Where we we?

Recall .0.1

We had an elliptic curve $E/\overline{\mathbb{Q}}$ with ordinary reduction at , $Q \in E$ a point of order N, and $C_0 = \ker(E[p] \to \widetilde{E}[p])$, with $p \nmid N$.

Lemma .0.1

If $C \subseteq E$, $|E| = p$, then

$$[\widetilde{E/C}, \widetilde{Q+C}] = \begin{cases} [\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}] & \text{if } C = C_0 \\ (\widetilde{E}^{\sigma_p^{-1}}, [p]\widetilde{Q}^{\sigma_p^{-1}}) & \text{if } C \neq C_0 \end{cases}.$$

where σ_p is the Frobenius map.

We did the proof when $C = C_0$ last time! The proof for $C \neq C_0$ is similar.

Fact: $E[p]$ has $p+1$ subgroups of order p (this is $(\mathbb{Z}/p\mathbb{Z})^2$, which we can view as a vector space). We had the reduction of the diamond operator, which when $(d, N) = 1$ had the form

$$\begin{aligned} \langle \widetilde{d} \rangle : \widetilde{S_1(N)} &\to \widetilde{S_1(N)} \\ [E, Q] &\mapsto [E, [d]Q]. \end{aligned}$$

We should have something like

$$\begin{aligned} T_p[E, Q] &= \sum_C [E/C, Q + C] \\ \widetilde{T}_p[\widetilde{E}, \widetilde{Q}] &= \sum_C [\widetilde{E/C}, \widetilde{Q+C}] \\ &= (\sigma_p + p\langle \widetilde{p} \rangle \sigma_p^{-1})[\widetilde{E}, \widetilde{Q}]. \end{aligned}$$

This is all in the case of ordinary reduction. In the supersingular case, we can take the same setup as before. This ends up showing that

$$[\widetilde{E/C}, \widetilde{Q+C}] = [\widetilde{E}^{\sigma_p}, \widetilde{Q}^{\sigma_p}] = [\widetilde{E}^{\sigma_p^{-1}}, [p]\widetilde{Q}^{\sigma_p^{-1}}].$$

This implies the same formula is true, but there's some collapsing so it is less interesting in some sense.

In general we have that

$$\begin{array}{ccc} S_1(N)'_{\text{good}} & \xrightarrow{T_p} & \text{Div}(S_1(N)'_{\text{good}}) \\ \downarrow & & \downarrow \\ \widetilde{S_1(N)}' & \xrightarrow[\sigma_p + p\langle \widetilde{p} \rangle \sigma_p^{-1}]{} & \text{Div}(\widetilde{S_1(N)}'). \end{array}$$

We define a map $\sigma = \sigma_{p_*} + \langle \widetilde{\sigma} \rangle \sigma_p^*$ from $\text{Pic}^0(\widetilde{X}_1)$ to itself.

It turns out $\text{Div}^0(\widetilde{S}'_1)$ to this picard group is surjective.

Theorem .0.2 (Eichler-Shimura)

We have a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X_1(N)}) & \xrightarrow[\sigma_{p_*}+\langle\widetilde{p}\rangle_*\sigma_p^*]{} & \mathrm{Pic}^0(\widetilde{X_1(N)}) \end{array}$$

There is also an $X_0(N)$ version.

$$\begin{array}{ccc} \mathrm{Pic}^0(X_0(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_0(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X_0(N)}) & \xrightarrow[\sigma_{p_*}+\sigma_p^*]{} & \mathrm{Pic}^0(\widetilde{X_0(N)}) \end{array}$$

Definition .0.1

We let $a_p(E) = p + 1 - \left|\widetilde{E}(\mathbb{F}_p)\right|$ when E has good reduction at p.

There is in fact a Lefschetz formula

$$\widetilde{E}(\mathbb{F}_p) = \sum_i (-1)^i \operatorname{tr}(\mathrm{Frob}(H^i_{\mathrm{et}}(E, \mathbb{Q}_p)).$$

This gives a good reason to care about $a_p(E)$. In H^0 we'll have a contribution of 1, and in H^2 we'll have a contribution of p. In H^1 we'll have what's called a Tate Module, and we're computing the trace of frobenius on this Galois representation.

