Contents

1 Motivation and statement

1.1 L-function for modular forms

The Eichler-Shimura relation relates the eigenvalues of the Hecke operator with the trace of Frobenius (on an abelian variety; if we take a quotient we can get an elliptic curve). An important corollary is that for every $f \in S_2(\Gamma_1(N))$, there exists some elliptic curve E_f for which $L(s, f) = L(s, E_f)$.

First, let's define the L-function and explain why we expect L-functions of modular forms and elliptic curves to correspond to one another.

Definition 1.1: Let $f \in S_2(\Gamma)$ for some congruence subgroup $\Gamma \supseteq \Gamma(N)$. Write $f = \sum_{n\ge 1} a_n e^{2\pi i\tau} = \sum_n a_n q^n$ ($q = e^{2\pi i\tau}$). Note: we can have fractional values of n in the sum?Define the L-function of f by

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Why do we form an L-function? Whenever we have an almost-multiplicative function a_n, if we let them be coefficients of a Dirichlet series, we get a nice Euler product expansion.

Here, the multiplicativity comes from that of the Hecke operators. Recall that we have for Hecke operators on $M_k(\mathrm{SL}_2(\mathbb{Z}))$, that

$$\begin{aligned} T(mn) &= T(m)T(n) \qquad m \perp n, \\ T(p^\alpha) &= T(p)T(p^{\alpha-1}) - p^{k-1}T(p^{\alpha-2}), \end{aligned}$$

and that the Hecke operators commute. (Where the relations come from: The lattices of index mn are the lattices of index m inside the lattices of index n, with a correction factor if $m \not\perp n$.) If we could treat the $T(m)$ as numbers, then this gives a Euler product expansion

$$\sum_{n=1}^{\infty} \frac{T_n}{n^s} = \prod_p \frac{1}{1 - T(p)p^{-s} + p^{k-1}p^{-2s}}.$$

We can't do this, but we can "operate" this on an *eigenform* f, and the relation on T_m's becomes a relation on the eigenvalues of the T_m's on f. Normalizing f so that $a_1 = 1$, the eigenvalue of T_m on f is just a_m. Then we get

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \frac{1}{1 - a_p p^{-s} + p^{k-1}p^{-2s}}.$$

Note two things.

1. We'll want Hecke operators on $\Gamma_1(N)$ instead of $\mathrm{SL}_2(\mathbb{Z})$. The relation involving T_{p^α} will be a bit different (involve the diamond operator). (In general, recall that Hecke operators for a congruence subgroup are defined by $f \mapsto (z \mapsto \sum_{\gamma_i} f(\gamma z))$ where $\Gamma \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right) \Gamma = \bigsqcup \Gamma \gamma_i$.)

2. We'll take $k = 2, k - 1 = 1$. In this case, the Euler product really looks like the Euler product for an elliptic curve, which we'll review below.

1.2 L-functions for elliptic curves

Definition 1.2: Let E be an elliptic curve. Define the local L-function of E at p by

$$L(E/\mathbb{F}_p, s) = \det(1 - \mathrm{Frob}_p\, t | V_\ell E^{I_p}).$$

This is the familiar $\frac{1}{1-a_p p^{-s}+pp^{-2s}}, a_p = \mathrm{Tr}(\mathrm{Frob}_p) = p + 1 - |E(\mathbb{F}_p)|$ when there is good reduction at p (here reduction is injective on $E[\ell]$, i.e., inertia, which can't change the residue modulo p, acts trivially on it). When reduction is bad, it degenerates into a constant or linear term.

Define the L-function for E as a product of local L-functions

$$L(E, s) = \prod_p L(E/\mathbb{F}_p, s) = \prod_{p \text{ good reduction}} \frac{1}{1 - a_p p^{-s} + pp^{-2s}} \prod_{p \text{ bad reduction}} (\cdots).$$

So for the L-functions to correspond, we want to relate the eigenvalues of Hecke with the trace of Frobenius.

1.3 What does Hecke have to do with Frobenius?

The intuition is taken from here: `http://mathoverflow.net/questions/19390/intuition-behind-the-`

The Hecke operator should really be thought of as a correspondence.

Definition 1.3 (Take 1)**:** Let A, B be sets. A correspondence $A \to B$ is a map that takes each $a \in A$ to a finite set $c(a) \subset B$. A correspondence $A \to A$ induces a map on functions on A: $f \mapsto \left(z \mapsto \sum_{b \in c(a)} f(b)\right)$. (We'll actually include a constant factor below.)

Here is a more general way to think about it.

Definition 1.4 (Take 2)**:** A correspondence is (Z, X, φ, ψ) where Z is a set and $\varphi, \psi : Z \to X$ are functions. (For instance, Z is the graph of a function, in $X \times X$.) We recover the correspondence as defined above by taking $c = \psi \circ \varphi^{-1}$.

$$\begin{tikzcd}
 & Z \arrow[dl, "\varphi"'] \arrow[dr, "\psi"] & \\
X \arrow[rr, dashed, "c"] & & X.
\end{tikzcd}$$

This defines correspondences on points. We'll actually want more structure (Z to be a scheme), but this is the basic idea.

Definition 1.5 (Take 3)**:** A correspondence is (Z, X, φ, ψ) where Z, X are schemes, $\varphi, \psi : Z \to X$ are morphisms. The correspondence gives a map $X \to \operatorname{Div}(X)$ defined as in the diagram below, and induces a map on the Picard groups (which can be given scheme structure as the Jacobians), notated by the maps below.

eq:e-s-pico

$$\begin{tikzcd}
X \arrow[d] & Z \arrow[l, "\varphi"'] \arrow[r, "\psi"] \arrow[d] & X \arrow[d] \\
\operatorname{Div} X \arrow[r, "\varphi^*"] & \operatorname{Div} Z \arrow[r, "\psi_*"] & \operatorname{Div} X \\
\operatorname{Div}^0 X \arrow[u] \arrow[r] \arrow[d] & \operatorname{Div}^0 Z \arrow[u] \arrow[r] \arrow[d] & \operatorname{Div}^0 X \arrow[u] \arrow[d] \\
\operatorname{Pic}^\circ X \arrow[r, "\operatorname{Pic}\varphi"] & \operatorname{Pic}^\circ Z \arrow[r, "\operatorname{Alb}\psi"] & \operatorname{Pic}^\circ X
\end{tikzcd} \tag{1}$$

There is a natural map $X \to \operatorname{Pic}^\circ X$? I think it's $x \mapsto [x] - [x_0]$. Do we need a basepoint, or is it canonical?

As a correspondence, on the Div level the Hecke operator for $M_k(\mathrm{SL}_2(\mathbb{Z}))$ is

$$T_n : [\Lambda] \mapsto \sum_{[\Lambda:\Lambda']=n} [\Lambda'].$$

(We get the usual Hecke operator by $(T_n F)(\Lambda) = n^{k-1} \sum_{[\Lambda:\Lambda']=n} F(\Lambda')$, where F is the function on lattices corresponding to f, $F(\langle 1, \tau \rangle) = f(\tau)$.) Now *lattices correspond to elliptic curves*, so the pairs (Λ, Λ') with $[\Lambda : \Lambda'] = n$ correspond to pairs of elliptic curves with an isogeny of degree n, $\varphi : E \to E'$. When $n = p$, we ask: what are the isogenies of degree p? There are only 2 possibilities, Frobenius and the dual of Frobenius; the Frobenius occurs once (with the lattice Λ_0' that is the kernel of reduction) and the rest are dual of Frobenius.

