# Elliptic Curves over Local Fields (continued)

$K, R, \mathfrak{m}, \pi, k = R/\mathfrak{m}$.

$E'/K \rightsquigarrow$ minimal model $E/K$ with $\begin{cases} a_i \in R, \\ \text{minimal } v(\Delta). \end{cases}$

reduction mod $\mathfrak{m}$ $\downarrow$

$\tilde{E}/k$

$\begin{cases} \tilde{E}_{ns}(k) & \text{non-sing. points on } \tilde{E} \\ E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\} \\ E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{O}\} \end{cases}$

**Thm.** • There is an exact sequence:

$$0 \to E_1(K) \to E_0(K) \xrightarrow{\sim} \tilde{E}_{ns}(k) \to 0$$

$$\| ?$$

$$\hat{E}(\mathfrak{m})$$

• $E_1(K) \cong \hat{E}(\mathfrak{m})$.

$\hat{E}(\mathfrak{m})$ ← the group associated to the formal gp of $E$

↳ Use this to study points of finite order in $E(K)$.

# Points of Finite Order

**Prop** Let $E/k$ be an ell. curve and $m \geq 1$ an integer rel. prime to $p = \mathrm{char}(k)$. Then:

(a) The subgp $E_1(k)$ has no non-trivial points of order $m$.

(b) If the reduced curve $\tilde{E}/k$ is non-singular then the red'n map

$$E(k)[m] \hookrightarrow \tilde{E}(k)$$

is injective.

# Points of Finite Order

**Prop** Let $E/k$ be an ell. curve and $m \geq 1$ an integer rel. prime to $p = \mathrm{char}(k)$. Then:

(a) The subgp $E_1(k)$ has no non-trivial points of order $m$.

(b) If the reduced curve $\tilde{E}/k$ is non-singular then the red'n map

$$E(k)[m] \longrightarrow \tilde{E}(k)$$

is injective.

**Proof.**

(a) We know an exact sequence:

$$0 \to E_1(k) \to E_0(k) \to \underset{ns}{\tilde{E}}(k) \to 0$$

$$\| \wr$$

$$\hat{E}(\mathfrak{m})$$

By PROP (IV.3.2(b)) $\hat{E}(\mathfrak{m})$ has no points of order $m$ when $\gcd(m, p) = 1$. ✓

(b) If $\tilde{E}$ is non-sing. then

$$0 \to E_1(k) \to E(k) \xrightarrow{\sim} \tilde{E}(k) \to 0$$

and $E_1(k)[m] = \ker(\sim)[m]$ is trivial by (a)

Thus $E(k)[m] \hookrightarrow \tilde{E}(k)$. ∎

## EXAMPLE

Let $E/\mathbb{Q} : y^2 = x^3 + 3$

$$\Delta_E = -2^4 \cdot 3^5 \to \text{non-sing. at } p > 3.$$

$p = 5$ $\quad \#\tilde{E}(\mathbb{F}_5) = 6$

$p = 7$ $\quad \#\tilde{E}(\mathbb{F}_7) = 13$

- If $q \neq 5, 7$, then $\#E(\mathbb{Q})[q] \mid \gcd(6, 13) = 1$.
- If $q = 5$, $\#E(\mathbb{Q})[5] \mid \gcd(13, 25) = 1$.
- If $q = 7$, $\#E(\mathbb{Q})[7] \mid \gcd(6, 49) = 1$.

$\Rightarrow E(\mathbb{Q})_{\text{tors}}$ is trivial.

## EXAMPLE $E: y^2 + y = x^3 - x$

prime bad reduction

| $p$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\#\tilde{E}(\mathbb{F}_p)$ | 5 | 5 | 5 | 10 | 11 | 10 | 20 | 20 | 25 | 30 | 25 | ... |

Indeed, we will see $E(\mathbb{Q})$