Lecture Notes on Eichler-Shimura Theory

Pete L. Clark

March 10, 2000

1 Hecke Operators

In order to state the Eichler-Shimura congruence we will need to review the notion of Hecke operators on $\Gamma_0(N)$. We begin with the modular interpreation. A *modular pair* is a pair (Λ, C) with Λ a lattice in $\mathbb{C}$, C a cyclic order N subgroup of $\mathbb{C}/\Lambda$. Let $\mathcal{D}$ be the free abelian group on the set of modular pairs. Let n be a positive integer, and for simplicity assume $(n, N) = 1$. Then we define

$$T(n)(\Lambda, C) = \sum_{[\Lambda:\Lambda']=n, C' \mapsto C} (\Lambda', C') \tag{1}$$

that is, there is one term for each index n sublattice Λ' (NB: it would not necessarily be so if $(n, N) > 1$) and C' is the unique cyclic order N subgroup of $\mathbb{C}/\Lambda'$ getting mapped to $C \leq \mathbb{C}/\Lambda$ via the quotient map. (For n not necessarily prime to N, the definition would be similar except that we would sum over pairs with nC mapping onto C'.) We say that the modular pairs (Λ', C') in the sum *correspond* to (Λ, C) under the map $T(n)$. In terms of matrices, let (Λ', C') correspond to (Λ, C), and choose positively oriented bases (ω_1, ω_2) (resp. (ω_1', ω_2')) of Λ (Λ') such that $(1/N\omega_1, \omega_2)$ ($(1/N\omega_1', \omega_2')$) is a basis for $q_\Lambda^{-1}(C)$ ($q_{\Lambda'}^{-1}(C')$), and let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be the integer matrix such that

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

We easily see that A is constrained to lie in the set $M(n, N) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $ad - bc = n$, N divides c, $(a, N) = 1$ $\}$, and conversely any such matrix carries (Λ, C) to a corresponding modular pair (Λ', C'). Moreover, $\Gamma_0(N)$ acts on $M(n, N)$ and stabilizes the set of suitable bases (as above) (ω_1', ω_2') for Λ', so the modular pairs indexed in (1) are parameterized by $\Gamma_0(N)\backslash M(n, N)$. Indeed, it is easy to give an explicit set of coset representatives, e.g. $\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, ad = n; a, d > 0, (a, N) = 1, 0 \leq b < d\}$. Taking $n = p$ we see that there are $p + 1$ terms in the sum; we say that $T(p)$ is a correspondence of degree $p+1$. We could now define $T(n)$ as a linear endomorphism on the space of $\Gamma_0(N)$-automorphic forms of weight $2k$, via $f \mapsto n^{k-1} \sum_{\gamma \in \Gamma_0(N) \backslash M(n,N)} f|_k\gamma$; in fact this interpretation of the Hecke operators will not be explicitly used in the sequel.

Double cosets: We might as well consider a slightly more general situation, namely let $\Gamma \leq \Gamma(1)$ be any finite index subgroup (a modular group), and let Δ be the set of integer matrices of positive determinant.

We need a technical lemma that will be used in the next section. Namely, for $\alpha \in \Delta$, write $\Gamma^\alpha := \alpha^{-1}\Gamma\alpha$; observe that Γ^α still has finite index in $\Gamma(1)$, hence $\Gamma_\alpha := \Gamma \cap \Gamma^\alpha$ has finite index in $\Gamma(1)$ (in particular, Γ and Γ^α are commensurable as subgroups of $\Gamma(1)$).

