Tim
6-27-11
pg 1

Goals: $E/\mathbb{Q}$ elliptic curve $\rightsquigarrow V_\ell(E)$ ℓ-adic rep.

$\rightsquigarrow L(E,s)$ L-function

$$L(E/\mathbb{Q}, s) = \sum_{n \geq 1} a_n n^{-s} = \prod_p F_p(p^{-s})^{-1}$$

$$F_p(T) = \det(1 - \mathrm{Frob}_p^{-1} T \mid (V_\ell(E)^\vee)^{I_p})$$

$$\overset{(*)}{=} \begin{cases} 1 - a_p T + pT^2 & E \text{ good red. at } p \\ & a_p = p+1-\#\tilde{E}(\mathbb{F}_p) \\ 1 - T & \text{split mult.} \\ 1 + T & \text{non-split mult.} \\ 1 & \text{add. red.} \end{cases}$$

Similarly, K number field, E/K elliptic curve, then

$$L(E/K, s) = \prod_{\substack{\mathfrak{p} \\ \text{primes of } K}} F_{\mathfrak{p}}((N\mathfrak{p})^{-s})^{-1} \qquad (\mathrm{Re}(s) > 3/2)$$

Set $\hat{L}(E/K, s) = \left(\frac{N}{\pi^d}\right)^{3/2} \left(\frac{\Gamma(s/2)^d}{\Gamma(\frac{s+1}{2})^d}\right) L(E/K, s)$, $d = [K:\mathbb{Q}]$

This is the completed L-function; N = conductor of E

Conjecture: (Hasse-Weil) $L(E/K, s)$ has analytic continuation to $\mathbb{C}$ and satisfies functional equation

$$\hat{L}(E/K, 2-s) = W \hat{L}(E/K, s)$$

where $W = W(E/K) = \pm 1$ is the global root number.

This is known $/\mathbb{Q}$ by Wiles, et. al, and over totally real fields with "analytic" replaced by "meromorphic". (Taylor)

$$W(E/K) = \prod_{\substack{v \\ \text{places of} \\ K}} W(E/K_v) \quad \text{local root numbers, all } \pm 1.$$

$$W(E/K_v) \overset{(**)}{=} \begin{cases} -1 & v \mid \infty \text{ or } v \text{ split mult. red.} \\ +1 & v \text{ good or } v \text{ non-split mult. red.} \\ (-1)^{\left\lfloor \frac{|k_v| \, v(\Delta)}{12} \right\rfloor} & v \text{ additive}, \nmid 2,3 \quad v(j) \geq 0 \text{ (valuation)} \\ (-1)^{\left\lfloor \frac{|k_v|}{2} \right\rfloor} & v \text{ additive}, v \nmid 2,3 \quad v(j) < 0 \end{cases}$$

(formula at 2, 3 defined, just a mess.)

Structure: 1) $V_\ell(E)$

2) L, N, $(*)$

3) W, $(**)$

Part I ℓ-adic representations of elliptic curves:

$E/\mathbb{Q}$ elliptic curve, $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Q}$.

Recall: $E[n] = \{ P \in E(\bar{\mathbb{Q}}) : nP = 0 \}$

$\cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as an abelian group for any $n \geq 1$.

This is called the n-torsion subgroup.

Example: $(n=2)$ $\quad y^2 = x^3 + ax + b$

$= (x-\alpha)(x-\beta)(x-\gamma)$. over $\bar{\mathbb{Q}}$

$E[2] = \{ \mathcal{O}, (\alpha, 0), (\beta, 0), (\gamma, 0) \}$

__Example:__ ($n=4$)

$$E[4] = E[2] \cup \{(\alpha_i, \pm\sqrt{\alpha_i^3 + a\alpha_i + b})\}$$

α_i are roots of $x^6 + 5ax^4 + 20abx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3$

$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$, and it acts linearly. This is because the action of Galois on $E(\overline{\mathbb{Q}})$ commutes with addition. So we obtain

$$\bar{\rho}_n : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[n]) \cong GL_2(\mathbb{Z}/n\mathbb{Z})$$

This is referred to as the "mod n" representation.

__Example:__ $y^2 = x^3+1 = (x+1)(x+\zeta)(x+\zeta^2)$ $\quad \zeta = \zeta_3$.

$$E[2] = \mathbb{F}_2(-1,0) + \mathbb{F}_2(-\zeta,0). \quad \cong \mathbb{F}_2^2.$$

$$\bar{\rho}_2 : G_{\mathbb{Q}} \longrightarrow \underset{\substack{\text{id},\ c = \text{complex conj.}}}{\underset{\mathbb{Z}/2\mathbb{Z}}{\underset{\shortparallel}{\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})}}} \longrightarrow GL_2(\mathbb{F}_2)$$

$$\mathrm{id} \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$c \longmapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

So $\mathrm{im}(\bar{\rho}_2) \simeq \mathbb{Z}/2\mathbb{Z}$.

__Example:__ $y^2 = x^3 + 5^2 = (x+5^{2/3})(x+\zeta 5^{2/3})(x+\zeta^2 5^{2/3})$

$$\bar{\rho}_2 : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_2).$$

(Check this as an exercise.)

__Remark:__ $\cdot$ $\ker \bar{\rho}_n = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$

$\cdot$ $\mathrm{im}\, \bar{\rho}_n \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$

- If $n = \prod l_i^{m_i}$, then as an abelian group we can factor $E[n]$ into its p-Sylow subgroups:

$$E[n] \cong \prod E[l_i^{m_i}].$$

In fact, this factorization is as Galois modules so it is enough to study torsion modules for prime powers.

<u>Def</u>: The Tate module is defined by

$$T_\ell E = T_\ell(E) = \varprojlim_{n} E[\ell^n]$$

$$\cong \mathbb{Z}_\ell^2 \quad \text{(after picking bases in compatible ways)}$$

$$V_\ell E = T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell^2.$$

Both $T_\ell E$, ~~and~~ $V_\ell E$ and $V_\ell E^\vee$ are called the ℓ-adic reps. of E.
dual space.