Some notes.

1. Actually, we'll want to look at pairs (E, P) instead of just E, so the correspondence is on $X_1(N)$ instead of $X_0(N)$.
2. What is the space Z in the correspondence? We'll have to create another moduli space to parametrize not just elliptic curves but maps $E \to E'$ of degree p. We can do this.
3. We should think of T_n as acting on the Jacobian, $\mathrm{Pic}^\circ X \to \mathrm{Pic}^\circ X = \mathrm{Jac}(X_1(N))$. (The Jacobian "turns a variety into an abelian variety" so we can add on it.) The Frobenius map is defined on the Jacobian, and we relate the eigenvalues of Hecke with the Frobenius on the Jacobian.

We'll now go through all of this more rigorously.

1. First, we'll take go through an "elementary" proof (but there may be some holes here due to compatibility, defining varieties over different rings, etc.) following Rohrlich's Modular Curves in [CSS97].
2. Then we'll give a scheme-theoretic proof following Conrad in [Con].

1.4 Theorem statement

The theorem we'll prove is the following.

Theorem 1.6 (Eichler-Shimura, Theorem 5.16 in [Con])**:** On $J_p := \mathrm{Pic}^\circ_{X_0(N)/\mathbb{Z}[\frac{1}{N}]}(\overline{\mathbb{F}_p}) = \mathrm{Pic}^\circ X_0(N)/\overline{\mathbb{F}_p}$, let F be the Frobenius, and let $(T_p)_*$ be the map induced from the Hecke correspondence.[1]

Then

$$(T_p)_* = F + \langle p \rangle_* F^\vee$$

The most important corollary is the following. First, some notation.

1. Let $T_1(N)$ be the Hecke algebra $\mathbb{Q}(\{T_p : p \nmid N\}, \{\langle p \rangle : p \nmid N\})$ acting with the $()_*$ action on $\mathrm{Pic}^\circ_{X_0(N)/\mathbb{Z}[\frac{1}{N}]}(\overline{\mathbb{Q}})$.[2]
2. Write $V_\ell(N) := V_\ell(\mathrm{Pic}^\circ_{X_1(N)/\mathbb{Z}[\frac{1}{N}]}(\overline{\mathbb{Q}}))$.
3. Let $\rho_{N,\ell}$ be the representation $G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(V_\ell(N)) \cong \mathrm{GL}_2(\mathbb{Q}_\ell \otimes T_1(N))$. (It is unramified at $p \nmid N\ell$.) (The Hecke operator acts freely because its action on the inner product defined last time is self-adjoint and...?.)

Using Eichler-Shimura and the fact about the Atkin-Lehner involution from the last talk,

$$w_\zeta^{-1} F w_\zeta = \langle p \rangle_*^{-1} F,$$

we can prove the following (See Conrad's notes).

[1] Note this is not *a priori* defined over $\mathbb{Z}[\frac{1}{N}]$. See 3.2 for a discussion of this.

[2] Alternatively if we define Hecke operators using matrices we can define it as simply generated by T_A, $A \in \mathrm{SL}_2(\mathbb{Z})$.

Theorem 1.7 (Theorem 5.16 in [Con])**:** The characteristic polynomial $\mathrm{Frob}_{\mathfrak{p}}$ on $V_\ell(X)$ considered as a $\overline{\mathbb{Q}_\ell} \otimes_{\mathbb{Q}} T_1(N)$-vector space is

$$X^2 - (T_p)_* X + \langle p \rangle_* \, p.$$

To get a 2-dimensional representation over $\mathbb{Q}_\ell$ instead of the larger algebra $\overline{\mathbb{Q}_\ell} \otimes_{\mathbb{Q}} T_1(N)$, we do the following: choose a newform f and mod out by the maximal ideal $\mathfrak{p}_f \subset T_1(N)$ corresponding to f. See the last lecture.

2 Elementary approach

Here we can't quite prove Theorem 1.6 the way it's stated because it's not obvious how to define $(T_p)_*$ for J_p. We'll prove something in the same spirit, however, basically the statement lifted up to $\mathbb{Q}$ instead of in $\overline{\mathbb{F}_p}$.

Theorem 2.1 (Eichler-Shimura congruence relation)**:** thm:es2 Let $\sigma_{\mathfrak{p}} \in G(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at $\mathfrak{p}$. Then for $\ell \neq p$,

$$T_p = \sigma_{\mathfrak{p}} + p \, \langle p \rangle \, \sigma_{\mathfrak{p}}^{-1}$$

as endomorphisms of $J_1(N)[\ell^n]$. (Here $J_1(N) = \mathrm{Pic}^\circ X_1(N)/\overline{\mathbb{Q}}$.)

2.1 Moduli spaces: intro

Recall

$$\begin{aligned}
\Gamma(N) &= \left\{ M \in \mathrm{SL}_2(\mathbb{Z}) : M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\} \\
\Gamma_1(N) &= \left\{ M \in \mathrm{SL}_2(\mathbb{Z}) : M \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\} \\
\Gamma_0(N) &= \left\{ M \in \mathrm{SL}_2(\mathbb{Z}) : M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}
\end{aligned}$$

and

$$\Gamma(N) \overset{N}{\trianglelefteq} \Gamma_1(N) \overset{\varphi(N) = N \prod_{p|N}(1-\frac{1}{p})}{\trianglelefteq} \Gamma_0(N) \overset{N \prod_{p|N}(1+\frac{1}{p})}{\subseteq} \mathrm{SL}_2(\mathbb{Z}).$$

Define

$$\begin{aligned}
Y_1(N) &= \mathcal{H}/\Gamma_1(N) \\
Y_0(N) &= \mathcal{H}/\Gamma_0(N)
\end{aligned}$$

and let $X_i(N)$ be the compactifications. We need to do several things.

1. Understand $Y_1(N), Y_0(N)$ as moduli spaces. Also come up with a moduli space for the Z we'll use in the Hecke correspondence.

2. Show how a general $\mathcal{H}/\Gamma$ can be defined as an *algebraic* variety, Γ a congruence subgroup. We understand the X_i, Y_i as moduli spaces over any algebraically closed field.

3. Define the Hecke correspondence (Z, X, φ, ψ).

2.2 Understanding moduli spaces over $\mathbb{C}$

We first understand how quotients of $\mathcal{H}$ parametrize elliptic curves. This won't be enough for us as we want to work over other fields $(\overline{\mathbb{Q}}, \overline{\mathbb{F}_p})$, but is a good starting point for intuition.

We have the following.

1. $Y_0(1) = \mathcal{H}/\operatorname{SL}_2(\mathbb{Z})$ parametrizes isomorphism classes of elliptic curves over $\mathbb{C}$, via
$$\tau \mapsto \mathbb{C}/\left\langle \tau, 1 \right\rangle.$$
$\operatorname{SL}_2(\mathbb{Z})$ are exactly the linear transformations that stabilize lattices.