Lemma 1 *If $\Gamma = \coprod_{i=1}^k \Gamma_\alpha\beta_i$, then $\Gamma\alpha\Gamma = \coprod_{i=1}^k \Gamma\alpha\beta_i$. In particular, the second decomposition has only finitely many right cosets.*

See p. 75 of [Milne] for the (easy) proof.
We can now define an *abstract* ring of "Hecke operators" as follows: let $H(\Gamma, \Delta)$ be the free abelian group on the set of double cosets $\{\Gamma\alpha\Gamma | \alpha \in \Delta\}$. We define a multiplication operation on $H(\Gamma, \Delta)$ as follows: write $\Gamma\alpha\Gamma = \coprod \Gamma\alpha_i$, $\Gamma\beta\Gamma = \coprod \beta_i$; then

$$(\Gamma\alpha\Gamma).(\Gamma\beta\Gamma) = \sum c_{\alpha,\beta}^{[\gamma]} \Gamma\gamma\Gamma$$

where we sum over the double cosets $\Gamma\gamma\Gamma$ with $\Gamma\gamma\Gamma \subseteq \Gamma\alpha\Gamma\beta\Gamma$ and put $c_{\alpha,\beta}^{[\gamma]} = \#\{(i,j) | \Gamma\alpha_i\beta_j = \Gamma\gamma\}$ (observe that Lemma 1 implies that all the above coset decompositions are finite.) We call $H(\Gamma, \Delta)$ the *Hecke algebra.*

Now take $\Gamma = \Gamma_0(N), n = p$ (with $(p, N) = 1$). We have the identity $M(p, N) = \Gamma_0(N) \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \Gamma_0(N)$. Thus the Hecke operator $T(p)$ corresponds to the element $\Gamma_0(N) \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \Gamma_0(N)$ of the Hecke algebra, via switching from double cosets to right cosets. (NB: in general, $M(n, N)$ is not itself a double coset but rather a finite union of double cosets, and in this case $T(n)$ corresponds to the element $\sum \Gamma_0(N)\alpha_i\Gamma_0(N)$, where $M(n, N) = \coprod \Gamma_0(N)\alpha_i\Gamma_0(N)$.)

2 Algebraic correspondences on curves

Let X, X' be nonsingular projective curves over an algebraically closed field k. A *correspondence* T from X to X' is a pair $X \overset{\alpha}{\leftarrow} Y \overset{\beta}{\rightarrow} X'$, where Y is a nonsingular projective curve and α, β are finite morphisms. There is an induced map $\beta \circ \alpha^* : \operatorname{Div} Y \to \operatorname{Div} X$, where α^* is the usual pullback of divisors. Observe that if α has degree n, then α^* multiplies the degree by n, whereas β has degree 1 as a map on divisor groups, so that the composite map $\beta \circ \alpha^*$ multiplies degrees by n; in particular it is well-defined as a map from $\operatorname{Div}_0 X \to \operatorname{Div}_0 X'$. Moreover, it can be shown that $\beta \circ \alpha^*$ preserves principal divisors and hence induces a map on Jacobian varieties $J(\beta \circ \alpha^*) : J(X) \rightarrow J(X')$. In particular, when $X = X'$ (as will be the case for us), a correspondence on X induces an endomorphism on $J(X)$, and we have the ring of correspondences, $\mathcal{A(X)}$ embedded as a subring of End(J(X)). Here are some examples of correspondences: if $T = X \overset{\alpha}{\leftarrow} Y \overset{\beta}{\rightarrow} X$ is a correspondence on X, we can consider $T' = X \overset{\beta}{\leftarrow} Y \overset{\alpha}{\rightarrow} X'$,the dual correspondence. Or, let $f : X \rightarrow X$ be a morphism. Then f induces a correspondence by taking Y to be the graph of f, and taking T =X $\overset{\pi}{\leftarrow} Y \overset{f}{\rightarrow} X'$. Then the correspondence, which we also denote by f, has degree 1 and indeed is just f acting on $\operatorname{Div} X$.