Theorem .0.3

Supposing E has good reduction, $a_p(E) = 0$ if and only if E has supersingular reduction at p.

Supposing E has bad reduction, we define,

$$a_p(E) = \begin{cases} 1 & \text{if } E \text{ split} \\ -1 & \text{if } E \text{ nonsplit} \\ 0 & \text{if } E \text{ additive} \end{cases},$$

and this will fit into the general theory.

Proposition .0.4

$E/\mathbb{Q}$ has good reduction at p, then

$$[a_p(E)] = \sigma_{p_*}\sigma_p^*$$

on $\mathrm{Pic}^0(E)$.

We know $\widetilde{E}[\mathbb{F}_p] = \ker(\sigma_p - \mathrm{Id})$, $h_* \circ h^* = \deg(h)$, and so

$$\left|\widetilde{E}[\mathbb{F}_p]\right| = \deg(\sigma_p - 1) = (\sigma_p - 1)_*(\sigma_p - 1)^*.$$

If we FOIL this we get

$$\sigma_{p_*}\sigma_p^* + 1_*1^* - (\sigma_{p_*} + \sigma_p^*).$$

The modularity theorem can now be restated as

Theorem .0.5 (Modularity)

If $E/\mathbb{Q}$ is an elliptic curve and the conductor is N_E. Then there exists a newform $f \in S_2(\Gamma_0(N_E))$ such that $a_p(f) = a_p(E)$ for each prime p.

(Before: $X_0(N_E) \twoheadrightarrow E$).

Theorem .0.6

Let $E/\mathbb{Q}$ be a curve, with N_E a conductor, $\alpha : X_0(N) \twoheadrightarrow E$.

Then in fact there is an $f \in S_2(\Gamma_0(M_F))$ with $M_F \mid N$ so that $a_p(f) = a_p(E)$ for all $p \nmid N_E N$.

Proof. Recall that $S_2(\Gamma_0(N))$ has a basis $\bigcup_f \bigcup_{n|N} \bigcup_\sigma f^\sigma(n\tau)$ where f is a newform.

This told us we had an isogeny

$$\mathrm{Pic}^0(X_0(N)) \twoheadrightarrow \bigoplus_{f,n} A'_{f,\mathbb{C}},$$

and we can consider the dual isogeny, and then write down

$$\oplus_{f,n} A'_{f,\mathbb{C}} \xrightarrow{\prod_{f,n} a_p(f) - a_p(E)} \oplus_{f,n} A'_{f,\mathbb{C}}$$

$$\mathrm{Pic}^0(X_0(N), \mathscr{C}) \xrightarrow[T_p - a_p(E)]{} \mathrm{Pic}^0(X_0(N), \mathbb{C}) \xrightarrow{\alpha_*} \mathrm{Pic}^0(E_{\mathbb{C}}).$$

We now have some facts

- If $a_p(f) \neq a_p(E)$ then the top map $\oplus_n A'_{f,\mathbb{C}}$ (should be believable, it's nonzero)
- The square commutes.
- The composition of bottom maps is 0.

If for some p, $a_p(f) \neq a_p(E)$, then the image of $\oplus_n (A'_f)_{\mathbb{C}}$ lies in $\ker \alpha_*$. Now suppose for each f, there is a p such that $a_p(f) \neq a_p(E)$. This implies that the image of $\oplus_{f,n} A'_{f,\mathbb{C}} \subseteq \ker(\alpha_*)$.

But this is bad because the map above $\oplus_{f,n} A'_{f,\mathbb{C}} \to \mathrm{Pic}^0(X_0(N), \mathbb{C})$ is surjective. This would imply $\mathrm{Pic}^0(E_{\mathbb{C}})$ is trivial!!!

But this isn't true, so there is a p with $a_p(f) \neq a_p(E)$.