2. $Y_0(N) = \mathcal{H}/\Gamma_0(N)$ parametrizes isomorphism classes of elliptic curves over $\mathbb{C}$, along with a cyclic subgroup of order N, via
$$\tau \mapsto \mathbb{C} = (\mathbb{C}/\left\langle \tau, 1 \right\rangle, \left\langle \frac{1}{N} \right\rangle).$$
We check that the stabilizer of any $(\mathbb{C}/\left\langle \tau, 1 \right\rangle, \left\langle \frac{1}{N} \right\rangle)$ is exactly $\Gamma_0(N)$. We have
$$\gamma(\mathbb{C}/\left\langle \tau, 1 \right\rangle, \left\langle \frac{1}{N} \right\rangle) = (\mathbb{C}/\left\langle a\tau + b, c\tau + d \right\rangle, \left\langle \frac{c\tau + b}{N} \right\rangle).$$
This generates the same group of order N exactly when $a \perp N$ and $c \equiv 0 \pmod{N}$.

3. $Y_1(N) = \mathcal{H}/\Gamma_1(N)$ parametrizes isomorphism classes of elliptic curves over $\mathbb{C}$, along with a point of order N, via
$$\tau \mapsto \mathbb{C} = \left(\mathbb{C}/\left\langle \tau, 1 \right\rangle, \frac{1}{N}\right).$$
Here fewer $\gamma \in \operatorname{SL}_2(\mathbb{Z})$ fix the data: the difference is that c has to be $1 \pmod{N}$ now, and we get $\Gamma_1(N)$.

4. Next we want to parametrize $Y_0(N, p)$, isomorphism classes of $(\varphi : E \to E', \langle P \rangle)$, φ of degree p and $\langle P \rangle$ a cyclic subgroup of order N intersecting $\ker\varphi$ only trivially.

   We claim $Y_0(N, p) = \mathcal{H}/\Gamma_0(N, p)$ where
$$\Gamma_0(N, p) = \left\{ M \in \operatorname{SL}_2(\mathbb{Z}) : M = \begin{pmatrix} * & 0 \pmod{N} \\ 0 \pmod{p} & * \end{pmatrix} \right\} \supset \Gamma_0(\gcd(N, p)),$$
via
$$\tau \mapsto \mathbb{C} = \left(\mathbb{C}/\left\langle \tau, 1 \right\rangle, \left\langle \frac{1}{p} \right\rangle, \left\langle \frac{\tau}{N} \right\rangle\right).$$
Indeed,
$$\gamma(\mathbb{C}/\left\langle \tau, 1 \right\rangle, \left\langle \frac{1}{p} \right\rangle, \left\langle \frac{\tau}{N} \right\rangle) = (\mathbb{C}/\left\langle a\tau + b, c\tau + d \right\rangle, \left\langle \frac{c\tau + d}{p} \right\rangle, \left\langle \frac{a\tau + b}{N} \right\rangle),$$
so γ fixes the data exactly when $c \equiv 0 \pmod{p}$ and $b \equiv 0 \pmod{N}$.

   Note: There is something to check here: we hit all possibilities this way. For $N \perp p$, note $\left\langle \frac{1}{p}, \frac{\tau}{N} \right\rangle$ is a cyclic subgroup of order pN, so it's the same as specifying an element of order pN, and SL_2 acts transitively (fixing the Weil pairing). For $p \mid N$, what happens? (I don't think we really need this case.

5. Now we parametrize $Y_1(N,p)$, isomorphism classes of $(\varphi : E \to E', P)$, φ of degree p and P a point subgroup of order N, generating a subgroup intersecting $\ker\varphi$ only trivially.

   We claim $Y_1(N,p) = \mathcal{H}/\Gamma_1(N,p)$ where

   $$\Gamma_1(N,p) = \left\{ M \in \mathrm{SL}_2(\mathbb{Z}) : M = \begin{pmatrix} 1 \pmod p & 0 \pmod N \\ 0 \pmod p & * \end{pmatrix} \right\} \supset \Gamma_0(\gcd(N,p)).$$

   The analysis is the same as above except now we need $d \equiv 1 \pmod p$, so that $\frac{c\tau+d}{p}$ is the same as $\frac{1}{p}$.

Note: we can further mod out by $\{\pm I\}$ if we wish, working inside $\mathrm{PSL}_2(\mathbb{Z})$ instead of $\mathrm{SL}_2(\mathbb{Z})$; the only change this makes is to make the action of the quotient group faithful. Also, considering these spaces as quotients of $\mathcal{H}/\Gamma(N)$ or $\mathcal{H}/\Gamma(\gcd(N,p))$, we can think of the actions as being of $\mathrm{SL}_2(\mathbb{Z}/N)$ or $\mathrm{PSL}_2(\mathbb{Z}/N)$.

Note we have bad reduction at $0, 1728, \infty$ because either the automorphism group is greater than $\mathbb{Z}/2$, or the elliptic curve is degenerate. In the first case, different points get identified.

2.3 Galois action on modular forms, Moduli spaces over K

The above is unsatisfactory for our purposes because we need to define $Y_0(N)$, etc. over different fields K in order to parametrize elliptic curves (and related data) over K.

To do this, we will consider the field extension $K(t, E[N])$ of $K(t) \cong K(j)$ and subfield extensions that are fixed by subgroups of $G(K(t, E[N])/K(t))$, for K algebraically closed. We define the moduli spaces as the curves corresponding to these fixed fields. Before we can do anything else, however, we have to compute $G(K(t, E[N])/K(t))$. We do this for $\mathbb{C}$ first, and find that it is "as large as can be."

We know that $\mathcal{H}/\Gamma_0(N)$ can be defined over $\mathbb{Q}$: its equation is given by the modular polynomial $\Phi_N(X,Y)$ which has coefficients in $\mathbb{Z}$. (Φ_N is defined as the minimal polynomial of $\mathbb{C}(j(\tau), j(N\tau))$).

How do we do this more generally, make sure all the spaces we work with can be defined over $\mathbb{Q}$, and the morphisms are also defined over $\mathbb{Q}$?

Rather than do something for each space separately, we can get everything in one fell swoop by showing that $\mathcal{H}/\Gamma(N)$ can be defined over $\mathbb{Q}$, and then using Galois theory.

First note that the theory of elliptic curves over $\mathbb{C}(t)$ is very nice. In fact, the endomorphism ring is the nicest that we can hope for, and we get that the action of Galois on $E[N]$ is exactly the entire $\mathrm{GL}_2(\mathbb{Z}/N)$, no questions asked! When we try to substitute concrete values for t, that's where the messy number theory and representation theory come in.

Theorem 2.2: Let E be an elliptic curve over $\mathbb{C}(t)$ with j-invariant equal to t. Then there is an isomorphism/representation

$$\rho : G(\mathbb{C}(t, E[N])/\mathbb{C}(t)) \xrightarrow{\cong} \mathrm{SL}_2(\mathbb{Z}/N)$$
$$G(\mathbb{C}(t, x(E[N])/\mathbb{C}(t)) \xrightarrow{\cong} \mathrm{PSL}_2(\mathbb{Z}/N)$$

given by choosing a basis of $E[N] \cong \mathbb{Z}/N \times \mathbb{Z}/N$ and looking at the action of Galois on this basis.

