## § Good reduction



<u>Thm</u> (Néron-Ogg-Shafarevich) $E/\mathbb{Q}_p$ ell. curve, $\ell \neq p$.

$E/\mathbb{Q}_p$ has good red. $\iff$ $E[\ell^n]$ unramified $\forall n \geq 1$ $\iff$ $T_\ell E$ unramified

$\iff$ $V_\ell E$ unramified

In this case, Frob $\circlearrowleft$ $T_\ell E$ as a matrix with char. poly

$$T^2 - aT + p \qquad\qquad a = p + 1 - \#\tilde{E}(\mathbb{F}_p)$$

and so does $\underset{\text{invert eigenvalues}}{\text{Frob}^{-1}}$ on $\underset{\text{invert again.}}{(V_\ell E)^*}$

$$\boxed{F(T) = \det(1 - \mathrm{Frob}^{-1} \cdot T \mid (V_\ell E^*)^I) = 1 - aT + pT^2}$$

<u>Ex</u> $E = E_1/\mathbb{Q}_5$ : $y^2 = x^3 - 1$ good red.

$\tilde{E}_1/\mathbb{F}_5$ : $y^2 = x^3 - 1$ has 6 pts $\{O, (0, \pm 2), (1, 0), (3, \pm 2)\}$

$$T^2 - aT + q = T^2 + 5 \quad \text{and} \quad F(T) = \underline{1 + 5T^2}$$

Here $I \circlearrowleft T_2 E$ as $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and Frob as $\begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}$ in some basis.

So $\mathbb{Q}_5(E[2^n])/\mathbb{Q}_5$ unramified of degree

$$f = \text{order of } \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{Z}/2^n\mathbb{Z}) = \overbrace{2, 4, 4}^{\text{last page}}, 8, 16, \ldots$$

$$\text{for } n = 1, 2, 3, 4, 5, \ldots$$

lecture 8

---

## § Multiplicative reduction

For $E/\mathbb{C}$

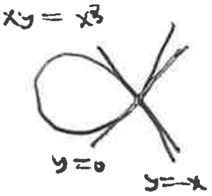
$$E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z} + \tau\mathbb{Z} \xrightarrow[\exp(2\pi i\,\cdot)]{\sim} \mathbb{C}^*/q^{\mathbb{Z}} \qquad q = e^{2\pi i \tau}$$

[$\cong$ given by transcendental fncs]

as complex Lie groups.

two tangent lines at the node defined $/\mathbb{F}_p$

$\iff \tilde{E}/\mathbb{F}_p \cong y^2 + xy = x^3$




**Thm** (Tate) If $E/\mathbb{Q}_p$ has split mult. red., then

- $\exists!\ q \in p\mathbb{Z}_p$ s.t.

$$E \cong y^2 + xy = x^3 + a_4(q) + a_6(q) \quad \leftarrow \text{Tate curve}$$

$$a_4(q) = -5 \sum_{n\geq 1} \frac{n^3 q^n}{1-q^n}$$

$$a_6(q) = \frac{1}{12}\left[a_4(q) + 7\sum_{n\geq 1} \frac{n^5 q^n}{1-q^n}\right]$$

$$\Delta(q) = q \prod_{n\geq 1} (1-q^n)^{24}$$

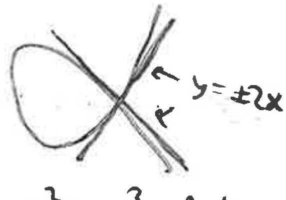
$$j(q) = \frac{1}{q} + 744 + 196884q + \dots$$

- $$E(\overline{\mathbb{Q}}_p) \xrightarrow[\text{some power series}]{\sim} \overline{K}^\times / q^{\mathbb{Z}}$$ as $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules, so

$$E(\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Q}_p^\times / q^{\mathbb{Z}}$$

**Cor** $E[\ell^n] \cong \langle \zeta_{\ell^n}, q^{1/\ell^n} \rangle$ as $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules.