Hecke Correspondences: Let Γ be a modular group and $\alpha \in \Delta$ giving a Hecke operator $\Gamma\alpha\Gamma \in H(\Gamma, \Delta)$. Then $\Gamma\alpha\Gamma$ induces a correspondence on the modular curve $\Gamma\backslash\mathcal{H}^*$ by $\Gamma\backslash\mathcal{H}^* \overset{\pi}{\leftarrow} \Gamma_\alpha\backslash\mathcal{H}^* \overset{\alpha}{\rightarrow} \Gamma\backslash\mathcal{H}^*$, where π is just the quotient map and α acts by $\Gamma_\alpha z \mapsto \Gamma\alpha z$ – this is well-defined by Lemma 1. The induced map $\alpha \circ \pi^*$ on $\operatorname{Div}(\Gamma\backslash\mathcal{H}^*)$ is the usual Hecke operator correspondence: writing $\Gamma = \coprod \Gamma_\alpha \beta_i$, we get $\Gamma z \mapsto \sum \Gamma_\alpha \beta_i z \mapsto \sum \Gamma\alpha\beta_i z$, which corresponds to the double-to-right coset decomposition $\Gamma\alpha\Gamma = \coprod \Gamma\alpha\beta_i$ by Lemma 1. In particular, taking $X = X_0(N)$, $\alpha = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$, we recover the Hecke operator $T(p)$ of the previous section as an algebraic correspondence $T(p) : \operatorname{Div}(X_0(N)) \rightarrow \operatorname{Div}(X_0(N))$. More precisely, viewing $Y_0(N)(\mathbb{Q})$ as the moduli variety for $\mathcal{E}_{0,N}(\mathbb{Q})$, the correspondence $T(p)$ acts on the free abelian group generated by the set of pairs $(j(E), j(E'))$, with $\alpha : E \rightarrow E'$ a cyclic N-isogeny as the matrices in the right-coset decomposition would act on representative lattices Λ, Λ'. Indeed we can view this more instrinsically in terms of the elliptic curves as follows: let $S_0, \ldots, S_p$ be an enumeration of the $p+1$ p-torsion subgroups of E. Then

$$T(p) : (j(E), j(E')) \rightarrow \sum_{i=0}^{p} (j(E/S_i), j(E'/\alpha(S_i)).$$

This is not hard to see: the only subtlety is that the elliptic curves E/S_i are order p quotients of E, so the corresponding lattices are index p overlattices of the lattice Λ of E, whereas in the definition of the Hecke correspondence we should be summing over index p, sublattices. But multiplication by p is a homothety that carries the one set of lattices into the other and preserves the j-invariants.

3 Reduction of $X_0(N)$ modulo p

We want to view the Eichler-Shimura "congruence relation" as an equality of algebraic correspondences; necessarily these correspondences must live in the *reduced* variety $\tilde{X}_0(N)$ defined over $\mathbb{F}_p$. Unfortunately the general notion of reducing a variety defined over a global field modulo a prime of that field is a sticky one: one needs only to reflect on the definition of reduction of an elliptic curve to see how poorly it will generalize to arbitrary varieties: reduction of an elliptic curve proceeds by choosing a Weierstrass equation with discriminant Δ of minimal valuation wih respect to the given prime, and then we literally reduce the equation coefficientwise. Then, one is able to check that any two minimal Weierstrass equations are related by a change of variables of a special form, such that the reduction of the change of variables survives to give an isomorphism between the reductions of the minimal Weierstrass equations. This is not possible for curves of higher genus. Thus we are forced into a more *ad hoc* approach: we work with the particular birational model of $X_0(N)$ over $\mathbb{Q}$ given by the modular polynomial $F_N(X,Y) = 0$. The reduction process is made easier in this special case by clinging to the interpretation of $X_0(N)$ as the moduli variety for the moduli problem $\mathcal{E}_{0,N}$. There is the following result:

Theorem 2 *Let C be the (singular) $\mathbb{Q}$-projective curve defined by $F_N(X,Y,Z) = 0$. Since F_N has integer coefficients we can reduce them modulo p to get an $\mathbb{F}_p$-projective curve C_p. Let C_p^n be its normalization. The following are equivalent.*

a) C_p^n is irreducible and has the same genus as that of C.
b) C_p^n is the projective completion of the moduli variety for $\mathcal{E}_{0,N}(\mathbb{F}_p)$.
c) p does not divide N.

Under these conditions, we say that $X_0(N)$ has good reduction at p and write $\tilde{X}_0(N)$ for C_p^n. The theorem implies that, birationally, we can view $\tilde{X}_0(N)$ as the set of pairs $(j(\tilde{E}), j(\tilde{E}'))$, where $\tilde{E}$ and $\tilde{E}'$ are cyclic-N-isogenous elliptic curves over $\overline{\mathbb{F}_p}$.