Proof. First, we note the reason for SL_2 rather than GL_2: the Weil pairing is invariant under any Galois group element because the Galois group fixes $\mathbb{C}(t) \supseteq \mu_n$. Choosing a basis of $E[N]$, the Weil pairing is just the determinant. The linear transformations that preserve the determinant are the ones in SL_2. Because ρ is determined by its action on $E[N]$, we have an injection $\rho : G(\mathbb{C}(t, E[N])/\mathbb{C}(t)) \hookrightarrow \mathrm{SL}_2(E[N])$. We show it is surjective.

In fact we give an explicit way to construct the field extension in terms of analytic functions: we find the missing field in the following:

eq:Ctjt

$$\begin{tikzcd}
\mathbb{C}(t, x(E[N])) \arrow[r, equal, "\sim"] \arrow[d, dash] & ? \arrow[d, dash] \\
\mathbb{C}(t) \arrow[r, equal, "\sim"] & \mathbb{C}(j).
\end{tikzcd} \tag{2}$$

(It is easier to just work with x-coordinates. I don't this is necessary... however we only get the correspondence with modular functions if we look at x-coordinates.) It suffices to consider the elliptic curve

$$y^2 = 4x^3 - \frac{27t}{t-1728}x - \frac{27t}{t-1728}.$$

Why? (Any two elliptic curves over a field K that become isomorphic over an algebraic closure are quadratic twists of each other.) Here t is the j-invariant. Under the isomorphism in (2), our task now becomes to *find analytic functions that map τ to a point of order N on the curve $y^2 = 4x^3 - \frac{27j(\tau)}{g(\tau)-1728}x - \frac{27j(\tau)}{j(\tau)-1728}$.*

We can parametrize an elliptic curve analytically, if it is in Weierstrass form. Let's put the elliptic curve in Weierstrass form. Firstly, E can be put into the form

$$y^2 = 4x^3 - g_2 x - g_3.$$

Recall that the substitution $x \mapsfrom c^2 x, y \mapsfrom c^3 y$ makes the coefficients change as $A \mapsfrom \frac{A}{c^4}, B \mapsfrom \frac{B}{c^6}$. We hence want $c = \sqrt[4]{\frac{27j/(j-1728)}{g_2}}$. But $j = \frac{1728 g_2^3}{g_2^3 - 27g_3^2}$ by definition so $\frac{27j}{j-1728} = \frac{g_2^3}{g_3^2}$, and $\sqrt[4]{\frac{27j/(j-1728)}{g_2}} = \sqrt{\frac{g_2}{g_3}}$. The desired change of variables is

$$x \mapsfrom \frac{g_3}{g_2}x, \qquad y \mapsfrom \left(\frac{g_3}{g_2}\right)^{\frac{3}{2}}.$$

Then given τ, the map

$$\begin{aligned} \mathbb{C}/\langle \tau, 1\rangle &\to (E : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)) \\ z &\mapsto \left(\frac{g_2}{g_3}\wp(z; \langle \tau, 1\rangle), \left(\frac{g_3}{g_2}\right)^{\frac{3}{2}} \wp(z; \langle \tau, 1\rangle)\right) \end{aligned}$$

parametrizes the elliptic curve corresponding to the lattice $\langle \tau, 1\rangle$. To get a point of order N from τ, we evaluate at $(r \quad s)\begin{pmatrix}\tau\\1\end{pmatrix}$ to get the functions

$$x_{r,s}(\tau) = \frac{g_2(z)}{g_3(\tau)}\wp\left(\frac{1}{N}(r \quad s)\begin{pmatrix}\tau\\1\end{pmatrix}; \langle \tau, 1\rangle\right).$$

(Let the y function be $y_{r,s}$.) We have

$$\mathbb{C}(t, x(E[N])) \cong \mathbb{C}(j, \{x_{r,s} : (r, s) \not\equiv (0, 0) \pmod N\}).$$

This is an algebraic extension of $\mathbb{C}(j)$ because the functions satisfy

$$P_N\left(x_{r,s}, \frac{27j}{j-1728}, \frac{27j}{j-1728}\right) = 0$$

where $P \in \mathbb{Z}[X, A, B]$ is the Nth division polynomial: $P(w, A, B) = 0$ iff w is the x-coordinate of a (affine) N-torsion point on the elliptic curve $y^2 = 4x^3 + Ax + B$. (We can show, but won't need, $\mathbb{C}(j, \{x_{(r,s)}\}) \cong \mathbb{C}(j, X)/P_N\left(X, \frac{27j}{j-1728}, \frac{27j}{j-1728}\right)$.)

We find $G(\mathbb{C}(j, \{x_{r,s} : (r, s) \not\equiv (0, 0) \pmod N\})/\mathbb{C}(j))$ explicitly. For each $A \in \mathrm{PSL}_2(\mathbb{Z}/N)$, define Af by $(Af)(\tau) = f(A\tau)$.

This action is...

1. well-defined because $A \in \Gamma(N)$ acts trivially on the $x_{r,s}$ and $-I \in \Gamma(N)$ acts trivially because $\wp$ is even, and
2. faithful because $\wp(z) = \wp(z')$ iff $z \in \pm z' + \langle \tau, 1\rangle$.

Hence the Galois group equals $\mathrm{PSL}_2(\mathbb{Z}/N)$. □

Remark 2.3: The functions $x_{r,s}$ are modular functions on $\Gamma_0(N)$. Indeed, in light of item (a) above the only thing we have to check is that they are holomorphic on cusps. We omit the proof.

We have $\mathbb{C}(t, \{x_{r,s}\}) = \mathbb{C}(t, x(E[N]))$ by construction of the $x_{r,s}$. We have $G(\mathbb{C}(t, \{x_{r,s}\})/\mathbb{C}(t)) = \mathrm{PSL}_2(\mathbb{Z}/N)$. As

$$\mathbb{C}(t, \{x_{r,s}\}) \hookrightarrow M(\Gamma(N)), \qquad G(M(\Gamma(N))/M_0(1)) \hookrightarrow \mathrm{PSL}_2(\mathbb{Z}/N)$$

we conclude that $\cong$ actually holds.

Corollary 2.4: Over $\mathbb{Q}$, we get instead

$$G(\mathbb{Q}(t, E[N])/\mathbb{Q}(t)) \cong \mathrm{GL}_2(\mathbb{Z}/N).$$

Proof. The field extension $\mathbb{C}(t, E[N]) \cong \mathbb{C}(j, x_{r,s}, y_{r,s})/\mathbb{C}(j)$ can be defined over $\mathbb{Q}(j)$ instead of $\mathbb{C}(j)$ since the polynomial that $j, x_{r,s}, y_{r,s}$ satisfy has coefficients in $\mathbb{Q}$.