**Ex** $E = E_2/\mathbb{Q}_5$ $\quad y^2 = (x-1)(x^2-5)$ split mult. red.,




$j = \frac{2^{14}}{5}$ $\quad \Delta = 2^{10}\cdot 5 \quad \Rightarrow \quad v(q) = v(\Delta) = -v(j) = 1$

So $q = 5\cdot\text{unit}$ $\quad [= -5 + 2\cdot 5^2 + 5^4 + 3\cdot 5^5 + O(5^6)]$

$$\mathbb{Q}_5(E[2^n]) = \mathbb{Q}_5(\underset{\text{unramified}}{\zeta_{2^n}}, \underset{\text{tamely ramified, ram. degree } 2^n}{\sqrt[2^n]{5\cdot\text{unit}}})$$

For a Tate curve,

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \circlearrowright T_\ell E \text{ as } \begin{pmatrix} \chi_\ell & * \\ 0 & 1 \end{pmatrix}$$

$\chi_\ell$ = $\ell$-adic cyclotomic character (unramified)

$$I \circlearrowright T_\ell E \text{ as } \begin{pmatrix} 1 & v_p(q)\cdot\tau_\ell \\ 0 & 1 \end{pmatrix}$$

where $\tau_\ell : \sigma \longmapsto \left(\frac{\sigma(\sqrt[\ell^n]{p})}{\sqrt[\ell^n]{p}}\right)_{n\geq 1} \in \mathbb{Z}_\ell(1)$ is called the $\ell$-adic tame character

$\ell^n$ root of 1

On $V_\ell(E)$: Frob. acts as $\begin{pmatrix} p & * \\ 0 & 1 \end{pmatrix}$, $I$ as $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$

$V_\ell(E)^*$: Frob acts as $\begin{pmatrix} p^{-1} & 0 \\ * & \boxed{1} \end{pmatrix}$, $I$ as $\begin{pmatrix} 1 & \boxed{0} \\ * & \boxed{1} \end{pmatrix}$

transpose inverse

This rep. is called $Sp_2$

inertia invariants of dim 1

and

$$\boxed{F(T) = \det(1-\mathrm{Frob}^{-1}T \mid (V_\ell E^*)^I) = 1-T}$$

## § Potentially multiplicative reduction

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

$v(j)<0 \iff E$ has potentially mult. red.

$\iff E$ split mult. $/F=\mathbb{Q}_p(\sqrt{-6b})$.

$\iff$ quad twist $E_{-6b}$ has split mult. red.

$F = \mathbb{Q}_p \iff$ split mult.

$F/\mathbb{Q}_p$ quad unr. $\iff$ non-split mult.

$F/\mathbb{Q}_p$ quad ram. $\iff$ additive pot. mult. red.

Write $\psi : \mathrm{Gal}(F/\mathbb{Q}_p) \longrightarrow \{\pm 1\}$ for the unique non-trivial char. if $F\neq\mathbb{Q}_p$ and $\psi = \mathbb{1}$ if $F=\mathbb{Q}_p$.

$E_{-6b} = E_\psi$ : $-6by^2 = x^3+ax+b$ $\quad [\cong y^2 = x^3 + (-6b)^2ax + (-6b)^3 b]$

$P=(x,y)\in E(\overline{\mathbb{Q}}_p) \xleftrightarrow{1:1} \tilde{P} = (x, \frac{1}{\sqrt{-6b}}y) \in E_\psi(\overline{\mathbb{Q}}_p)$

$\sigma(P) \longleftrightarrow \psi(\sigma)\,\sigma(\tilde{P})$ for $\sigma\in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

In particular,

$$E_\psi[\ell^n] \cong E[\ell^n]\otimes\psi$$
$$T_\ell E_\psi \cong T_\ell E\otimes\psi$$
$$V_\ell E_\psi \cong V_\ell E\otimes\psi$$
$$V_\ell E_\psi^* \cong V_\ell E^*_\psi\otimes\psi.$$

In the non-split multiplicative case ; $\psi$ unramified, $\psi(\mathrm{Frob}) = -1$, so

$I$ act on $V_\ell E^*$ as $\begin{pmatrix} 1 & \boxed{0} \\ * & \boxed{1} \end{pmatrix}$, Frob as $\begin{pmatrix} -1 & 0 \\ * & \boxed{-1} \end{pmatrix}$, and

$$\boxed{F(T) = 1 + T}$$

In the additive pot. mult. case, $\psi$ ramified,

$I$ acts on $V_\ell E^*$ as $\begin{pmatrix} \pm 1 & 0 \\ * & \pm 1 \end{pmatrix}$, $(V_\ell E^*)^I = 0$ and

$$\boxed{F(T) = 1}$$

## § Additive potentially good case

Finally suppose

$E/\mathbb{Q}_p$ has additive red., $v(j) \geq 0$.

$\tilde{E}/\mathbb{F}_p$.

