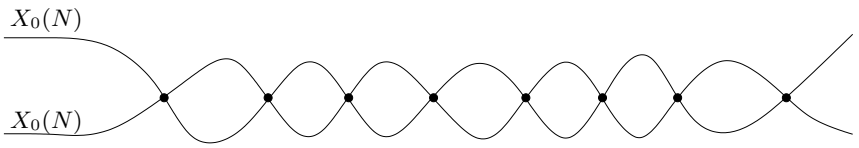


FIGURE 1.6.1. The reduction mod p of the Deligne-Rapoport model of $X_0(Np)$

1.6 The Eichler-Shimura Relation

Suppose $p \nmid N$ is a prime. The Hecke operator T_p and the Frobenius automorphism Frob_p induce, by functoriality, elements of $\mathrm{End}(J_0(N)_{\mathbf{F}_p})$, which we also denote T_p and Frob_p. The Eichler-Shimura relation asserts that the relation

$$T_p = \mathrm{Frob}_p + p\,\mathrm{Frob}_p^{-1} \tag{1.6.1}$$

holds in $\mathrm{End}(J_0(N)_{\mathbf{F}_p})$. In this section we sketch the main idea behind why (1.6.1) holds. For more details and a proof of the analogous statement for $J_1(N)$, see [1].

Since $J_0(N)$ is an abelian variety defined over $\mathbf{Q}$, it is natural to ask for the primes p such that $J_0(N)$ have good reduction. In the 1950s Igusa showed that $J_0(N)$ has good reduction for all $p \nmid N$. He viewed $J_0(N)$ as a scheme over $\mathrm{Spec}(\mathbf{Q})$, then "spread things out" to make an abelian scheme over $\mathrm{Spec}(\mathbf{Z}[1/N])$. He did this by taking the Jacobian of the normalization of $X_0(N)$ (which is defined over $\mathbf{Z}[1/N]$) in $\mathbf{P}^n_{\mathbf{Z}[1/N]}$.

The Eichler-Shimura relation is a formula for T_p in characteristic p, or more precisely, for the corresponding endomorphisms in $\mathrm{End}(J_0(N)_{\mathbf{F}_p})$) for all p for which $J_0(N)$ has good reduction at p. If $p \nmid N$, then $X_0(N)_{\mathbf{F}_p}$ has many of the same properties as $X_0(N)_{\mathbf{Q}}$. In particular, the noncuspidal points on $X_0(N)_{\mathbf{F}_p}$ classify isomorphism classes of enhanced elliptic curves $\underline{E} = (E, C)$, where E is an elliptic curve over $\mathbf{F}_p$ and C is a cyclic subgroup of E of order N. (Note that two pairs are considered *isomorphic* if they are isomorphic over $\overline{\mathbf{F}}_p$.)

Next we ask what happens to the map $T_p : J_0(N) \to J_0(N)$ under reduction modulo p. To this end, consider the correspondence

$$\begin{array}{ccc} & X_0(Np) & \\ {\scriptstyle\alpha}\swarrow & & \searrow{\scriptstyle\beta} \\ X_0(N) & & X_0(N) \end{array}$$

that defines T_p. The curve $X_0(N)$ has good reduction at p, but $X_0(Np)$ typically does not. Deligne and Rapaport [4] showed that $X_0(Np)$ has relatively benign reduction at p. Over $\mathbf{F}_p$, the reduction $X_0(Np)_{\mathbf{F}_p}$ can be viewed as two copies of $X_0(N)$ glued at the supersingular points, as illustrated in Figure 1.6.1.

The set of supersingular points

$$\Sigma \subset X_0(N)(\overline{\mathbf{F}}_p)$$

is the set of points in $X_0(N)$ represented by pairs $\underline{E} = (E, C)$, where E is a supersingular elliptic curve (so $E(\overline{\mathbf{F}}_p)[p] = 0$). There are exactly $g+1$ supersingular points, where g is the genus of $X_0(N)$.