<u>Note</u>: We have a representation

$$\rho_\ell = \varprojlim \bar{\rho}_{\ell^n} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell E)$$

$$\cong GL_2(\mathbb{Z}_\ell)$$

$$: G_\mathbb{Q} \to \mathrm{Aut}(V_\ell E) \cong GL_2(\mathbb{Q}_\ell).$$

<u>Theorem (Serre)</u>: If E has no CM, then $\rho_\ell : G_\mathbb{Q} \to GL_2(\mathbb{Z}_\ell)$ is surjective for almost all ℓ. So $\bar{\rho}_{\ell^n}$ are surj. almost always.

<u>Exercise</u>: Prove if E has CM then this statement is false for all ℓ.

<u>Open</u>: Serre's thm true for all $\ell > 163$, or even for some $\ell > c$

for some constant c that does not depend on E.

Structure of $E[\ell^n]$ over local fields:

Problem: $E/\mathbb{Q}_p$, describe the action of $G_{\mathbb{Q}_p}$ on $E[\ell^n]$, $T_\ell E$, and $V_\ell E$.

$K/\mathbb{Q}_p$ finite.

$$\begin{array}{ccc} K & \mathcal{O}_K/\varpi & = \mathbb{F}_q \\ | & | & | \\ \mathbb{Q}_p & \mathbb{Z}_p/p\mathbb{Z}_p & = \mathbb{F}_p. \end{array}$$

$(p) = (\varpi^e)$, $q = p^f$ $\quad$ e = ramification index of $K/\mathbb{Q}_p$
f = residue degree

$ef = [K:\mathbb{Q}_p]$.

If $K/\mathbb{Q}_p$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}_p) = G$.

Def: $G_i = \{ \sigma \in G : \sigma(x) \equiv x \pmod{\varpi^{i+1}} \ \forall x \in \mathcal{O}_K \}$.

(This checks how "visible" the action of Galois is.. can you see it in residue fields..)

$G \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq \{1\}$. This is called the ramification filtration.

$G_0 = I$ = inertia

$G_1 = I^{\text{wild}}$ = wild inertia

Tim
6-28-11
pg 1

$K/\mathbb{Q}_p$ finite Galois (ram. degree e, res. degree f)

$G = \mathrm{Gal}(K/\mathbb{Q}_p)$

$$G \trianglerighteq \underset{\substack{\parallel \\ \text{inertia}}}{G_0} \trianglerighteq \underset{\substack{\text{wild} \\ \text{inertia}}}{G_1} \trianglerighteq \cdots$$

$G_i = \{ \sigma \in G : \sigma(x) \equiv x \pmod{\varpi^{i+1}} \ \forall x \in \mathcal{O}_K \}$

<u>Exercise:</u> Describe G_i for $K = \mathbb{Q}_2(\zeta_{12})$ or $\mathbb{Q}_2(\zeta_8)$.

$I_{K/\mathbb{Q}_p} = G_0 = \{ \sigma : \bar{\sigma} : \mathbb{F}_q \to \mathbb{F}_q \text{ is trivial} \}.$

$$1 \to \underset{\text{size } e}{I_{K/\mathbb{Q}_p}} \to G \to \underset{\substack{\text{cyclic gen} \\ \text{by } x \mapsto x^p \\ \text{size } f.}}{\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \to 1$$

$G_1 \trianglelefteq I$ is its p-Sylow subgroup.

G_0/G_1 = tame inertia (prime to p, cyclic, $\hookrightarrow k_{\mathbb{Q}_p}^\times$)

Pass to $\overline{\mathbb{Q}}_p = \bigcup_{\substack{K/\mathbb{Q}_p \\ \text{fin}}} K$:

$\overline{\mathbb{Q}}_p$

wild inertia | pro-p

$\mathbb{Q}_p^{\text{tame}} = \bigcup_{(n,p)=1} \mathbb{Q}_p(\zeta_n, \sqrt[n]{p})$

tame inertia | pro-cyclic

$\mathbb{Q}_p^{\text{un}} = \bigcup_{(n,p)=1} \mathbb{Q}_p(\zeta_n)$ max unram. ext. of $\mathbb{Q}_p$.

$G_{\mathbb{F}_p}$ | pro-cyclic

$\mathbb{Q}_p$

inertia

$G_{\mathbb{Q}_p}$

$$1 \longrightarrow I_{\mathbb{Q}_p} \longrightarrow G_{\mathbb{Q}_p} \longrightarrow G_{\mathbb{F}_p} \longrightarrow 1$$

$G_{\mathbb{F}_p} = \hat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$, pro-cyclic, generated by $x \mapsto x^p$.

<u>Def:</u> An <u>arithmetic Frobenius</u> Frob_p is any element of $G_{\mathbb{Q}_p}$ reducing to $x \mapsto x^p$ in $G_{\mathbb{F}_p}$. (Only well-defined up to inertia.)

<u>Def:</u> A $G_{\mathbb{Q}_p}$-module M is <u>unramified</u> if $I_{\mathbb{Q}_p}$ acts trivially on M. In this case, we have a well-defined action of Frobenius.

<u>Def:</u> M is <u>tamely ramified</u> if wild inertia acts trivially, and <u>wildly ramified</u> otherwise.

<u>Example:</u> $E/\mathbb{Q}_5$ $\quad y^2 = x^3+1$. $\quad \zeta = \zeta_3$.

$E[2] = \{\mathcal{O}, (-1,0), (-\zeta,0), (-\zeta^2,0)\}$ unramified.

($\Leftrightarrow$ $\mathbb{Q}_5(E[2])/\mathbb{Q}_5$ is unramified)

$\mathbb{Q}_5(E[2]) = \mathbb{Q}_5(\zeta) \subseteq \mathbb{Q}_5^{unr}$.

Alternatively, x^3+1 has distinct roots in $\overline{\mathbb{F}}_5 \Rightarrow$ $G_{\mathbb{Q}_5}$ acts on them through $G_{\mathbb{F}_5}$.

Over $\mathbb{Q}_3$, this would be tamely ramified.