Note that $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(t, E[N])$ because any field extension containing $E[N]$ must contain ζ_n (the proof uses the Weil pairing). Now we have

$$G(\mathbb{Q}(t, E[N])/\mathbb{Q}(\zeta_n, t)) \hookrightarrow \mathrm{SL}_2(\mathbb{Z}/N):$$

elements of the Galois group fix ζ_n so fix the Weil pairing, so the image is in $\mathrm{SL}_2(\mathbb{Z}/N)$ rather than $\mathrm{GL}_2(\mathbb{Z}/N)$. Since this is an isomorphism when the field is extended to $\mathbb{C}$, it must be an isomorphism here. Now

$$G(\mathbb{Q}(t, E[N])/\mathbb{Q}(t)) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N)$$

and by counting, it must actually be equal. □

2.4 Moduli spaces over K

Now we give a different definition of the moduli spaces so that they still parametrize the correct data even if we change from $\mathbb{C}$ to another algebraically closed field K (we'll need $\overline{\mathbb{Q}}$ or $\overline{\mathbb{F}_p}$). We'll show that over $\mathbb{C}$ this is equivalent to the earlier description by giving maps from the compact Riemann surface to the algebraic varieties we'll define here.

The fundamental result we use is the following.

Theorem 2.5: Let K be algebraically closed. There is a contravariant equivalence of categories between field extensions of $K(t)$ and curves over K.

Let $X(N)$ be the curve corresponding to the field extension $K(t, x(E[N]))/K(t)$. We claim outside of points of bad reduction, the points on this curve correspond to an elliptic curve along with a N-torsion point, up to automorphism (so for instance $[E, P] = [E, -P]$. Warning: we have to exclude $t = \infty$ because the elliptic curve is degenerate there. For $t = 0, 1728$ the automorphism group is larger so more than just $\pm P$ are identified—this might be a problem (is it?), so exclude these values as well.

The correspondence is as follows. Consider the universal elliptic curve over $K(t)$, and base-extend to $K(t, E[N])$. The points $x \in X$ correspond to valuations on $K(t, E[N])$ (what algebraic geometry fact is this?). $K(t)$ simply corresponds to $\mathbb{P}^1(K)$. Suppose t_0' lies above $t_0 \in \mathbb{P}^1(K)$, and E has good reduction at t_0. ($t_0 \neq 0, 1728, \infty$.) Not sure about this actually: The field extension corresponding to the fiber above t_0 is $K(E_{t_0}[N])/K$, and the points are exactly the N-torsion points of t_0. Explain bad reduction here.

Let $\mathcal{P}$ be some data depending on some points $P_i \in E[N]$, for example a single point P_1, the cyclic subgroup generated $\langle P_1 \rangle$, or a pair $(\langle P_1 \rangle, P_2)$ where P_1 is of order m_1, $\langle P_2 \rangle \cap \langle P_1 \rangle = \phi$, such that $\mathrm{GL}_2(\mathbb{Z})$ operates transitively on the set of possible data. (It's not worth it to make this precise.) Recall that whenever we have a group action G on S, then $G/\operatorname{Stab}(s) \xrightarrow{\cong} \operatorname{Orbit}(s)$. Suppose $H = \operatorname{Stab}(s)$. Letting $X(N)$ be as before, we claim that outside of bad points, $X(n)^H$ parametrizes the data. Indeed, the points above $X(n)^H$ are exactly the orbits of s.

We can apply this to the same spaces as in 2.1:

1. $X_0(1)$: no data.
2. $X_0(N)$: a subgroup $\langle P_2 \rangle$, where the action is on a basis P_1, P_2.
3. $X_1(N)$: a point P_2 of order N, where the action is on a basis P_1, P_2.

4. $X_0(N,p)$: Move to $\mathrm{GL}_2(\mathbb{Z}/\gcd(N,p))$. A group $\langle P_1\rangle$ of order p and a point P_2 of order N such that $\langle P_1\rangle \cap \langle P_2\rangle = \{0\}$.

5. $X_1(N,p)$: Move to $\mathrm{GL}_2(\mathbb{Z}/\gcd(N,p))$. A point P_1 of order p and a point P_2 of order N, such that $\langle P_1\rangle \cap \langle P_2\rangle = \{0\}$. [3]

If $G(K(t,E[N])/K(t)) = \mathrm{GL}_2(\mathbb{Z}/N))$ (or $\mathrm{SL}_2(\mathbb{Z}/N)$) then the respective stabilizers are the same as in 2.1 (the P_1 here correspond to τ and P_2 here correspond to 1) except that in the case of GL_2 we allow the determinant to be not necessarily 1, and in $\Gamma_1(N)$ we allow matrices of the form $\left(\begin{smallmatrix} \pm 1 & b \\ * & c \end{smallmatrix}\right) \pmod N$. Check this! The quotients of $\mathrm{GL}_2(\mathbb{Z}/N)$ induced here are the same as the quotients of $\mathrm{SL}_2(\mathbb{Z}/N)$ induced there. Check this!

When G is smaller than $\mathrm{GL}_2(\mathbb{Z}/N)$, this still works; the subgroups H will be smaller though. When not in characteristic 0, we must be careful. We need the fact (not easy) that $X_1(N)$ can be defined over $\mathbb{Z}[\frac{1}{N}]$. See p. 66 in Conrad for a discussion. For $p \nmid N$, this construction then goes through.

The parametrized data is the same as in 2.1, without mention to $\tau \in \mathbb{C}$.

2.5 Hecke correspondence

Note that points of $X_0(N,p)$ represent isomorphism classes

$$\varphi : E \to E', \langle P\rangle, \qquad \deg\varphi = p, P \text{ of order } n, \langle P\rangle \cap \ker\varphi = \phi$$

We want to define the Hecke correspondence T_p on $X_0(N)$ as taking $[E,\langle P\rangle]$ to all the $[E',\langle P\rangle]$ where there is a map $\varphi : E \to E'$ of degree p and $P \nmid \ker\varphi$. Putting this in the framework of 1.4, $Z = X_0(N,p)$ and $X = X_0(N)$, we define the correspondence as follows.

Definition 2.6: Define the **Hecke correspondence** $(X_0(N,p), X_0(N), \Phi, \Psi)$ by

eq:hecke-corr

$$\begin{tikzcd}
& {[\varphi : E \to E', \langle P\rangle]} \arrow[dl, mapsto, "\Phi"'] \arrow[dr, mapsto, "\Psi"] & \\
{[E, \langle P\rangle]} & & {[E', \langle P\rangle].}
\end{tikzcd} \tag{3}$$

Concretely on $\mathcal{H}$, it sends

$$\begin{tikzcd}
& {\left(\langle \tau, 1\rangle, \left\langle \frac{\tau}{p}\right\rangle, \frac{1}{N}\right)} \arrow[dl, mapsto, "\Phi"'] \arrow[dr, mapsto, "\Psi"] & \\
{\left(\langle \tau, 1\rangle, \left\langle \frac{1}{N}\right\rangle\right)} & & {\left(\left\langle \frac{\tau}{p}, 1\right\rangle, \left\langle \frac{1}{N}\right\rangle\right).}
\end{tikzcd}$$

Similarly define the Hecke correspondence $(X_1(N,p), X_1(N), \Phi, \Psi)$, but with P instead of $\langle P\rangle$.

[3] It's not obvious from this definition that the action is transitive—what if P_1, P_2 are multiples of the same point? But the intuition here is wrong because $N \perp p$. For example, we can send $P_1 = \frac{1}{3}$ and $P_2 = \frac{1}{2}$ to $P_1 = \frac{\tau}{3}$ and $P_2 = \frac{1}{2}$ by sending $\frac{1}{6} \mapsto \frac{1}{2} + \frac{2}{3}\tau$. See Note.