Consider the correspondence $T_p : X_0(N) \rightsquigarrow X_0(N)$ which takes an enhanced elliptic curve $\underline{E}$ to the sum $\sum \underline{E}/D$ of all quotients of $\underline{E}$ by subgroups D of order p.

This is the correspondence

$$\begin{array}{ccc} & X_0(pN) & \\ {\scriptstyle\alpha}\swarrow & & \searrow{\scriptstyle\beta} \\ X_0(N) & & X_0(N), \end{array} \tag{1.6.2}$$

where the map α forgets the subgroup of order p, and β quotients out by it. From this one gets $T_p : J_0(N) \to J_0(N)$ by functoriality.

Remark 1.6.1. There are many ways to think of $J_0(N)$. The cotangent space $\operatorname{Cot} J_0(N)$ of $J_0(N)$ is the space of holomorphic (or translation invariant) differentials on $J_0(N)$, which is isomorphic to $S_2(\Gamma_0(N))$. This gives a connection between our geometric definition of T_p and the definition, presented earlier, of T_p as an operator on a space of cusp forms.

The Eichler-Shimura relation takes place in $\operatorname{End}(J_0(N)_{\mathbf{F}_p})$. Since $X_0(N)$ reduces "nicely" in characteristic p, we can apply the Jacobian construction to $X_0(N)_{\mathbf{F}_p}$.

Lemma 1.6.2. *The natural reduction map*

$$\operatorname{End}(J_0(N)) \hookrightarrow \operatorname{End}(J_0(N)_{\mathbf{F}_p})$$

is injective.

Proof. Let $\ell \nmid Np$ be a prime. By [11, Thm. 1, Lem. 2], the reduction to characteristic p map induces an isomorphism

$$J_0(N)(\overline{\mathbf{Q}})[\ell^\infty] \cong J_0(N)(\overline{\mathbf{F}}_p)[\ell^\infty].$$

If $\varphi \in \operatorname{End}(J_0(N))$ reduces to the 0 map in $\operatorname{End}(J_0(N)_{\mathbf{F}_p})$, then $J_0(N)(\overline{\mathbf{Q}})[\ell^\infty]$ must be contained in $\ker(\varphi)$. Thus φ induces the 0 map on $\operatorname{Tate}_\ell(J_0(N))$, so $\varphi = 0$. □

Let $F : X_0(N)_{\mathbf{F}_p} \to X_0(N)_{\mathbf{F}_p}$ be the Frobenius map in characteristic p. Thus, if $K = K(X_0(N))$ is the function field of the nonsingular curve $X_0(N)$, then $F : K \to K$ is induced by the pth power map $a \mapsto a^p$.

Remark 1.6.3. The Frobenius map corresponds to the pth powering map on points. For example, if $X = \operatorname{Spec}(\mathbf{F}_p[t])$, and $z = (\operatorname{Spec}(\overline{\mathbf{F}}_p) \to X)$ is a point defined by a homomorphism $\alpha : \mathbf{F}_p[t] \mapsto \overline{\mathbf{F}}_p$, then $F(z)$ is the composite

$$\mathbf{F}_p[t] \xrightarrow{x \mapsto x^p} \mathbf{F}_p[t] \xrightarrow{\alpha} \overline{\mathbf{F}}_p.$$

If $\alpha(t) = \xi$, then $F(z)(t) = \alpha(t^p) = \xi^p$.