<u>Example:</u> $E/\mathbb{Q}_5$ $\quad y^2 = x^3 + 5^2$

$E[2] = \{\mathcal{O}, (-5^{2/3},0), (-5^{2/3}\zeta,0), (-5^{2/3}\zeta^2,0)\}$

tamely ramified.

$\mathbb{Q}_5(E[2])$: $\quad x^3 + 5^2.$

$$
\begin{tikzcd}
\mathbb{Q}_5(\zeta, \sqrt[3]{5}) \arrow[d, dash, "\text{tame}"', "3"] \\
\mathbb{Q}_5(\zeta) \arrow[d, dash, "\text{unram}"', "2"] \\
\mathbb{Q}_5
\end{tikzcd}
$$

Could continue and look at $\mathbb{Q}_5(E[4])$, $\mathbb{Q}_5(E[8])$, ...
This just gets messy very fast. One gets

$$
\begin{tikzcd}
\mathbb{Q}(\zeta_?, \sqrt[3]{5}) \arrow[d, dash] \\
\mathbb{Q}(\zeta_?) \arrow[d, dash] \\
\mathbb{Q}_5
\end{tikzcd}
$$

and so one can convince oneself that $I_{\mathbb{Q}_5}$ acts on $T_2 E$ through $\mathbb{Z}/3\mathbb{Z}$. It turns out this is true. See below.

Good reduction:

Theorem (Neron-Ogg-Shafarevich) (N.O.S): Let $F/\mathbb{Q}_p$ be finite, residue field $\mathbb{F}_q$, E/F an elliptic curve. Then E/F has good reduction iff $T_\ell E$ is unramified $\forall\, \ell \neq p$. If I_F does act trivially, then char. poly. of Frob_p on $T_\ell E$ is $x^2 - ax + q$ where $a = q + 1 - \#\widetilde{E}(\mathbb{F}_q)$. (indep. of ℓ)

Tim
6-28-11
pg 4

Def: E/F elliptic curve. The local polynomial

$$F_p(T) = \det\left(1 - \mathrm{Frob}_p^{-1} T \mid (V_\ell E^\vee)^{I_F}\right).$$

Cor: If $E/\mathbb{Q}_p$ has good reduction, then

$$F_p(T) = 1 - a_p T + p T^2$$

where $a_p = p + 1 - \widetilde{E}(\mathbb{F}_p)$.

Proof: $T_\ell E$ unram., $V_\ell E$, $V_\ell E^\vee = \mathrm{Hom}(V_\ell E, \mathbb{Q}_\ell)$ are all unram. So

$$(V_\ell E^\vee)^{I_{\mathbb{Q}_p}} = V_\ell E^\vee,$$

which is 2-dim. The eigenvalues of Frob_p^{-1} = inverses of those of Frob_p $\Rightarrow$ get char. poly. $\blacksquare$

Potentially Good Reduction:

Ex: $E/\mathbb{Q}_5 : y^2 = x^3 + 5^2$ has bad reduction.

$\overset{\text{N.O.S.}}{\Longrightarrow} I_{\mathbb{Q}_5}$ acts nontrivially on $T_\ell E$, all $\ell \neq 5$.

Over $\mathbb{Q}_5(\sqrt[3]{5})$ has good reduction: $y^2 = x^3 + \varpi^6 \simeq y^2 = x^3 + 1$.

where $\varpi = \sqrt[3]{5}$. $\overset{\text{N.O.S.}}{\Longrightarrow} I_{\mathbb{Q}_5(\sqrt[3]{5})}$ acts trivially.

So inertia $I_{\mathbb{Q}_5}$ acts through

$I_{\mathbb{Q}_5(\sqrt[3]{5}, \zeta)/\mathbb{Q}_5} \simeq \mathbb{Z}/3\mathbb{Z}$ on $T_\ell E$

for all $\ell \neq 5$.

$$\begin{array}{c} \overline{\mathbb{Q}}_5 \\ | \\ \mathbb{Q}_5(\sqrt[3]{5}, \zeta) \\ | \\ \mathbb{Q}_5 \end{array}$$

In general, if $E/\mathbb{Q}_p$ has potentially good reduction, $p \neq 2, 3$, then E acquires good reduction over $\mathbb{Q}_p(\sqrt[12]{\Delta_E})$, and so $I_{\mathbb{Q}_p}$ acts through $I_{\mathbb{Q}_p(\zeta_{12}, \sqrt[12]{\Delta_E})}$, which is cyclic of order

$$e = \frac{12}{\gcd(v(\Delta_E), 12)}$$

valuation

i.e., it is cyclic of order 1, 2, 3, 4, 6, 12.

<u>Exercise:</u> Prove $\mathbb{Z}/12\mathbb{Z}$ cannot happen. (Can look at Tate's algorithm for this, or try to do directly from the material in the lecture.)

Recall:

Example: $y^2 = x^3 + 5^2$

bad (additive) red. $/\mathbb{Q}_5$

good red. $/\mathbb{Q}_5(\sqrt[3]{5})$

$I_{\mathbb{Q}_5}$ acts on $V_\ell E$ through $\mathbb{Z}/3\mathbb{Z}$ for all $\ell \neq 5$.

In this example, $I_{\mathbb{Q}_5} \curvearrowright V_\ell E \otimes \overline{\mathbb{Q}}_\ell$ as $\begin{pmatrix} \varphi & 0 \\ 0 & \varphi^{-1} \end{pmatrix}$
where φ char of $\mathbb{Z}_3$ of order 3.

Def: $\chi_\ell : G_{\mathbb{Q}_p} \to \mathbb{Z}_\ell^\times$ is the ℓ-adic cyclotomic character
(= action of $G_{\mathbb{Q}_p}$ on $\varprojlim \mu_{\ell^n} \simeq \mathbb{Z}_\ell$ as abelian groups,
and Galois acts on $\varprojlim \mu_{\ell^n}$, so on $\mathbb{Z}_\ell$ via this isom.
Can write $\mathbb{Z}_\ell(1)$ to denote this.) $I_{\mathbb{Q}_p} \to 1$, $\mathrm{Frob}_p \mapsto p$

Recall: $\Lambda^2 T_\ell E \simeq \chi_\ell$ by Weil pairing, i.e. $\det \rho_\ell = \chi_\ell$.
In particular, $\det(\rho_\ell(\sigma)) = 1$ for $\sigma \in I_{\mathbb{Q}_p}$.

