**Elliptic Curves over Local Fields**

1. **The Action of Inertia**
   - \( K \): local field, complete wrt \( \nu \).
   - \( \overline{K} \): algebraic closure.
   - \( \overline{K}^{\nu} \): maximal unramified extn of \( K \) in \( \overline{K} \).
   - \( G_k = \text{Gal}(\overline{K}/K) = \text{D}(M_{\overline{k}}/M_k) \)
   - \( I_{\nu} = \text{Gal}(\overline{K}/K^{\nu}) = \text{I}(M_{\overline{k}}/M_k) \)

   \[
   1 \rightarrow \text{Gal}(\overline{K}/K^{\nu}) \rightarrow \text{Gal}(\overline{K}/K) \rightarrow \text{Gal}(K^{\nu}/K) \rightarrow 1
   \]

   \[
   0 \rightarrow I_{\nu} \rightarrow G_k \rightarrow \text{Gal}(\overline{K}/K) \rightarrow 0
   \]

   **Def.** \( \Sigma \) is unramified at \( \nu \) if \( I_{\nu} \) acts trivially on \( \Sigma' \).
Prop. Let $E/k$ be an ell. curve, s.t. $\tilde{E}/k$ is non-singular. (Good Reduction!)

(a) Let $m \geq 1$ s.t. $\gcd(m, \text{char}(k)) = 1$.
Then $E[m]$ is unramified at $v$.
(b) Let $l \neq \text{char}(k)$, then $T_l(E)$ is unramified at $v$.

Q: Converse? The Criterion of Néron-Ogg-Shafarevich.

Thm. $E/K$ ell. curve. TFAE:

(a) $E$ has good reduction over $K$.
(b) $E[m]$ is unramified at $v$ for all integers $m \geq 1$ rel. prime to $\text{char}(k)$.
(c) The Tate module $T_l(E)$ is unramif. at $v$ for some (all) primes $l$ rel. prime to $p$.
(d) $E[m]$ is unramif. at $v$ for only many integers $m \geq 1$ rel. pr. to $p$. 
Good And Bad Reduction

\[ E/k \rightarrow \tilde{E}/k \]

**Def.**

(a) E has good (or stable) reduction over K if \( \tilde{E} \) is non-singular.

(b) E has multiplicative (or semi-stable) reduction over K if \( \tilde{E} \) has a node \( \times \) two "tangent" lines at sing.

(b.1) If the slopes are in \( k \) then, it is split multi.

(b.2) If the slopes are not in \( k \), it is non-split multi.

(c) E has additive reduc (or unstable) if \( \tilde{E} \) has a cusp\( < \) only one "tangent" line
Let $E/K$ be given by a minl Weier. eqn $y^2 + ax + y + \ldots = x^2 + \ldots$.
Let $\Delta_E$ be the disc., and $C_4, c$ be as usual.

(a) $E$ has good red'n $\iff \nu(\Delta) = 0$ (i.e., $\Delta \in \mathbb{R}^*$).
In this case $\tilde{E}/\tilde{k}$ is a ell. curve.

(b) $E$ has mult. red'n $\iff \nu(\Delta) > 0$, $\nu(C_4) = 0$.
In this case $\tilde{E}_{ns}(\tilde{k}) \cong \tilde{k}^*$.

(c) $E$ has odd red'n $\iff \nu(\Delta) > 0$, $\nu(C_4) > 0$.
In this case $\tilde{E}_{ns}(\tilde{k}) \cong (\tilde{k}, +)$.
Examples

(1) \( E_1 : y^2 = x^3 + 35x + s \), \( \Delta = -2^4 \cdot 5^2 \cdot 7 \cdot 97 \)
\[ C_4 = -2^4 \cdot 3 \cdot 5 \cdot 7. \]

- has good red\'n at \( p=7 \) \( (\tilde{E}_1 : y^2 = x^3 + 5/\mathbb{F}_7) \)
- At \( p=5 \) there is bad red\'n, \( \Delta = C_4 \equiv 0 \) mod 5 \( \Rightarrow \) additive red\'n.
\[ \tilde{E} : y^2 = x^3 / \mathbb{F}_5 \quad (y - 0 \cdot x)^2 - x^3 = 0 \]
\( y=0 \) is the "tangent" line at \( (0,0) \).

\( f(x,y) = 0 \), \( P = (x_0, y_0) \) singularity \( \Rightarrow \frac{\partial f}{\partial x} \bigg|_P = \frac{\partial f}{\partial y} \bigg|_P = 0 \)

\( \text{Taylor} \)
\[ f(x,y) - f(x_0, y_0) = \underbrace{(y - y_0 - \alpha(x-x_0)) \cdot (y - y_0 - \beta(x-x_0))}_{\text{"tangent" lines at sing.}} - (x-x_0)^3 \]
Example

\[ E_2 : \quad y^2 = x^3 - x^2 + 3s \quad , \quad \Delta = -2^4 \cdot 5 \cdot 7 \cdot 941 \]
\[ C_4 = 16. \]

\[ \begin{align*}
3 \Rightarrow & \quad y^2 + x^2 - 3s - x^3 = 0 \\
& \quad y^2 + x^2 - x^3 \equiv 0 \mod 5 \, \, \, \, \text{(bad)} \\
& \quad (y - 2x)(y + 2x) - x^3 \equiv 0 \quad \rightarrow \quad \text{split mult. red\'n at 5.} \\
\end{align*} \]

\[ \begin{align*}
7 \Rightarrow & \quad y^2 + x^2 - x^3 \equiv 0 \mod 7 \, \, \, \, \text{(bad)} \\
& \quad \text{DOES NOT FACTOR} \\
& \quad -1 \notin (\mathbb{F}_7^\times)^2 \\
& \quad \rightarrow \quad \text{non-split mult. red\'n at 7.} \\
\end{align*} \]
**Example**

\( E/\mathbb{Q} : y^2 = x^3 + 7^3 \quad \Delta = -2^4 \cdot 3^3 \cdot 7^6 \)

\( \Rightarrow p = 7 \) is bad additive.