**Thm** $E$ acquires good red. over some $F/\mathbb{Q}_p$ finite Galois.

[When $p \geq 5$, $v(j) \geq 0$, $E$ good$/F \iff 12 \mid v_F(\Delta)$, so take

$F = \mathbb{Q}_p(\zeta_e, \sqrt[e]{p})$, $e = \frac{12}{\gcd(12, v(\Delta))} \in \{2,3,4,6\}$ ]

By Néron - Ogg - Shafarevich,

$I = I_{\bar{\mathbb{Q}}_p/\mathbb{Q}_p}$ acts non-trivially on $V_\ell E$

$I_{\bar{\mathbb{Q}}_p/F}$ acts trivially on $V_\ell E$

So $I$ acts through a finite quotient $\Phi = I_{F/\mathbb{Q}_p}$.

[ in fact $I$ acts through $\Phi = \underbrace{C_2, C_3, C_4, C_6}_{\text{tame when } p \neq 2,3}, C_3 \rtimes C_4$ (only possible when $p=3$, wild), $Q_8, SL_2(\mathbb{F}_3)$. (only possible when $p=2$, wild)

Such a rep. is semisimple, so if $(V_\ell E^*)^I \neq \emptyset$,

then $V_\ell E^* \cong \mathbb{1} \oplus \varphi$ for some $\varphi$.

But $\det V_\ell E^* = \chi_\ell^{-1}$ by Weil pairing which is $= \mathbb{1}$ on $I$.

So $\varphi = \mathbb{1}$, contradiction. In other words, $(V_\ell E^*)^I = 0$, and

$$\boxed{F(T) = 1}.$$

Ex $E = E_3/\mathbb{Q}_5$ : $y^2 = x^3 - 5^2$ additive red., $\Delta = -2^4 3^4 5^4$

Becomes good over $F = \mathbb{Q}_5(\sqrt[3]{5}, \zeta_3)$ $\leftarrow 12 \mid v_F(\Delta)$

$$y^2 = x^3 - (\sqrt[3]{5})^6 \quad \cong \quad y^2 = x^3 - 1 \quad \text{over } F$$

good.

So $T_\ell E$ is unramified over $F$, and

$$F \subseteq \mathbb{Q}_5(E[2^n]) \subseteq F^{nr} \quad \text{for all } n \geq 1.$$

$\mathbb{Q}_5(E[2]) = F$

Describe $\mathrm{Gal}(\overline{\mathbb{Q}}_5/\mathbb{Q}_5) \circlearrowright V_\ell E$, any $\ell \neq 5$.

- Action factors through $G = \mathrm{Gal}(F^{nr}/\mathbb{Q}_5) \cong C_3 \rtimes \mathrm{Gal}(\overline{\mathbb{F}}_5/\mathbb{F}_5)$

  inertia $I$ — unr., gen by Frob.

- $\mathrm{Frob}^2$ acts as $\begin{pmatrix} -5 & 0 \\ 0 & -5 \end{pmatrix}$ $\leftarrow$ because char. poly. $T^2+5$ on $T_\ell(y^2=x^3+1)/\mathbb{F}_5$

  $\Rightarrow (T-(\sqrt{-5})^n)(T+(\sqrt{-5})^n)$ / $\mathbb{F}_{5^n}$

  $\Rightarrow (T+5)^2$ / $\mathbb{F}_{5^2}$.

- Let $\chi : G \longmapsto \overline{\mathbb{Q}}_\ell^\times$ be the unr. char.

  $I \longmapsto 1$

  $\mathrm{Frob} \longmapsto \sqrt{-5}$

Then $V_\ell E \otimes \chi^{-1}$ : $\mathrm{Frob}^2 \longmapsto 1$ and so factors through

$\mathrm{Gal}(F/\mathbb{Q}_5) \cong S_3$.

$\Rightarrow$ direct sum of $\underbrace{\mathbb{1}, \varepsilon}_{\text{unr.}}, \Delta$'s ; ramified of dim 2 $\Rightarrow$ $\cong \Delta$.

Conclusion $V_\ell E \cong \chi \otimes \Delta$

$\chi$ as above (unr., infinite order)

$\Delta$ unique irr. rep. of $\mathrm{Gal}(\mathbb{Q}_5(\zeta_3, \sqrt[3]{5})/\mathbb{Q}_5) \cong S_3$ of dim 2

## Summary

We showed that for $E/\mathbb{Q}$, $\ell \neq p$,

$$F_p(T) = \det(1 - \mathrm{Frob}_p^{-1} T \mid (V_\ell E^*)^{I_p}) = \begin{cases} 1 - aT + pT^2 & E \text{ good red at } p \\ & a = p+1-\#\tilde{E}(\mathbb{F}_p) \\ 1-T & E \text{ split mult.} \\ 1+T & E \text{ non-split mult.} \\ 1 & E \text{ additive red.} \end{cases}$$

independently of $\ell$.