In general for pot. good red, additive

(a) $I_{\mathbb{Q}_p}$ acts on $V_\ell E \otimes \overline{\mathbb{Q}}_\ell$ as $\begin{pmatrix} \varphi & 0 \\ 0 & \varphi^{-1} \end{pmatrix}$ for φ a primitive char. of $\mathbb{Z}_c$, $c = 1, 2, 3, 4$, or 6.
for $p \neq 2, 3$.

(b) $F_p(T) = 1$.

Proof: (a) Use $\det \rho_\ell = \chi_\ell$

(b) $(V_\ell E^\vee)^{I_{\mathbb{Q}_p}} = 0$. This is clear from (a) if $p \neq 2, 3$.
If this were not 0, then I_p would act on $V_\ell E^\vee$

as $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ (says it has at least one invariant).

Since $\det = 1$, we must have it act as $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

$\Rightarrow$ acts as $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\hookrightarrow$ $I_{\mathbb{Q}_p}$ acts as a formula through a finite group, but if $* \neq 0$ this would have inf. order. ■

<u>Note:</u> If $p = 2, 3$, $I_{\mathbb{Q}_p}$ may act through Q_8, $SL_2(\mathbb{F}_3)$, or $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$.

<u>Split multiplicative reduction:</u>

<u>Theorem (Tate curve):</u> $E/\mathbb{Q}_p$ split mult. red. Then $\exists\, q \in \mathbb{Z}_p$, $v(q) = v(\Delta) = -v(j)$ s.t.

$$E(\overline{\mathbb{Q}}_p) \simeq \overline{\mathbb{Q}}_p^{\times} / q^{\mathbb{Z}} \quad \text{as } G_{\mathbb{Q}_p}\text{-modules}.$$

(like $E(\mathbb{C}) \simeq \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau \overset{\exp}{\simeq} \mathbb{C}^{\times}/q^{\mathbb{Z}}$ where $q = e^{2\pi i \tau}$)

This immediately gives

$$E[\ell] = \langle \zeta_\ell, q^{1/\ell} \rangle \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$$

$$E[\ell^n] = \langle \zeta_{\ell^n}, q^{1/\ell^n} \rangle$$

Therefore, we have $G_{\mathbb{Q}_p}$ acts on $T_\ell E$ as

$$\left(\begin{array}{l} \sigma(\zeta_\ell) = \zeta_\ell^{a} \\ \sigma(q^{1/\ell}) = \zeta_\ell^{b} q^{1/\ell} \end{array} \right)$$

so $\begin{pmatrix} \chi_\ell & * \\ 0 & 1 \end{pmatrix}$. ($\chi_\ell$ corresponds to $G_{\mathbb{Q}_p}$ acting on powers of ζ_ℓ, 1 b/c $q^{1/\ell} \mapsto q^{1/\ell}$ and $*$ for the power of ζ_ℓ that goes in front of $q^{1/\ell}$)

We also have $I_{\mathbb{Q}_p}$ acts as $\begin{pmatrix} 1 & v(q) t_\ell \\ 0 & 1 \end{pmatrix}$. where

Tim
6-29-11
pg 3

<u>Def:</u> ψ_ℓ is the tame character $I_{\mathbb{Q}_p} \to \mathbb{Z}_\ell$

$$\sigma \longmapsto \left(\frac{\sigma(q^{1/\ell^n})}{q^{1/\ell^n}} \right)_n \in \varprojlim \mu_{\ell^n} = \mathbb{Z}_\ell(1)$$

$$\left(I_{\mathbb{Q}_p}/G_1 \cong \prod_{\ell \neq p} \mathbb{Z}_\ell \xrightarrow{\text{proj}} \mathbb{Z}_\ell \right)$$

<u>Cor:</u> If $E/\mathbb{Q}_p$ has split mult. red. then

$$F_p(T) = 1 - T.$$

<u>Proof:</u> $I \circlearrowright V_\ell E$ as $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

$I \circlearrowright V_\ell E^\vee$ as $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$

$(V_\ell E^\vee)^I$ 1-dim.

$\mathrm{Frob}_p \circlearrowright V_\ell E^\vee$ as $\begin{pmatrix} p & 0 \\ * & 1 \end{pmatrix}$

$\Rightarrow \det(1 - \mathrm{Frob}_p^{-1} T \mid (V_\ell E^\vee)^{I_p}) = 1 - 1 \cdot T$ ∎

<u>Potentially Mult. Reduction:</u>

<u>Def:</u> E/K $y^2 = x^3 + ax + b$, $d \in K^\times$. The <u>quadratic twist</u> of E by d is

$$E_d/K : \ dy^2 = x^3 + ax + b$$

or an isomorphic curve:

$$y^2 = x^3 + d^2 a x + d^3 b.$$

<u>Note:</u> $E \cong E_d$ over $K(\sqrt{d})$.

Let $\varphi : \mathrm{Gal}(K(\sqrt{d})/K) \longrightarrow \{\pm 1\}$ be the nontrivial char.
$\mathbb{Z}_2$

Tim
6-29-11
PS4

<u>Exercise:</u> Prove $V_\ell(E_d) \simeq V_\ell(E) \otimes \varphi$

If $E/\mathbb{Q}_p$ has $\overset{(I)}{\text{non-split}}$ / $\overset{(II)}{\text{add. pot. mult}}$ reduction

$$E: y^2 = x^3 + ax + b.$$

In both cases the quadratic twist E_{-6b} has split mult. reduction. (b/c $E_{-6b}: y^2 = x^3 + \underbrace{a(-6b)^2}_{a'} x + \underbrace{(-6b)^3 b}_{b'}$

and $-6b'$ is a square.)