By both functorialities, F induces maps on the Jacobian of $X_0(N)_{\mathbf{F}_p}$:

$$\operatorname{Frob}_p = F_* \quad \text{and} \quad \operatorname{Ver}_p = \operatorname{Frob}_p^\vee = F^*,$$

which we illustrate as follows:

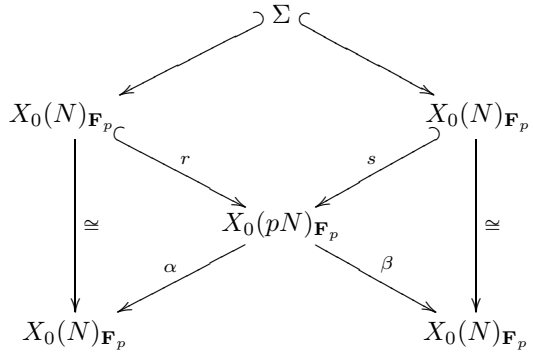
$$J_0(N)_{\mathbf{F}_p} \underset{\operatorname{Frob}_p}{\overset{\operatorname{Ver}_p}{\rightleftarrows}} J_0(N)_{\mathbf{F}_p}$$

Note that $\mathrm{Ver}_p \circ \mathrm{Frob}_p = \mathrm{Frob}_p \circ \mathrm{Ver}_p = [p]$ since p is the degree of F (for example, if $K = \mathbf{F}_p(t)$, then $F(K) = \mathbf{F}_p(t^p)$ is a subfield of degree p, so the map induced by F has degree p).

Theorem 1.6.4 (Eichler-Shimura Relation). *Let N be a positive integer and $p \nmid N$ be a prime. Then the following relation holds:*

$$T_p = \mathrm{Frob}_p + \mathrm{Ver}_p \in \mathrm{End}(J_0(N)_{\mathbf{F}_p}).$$

Sketch of Proof. We view $X_0(pN)_{\mathbf{F}_p}$ as two copies of $X_0(N)_{\mathbf{F}_p}$ glued along corresponding supersingular points Σ, as in Figure 1.6.1. This diagram and the correspondence (1.6.2) that defines T_p translate into the following diagram of schemes over $\mathbf{F}_p$:



The maps r and s are defined as follows. Recall that a point of $X_0(N)_{\mathbf{F}_p}$ is an enhanced elliptic curve $\underline{E} = (E, C)$ consisting of an elliptic curve E (not necessarily defined over $\mathbf{F}_p$) along with a cyclic subgroup C of order N. We view a point on $X_0(Np)$ as a triple $(E, C, E \to E')$, where (E, C) is as above and $E \to E'$ is an isogeny of degree p. We use an isogeny instead of a cyclic subgroup of order p because $E(\overline{\mathbf{F}}_p)[p]$ has order either 1 or p, so the data of a cyclic subgroup of order p holds very little information.

The map r sends $\underline{E}$ to $(\underline{E}, \varphi)$, where φ is the isogeny of degree p,

$$\varphi : E \xrightarrow{\mathrm{Frob}} E^{(p)}.$$

Here $E^{(p)}$ is the curve obtained from E by hitting all defining equations by Frobenious, that is, by pth powering the coefficients of the defining equations for E. We introduce $E^{(p)}$ since if E is not defined over $\mathbf{F}_p$, then Frobenious does not define an endomorphism of E. Thus r is the map

$$r : \quad \underline{E} \mapsto (\underline{E}, E \xrightarrow{\mathrm{Frob}_p} E^{(p)}),$$

and similarly we define s to be the map

$$s : \quad \underline{E} \mapsto (E^{(p)}, C, E \xleftarrow{\mathrm{Ver}_p} E^{(p)})$$

where Ver_p is the dual of Frob_p (so $\mathrm{Ver}_p \circ \mathrm{Frob}_p = \mathrm{Frob}_p \circ \mathrm{Ver}_p = [p]$).

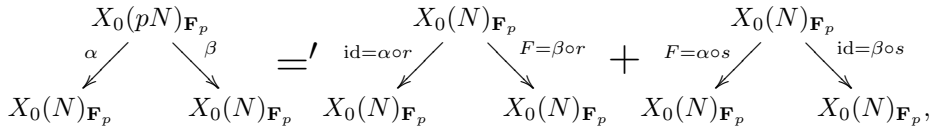
We view α as the map sending $(\underline{E}, E \to E')$ to $\underline{E}$, and similarly we view β as the map sending $(\underline{E}, E \to E')$ to the pair (E', C'), where C' is the image of C in

E' via $E \to E'$. Thus

$$\begin{aligned} \alpha: &\quad (E \to E') \mapsto E \\ \beta: &\quad (E' \to E) \mapsto E' \end{aligned}$$

It now follows immediately that $\alpha \circ r = \mathrm{id}$ and $\beta \circ s = \mathrm{id}$. Note also that $\alpha \circ s = \beta \circ r = F$ is the map $E \mapsto E^{(p)}$.

