dashrightarrow} \mathbb{P}^n(k)$$

no map $K \to k$

Bijection by clearing denom (valuative criterion)

$$\mathbb{P}^n(\mathcal{O}_K)$$

Anyways, $E(K) \longrightarrow \overline{E}(k)$, which is not surjective in general

$\uparrow$ $\uparrow$

$E_0(K) \longrightarrow \widetilde{E_{ns}}(k)$

Let $E_1(K)$ be the kernel, which yields

Prop. $0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \widetilde{E_{ns}}(k) \longrightarrow 0$ exact

ps. $E_1(K)$: subgroup; $E_0(K)$: def. of E_1; $\widetilde{E_{ns}}(k)$: kernel, at least one partial is non-zero

why is this a group hom?

- algorithm is rational functions. what if we divide by 0? char 2? well...
- reduce lines mod π. same clearing denominators (lines in $\mathbb{P}^2 \to \mathbb{P}^2$) and show the geometry works.

ok, so we have

$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \widetilde{E_{ns}}(k) \longrightarrow 0$

(1) (2) yay!

$E(K)$

(1) Prop, $\widehat{E}(\mathfrak{m}) \xrightarrow{\sim} E_1(K)$

$$z \longmapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$$

where $\widehat{E}$ is the formal group of expansion about $\mathcal{O}$.

pf. Recall we did the change of variables

$$x = \frac{z}{w}, \quad y = \frac{-1}{w}$$

Turns Weierstrass $f(x,y)=0$ into $w = g(z,w)$ and iteration,

- $z/w(z)$ so w converges on $\mathfrak{m}$.
- This is injective as only $0 \longmapsto \infty$
- Group hom by def of formal group $\widehat{E}$
- onto. Let $(x,y) \in E_1(K)$.

$$\overline{(x,y)} = \mathcal{O}$$

so $[\bar{x}:\bar{y}:1] = [0:1:0]$

$[x:y:1] = [\pi^e x : \pi^e y : \pi^e]$, $e = -v(y)$.

$e \geq 1$ as $\pi^e \equiv 0 \bmod \pi$ to get $[0:1:0]$

similarly, $v(\pi^e x) \geq 1$ so $e + v(x) \geq 1$

$\| $

$v(x) - v(y)$

$= v(x/y)$

that is, $\frac{x}{y} \in m$

so inverse is $(x,y) \longmapsto -\frac{x}{y}$

(2) $E/E_0(k)$ is finite

pf. - Give k its v-adic topology.

k^{n+1} product

$\mathbb{P}^n(k)$ quotient

- $\mathbb{P}^n(k)$ is compact. Indeed, k is locally compact and hence a closed ball is compact, whence the sphere is $\mathbb{P}^2(k)$ closed in compact

- $E(k) \subseteq \mathbb{P}^2(k)$

- $E(k) \longrightarrow \bar{E}(k)$ continuous

- $E_0(k)$ is the preimage of the nonsingular points, and the singular locus is closed. So $E_0(k)$ is an open subgroup of a compact group. Thus, finite index.

Torsion

Recall $0 \to E_1(k) \to E_0(k) \to \overline{E_{ns}}(k) \to 0$

Apply $(-)[m] = \mathrm{Hom}(\mathbb{Z}/m, -)$

$$0 \to E_1(k)[m] \to E_0(k)[m] \to \overline{E_{ns}}(k)[m]$$

If $(m,p)=1$ then $\hat{E}$ has no m torsion.

$$0 \to E_0(k)[m] \to \overline{E_{ns}}(k)[m]$$

Rmk. Let k be a global field, v a finite prime so that $\overline{E}(k_v)$ is nonsingular. Let $(m,v)=1$.

Then $E(k)[m] \hookrightarrow E(k_v)[m] \hookrightarrow \overline{E}(k_v)[m]$

only need to understand finite!

ex. $y^2+y = x^3-x+1$

$\Delta = -13 \cdot 47$

$\overline{E}$ nonsingular for $v=2$-adics

$\overline{E}(\mathbb{F}_2)$ trivial. Thus $E(\mathbb{Q})[m] = 0$ for m odd

$E(\mathbb{Q})[2] = 0$

so $E(\mathbb{Q})$ torsion free

This also yields bounds on denominators

Let $P \in E(K)$ order m

- m not a power of p, $x(P), y(P) \in \mathcal{O}_K$

- $m = p^n$. $v(x(P)) \leq -2r$

$$v(y(P)) \leq -3r$$

$$r = \left\lfloor \frac{v(p)}{p^n - p^{n-1}} \right\rfloor$$

Corollary. Let E be defined over $\mathbb{Z}$

$P \in E(\mathbb{Q})$ order $\neq 3$. Then $P \in E(\mathbb{Z})$!

