p. 1. (24)

Start with a <u>local</u> <u>field</u> K.

Think: $\mathbb{Q}_p$ (define what $\mathbb{Z}_p$, $\mathbb{Q}_p$ are)

Let R be its <u>ring of integers</u>

$\mathfrak{m}$ its maximal ideal

k = residue field ($\mathbb{F}_p$).

v the associated valuation.

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

or $y^2 = x^3 + a_4 x + a_6$ (char $k \neq 2, 3$).

A Weierstrass equation is <u>minimal</u> if $v(\Delta)$ is minimized.

<u>Example.</u> $y^2 = x^3 + 7^6$.

This is isomorphic to $y^2 = x^3 + 1$ over $\mathbb{Q}$ or $\mathbb{Q}_7$.

The latter can be reduced mod 7.

To do a change of variable

$$u^6 y^2 = u^6 x^3 + u^6 a_4 x + u^6 a_6$$

$$(u^3 y)^2 = (u^2 x)^3 + u^4 a_4 (u^2 x) + u^6 a_6.$$

So replace a_4 with $u^4 a_4$ and $u^6 a_6$.

In particular, if $v(a_4) \geq 4$ and $v(a_6) \geq 6$, can cut the problem down to size.

So we get a <u>reduction</u> <u>map</u> mod $\mathfrak{m}$ (or mod π where $\mathfrak{m} = (\pi)$).

Over $\mathbb{Q}$, this just means we choose coeffs. over $\mathbb{Z}$ and try to do it as efficiently as possible.

<u>Proposition</u>. Define

$$\underbrace{E_0(K)}_{K \text{ local field}} = \{ P \in E(K) : \underbrace{\tilde{P}}_{\text{reduction mod } \pi} \in \underbrace{\tilde{E}_{ns}(k)}_{k \text{ residue field}} \}.$$

$\tilde{E}_{ns}(k)$: nonsingular points of $\tilde{E}$ as a curve over k.

If E has <u>good reduction</u> at π, then $\tilde{E}_{ns}(k) = \tilde{E}(k)$.

$$E_1(K) = \{ P \in E(K) : \tilde{P} = \tilde{O} \}.$$

(<u>kernel of reduction</u>)

There is an exact sequence

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \xrightarrow[\text{mod } \pi]{\text{reduction}} \tilde{E}_{ns}(k) \longrightarrow 0.$$

<u>Proof</u>. For simplicity assume E has good reduction, so $\tilde{E}_{ns}(k) = \tilde{E}(k)$. Then $E_0(K) = E(K)$, (then)

Injectivity is obvious.

Exactness in the middle is also obvious.

But why the hell is it surjective?

Let $f(x,y) = y^2 - (x^3 + a_4 x + a_6) = 0$ be a min Weierstrass equation.

Given any $\tilde{P} = (\alpha, \beta) \in \tilde{E}(k)$ not the identity.
(∞ maps to $\tilde{\infty}$, so surjectivity is automatic there.)

Then $\dfrac{\partial \tilde{f}}{\partial x}(\tilde{P}) \neq 0$ or $\dfrac{\partial \tilde{f}}{\partial y}(\tilde{P}) \neq 0$.

Assume (more or less WLOG) $\dfrac{\partial \tilde{f}}{\partial x}(\tilde{P}) \neq 0$.

We can lift β (arbitrarily) to $y_0 \in R$.
Look at $f(x, y_0) = 0$. (equ. in the one variable x over R)

Reduce it modulo π.
Then α is a root, and it is a simple root since

$$\frac{\partial \tilde{f}}{\partial x}(\alpha, \tilde{y}_0) \neq 0.$$

Invoke Hensel's Lemma. There is $x_0 \in R$ with $\tilde{x}_0 = \alpha$ and $f(x_0, y_0) = 0$. That's the solution we're looking for.

~~Consequences.~~

Proposition. Let $m \geq 1$ be coprime to $\mathrm{char}(k)$.

(1) $E_1(K)$ has no non-trivial points of order m.

(won't be proved)

(2) If $\tilde{E}/k$ is nonsingular, then the map

$$E(K)[m] \longrightarrow \tilde{E}(k) \text{ is } \underline{\text{injective}}.$$

Sato-Tate Conjecture.

Given an EC $E/\mathbb{Q}$ without CM.

Recall, if E has good reduction at p,

$\#E(\mathbb{F}_p)$ is between $p+1-2\sqrt{p}$, $p+1+2\sqrt{p}$.

Write $p+1-\#E(\mathbb{F}_p) = 2\sqrt{p}\cos\theta_p$

with $\theta_p \in [0,\pi]$.

Theorem. For any E, α, β,

$$\lim_{N\to\infty} \frac{\#\{p \leq N : \alpha \leq \theta_p \leq \beta\}}{\#\{p \leq N\}} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta \, d\theta.$$

Why $\sin^2\theta \, d\theta$?

$$SU(2) = \left\{ \begin{bmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{bmatrix} : \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

Conj. classes determined by eigenvalues $e^{\pm i\theta}$.

Get the pushforward of Haar measure.