So $(V_\ell E)^\vee \simeq \varphi \otimes V_\ell(E_{-6b})^\vee$

$$\simeq \varphi \otimes \begin{pmatrix} \chi_\ell & 0 \\ * & 1 \end{pmatrix}$$

where $\varphi: \mathrm{Gal}(\mathbb{Q}_p(\sqrt{-6b})/\mathbb{Q}_p) \to \{\pm 1\}$ is nontrivial, i.e.

(I) φ: $I_{\mathbb{Q}_p} \to 1$ b/c nonsplit means $\mathbb{Q}_p(\sqrt{-6d})/\mathbb{Q}_p$ is unram.
$\mathrm{Frob}_p \mapsto -1$ b/c φ nontrivial

(II) φ $I_{\mathbb{Q}_p} \to \pm 1$ add. pot. mult $\Leftrightarrow$ $\mathbb{Q}_p(\sqrt{-6d})/\mathbb{Q}_p$ is ram.
$\mathrm{Frob}_p \mapsto *$

i.e., in case (I) $I_{\mathbb{Q}_p}$ acts as $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$, Frob_p acts as $\begin{pmatrix} -p & 0 \\ -* & -1 \end{pmatrix}$ and so $\det(1 - \mathrm{Frob}_p^{-1} T \mid (V_\ell E^\vee)^{I_p}) = 1 + T$

in case (II) $I_{\mathbb{Q}_p}$ acts as $\pm\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$ and so $(V_\ell E^\vee)^{I_p} = 0$, $\det(1 - \mathrm{Frob}_p^{-1} T \mid (V_\ell E^\vee)^{I_p}) = 1$.

<u>Conclusion:</u> $F_p(T) = \det(1 - \mathrm{Frob}_p^{-1} T \mid (V_\ell E^\vee)^{I_p})$

$$= \begin{cases} 1 - a_p T + pT^2 & \text{good red.} \\ 1 - T & \text{split mult.} \\ 1 + T & \text{non-split mult.} \\ 1 & \text{add.} \end{cases}$$

Part II: General L-functions:

Fix $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p \to \mathbb{C}$. This induces $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$. Denote the image of Frob_p in $G_{\mathbb{Q}}$ under this inclusion by Frob_p again. Denote the image of $I_{\mathbb{Q}_p}$ by I_p.

Let $V/\mathbb{Q}$ be a non-singular projective variety. This gives rise to étale cohomology groups $H^i(V) = H^i_{et}(V, \mathbb{Q}_\ell)$ ~~where~~ $0 \le i \le 2\dim V$. These are $\mathbb{Q}_\ell$-vector spaces with a $G_{\mathbb{Q}}$-action. These have the same dimension as $H^i_B(V(\mathbb{C}), \mathbb{Q})$.

<u>Example:</u> $E/\mathbb{Q}$.

$H^0(E) = \mathbb{Q}_\ell$ 1-dim

$H^1(E) = V_\ell E^\vee$ 2-dim

$H^2(E) = \mathbb{Q}_\ell(1)$ 1-dim

<u>Grothendieck Monodromy Theorem:</u> ~~After~~ Let p be a prime and $\ell \ne p$. After a finite extension $K/\mathbb{Q}_p$, I_K acts on $H^i(V)$ as $1 + \psi N$ where $\psi: G_K \to \mathbb{Z}_\ell$ is the tame character and $N \in \mathrm{End}(H^i)$ nilpotent.

i.e. I_K act by $1+\psi N$ after a finite ext.

[If $\rho: G_K \to GL_d(\overline{\mathbb{Q}}_\ell)$ is such a rep, we say ρ is a Weil-Deligne representation. It is a Weil rep. if $N = 0$, i.e. I_K acts through a finite quotient.]

For elliptic curves, $N = 0$ in potentially good case and $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ in pot. mult. case.

Tim
6-30-11
p92

A 1-dim. WD-rep. = 1-dim Weil rep. is a quasi-character, i.e., $\varphi: G_K \to \mathbb{C}^\times$ s.t. $\varphi(I_K)$ is finite. For ex., the cyclotomic character χ_ℓ is such a 1-dim WD-rep.

Def: For a variety $V/\mathbb{Q}$,

$$L(H^i(V), s) = \prod_p F_p(p^{-s})^{-1}.$$

where

$$F_p(T) \overset{?}{=} \det(1 - \mathrm{Frob}_p^{-1} T \mid H^i(V)^{I_p})$$

[Problem: It is not known in general this is independent of ℓ when p is a prime of bad reduction for V.
This is ok for curves and abelian varieties.]

For a curve $C/\mathbb{Q}$, genus g

$$H^0(C) = \mathbb{Q}_\ell$$

$$H^1(C) = V_\ell(\mathrm{Jac}\, C)^\vee = 2g\text{-dim } (\mathrm{Jac}\, C \text{ } g \text{ dim. abelian variety})$$

$$H^2(C) = \mathbb{Q}_\ell(1)$$

$$L(H^1(C), s) = L(H^1(\mathrm{Jac}\, C), s) = L(C, s),$$

Fact: If $V/\mathbb{Q}_p$ has good reduction,

$$\prod_i F_p(H^i(V), T)^{(-1)^i} = \zeta_{\tilde{V}/\mathbb{F}_p}(T)^{-1}.$$

Example: If $E/\mathbb{Q}$ has good reduction at p,

$$\zeta_{\tilde{E}/\mathbb{F}_p}(T) = \frac{1 - a_p T + pT^2}{(1-T)(1-pT)}.$$

Generally, this definition of L-functions applies to any "compatible system of ℓ-adic representations."

A compatible system is:

$$\rho = (\rho_\ell)_\ell \,, \quad \rho_\ell : G_K \to GL_d(\bar{\mathbb{Q}}_\ell)$$

- must be unramified outside $\{\ell\} \cup \underbrace{\{\text{fixed finite set of primes}\}}_{S}$
- and have same char. poly. of Frob_p for $p \notin S$.