<u>Exc</u> $F_p(T) = \begin{cases} 1-aT+pT^2 & p \text{ good} \\ 1-aT & p \text{ bad} \end{cases}$ $\quad a = p+1-\#\tilde{E}(\mathbb{F}_p)$ in all cases.

<u>Exc</u> $E/\mathbb{Q}$ elliptic curve.
$\mathcal{E}/\mathbb{Z}$ minimal Weierstrass model. Then

$$\zeta_{\mathcal{E}}(s) = \frac{\zeta(s)\zeta(s-1)}{L(E,s)}$$

have analogue for all curves and AVs (Deligne-Mumford)

Elliptic curves $E/\mathbb{Q}_p$ are <u>potentially semistable</u>, i.e. become good or mult. after a fin. ext. $K/\mathbb{Q}_p$. So $I = I_{\bar{\mathbb{Q}}_p/\mathbb{Q}_p}$ has a sgp. of finite index $I_{\bar{\mathbb{Q}}_p/K}$ which acts as $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (pot. good.) or

$\begin{pmatrix} 1 & 0 \\ t_\ell & 1 \end{pmatrix}$ (pot. mult.) on $H^1_{et}(E_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_\ell)$.

tame character

This is true in general:

<u>Thm</u> (Grothendieck Monodromy Thm.) $X/\mathbb{Q}_p$ nonsing. proj. variety, $\ell \neq p$, $0 \le i \le 2\dim X$.
There is $K/\mathbb{Q}_p$ finite s.t. $I_{\bar{\mathbb{Q}}_p/K}$ acts on $H^i_{et}(X_{\bar{\mathbb{Q}}_p}, \mathbb{Q}_\ell)$ as $\mathrm{Id} + t_\ell \cdot N$, $N$ nilpotent matrix.

A geometric analogue of this is not known, i.e. we don't know if varieties acquire semistable red. over a fin. ext. of $\mathbb{Q}_p$.

**Rmk** For elliptic curves,

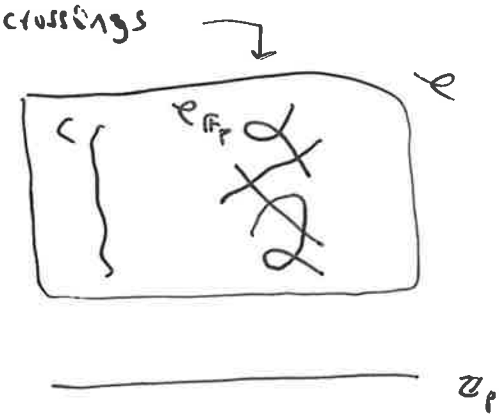
$$N = 0 \iff E \text{ pot. good.}$$

$$N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \iff E \text{ pot. mult.}$$

Generally $N^2 = 0$ for $H^1_{et}$ (curves and abelian varieties).

For curves of genus $g \geq 2$:

$C/\mathbb{Q}_p$ is <u>semistable</u> if there is a proper flat model $\mathcal{C}/\mathbb{Z}_p$ whose special fibre $\mathcal{C}_{\mathbb{F}_p}$ reduced with normal crossings




**Thm** $C$ semistable $\iff$ $I_{\overline{\mathbb{Q}}_p/\mathbb{Q}_p}$ acts on $H^1_{et}(C_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_\ell)$ as $\mathrm{Id} + t_\ell N$ with $N^2 = 0$

$$\iff H^1_{et}(C_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_\ell) \cong \underbrace{A \oplus (T \otimes Sp_2)}_{\text{unramified}}$$

split mult. ell. curve

$\dim A = 2 \cdot \sum$ geom. genera of components of $\mathcal{C}_{\mathbb{F}_p}$.

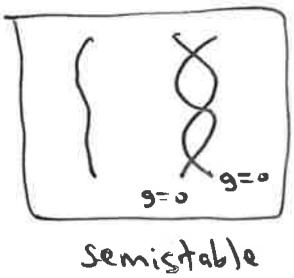
$\dim T = \#$ loops $= \dim H_1^{top}(\text{dual graph of } \mathcal{C}_{\mathbb{F}_p}, \mathbb{Z})$

For non-semistable $C$, the same is true but $A$, $T$ are ramified, and become unramified after a fin. ext. of $\mathbb{Q}_p$ (inertia image is finite)

**Ex** $C: y^2 = (x^2-5)((x-1)^2-5)((x-2)^2-5)$ genus 2

Here $A = 0$, $\dim T = 2$ and

$H^1_{et}(C_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_\ell) \cong T \otimes Sp_2$ has dim. $2g = 4$.




semistable