Inertia

$(K, k$ perfect$)$

$$1 \longrightarrow G(\bar{K}/K^{ur}) \longrightarrow G(\bar{K}/K) \longrightarrow G(K^{ur}/K) \longrightarrow 1$$

$$\| \qquad\qquad\qquad\qquad \| \qquad\qquad\qquad\qquad \| \; G(\bar{k}/k) = \vec{e}$$

I_v inertia

Def. Let A be a $G(\bar{K}/K)$ set. It's unramified if I_v acts trivially on it.

If $\bar{k}/L/K$ then L is a $G(\bar{K}/K)$ set via

$G(\bar{K}/K) \longrightarrow G(L/K)$

for I_v to act trivially means I_v is in the kernel of this map, so

$$\begin{array}{ccc} G(\bar{K}/K) & \longrightarrow & G(L/K) \\ \downarrow & \nearrow & \\ G(K^{ur}/K) & & \end{array}$$

i.e. L/K is unramified!

Prop. $\bar{E}/k$ nonsingular

$(m, p) = 1$

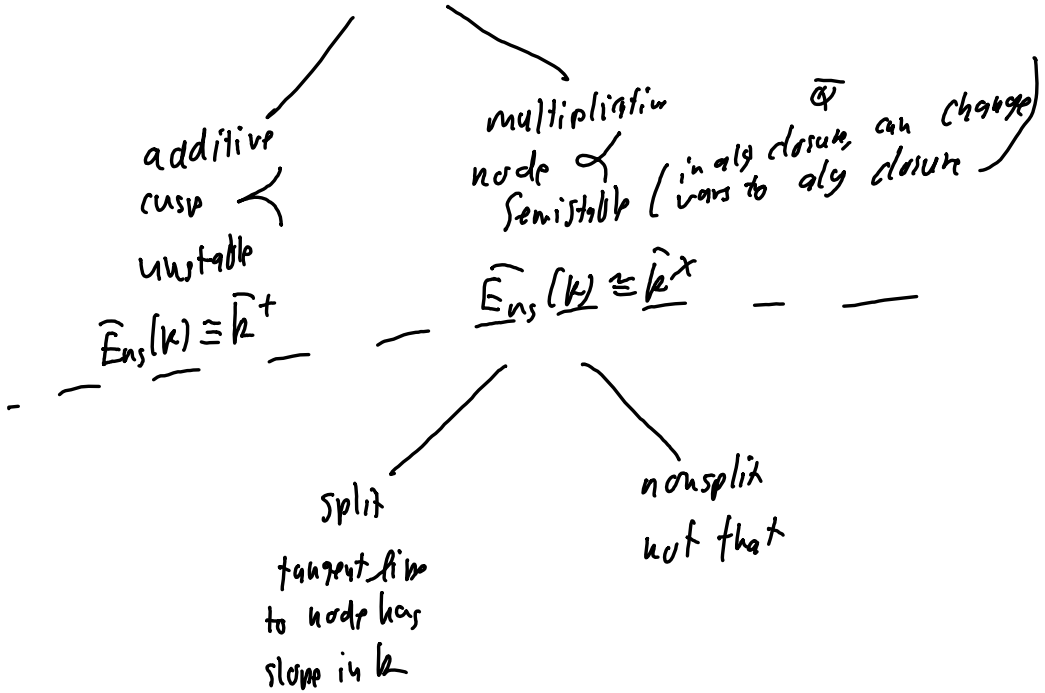
Then $E[m]$ is unramified

pf. $E[m] \hookrightarrow \bar{E}(k)[m] \hookrightarrow \bar{E}(k)$, unramified

Good and Bad reduction

Def. good reduction is $\tilde{E}/k$ nonsingular

bad reduction - $\tilde{E}/k$ singular



Prop. The conditions above the dashed line are determined by v and the minimal Weierstrass equation

pf. $v(\Delta) = 0$ good

$v(\Delta) \neq 0$ bad

$v(c_4) = 0$ multiplicative

$v(c_4) > 0$ additive

Corollary. Let L/K unramified

The reduction type over K is the same as over L

Pf. V is unchanged when unramified (roughly)

Néron - Ogg - Shafarevich

Recall. The Tate module $T_\ell(E)$ is the inverse limit.

$$\cdots \to E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n] \to \cdots$$

Remark. Each $E[\ell^n]$ is a $G(\bar{K}/K)$ module, so $T_\ell(E)$ is.