<u>Example:</u> $\rho = (\mathbb{1})_\ell$, $S = \phi.$, $K = \mathbb{Q}.$

$F_p(T) = 1 - T \quad \forall p.$

$L(\rho, s) = \zeta(s)$ Riemann zeta function

<u>Example:</u> $K/\mathbb{Q}$ finite, $\rho = (\mathbb{1})$ rep of G_K

$L(\rho, s) = \zeta_K(s)$ Dedekind ζ-function.

<u>Example:</u> $K = \mathbb{Q}$, $\rho = (\chi_\ell)_\ell$

$F_p(T) = 1 - pT$

$$L(\rho, s) = \prod_p (1 - p\, p^{-s})^{-1}$$

$$= \zeta(s-1).$$

<u>Example:</u> $\rho = (V_\ell E^\vee)_\ell$

$L(\rho, s) = L(E, s).$

<u>Example:</u> $\rho : G_\mathbb{Q} \to GL_d(\mathbb{C})$ Artin rep. (i.e, factors through $G_\mathbb{Q} \to \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\rho} GL_d(\mathbb{C})$, some $K/\mathbb{Q}$ finite Galois.) Take $\rho_\ell = \rho$ for all ℓ. This gives the Artin L-function $L(\rho, s)$.

Tim
6-30-11
pg 4

Example: $E/\mathbb{Q}$, $\rho: Gal(F/\mathbb{Q}) \to GL_d(\mathbb{C})$ Artin representation.

$$\underbrace{\underbrace{(V_\ell E)^\vee \otimes \mathbb{C}}_{2\text{-dim}} \otimes \underbrace{\rho}_{d\text{-dim}}}_{2d\text{-dim}}$$

[To get char poly, take roots of each and multiply together pairwise to get roots of new char. poly.]

These form a compatible system.

Def: The twisted L-function
$$L(E,\rho,s) = L(V_\ell E^\vee \otimes \rho, s).$$

Exercise: $E/\mathbb{Q}$ good or mult. red. at 3. $L(E,s) = \sum_{n\geq 1} a_n n^{-s}$.

$\rho: Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \to \{\pm 1\}$ non-trivial 1-dim char.

Prove that
$$L(E,\rho,s) = \sum_{n\geq 1} \left(\frac{n}{3}\right) a_n n^{-s}.$$
(Explain why this doesn't work in the additive case.)

Artin Formalism:

Thm: $K/F/\mathbb{Q}$ number fields. Let ρ, σ be systems of ℓ-adic reps. of G_K.

(a) $L(\rho \oplus \sigma) = L(\rho)L(\sigma)$ (pf: look at char. polys)

(b) $L(\mathrm{Ind}_K^F \rho, s) = L(\rho, s)$ (Pf: Representation theory)

Main application: $E/\mathbb{Q}$ elliptic curve

K = number field

F = Galois closure of F.

$G = \mathrm{Gal}(F/\mathbb{Q})$

$H = \mathrm{Gal}(F/K)$

$$\begin{array}{c} F \\ {\scriptstyle H}\,| \\ K \\ | \\ \mathbb{Q} \end{array} \Bigg\} G$$

Then

$$L(E/K, s) = L(E, \underbrace{\mathbb{C}[G/H]}_{=\,\mathrm{Ind}_H^G \mathbb{1}}, s)$$

permutation rep. of G on left cosets of H in G., $\dim = [G:H]$

Proof: $L(E/K, s) = L(V_\ell(E/K)^\vee, s)$

Note $V_\ell(E/K) = V_\ell(E/\mathbb{Q})|_{G_K}$. So then

$$L(V_\ell(E/K)^\vee, s) \overset{\text{Artin formalism}}{=} L(\mathrm{Ind}_K^{\mathbb{Q}}(\mathrm{Res}_{\mathbb{Q}}^K V_\ell(E/\mathbb{Q})^\vee), s)$$

$$\overset{\text{Frob recip.}}{=} L(V_\ell(E/\mathbb{Q})^\vee \otimes \mathrm{Ind}_K^{\mathbb{Q}} \mathbb{1}, s)$$

$$= L(E, \mathbb{C}[G/H], s). \blacksquare$$

Note this is a representation theoretic proof, not really depending on elliptic curves.

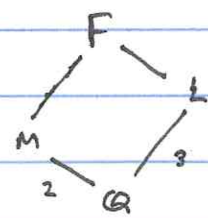
__Example:__ $F/\mathbb{Q}$ $\mathbb{Z}_3$-extension, $E/\mathbb{Q}$ elliptic curve.

$G = \mathbb{Z}_3$; reps $1, \chi, \bar{\chi}$. $K = F$, $H = 1$.

$$L(E/F, s) = L(E, \mathbb{C}[G], s) = L(E, 1 \oplus \chi \oplus \bar{\chi}, s) = L(E,s)\,L(E,\chi,s)\,L(E,\bar{\chi},s).$$

__Example:__ $E/\mathbb{Q}$ elliptic curve, $\mathrm{Gal}(F/\mathbb{Q}) \simeq S_3 = G$

G has 4 subgps up to conjugacy: $1, \mathbb{Z}_2, \mathbb{Z}_3, S_3$.



G has 3 irred. reps:

$\mathbb{1}$,

$\varepsilon = \mathrm{sgn}$,

2-dim ρ.

$$\mathbb{C}[G/G] = \mathbb{1}$$
$$\mathbb{C}[G/\mathbb{Z}_3] = \mathbb{1} \oplus \varepsilon$$
$$\mathbb{C}[G/\mathbb{Z}_2] = \mathbb{1} \oplus \rho$$
$$\mathbb{C}[G/1] = \mathbb{1} \oplus \varepsilon \oplus \rho \oplus \rho$$

If we pick $H \leq G$, then in the previous thm we get

$$\Rightarrow L(E/\mathbb{Q}, s) = L(E, \mathbb{1}, s)$$
$$L(E/M, s) = L(E, \mathbb{1}, s)\,L(E, \varepsilon, s)$$
$$L(E/L, s) = L(E, \mathbb{1}, s)\,L(E, \rho, s)$$
$$L(E/F, s) = L(E, \mathbb{1}, s)\,L(E, \varepsilon, s)\,L(E, \rho, s)^2.$$

Exercise: $F = \mathbb{Q}(i, \sqrt{-3})$, $E/\mathbb{Q}$ ell. curve.
Write down all $L(E/K, s)$ for $K \subseteq F$ and find a relation between them.