Over \( E/\mathbb{Q}(\sqrt[3]{7}) : \quad E : y^2 = x^3 + (\sqrt[3]{7})^6 \quad \text{not minimal at } 7 \)

change vars: \( y' = (\sqrt[3]{7}) y, \quad x' = (\sqrt[3]{7})^2 x \)

\( \Rightarrow E' : y'^2 = x'^3 + 1 \quad \text{which has good red'n at the prime } (\sqrt[3]{7}) \text{ of } \mathbb{Q}(\sqrt[3]{7}) \)

\( \rightarrow \text{additive red'n is "unstable"} \)
Def. Let $E/K$ be an ell. curve. $E$ has potential good red'n over $K$ if there is a finite ext'n $K'/K$ s.t. $E$ has good red'n over $K'$.

ex. $E/\mathbb{Q}_9 : y^2 = x^3 + 7^3$ has pot. good red'n (bad add.) and good red'n at $(17)$ of $\mathbb{Q}_9(17)$.

Prop. (Semi-stable red'n thm.) $E/K$ be an ell. curve.

a) Let $K'/K$ be an unramified ext'n. Then the red'n type of $E/K$ (good, mult., add) is the same as the red'n type of $E/K'$.

b) Let $K'/K$ be any finite ext'n. If $E$ has either good or mult. red'n over $K$ then it has the same type of red'n over $K'$ (non-split mult. may become split mult.).

c) There exists a finite ext'n $K'/K$ s.t. $E/K'$ has either good or split mult. reduction.
Proof of (c) \( E/K \rightarrow E/K' \) with good or split mult. redn.

\( \text{Chor}(K) \neq 2 \)

- Extend \( K \) by a finite ext'n s.t. \( E \) can be given by a model

\[
E: y^2 = x(x-1)(x-\lambda) \quad \text{(Legendre Normal Form)}
\]

\[
C_4 = 16 \cdot (\lambda^2 - \lambda + 1), \quad \Delta = 16 \cdot \lambda^2 (\lambda - 1)^2
\]

**CASE 1.** \( \lambda \in \mathbb{R}, \lambda \neq 0, 1 \mod M \) \( \Rightarrow \Delta \in \mathbb{R}^\times \) so good reduction \( \bigcirc \)

**CASE 2.** \( \lambda \in \mathbb{R}, \lambda \equiv 0 \pm 1 \mod M \) \( \Rightarrow \Delta \in M \), \( C_4 \equiv 16 \mod M \)

So reduc. is multipllicative, after possibly a good ext'n, reduc. is split multi.

**CASE 3.** \( \lambda \notin \mathbb{R} \) Choose \( r \geq 1 \) s.t. \( r \lambda \in \mathbb{R}^\times \). The change \( \text{var} \left\{ \begin{array}{l}
\lambda = \pi^{-r} x' \\
y = \pi^{\frac{r}{2}} y'
\end{array} \right. \)

change \( K' = K(\pi^r) \), gives

\[
E/K': (y')^2 = x'(x'-\pi^r)(x'-\pi^s) \Rightarrow \Delta' \in M, \quad C_4 \in \mathbb{R}^\times
\]

so split mult. redn. \( \blacksquare \)
The Group $E/E_0$

$E_0(k) = \{ P \in E(k) : \exists \tilde{P} \in \tilde{E}_{ns}(k) \}$ \subseteq E(k)

$E_1(k) = \text{kernel of } (E_0(k) \rightarrow \tilde{E}_{ns}(k))$

$0 \rightarrow E_1(k) \rightarrow E_0(k) \rightarrow \tilde{E}_{ns}(k) \rightarrow 0$

$\tilde{E}(M)$ \quad \text{GOOD!} \quad 0 \rightarrow E_1(k) \rightarrow E(k) \rightarrow \tilde{E}(k) \rightarrow 0$

\textbf{Theorem (Kodaira, Néron)} $E/k$ is an elliptic curve.

- If $E/k$ has split multiplicative reduction, then $E(k)/E_0(k)$ is a cyclic group of order $\nu(\Delta) = -\nu(j)$.
- In all other cases $E(k)/E_0(k)$ is a finite group of order at most 4.

\textbf{Key:} The existence of a Néron model!!
Prop: $K/\mathbb{Q}_p$ finite, $E/K$.

Then, $E(K)$ contains a subgroup of finite index isomorphic to $(\mathbb{R},+)$. 

Proof:

$E(K)/E_0(K)$ is finite (by $[E_0(K):	ext{ker}]$) AND $E_0(K)/E_1(K) \cong \hat{E}(k)$ finite.

$E_1(K) \subseteq E_0(K) \subseteq E(K)$

Suffices to show $(\mathbb{R},+) \subseteq E_1(K)$ of finite index.

- Filtration: $\hat{E}(m) \supseteq \hat{E}(m^2) \supseteq \hat{E}(m^3) \supseteq \ldots$

  and $\hat{E}(m^i)/\hat{E}(m^{i+1}) \cong \mathbb{M}/m^{i+1}$ (finite yet!)

- And for large enough $r$: $\hat{E}(m^r) \xrightarrow{\text{log}} \mathbb{M}^r = \pi^r R \cong (\mathbb{R},+)$ as ab. gps.