4 The Eichler-Shimura Congruence

Consider $\tilde{X}_0(N)(\overline{\mathbb{F}_p})$. The p-power Frobenius map induces a correspondence on $\tilde{X}_0(N)$ which we denote Fr_p; let Fr'_p denote its dual correspondence. We also have $T(p)$ as a correspondence on $X_0(N)(\overline{\mathbb{Q}_p})$ (a Lefschetz principle argument shows that for any field k of characteristic 0, $X_0(N)(k)$ is the moduli variety for $\mathcal{E}_{0,N}(k)$). The morphisms defining $T(p)$ are a priori defined over some number field K (hence a fortiori over its completion); in fact (see [Knapp]), they can be shown to be defined over $\mathbb{Q}$. We can then try to define a correspondence $\tilde{T}(p)$ on $\tilde{X}_0(N)$ by reducing $T(p)$. We have the following result:

Theorem 3 *(Eichler-Shimura Congruence): $\tilde{T}(p)$ is a well-defined algebraic correspondence and $\tilde{T}(p) = \mathrm{Fr}_p + \mathrm{Fr}'_p$ as algebraic correspondences on $\tilde{X}_0(N)$ (e.g. as endomorphisms of the Jacobian variety $J(\tilde{X}_0(N))$.*

Proof: If we can show that $\tilde{T}(p)(\tilde{P})$ when defined using a particular lifting to $P \in X_0(N)$ equals $\mathrm{Fr}_p(\tilde{P}) + \mathrm{Fr}'_p(\tilde{P})$, then visibly the choice of lift didn't matter, so $\tilde{T}(p)$ is well-defined on $\mathrm{Div}(\tilde{X}_0(N))$. Moreover, viewing $\tilde{T}(p)$ and $\mathrm{Fr}_p + \mathrm{Fr}'_p$ as maps $\tilde{X}_0(N) \to J(\tilde{X}_0(N))$, it's enough to show that they agree for

all but finitely many points $\tilde{P}$, for then, as rational maps from a nonsingular curve into a projective variety, they extend uniquely to morphisms on all of $\tilde{X}_0(N)$. Thus, it's enough to consider points $\tilde{P}$ of the form $(j(\tilde{E}), j(\tilde{E}'))$, with $\tilde{\alpha} : \tilde{E} \to \tilde{E}'$ a cyclic-N-isogeny. Moreover, recall that a supersingular elliptic curve $\tilde{E}$ must have j-invariant in $\mathbb{F}_{p^2}$, so there are only finitely many such curves and we may throw them out, thus assuming that our point $\tilde{P}$ is represented by a pair of elliptic curves with $\#\tilde{E}[p] = p$. Lift $\tilde{\alpha}$ to some $\alpha : E \to E'$ in characteristic zero. Then $E[p](\overline{\mathbb{Q}_p}) \to \tilde{E}[p](\overline{\mathbb{F}_p})$ has order p kernel. On the other hand, we can write $T_p(P) = T_p(j(E), j(E')) = \sum_{i=0}^{p} (j(E_i), j(E_i'))$ where $S_0, \dots, S_p$ is an enumeration of the order p torsion subgroups of E and $E_i = E/S_i, E_i' = E'/\alpha(S_i)$. We may assume that S_0 is the kernel of reduction, so that for all $i > 0$, S_i reduces to the unique p-torsion subgroup of $\tilde{E}$. We have $\tilde{T}(p)(\tilde{P}) = \sum_{i=0}^{p} (j(\widetilde{E/S_i}), j(\widetilde{E'/\alpha S_i}))$.
Case 1: $i = 0$. Then the reduction of $E \to E/S_0$ is purely inseparable of degree p, hence $\widetilde{E/S_0} \cong \tilde{E}^{(p)}$, i.e. $(j(\tilde{E}_0), j(\tilde{E}'_0)) = \mathrm{Fr}_p(\tilde{P})$.
Case 2: $i > 0$. Then $\tilde{S}_i$ survives to give an order p kernel, i.e. $\tilde{E} \to \tilde{E}/\tilde{S}_i$ is separable. Thus we can factor $[p]$ through it to get $\tilde{E} \to \tilde{E}/\tilde{S}_i \overset{\psi}{\to} \tilde{E}$; it must then be that ψ is purely inseparable of degree p, i.e. $\tilde{E} \cong (\tilde{E}/\tilde{S}_i)^{(p)}$, so