Exercise: $K = \mathbb{Q}(\sqrt{d})$, $\chi : \mathrm{Gal}(K/\mathbb{Q}) \to \pm 1$ non-trivial.
Prove that

$$\zeta_K(s) = \zeta_{\mathbb{Q}}(s)\, L(\chi, s).$$

(Prove directly, don't use Artin formalism.)

Conductors:

Let $\rho_\ell : G_{\mathbb{Q}_p} \to GL(V)$ d-dim. ℓ-adic rep.
(ex. $V_\ell(E/\mathbb{Q})^\vee$, $d=2$)

Recall ρ_ℓ unramified $\overset{\text{def}}{\Leftrightarrow} \rho_\ell(I_{\mathbb{Q}_p}) = 1$.
Conductor is a finer invariant of ramified reps.

Def: The conductor exponent is

$$n_{\rho,p} = (\text{tame part}) + (\text{wild part})$$

$$\begin{aligned} \text{tame part} &= \operatorname{codim} V^{I_{\mathbb{Q}_p}} \\ &= \dim V - \dim V^{I_{\mathbb{Q}_p}} \\ &= d - \deg F_p(\rho, T). \end{aligned}$$

$$\text{wild part} = \sum_{i=1}^{\infty} \frac{|G_i|}{|G_0|} \operatorname{codim} V_{ss}^{G_i}. \qquad (\text{is a finite sum})$$

($=0$ iff V is tamely ramified)

where

V_{ss} = semisimplification of V (kills N)

Tim
6-30-11
pg 8

V becomes a rep of some finite $G = Gal({}^{K}/\mathbb{Q}_p^{un})$ after s.s.
G_i ramification groups.

Example: $E/\mathbb{Q}_p$ an elliptic curve.

$$n_{V_\ell E^\vee, p} = \begin{cases} 0 + 0 & \text{good red.} \\ 1 + 0 & \text{mult red.} \\ 2 + \begin{cases} 0 & p \neq 2,3 \\ \geq 0 & p = 2,3 \end{cases} & \text{add. red.} \end{cases} \quad \text{(good, mult: semistable)}$$

Def: $E/\mathbb{Q}$ elliptic curve. The conductor

$$N = N_E = \prod_p p^{n_{V_\ell E^\vee, p}}$$ $\leftarrow$ this enters the functional equation for $L(E/\mathbb{Q}, s)$.

(similarly, K number field, E/K elliptic curve,

$$N_E = \prod_{\substack{\mathfrak{p} \\ \text{prime of } K}} \mathfrak{p}^{n_{V_\ell E^\vee, \mathfrak{p}}}$$ is an ideal in $\mathcal{O}_K$.

$N = \mathrm{Norm}_{K/\mathbb{Q}}(N_E) \cdot \Delta_{K/\mathbb{Q}}^2$. This N enters the functional equation for $L(E/K, s)$.)

Tim
7-1-11
PS1

Part III: Root Numbers:

Conjecturally all L-functions coming from systems of l-adic representations are entire and satisfy functional equation. (except for Riemann zeta)

We only know this

- for elliptic curves over $\mathbb{Q}$.
- (Hecke-Tate) for 1-dim. reps. (Hecke chars.)

$$\varphi : G_K \to \mathbb{C}^\times, \quad K = \#\text{ field}.$$

$L(\varphi, s)$ entire, satisfies

$$L^*(\varphi, 1-s) = W(\varphi) L^*(\varphi, s);$$

$$W(\varphi) = \prod_{\substack{v \\ \text{places} \\ \text{of } K}} \underbrace{W(\varphi|_{G_{K_v}})}_{\text{defined by Tate.}}$$

- Tate's Theory of signs in the functional eqn. for Hecke characters extends uniquely to all l-adic representations.

Fix a prime p, take all finite extensions $F/\mathbb{Q}_p$ and all Weil-Deligne reps.

$$\rho : G_F \to GL_d(\mathbb{C}), \quad \text{all } d.$$

<u>Theorem (Langlands-Deligne)</u>: There is a unique way to associate to each ρ its <u>ε-factor</u> $\varepsilon(\rho) \in \mathbb{C}^\times$ s.t.

1) (Multiplicativity) $\varepsilon(\rho_1 \oplus \rho_2) = \varepsilon(\rho_1)\varepsilon(\rho_2)$
2) (Inductivity in degree 0) If $\rho_1, \rho_2 : G_F \to GL_d(\mathbb{C})$

same d, then $\frac{\varepsilon(\rho_1)}{\varepsilon(\rho_2)} = \frac{\varepsilon(\mathrm{Ind}_F^K \rho_1)}{\varepsilon(\mathrm{Ind}_F^K \rho_2)}$.
F/K finite

(i.e., $\varepsilon(W) = \varepsilon(\mathrm{Ind}_F^K W)$ for virtual rep. W of dim. 0)

3) (1-dim.) For a quasi character $\varphi: G_F \to \mathbb{C}^\times$, its ε-factor $\varepsilon(\varphi)$ is as in Tate's thesis.

Tate's thesis: $\varphi: G_F \longrightarrow \mathbb{C}^\times$; via local reciprocity, can consider φ also as a map $F^\times \longrightarrow \mathbb{C}^\times$

$$\begin{tikzcd} F^\times \arrow[rr] \arrow[dr, "\text{local rec.}"'] & & \mathbb{C}^\times \\ & G_F^{ab} \arrow[ur, "\varphi"'] & \end{tikzcd}$$

$b_F := v_p(\Delta_{F/\mathbb{Q}_p})$

$h :=$ any elt. of $F^\times$ of valuation $-n_\varphi - b_F$,

ex. $\varpi_F^{-n_\varphi - b_F}$ w/ $n_\varphi =$ conductor of φ. (well, power on p..)

$$\varepsilon(\varphi) = \begin{cases} \displaystyle\int_{h\mathcal{O}_F^\times} \varphi(x^{-1}) e^{2\pi i \mathrm{Tr}_{F/\mathbb{Q}_p}(x)}\, dx & \varphi \text{ ramified} \\ \displaystyle\int_{h\mathcal{O}_F^\times} \varphi(h^{-1})\, dx = \frac{\varphi(h^{-1})}{|h|_F} \int_{\mathcal{O}_F^\times} dx & \varphi \text{ unram.} \end{cases}$$

These are just finite sums.