Away from the finitely many supersingular points, we may view $X_0(pN)_{\mathbf{F}_p}$ as the disjoint union of two copies of $X_0(N)_{\mathbf{F}_p}$. Thus away from the supersingular points, we have the following equality of correspondences:



where $F = \mathrm{Frob}_p$, and the $='$ means equality away from the supersingular points. Note that we are simply "pulling back" the correspondence; in the first summand we use the inclusion r, and in the second we use the inclusion s.

This equality of correspondences implies that the equality

$$T_p = \mathrm{Frob}_p + \mathrm{Ver}_p$$

of endomorphisms holds on a dense subset of $J_0(N)_{\mathbf{F}_p}$, hence on all $J_0(N)_{\mathbf{F}_p}$. □

1.7 Applications of the Eichler-Shimura Relation

1.7.1 The Characteristic Polynomial of Frobenius

How can we apply the relation $T_p = \mathrm{Frob} + \mathrm{Ver}$ in $\mathrm{End}(J_0(N)_{\mathbf{F}_p})$? Let $\ell \nmid pN$ be a prime and consider the ℓ-adic Tate module

$$\mathrm{Tate}_\ell(J_0(N)) = \left(\varprojlim J_0(N)[\ell^\nu]\right) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$$

which is a vector space of dimension $2g$ over $\mathbf{Q}_\ell$, where g is the genus of $X_0(N)$ or the dimension of $J_0(N)$. Reduction modulo p induces an isomorphism

$$\mathrm{Tate}_\ell(J_0(N)) \to \mathrm{Tate}_\ell(J_0(N)_{\mathbf{F}_p})$$

(see the proof of Lemma 1.6.2). On $\mathrm{Tate}_\ell(J_0(N)_{\mathbf{F}_p})$ we have linear operators Frob_p, Ver_p and T_p which, as we saw in Section 1.6, satisfy

$$\begin{aligned} \mathrm{Frob}_p + \mathrm{Ver}_p &= T_p, \qquad \text{and} \\ \mathrm{Frob}_p \circ \mathrm{Ver}_p &= \mathrm{Ver}_p \circ \mathrm{Frob}_p = [p]. \end{aligned}$$

The endomorphism $[p]$ is invertible on $\mathrm{Tate}_\ell(J_0(N)_{\mathbf{F}_p})$, since p is prime to ℓ, so Ver_p and Frob_p are also invertible and

$$T_p = \mathrm{Frob}_p + [p]\,\mathrm{Frob}_p^{-1}.$$

Multiplying both sides by Frob_p and rearranging, we see that

$$\mathrm{Frob}_p^2 - T_p \,\mathrm{Frob}_p + [p] = 0 \in \mathrm{End}(\mathrm{Tate}_\ell(J_0(N)_{\mathbf{F}_p})).$$

This is a beautiful quadratic relation, so we should be able to get something out of it. We will come back to this shortly, but first we consider the various objects acting on the ℓ-adic Tate module.

The module $\mathrm{Tate}_\ell(J_0(N))$ is acted upon in a natural way by

1. The Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ of $\mathbf{Q}$, and
2. $\mathrm{End}_{\mathbf{Q}}(J_0(N)) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ (which acts by functoriality).

These actions commute with each other since endomorphisms defined over $\mathbf{Q}$ are not affected by the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Reducing modulo p, we also have the following commuting actions:

3. The Galois group $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ of $\mathbf{F}_p$, and
4. $\mathrm{End}_{\mathbf{F}_p}(J_0(N)) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$.