Note these are maps of algebraic varieties. For Φ this is clear as it is just the projection map. For Ψ we check that this map corresponds to a field extension. We ask: what data stabilizes $(\left\langle \frac{\tau}{p}, 1\right\rangle, \left\langle \frac{1}{N}\right\rangle)$? It's a group isomorphic (conjugate) to $\Gamma_0(N)$, the group fixing $(\langle \tau, 1\rangle, \left\langle \frac{1}{N}\right\rangle)$, so corresponds to a field extension isomorphic to the field extension corresponding to $X_1(N)$. We hence get a map to $X_1(N)$. How does this whole argument actually work?

To get from a correspondence to a map in the form $[P] \mapsto \sum [Q]$, we simply take the map on divisors. This also defines a map on the Jacobians—as a group the Jacobian is just the divisor class group. We have a map $X_0(N) \to \mathrm{Div}(X_0(N))$, which we compute explicitly. It's compatible with the map on Jacobians.

We can compute the explicit action of Hecke. (Sometimes the Hecke operators are defined in this explicit way.)

Proposition 2.7: As maps $X_i(N) \to \mathrm{Div}(X_i(N))$, we have

$$X_0(N): \qquad T_p(\tau) = \sum_{i=0}^{p-1} \left[\frac{\tau+i}{p}\right] + \begin{cases} [p\tau], & p \nmid N \\ 0, & p \mid N. \end{cases} \tag{4}$$

$$X_1(N): \qquad T_p(\tau) = \sum_{i=0}^{p-1} \left[\frac{\tau+i}{p}\right] + \begin{cases} [p\,\langle p\rangle\,\tau], & p \nmid N \\ 0, & p \mid N. \end{cases} \tag{5}$$

Note the similarity to elliptic curves in that we get more stuff when we have "good reduction."

Note: no ramification in maps Φ, Ψ outside the cusps? This is important in making all the coefficients 1.

Proof. We use the description of the Hecke correspondence in (3). T_p will take a lattice Λ representing an elliptic curve to the lattices Λ' containing Λ as an lattice of index p, such that Λ' doesn't intersect $\langle P\rangle$ except trivially. The lattices of super-index p of $\langle \tau, 1\rangle$ are $\left\langle \frac{\tau+i}{p}, 1\right\rangle$ and $\left\langle \frac{1}{p}, \tau\right\rangle$ which is homothetic to $\langle 1, p\tau\rangle$ (recall homothetic lattices are identified).

$$[\langle \tau, 1\rangle] \mapsto \sum_{i=0}^{p-1}[\left\langle 1, \frac{\tau+i}{p}\right\rangle, \left\langle \frac{1}{N}\right\rangle] + \underbrace{\left[\left\langle \frac{1}{p}, \tau\right\rangle, \left\langle \frac{1}{N}\right\rangle\right]}_{?}.$$

The last one is valid only if $p \nmid N$, since otherwise the subgroup intersects $\left\langle \frac{1}{p}, \tau\right\rangle$ more than trivially. This gives (4). The reasoning for $X_1(N)$ is similar, except now we care about the actual point. We find

$$\left[\left\langle \tau, \frac{1}{p}\right\rangle, \frac{1}{N}\right] = \left[\langle p\tau, 1\rangle, \frac{p}{N}\right].$$

Hence we have to multiply τ by a matrix of the form $\left(\begin{smallmatrix} p^{-1} & 0 \\ 0 & p \end{smallmatrix}\right) \pmod N$ so that $1 \mapsto c\tau + d \equiv p \pmod N$; this is exactly the diamond operator. (This didn't appear for X_0 because the matrix is in $\Gamma_0(N)$ so acts as the identity on $X_0(N)$.) □

We now characterize all isogenies of E over $\mathbb{F}_p$.

Proposition 2.8: Suppose that E has ordinary reduction at p. Let $\varphi : E \to E'$ be an isogeny of degree p. Then either $E' \cong E^{(p)}, \varphi = \varphi_p$ (the Frobenius) or $\widehat{\varphi} : E' \to E \cong E'^{(p)}$ (so the dual to the Frobenius).

$\cong$ or $=$?

Proof. Because E is ordinary, $E(\overline{\mathbb{F}_p})[p] \cong \mathbb{Z}/p$.

We use the following fact: every isogeny φ between elliptic curves factors uniquely as $\lambda \circ \varphi_p^r$ where λ is separable and φ_p^r is the Frobenius (hence totally inseparable). Note $\deg \varphi = p^r \deg \lambda$. Consider 2 cases.

1. $\varphi : E \to E'$ factors as $\lambda \circ \varphi_p$. Then λ is an isomorphism so $E' \cong E^{(p)}$ and φ is just φ_p (under this identification?).

2. $\varphi : E \to E'$ is separable. Now $\widehat{\varphi} \circ \varphi = [p]$ is inseparable so $\widehat{\varphi}$ is totally inseparable. By item 1, it is the Frobenius. φ is the unique dual to the Frobenius $E' \to E$, the Vershiebung. (Note that there is one possibility for E' up to isomorphism, because they are all isomorphic to $E^{(p^{-1})}$, taking the pth root of all the coefficients of E.)

□

We just have this for ordinary – OK? Consider $p \nmid N$. Then T_p maps E to $p+1$ curves E'. Only 1 of them can have kernel corresponding to the kernel of Frobenius, and the others are duals to Frobenius.

Claim: if $\varphi : E \to E'$ reduces to the Frobenius map iff $\ker \varphi = \ker(E(\overline{\mathbb{Q}}) \to \widetilde{E}(\mathbb{F}_p))$. Proof: Let E correspond to $\langle \omega_1, \omega_2 \rangle$ and the map $E \to E'$ correspond to $\mathbb{C}/\langle \omega_1, \omega_2 \rangle \mapsto \mathbb{C}/\left\langle \omega_1, \frac{\omega_2}{p} \right\rangle$. We have maps

$$\begin{tikzcd}
E(\overline{\mathbb{Q}}) \arrow[r, "\varphi"] \arrow[d] & E'(\overline{\mathbb{Q}}) \arrow[r, "\widehat{\varphi}"] \arrow[d] & E(\overline{\mathbb{Q}}) \arrow[d] \\
\widetilde{E}(\overline{\mathbb{F}_p}) \arrow[r, "\widetilde{\varphi}"] & \widetilde{E}'(\overline{\mathbb{F}_p}) \arrow[r, "\widetilde{\hat{\varphi}}"] & \widetilde{E}(\overline{\mathbb{F}_p}).
\end{tikzcd}$$

Because E, E' are isogenous, they have the same kind of reduction (why?), namely ordinary. So taking p-torsion points gives

$$\begin{tikzcd}
\mathbb{Z}/p \times \mathbb{Z}/p \arrow[r, "{(1,p)}"] \arrow[d] & \mathbb{Z}/p \times \mathbb{Z}/p \arrow[r, "{(p,1)}"] \arrow[d] & \mathbb{Z}/p \times \mathbb{Z}/p \arrow[d] \\
\mathbb{Z}/p \arrow[r, "\widetilde{\varphi}"] & \widetilde{\mathbb{Z}}/p \arrow[r, "\widetilde{\hat{\varphi}}"] & \mathbb{Z}/p
\end{tikzcd}$$

The kernel of the reduction is the same as $\ker \varphi$ iff the left map is projection along the first factor. The left map is projection along the first factor iff the middle map is projection along the first factor (the easiest way to see this is to look at p^2-torsion points instead. If the left map is π_1, then we can choose basis for $\mathbb{Z}/p^2 \times \mathbb{Z}/p^2$ so it's still π_1 here. The second factor maps to 0 along either way of the left square, so the middle map is π_1. If the left map is not π_1 the argument is similar). This is true iff the bottom right map is 0, i.e., $|\ker \widetilde{\widehat{\varphi}}| = \deg \widetilde{\widehat{\varphi}}$, so $\widetilde{\widehat{\varphi}}$ is separable and the bottom left map is purely inseparable, i.e., the Frobenius. Working with actual groups is messy here. Working with group schemes is nicer, see the scheme-theoretic proof.