Furthermore, $T_\ell(E)$ is unramified iff each $E[\ell^n]$ is.

Thm. TFAE

a) E has good reduction

b) $E[m]$ is unramified for all $(m,p)=1$

c) $T_\ell(E)$ is unramified for all $\ell \neq p$

d) $E[m]$ is unramified for infinitely many $(m,p)=1$.

Pf. a) $\Rightarrow$ b) before

b) $\Rightarrow$ c) $\Rightarrow$ d) clear

d) $\Rightarrow$ a)

$$
\begin{array}{ccccccc}
 & & 0 & & & & \\
 & & \downarrow & & & & \\
0 & \longrightarrow & E_1(k^{ur}) & \longrightarrow & E_0(k^{ur}) & \longrightarrow & \widetilde{E_{ns}}(\bar{k}) \\
 & & & & \downarrow & & \uparrow \text{ no surj as not complete} \\
 & & & & E(k^{ur}) & & \\
 & & & & \downarrow & & \\
 & & & & E/E_0(k^{ur}) & & \\
 & & & & \downarrow & & \\
 & & & & 0 & &
\end{array}
$$

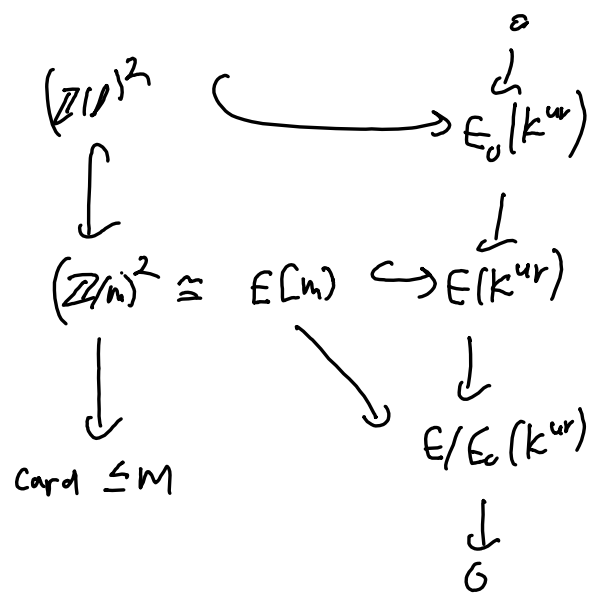
Let m s.t.

- $(m,p)=1$
- $m > |E/E_0(k^{ur})|$
- $E[m]$ unramified

As $(m,p)=1$, $E[m] \cong (\mathbb{Z}/m)^2$

$|E/E_0(k^{ur})| < m$

$E[m] \subseteq k^{ur}$ as unramified



via $0 \to E_1(k^{ur}) \to E_0(k^{ur}) \to \tilde{E}_{ns}(\bar{k})$

we get $E_0(k^{ur}) \hookrightarrow \tilde{E}_{ns}(\bar{k})$

$\cup$

$(\mathbb{Z}/\ell)^2$

So $\tilde{E}_{ns}(\bar{k})$ has $(\mathbb{Z}/\ell)^2$ in it

But $\tilde{E}_{ns}(\bar{k}) = \begin{cases} \bar{k}^\times & \text{if bad} \\ \bar{k}^+ \end{cases}$

And neither has that much ℓ torsion.

Corollary, E_i/K $\quad E_1 \xrightarrow{\varphi} E_2$ isogeny over K.

Then E_1 has good reduction iff E_2 does

pf, Let m s.t. $(m,p)=1$
$(m, \deg \varphi)=1$

only many such m

As $(m,p)=1$, $E_i[m] \cong (\mathbb{Z}/m)^2$

$|\ker(\varphi)| = \deg(\varphi)$ (K perfect)

So as $(m, \deg \varphi)=1$, $E_1[m] \cap \ker(\varphi)$ is trivial

Hence, $E_1[m] \longrightarrow E_2[m]$ injective, hence iso.

So follows by Neron-Ogg-Shafarevich,