Def: The <u>local root number</u>

$$W(\rho) = \mathrm{sgn}(\varepsilon(\rho))$$

where for $z \in \mathbb{C}^\times$, $\mathrm{sgn}\, z = \frac{z}{|z|} \in S^1$.

Fact: $|\varepsilon(\rho)| = p^{n e/2}$.

Example: $\rho = \varphi$ unramified character.

$(I_F \to 1,\ \mathrm{Frob}_p \mapsto c \in \mathbb{C}^\times)$

Tim
7-1-11
pg3

(χ_ℓ is such a character.)

$$W(\varphi) = \frac{\varphi(h^{-1})}{|\varphi(h^{-1})|}$$ where we use that $\int_{\mathcal{O}_p^\times} dx \in \mathbb{R}_{>0}$, so drops out of sgn.

(under local recip. $\varpi_p \mapsto \mathrm{Frob}_p^{-1}$)

$$= \left(\frac{\varphi(\mathrm{Frob}_p)}{|\varphi(\mathrm{Frob}_p)|}\right)^{b_F} = (\mathrm{sgn}\, c)^{b_F}.$$

<u>Example:</u> $\varphi = \mathbb{1}$ trivial $\Rightarrow \varphi(\mathrm{Frob}_p) = 1 \Rightarrow W(\varphi) = 1$

$\varphi = \chi_\ell \Rightarrow \varphi(\mathrm{Frob}_p) = p \Rightarrow W(\varphi) = 1.$

<u>Properties (Tate - Deligne):</u> • W's are Multiplicative, inductive in degree 0 (b/c ε-factors satisfy these properties)

• $W(\rho \oplus \rho^\vee) = \underset{\{\pm 1\}}{\underset{\cap}{(\det \rho)(-1)}}$ ← image of -1 under the map $\underset{F^\times}{\underset{\cap}{-1}} \xrightarrow{\text{loc rec.}} G_F^{ab} \xrightarrow{\det \rho} \mathbb{C}^\times$

• $W(\rho_1 \otimes \rho_2) = W(\rho_1)^{\dim \rho_2}\, \mathrm{sgn}\left[(\det \rho_2)(\varpi_F^{n_{\rho_1} + \dim \rho_1\, b_F})\right]$

if ρ_2 is unramified.

• $$W(\rho) = W(\rho_{ss}) \frac{\mathrm{sgn}\det(-\mathrm{Frob} \mid (\rho_{ss})^{I_F})}{\mathrm{sgn}\det(-\mathrm{Frob} \mid \rho^{I_F})}.$$

~~Example: E/F good reduction~~

<u>Def:</u> E/F elliptic curve. The (local) root number

$$W(E/F) := W(\rho)$$

where $\rho = (V_\ell E)^\vee \otimes_{\mathbb{Q}_\ell} \mathbb{C}$.

Tim
7-1-11
pg 4

For an elliptic curve E over a number field K, the global root number

$$W(E/K) = (-1)^{\#\{v|\infty\}} \cdot \prod_{\substack{\mathfrak{p} \\ \text{fin primes} \\ \text{of } K}} W(E/K_{\mathfrak{p}}).$$

<u>Example:</u> E/F good reduction. Then N.O.S. implies ρ is unramified, so

$$W(E/F) = W(\rho) = W(\mathbb{1} \otimes \overset{\text{unr.}}{\rho})$$

$$= \underbrace{W(\mathbb{1})^2}_{1} \operatorname{sgn}\left[\underbrace{\det \rho}_{\chi_\ell^{-1}} (\varpi_F^{\cdots})\right]$$

$$= \operatorname{sgn} p^{\cdots}$$

$$= 1.$$

<u>Example:</u> E/F split mult. red.

$$V_\ell E = \begin{pmatrix} \chi_\ell & * \neq 0 \\ 0 & 1 \end{pmatrix}, \quad \rho = \begin{pmatrix} \chi_\ell^{-1} & 0 \\ * \neq 0 & 1 \end{pmatrix}$$

$$\rho_{ss} = \begin{pmatrix} \chi_\ell^{-1} & 0 \\ 0 & 1 \end{pmatrix}$$

$$W(E/F) = W(\rho) = \underbrace{W(\rho_{ss})}_{\substack{=1 \\ \text{as bef. b/c} \\ \text{unram.}}} \frac{\operatorname{sgn} \det(-\mathrm{Frob} \mid \rho_{ss}^{I_F})}{\operatorname{sgn} \det(-\mathrm{Frob} \mid \rho^{I_F})}$$

$$= \frac{\operatorname{sgn} \det\left(-\mathrm{Frob} \mid \begin{pmatrix} \chi^{-1} & 0 \\ 0 & 1 \end{pmatrix}\right)}{\operatorname{sgn} \det(-\mathrm{Frob} \mid (1))}$$

Tim
7-1-11
p95

$$= \frac{\operatorname{sgn} \det \begin{pmatrix} -p^{-1} & 0 \\ 0 & -1 \end{pmatrix}}{\operatorname{sgn} \det (-1)} = \frac{\operatorname{sgn}(p^{-1})}{\operatorname{sgn}(-1)} = \frac{1}{-1} = -1$$

Exercises: 1) In the non-split mult. red. case show that
$$W(E/F) = +1.$$

2) $E/\mathbb{Q}_7 \; : y^2 = x^3 + 7^2$

- Describe the action of $I_{\mathbb{Q}_7}$ on $T_\ell E$ $(\ell \neq 7)$
- Describe the action of $G_{\mathbb{Q}_p}$ on $T_\ell E$.
- Compute $W(E/\mathbb{Q}_7)$.

(Hint: The action should turn out to be abelian)