In all other cases, the map is the dual to Frobenius.

Proposition 2.9: Define $\mathcal{E}\mathrm{ll}_1(N)(K)$ as the isomorphism classes of $(E/K, P)$ such that P is a point of order N on E. Then for $p \nmid N$ there is a natural reduction map $\mathcal{E}\mathrm{ll}_1(N)(\overline{\mathbb{Q}})_{\text{good}} \to \mathcal{E}\mathrm{ll}_1(N)(\overline{\mathbb{F}_p})$ where "good" means the subset of elliptic curves with good reduction. Then

$$\widetilde{T_p([E,P])} = [\widetilde{E}^p, \widetilde{P}^p] + p[\widetilde{E}^{p^{-1}}, p\widetilde{P}^{p^{-1}}].$$

Proof. Of the $p+1$ maps $E \to E'$, one of the maps reduces to Frobenius, namely, the map with $\ker \varphi$ equalling the kernel of reduction. The other p map to Vershiebung. □

Letting $\sigma_{\mathfrak{p}}$ be the map taking $[E, P] \mapsto [E', P']$ where $[E', P']$ is any elliptic curve reducing to $[\widetilde{E}^p, \widetilde{P'}^p]$. Does this actually correspond to the Frobenius map *on the Jacobian*? Let $\mathcal{E}\mathrm{ll}_1(N)(\overline{\mathbb{Q}})_{\text{ord}}$ be the subset of $\mathcal{E}\mathrm{ll}_1(N)(\overline{\mathbb{Q}})_{\text{good}}$ consisting of $[E, P]$ such that E has ordinary reduction at p. Then we get

$$T_p = \sigma_{\mathfrak{p}} + p\,\langle p\rangle\,\sigma_{\mathfrak{p}}^{-1}$$

as maps

$$\mathcal{E}\mathrm{ll}_1(N)(\overline{\mathbb{Q}})_{\text{ord}} \to \mathrm{Div}(\mathcal{E}\mathrm{ll}_1(N)(\mathbb{Q})_{\text{ord}})/\ker(\mathrm{red}_{\mathfrak{p}}).$$

Now the map T_p is computed from the correspondence $(X_1(N,p), X_1(N), \Phi, \Psi)$, so it is compatible with the actual map on Jacobians $\mathrm{Alb}\,\Psi \circ \mathrm{Pic}\,\Phi$.

From this we get Theorem 2.1.

3 Scheme-theoretic approach

3.1 Background on group schemes

We consider (FCGp/k) where FCGp stands for "finite locally free commutative group scheme."

Each such scheme can be decomposed in a canonical way, and the pieces can be identified using an explicit classification of all objects in (FCGp/k). We'll apply this to $E[p]$.

Definition 3.1: Let k be any field. Let $G \in (\mathrm{FCGp}/k)$.

1. G is **infinitesimal** if G is connected. (This is true iff $G_{\overline{k}}$ is connected, iff $G_{\text{top}} = \{\cdot\}$ (as G has a finite number of points), iff $G_{\overline{k},\,\text{top}} = \{\cdot\}$.)

2. G is **multiplicative** (diagonalizable) iff $G^\vee$ is étale.

3. G is **bi-infinitesimal** (local-local) iff G and $G^\vee$ are infinitesimal.

In summary,

$G \setminus G^\vee$	étale	infinitesimal
étale	char $k \neq p$	unipotent
infinitesimal	multiplicative	bi-infinitesimal

(The étale-étale case cannot happen unless char $k \neq p$.)

The classification of FCGp/k of order p (I haven't actually defined order) is easy.

Proposition 3.2: Let char $k = p$. The only FCGp/k of order p are the following, where the position in the table corresponds to the classification above.

	$\underline{\mathbb{Z}/p\mathbb{Z}}$
μ_p	α_p

Here

1. $\underline{G}$ is a constant group scheme,
2. $\mu_p = \ker([p] : \mathbb{G}_m \to \mathbb{G}_m)$
3. $\alpha_p := \ker(F_{\mathbb{G}_a} : \mathbb{G}_a \to \mathbb{G}_a)$.

Moreover, $\alpha_p^\vee \cong \alpha_p$.

The following decomposition is key.

Proposition 3.3: Suppose char $k = p$ and let $G \in (p\text{-FCGp}/k)$. (That is, some $[p^r]$ is the zero morphism.)

1. (Connected-étale sequence) There exists a canonical exact sequence

   $$0 \to G^0 \to G \to G_{\text{ét}} := G/G^0 \to 0$$

   where G^0 is the connected component of the identity element e, G^0 is infinitesimal, and $G_{\text{ét}}$ is étale.

   The sequence splits.

2. There is a unique decomposition

   $$G \cong G_{\text{mult}} \times G_{\text{bi}} \times G_{\text{ét}}$$

   where G_{mult} is multiplicative (with étale dual), G_{bi} is bi-infinitesimal, and $G_{\text{ét}}$ is étale. We have $G^0 = G_{\text{mult}} \times G_{\text{bi}}$.

The multiplicative part becomes the étale part in the dual and vice versa; the bi-infinitesimal part stays the same.

Now we apply this theory to elliptic curves over characteristic p. We can not only classify $E[p]$ as *groups* (it can be $\mathbb{Z}/p$ or $\{0\}$, in which case we say E is ordinary or supersingular), but classify $E[p]$ as *group schemes*

Proposition 3.4: Let E be an elliptic curve over k of characteristic p.

1. If E is ordinary, then $E[p] = \mu_p \times \underline{\mathbb{Z}/p}$.
2. If E is supersingular, then $E[p] = \alpha_p \times \alpha_p$.

Proof. We'll just need the case where E is ordinary, so we prove that. The étale part of $E[p]$ is nontrivial because $E[p]^0$ has 1 point while $E[p]$ has p points. Note $E[p]$ has order p^2 (I haven't defined order). An elliptic curve is canonically isomorphic to its dual, so the same is true of $E[p]^\vee = E^\vee[p] = E[p]$. The étale parts of $E, E^\vee$ are both nontrivial and they get matched up with the multiplicative parts of $E^\vee, E$. The only étale FCGp/k of order p is $\underline{\mathbb{Z}/p}$, so we get $E[p] = \mu_p \times \underline{\mathbb{Z}/p}$. □

3.2 Relating the different fields

At various stages of the proof, we need to think of the Jacobian $\mathrm{Pic}^\circ_{X_1(N)/\mathbb{Z}[\frac{1}{N}]}$ over different fields $\mathbb{Q}, \mathbb{Q}_p, \mathbb{F}_p$. What does working in these different fields accomplish for us?