$$\mathrm{Fr}_p'(\tilde{P}) = p.(j(\tilde{E}/\tilde{S}_i), j(\tilde{E}'/\tilde{S}_i')) = \sum_{i=1}^{p} (j(\tilde{E}/\tilde{S}_i), j(\tilde{E}'/\tilde{S}_i')).$$

Therefore $\tilde{T}(p)(\tilde{P}) = \sum_{i=0}^{p} (j(\tilde{E}/\tilde{S}_i), j(\tilde{E}'/\tilde{S}_i')) =$

$$(j(\widetilde{E/S_0}), j(\widetilde{E'/S_0'})) + p.(j(\tilde{E}/\tilde{S}_1), j(\tilde{E}'/\tilde{S}_1')) = \mathrm{Fr}_p(\tilde{P}) + \mathrm{Fr}_p'(\tilde{P}).$$

5 Modular Parameterizations of Elliptic Curves

Let E be an elliptic curved defined over $\mathbb{Q}$. Recall that a *modular parameterization of level* N is a finite $\mathbb{Q}$-rational morphism $F : X_0(N) \to E$. A modular parameterization is *minimal* if there is no modular parameterization of level M for any $M < N$. (Note that there are always nonminimal parameterizations, obtained by composing F with the natural map $X_0(NN') \to X_0(N)$.) Note also that being modular of level N is an isogeny invariant for E. A famous and recent theorem (Taniyama-Shimura-Weil-Taylor-Wiles-Conrad-Diamond...) implies that every elliptic curve over $\mathbb{Q}$ is modular. Observe that if we have a modular parameterization $F : X_0(N) \to E$, an invariant differential ω on E pulls back to $F^*(\omega)$, which we can take to be a weight 2 cusp form with integral coefficients (and other nice properties – it is a weak eigenform for the Hecke operators) on $X_0(N)$. The Eichler-Shimura construction shows how to run this process in the other direction.

Theorem 4 *(Eichler-Shimura Construction) Let $f(\tau) = \sum_{n=1}^{\infty} a_n q^n$ be a weight 2 cusp form for $\Gamma_0(N)$ which has $a_1 = 1$ and all a_n integers. Assume moreover that f is a strong eigenform (i.e. for all Hecke operators $T(n)$ – even those for which $(n, N) > 1$ – we have $T(n)f = a_n f$).*

a) There is a pair (E, ν), where $E/\mathbb{Q}$ is an elliptic curve and : $J(X_0(N)) \to E$ exhibits E as the quotient by a codimension one $\mathbb{Q}$-rational abelian subvariety A.
b) All the Hecke correspondences $T(n)$, viewed as endomorphisms of $J(X_0(N))$, stabilize A and act on the quotient E via multiplication by a_n. These two properties characterize (E, v) up to $\mathbb{Q}$-isomorphism.
c) The invariant differential ω on E pulls back to a scalar multiple of f viewed as a holomorphic differential on $X_0(N)$.
d) (Igusa) The L-functions of E and f coincide as Euler products prime-by-prime, except possibly at primes p dividing N.

We do not have time to discuss the proof; see [Knapp, Ch. XI] and [Milne]. Note that we can conclude from d) that for primes l not dividing N, the Fourier coefficient a_l is the same as the elliptic curve's a_l, i.e. the trace of Frobenius acting on $\tilde{E}(\mathbb{F}_l)$, and hence $T(l)$ acts on E by multiplication by a_l. This will be used in the next section.