Note that a decomposition group group $D_p \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts, after quotienting out by the corresponding inertia group, in the same way as $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ and the action is unramified, so action 3 is a special case of action 1.

The Frobenius elements $\varphi_p \in \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ and $\mathrm{Frob}_\in \mathrm{End}_{\mathbf{F}_p}(J_0(N)) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ induce the same operator on $\mathrm{Tate}_\ell(J_0(N)_{\mathbf{F}_p})$. Note that while φ_p naturally lives in a quotient of a decomposition group, one often takes a lift to get an element in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

On $\mathrm{Tate}_\ell(J_0(N)_{\mathbf{F}_p})$ we have a quadratic relationship

$$\varphi_p^2 - T_p\varphi_p + p = 0.$$

This relation plays a role when one separates out pieces of $J_0(N)$ in order to construct Galois representations attached to newforms of weight 2. Let

$$R = \mathbf{Z}[\ldots, T_p, \ldots] \subset \mathrm{End}\, J_0(N),$$

where we only adjoin those T_p with $p \nmid N$. Think of R as a reduced Hecke algebra; in particular, R is a subring of $\mathbf{T}$. Then

$$R \otimes \mathbf{Q} = \prod_{i=1}^{r} E_i,$$

where the E_i are totally real number fields. The factors E_i are in bijection with the Galois conjugacy classes of weight 2 newforms f on $\Gamma_0(M)$ (for some $M|N$). The bijection is the map

$$f \mapsto \mathbf{Q}(\text{coefficients of } f) = E_i$$

Observe that the map is the same if we replace f by one of its conjugates. This decomposition is a decomposition of a subring

$$R \otimes \mathbf{Q} \subset \mathrm{End}(J_0(N)) \otimes \mathbf{Q} \stackrel{\text{def}}{=} \mathrm{End}(J_0(N) \otimes \mathbf{Q}).$$

Thus it induces a direct product decomposition of $J_0(N)$, so $J_0(N)$ gets divided up into subvarieties which correspond to conjugacy classes of newforms.

The relationship

$$\varphi_p^2 - T_p\varphi_p + p = 0 \tag{1.7.1}$$

suggests that

$$\mathrm{tr}(\varphi_p) = T_p \qquad \text{and} \quad \det\varphi_p = p. \tag{1.7.2}$$

This is true, but (1.7.2) does not follow formally just from the given quadratic relation. It can be proved by combining (1.7.1) with the Weil pairing.

1.7.2 The Cardinality of $J_0(N)(\mathbf{F}_p)$

Proposition 1.7.1. *Let $p \nmid N$ be a prime, and let f be the characteristic polynomial of T_p acting on $S_2(\Gamma_0(N))$. Then*

$$\#J_0(N)(\mathbf{F}_p) = f(p+1).$$

[[Add details later, along with various generalizations.]]

References

[1] B. Conrad, *The shimura construction in weight 2 (appendix to Ribet-Stein, Lectures on Serre's Conjecture)*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 205–232. MR 2002h:11047

[2] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[3] H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Internat. Press, Cambridge, MA, 1994, pp. 1–154.

[4] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972) (Berlin), Springer, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.

[5] G. Frey and M. Müller, *Arithmetic of modular curves and applications*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 11–48.

[6] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[7] D. Mumford, *Abelian varieties*, Published for the Tata Institute of Fundamental Research, Bombay, 1970, Tata Institute of Fundamental Research Studies in Mathematics, No. 5.

[8] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, third ed., Springer-Verlag, Berlin, 1994.

[9] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 143–232. MR 2002h:11047

[10] O. F. G. Schilling (ed.), *Arithmetical algebraic geometry. (Proceedings of a Conference held at Purdue University, December 5–7, 1963)*, Harper & Row Publishers, New York, 1965.

[11] J-P. Serre and J. T. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

[12] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.

[13] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[14] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), no. 3, 372–384. MR 86m:11041