Let $E/\mathbb{Q}$. We saw a Gal. rep'n

$$G_{\mathbb{Q}} \curvearrowright T_\ell E = \varprojlim_{n \geq 1} E[\ell^n] \cong \mathbb{Z}_\ell^2$$

$$G_{\mathbb{Q}} \curvearrowright V_\ell E = T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell .$$

Recall: ℓ-adic cyclotomic character

$$G_{\mathbb{Q}} \curvearrowright \varprojlim \mu_{\ell^n}$$

Is $\{V_\ell E\}_\ell$ a compatible system of ℓ-adic reps?

Recall that this means:

- There is a fin set S s.t. $V_\ell E$ is unramified at all $p \notin S \cup \{\ell\}$.
- $\det(1 - T\mathrm{Fr}_p \mid V_\ell E^{I_p}) \in \mathbb{Q}_\ell[T]$ is actually in $\mathbb{Q}[T]$ and doesn't depend on $\ell \neq p$.

Ans: Yes!

Reducing ell. curves mod p

Let $E/\mathbb{Q}$ be an ell. curve, p be prime.
By a change of variables, it is possible to ensure the coefficients are in $\mathbb{Z}_{(p)}$.

If there is an equation for E s.t. reducing the coefficients mod p gives a nonsingular curve, then we say E has <u>good reduction</u> at p, write $\bar{E}$ for the resulting curve. Otherwise, E has <u>bad reduction</u> at p.

If E has good reduction at p, then $\overline{E}$ is an elliptic curve over $\mathbb{F}_p$! Moreover, the <u>reduction map</u>

$$\begin{array}{ccc} E(\overline{\mathbb{Q}}) & \longrightarrow & \overline{E}(\overline{\mathbb{F}_p}) \\ P & \longmapsto & \overline{P} \end{array}$$

is a group homomorphism!

<u>Obs</u> Let $\tau_p : \overline{\mathbb{F}_p} \longrightarrow \overline{\mathbb{F}_p}$ be Frobenius. Then

$$\{Q \in \overline{E}(\overline{\mathbb{F}_p}) : \tau_p(Q) = Q\} = \ker(1 - \tau_p) = \overline{E}(\mathbb{F}_p).$$

<u>Prop</u>

(1) Given an elliptic curve $E/\mathbb{Q}$, there is a natural number N, the <u>conductor</u>, s.t. E has good reduction at exactly the primes $p \nmid N$.

(2) If $p \nmid Nm$ then

$$E[m] \longrightarrow \overline{E}[m]$$

is injective.

<u>Prop</u> If $p \nmid Nl$, then $V_l E$ is unramified at p.

<u>Pf.</u> By the last proposition, we have

$$E[l^n] \hookrightarrow \overline{E}[l^n] \quad \text{for } l.$$

so

$$T_\ell E \hookrightarrow T_\ell \bar{E}.$$

If $\tau \in I_p$ (i.e. $\tau \in G_a$ s.t. τ acts as id on $\bar{\mathbb{F}}_p$) then for $P \in T_\ell E$, we have

$$\overline{P^\tau - P} = \bar{P}^\tau - \bar{P} = \bar{P} - \bar{P} = 0.$$

Then τ acts as id on $T_\ell E$ as well since $P^\tau - P = 0$. ∎

Prop If $p \nmid N\ell$, then

$$\det(1 - T\tau_p \mid V_\ell E) = 1 - a_p T + pT^2$$

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

In particular, $\det(1 - T\tau_p \mid V_\ell E) \in \mathbb{Q}[T]$ does not depend on ℓ.

Pf. (Sketch)

We will show that $\det(1 - T\tau_p \mid V_\ell \bar{E}) = 1 - a_p T + pT^2$.

Then since $V_\ell E \hookrightarrow V_\ell \bar{E}$, the minimal poly of τ_p on $V_\ell E$ divides $1 - a_p T + pT^2$. But also

$$\det(\tau_p \mid V_\ell E) = \chi_\ell(\tau_p) = p$$

(by a computation using the Weil pairing), so

$$\det(1 - T\tau_p \mid V_\ell E) = 1 - a_p T + pT^2 \text{ as well.}$$

Recall: $e_N : E[N] \times E[N] \longrightarrow \mu_N$ is compatible with the Gal. action! It gives a Galois-compatible pairing

$$e : T_\ell E \times T_\ell E \longrightarrow \varprojlim \mu_{\ell^n} \circlearrowleft G_{\mathbb{Q}}$$

(ℓ-adic cyclotomic char)

So it suffices to show

$\mathrm{Tr}(\sigma_p \mid V_\ell \bar{E}) = a_p$

$\det(\sigma_p \mid V_\ell \bar{E}) = p$.

Fun fact For a 2×2 matrix M,

$$\mathrm{Tr}\, M = 1 + \det M - \det(1 - M).$$

So it suffices to show:

(1) $\det(\sigma_p \mid T_\ell \bar{E}) = p$

(2) $\det(1 - \sigma_p \mid T_\ell \bar{E}) = \#\bar{E}(\mathbb{F}_p)$.

(1) A computation with the Weil pairing shows that if $\psi \in \mathrm{End}(E)$ then writing $\psi_\ell \in \mathrm{End}(V_\ell E)$ for the induced endomorphism, $\det(\psi_\ell) = \deg \psi$. So $\det(\sigma_p \mid V_\ell \bar{E}) = \deg(\sigma_p) = p$.

(2) $\deg(1 - \sigma_p) = \#\ker(1 - \sigma_p)$

$\det(1-\sigma_p)$ $= \#\bar{E}(\mathbb{F}_p)$.

□

Fun fact

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

$1+p$ is the "expected number of $\mathbb{F}_p$-points on $\bar{E}$"

So a_p = "error."

Hasse bound $|a_p| \leq 2\sqrt{p}$

Pf: $\#\bar{E}(\mathbb{F}_p) = \deg(1 - \tau_p)$.

Fun fact $\deg: \mathrm{End}(E) \longrightarrow \mathbb{Z}$ is a positive definite quadratic form.

For any pos. definite quadratic form d, can show

$$|d(\psi - \phi) - d(\psi) - d(\phi)| \leq 2\sqrt{d(\psi)d(\phi)}.$$

Applying that here:

$$|\deg(1-\tau_p) - \deg(1) - \deg(\tau_p)| \leq 2\sqrt{\deg(1)\deg(\tau_p)}$$

$$|\deg(1-\tau_p) - 1 - p| \leq 2\sqrt{p}. \qquad \square$$

So we have an L-function associated to an elliptic curve $E/\mathbb{Q}$: $L(E,s) = (*)\prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$.

The L-function of a wt. $2k$ Eigenform f on $\Gamma_0(N)$ was

$$L(f,s) = (*) \prod_{p \nmid N} \frac{1}{1 - a_p f + p^{2k-1-2s}}.$$

So if $2k=2$, these have a chance of converging!