For greatest generality, we seek the "smallest" scheme that $X_0(N)$ can be defined over; it is $\operatorname{Spec} \mathbb{Z}[\frac{1}{N}]$. Why? Then for every scheme S with $S \to \operatorname{Spec} \mathbb{Z}[\frac{1}{N}]$, we can define the Jacobian over S. Notably, we can define the $\mathbb{F}_p$-points because we have $\operatorname{Spec} \overline{\mathbb{F}_p} \to \operatorname{Spec} \mathbb{Z}[\frac{1}{N}]$ coming from $\mathbb{Z}[\frac{1}{N}] \to \overline{\mathbb{F}_p}$. (Basically we can reduce a variety modulo p as long as p doesn't appear in the denominator in the coefficients.)

The problem is that we defined $(T_p)_*$ from the correspondence $(X_1(N,p), X_1(N), \Phi, \Psi)$ and $X_1(N,p)$, as a quotient of $X_1(Np)$ is only defined over $\mathbb{Z}[\frac{1}{Np}]$.

We have a map $\mathrm{Pic}^\circ_{X_1(N)/\mathbb{Z}[\frac{1}{N}]} \to \mathrm{Pic}^\circ_{X_1(N)/\mathbb{Z}[\frac{1}{N}]}$ defined over $\mathbb{Z}[\frac{1}{Np}]$ but not necessarily over $\mathbb{Z}[\frac{1}{N}]$.

Definition 3.5 (Néron models)**:** Let R be a Dedekind domain with fraction field K. Let A_K be a smooth separated scheme (for instance, an abelian variety) defined over K. The **Néron model** of A over R (if it exists) is A_R defined over R, satisfying the following. (1) Its generic fiber (basechange to K) is A_K. (2) If X is smooth separated over R with generic fiber X_K and $\varphi : X_K \to A_K$, there is a unique $\varphi_R : X_R \to A_R$ making the following commute.

$$\begin{tikzcd}
 & & & X_K \arrow[rr, "\varphi"] \arrow[llld] \arrow[rd] & & A_K \arrow[llld] \arrow[ld] \\
X_R \arrow[rr, dashed, "\varphi_R"] \arrow[rd] & & A_R \arrow[ld] & & \operatorname{Spec} K \arrow[llld] & \\
 & \operatorname{Spec} R & & & &
\end{tikzcd}$$

Theorem 3.6: Every abelian variety has a Néron model.

Becuse $\mathrm{Pic}^\circ_{X_1(N)/\mathbb{Z}[\frac{1}{N}]}$ is an abelian variety, it follows we can define $(T_p)_*$ over $\mathbb{Z}[\frac{1}{N}]$.

Since we don't have a direct definition, though, we need to work in $\overline{\mathbb{Q}_p}$ or $\overline{\mathbb{Q}}$ rather than $\overline{\mathbb{F}_p}$. This is fine because $\overline{\mathbb{F}_p}$-points can always be lifted to $\overline{\mathbb{Q}_p}$. Note also that we don't in fact lose any ℓ^n-torsion points going from $\overline{\mathbb{Q}_p}$ to $\overline{\mathbb{Q}}$, as V_ℓ is equal to $\mathbb{Q}_\ell^{2g}$ in both cases.

3.3 Proof of Theorem 1.6

1. First, it suffices to check on a Zariski-dense subset. (If $f, g : X \to Y$ agree on a Zariski-dense subset, then they agree on all points. If they agree on all points and X, Y are reduced, then they are equal as morphisms (?).)

2. The ordinary points on $X_1(N)(\overline{\mathbb{F}_p})$—points representing (E, P) where E is ordinary—are dense. This is because E is ordinary iff $j(E) \notin \mathbb{F}_{p^2}$, and this excludes finitely many isomorphism classes $[E, P]$'s.

3. We calculate $(F + \langle p \rangle_* F^\vee) : J_p(\overline{\mathbb{F}_p}) \to J_p(\overline{\mathbb{F}_p})$. This is straightforward using $p = FF^\vee = F^\vee F$; we get that the map on Pic° is induced by the map on Div^0

$$[E, P] \mapsto [E^{(p)}, P^{(p)}] + p[E^{(p^{-1})}, pP^{(p^{-1})}].$$

4. For $(T_p)_*$ we can't directly calculate its action on J_p because the definition was indirect. Instead we have to lift to something that can map to $\mathrm{Spec}\, \mathbb{Z}[\frac{1}{Np}]$.

   We calculate on $R := \mathbb{Z}_p^{\mathrm{ur}}$. Why? First, note that the reduction map $Y_1(N)(R) \twoheadrightarrow Y_1(N)(\overline{\mathbb{F}_p})$ is surjective because R is henselian (because we chose $R = \mathbb{Z}_p^{\mathrm{ur}}$).

   Over $\overline{K} = \overline{\mathbb{Q}_p}$, the points of $X_1(N)$ are classes $[E, P]$ over $\overline{K}$, and $(T_p)_*$ acts as defined by the correspondence: it acts on Pic° as the map induced from Div^0:

$$[E, P] \mapsto \sum_C [E/C, P \pmod{C}]$$

   where the sum is over subgroup-schemes of order p, and hence contained in $E[p]$. (order again) *Suppose E is ordinary.* We claim that exactly one of the E/C is μ_p and the other p are $\underline{\mathbb{Z}/p}$.

   (a) We know $E[p]$ has a *unique* connected-étale sequence $1 \to \mu_p \to E[p] \to \underline{\mathbb{Z}/p\mathbb{Z}}$, so exactly 1 term is $[E/\mu_p, P \pmod{\mu_p}]$.

   (b) The only other possibility is $E/(\mathbb{Z}/p\mathbb{Z})$ and so appears p times. We match this up with 3, by showing $E/\mu_p \cong E^{(p)}$ and $E/\underline{\mathbb{Z}/p} \cong E^{p^{-1}}$.

5. The only 2 isogenies are the Frobenius and its dual. The Frobenius map $\varphi_p : E \to E^{(p)}$ has kernel that is trivial *on points*; since it is (finite flat) of degree p, the kernel must be μ_p. On points, the Vershiebung map $\varphi_p^\vee$ has nontrivial kernel (because on points, $[p]$ has nontrivial kernel, and φ_p has trivial kernel), so it must be $\underline{\mathbb{Z}/p\mathbb{Z}}$. Thus the terms in (a) and (b) in item 4 are $[E^{(p)}, P^{(p)}]$ and $[E^{(p)}, pP^{(p^{-1})}]$. (We get the P from $\varphi_p \varphi_p^\vee = \varphi_p^\vee \varphi_p = [p]$.)

Combining 3 and 5, we see that $F + \langle p \rangle_* F^\vee$ and $(T_p)_*$ match on the Zariski-dense subset of points corresponding to ordinary elliptic curves, so by (1) they are equal as morphisms.

References

[Con] B. Conrad. Appendix by brian conrad: The shimura construction in weight 2.

[CSS97] G. Cornell, J. Silverman, and G. Stevens, editors. *Modular Forms and Fermat's Last Theorem*. Springer-Verlag, 1997.