To give some intuition for this result, we remark that the subvariety A is defined as the intersection of the kernels of the endomorphisms $T(n) - a_n$ (which elucidates part b) at least). Moreover, we can see E as an elliptic curve over $\mathbb{C}$ as follows: fix any $\tau_0 \in \mathcal{H}$ and define $\Lambda_f = \{\int_{\tau_0}^{\gamma(\tau_0)} f(\zeta)d\zeta \mid \gamma \in \Gamma_0(N)\}$; then Λ_f turns out to be a lattice in $\mathbb{C}$ with $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_f$.

To understand how the Eichler-Shimura construction applies to minimal modular parameterizations, we need the notion of a *newform*, which we will not (alas) pause to motivate. An *oldform* on $\Gamma_0(N)$ is a weak eigenform – i.e. a simultaneous eigenvector those Hecke operators $T(n)$ with $(n, N) = 1$ – in $\mathcal{S}_{2k}(\Gamma_0(N))$ coming trivially from an eigenform of lower level: precisely, if $r_1 r_2/N$ and f is a weak eigenform for $\Gamma_0(\frac{N}{r_1 r_2})$, then $f(r_2\tau)$ is an oldform on $\Gamma_0(N)$. A newform is a weak eigenform in the orthogonal complement of the oldforms. The Atkin-Lehner theorem implies that every newform is a *strong* eigenform, hence a weight two newform is a candidate for the Eichler-Shimura construction.

Theorem 5 *(Carayol) Let $f \in \mathcal{S}_2(\Gamma_0(N))$ be a newform with $a_1 = 1$ and a_n integers, and let $E/\mathbb{Q}$ be the elliptic curve associated to f by the Eichler-Shimura construction. Then $L(s, E) = L(s, f)$; indeed, as Euler products their Euler factors agree prime-by-prime. In particular, we can read off the bad reduction primes as being precisely those dividing N.*

Corollary 6 *Let $F : X_0(N) \to E$ be a modular paramaterization. The following are equivalent.*

a) F is a minimal modular parameterization.
b) F factors as the Eichler-Shimura parameterization associated to a newform f followed by a $\mathbb{Q}$-isogeny of elliptic curves.
c) E has conductor N.

6 Verification of the axioms for the Heegner Point Euler System

Recall from [Ghitza] that we have defined for any n coprime to N a Heegner point on $X_0(N)(K_n)$; morally, a Heegner point of $X_0(N)$ is a point represented as $(j(E), j(E'))$, where E, E' are cyclic-N-isogenous elliptic curves with CM by the same order of a quadratic imaginary field, in this case by $\mathcal{O}_n$. Our Heegner points are chosen to be compatible with each other (in a way that we will shortly make precise), so explicitly we take $x_n = (j(\mathbb{C}/\mathcal{O}_n), j(\mathbb{C}/\mathcal{N}_n^{-1})) = (j(E_n), j(E'_n))$. Then we have the following key lemma:

Lemma 7 *We have $Tr_l x_n = T(l)x_m$ as divisors on $X_0(N)(K_m)$.*

Proof: Consider the exact sequence $1 \to G_l \to G_n \to G_m \to 1$. The action of $\operatorname{Pic}\mathcal{O}_n$ on the set of $\mathcal{O}_n$-CM elliptic curves by $[\mathfrak{a}] * \mathbb{C}/\Lambda := \mathbb{C}/\mathfrak{a}\Lambda$ is simply transitive, and by making $\sigma \in G(K_n/K)$ correspond to $[\mathfrak{a}] \in \operatorname{Pic}\mathcal{O}_n$ via $[\mathfrak{a}] * E = E^\sigma$, we obtain a group isomorphism $G(K_n/K) \cong \operatorname{Pic}\mathcal{O}_n$. (We remark that this is the composition of the usual isomorphism with inversion.) Now if $\sigma \in G_l$, σ determines an element of $\operatorname{Pic}\mathcal{O}_n$ which becomes trivial when pushed forward to $\operatorname{Pic}\mathcal{O}_m$; in terms of the fractional ideal $\mathfrak{a}_\sigma$, this means $\mathfrak{a}_\sigma\mathcal{O}_m = \alpha\mathcal{O}_m$, with $\alpha \in K^\times$; by adjusting $\mathfrak{a}$ within its class, we may assume that $\mathfrak{a}_\sigma\mathcal{O}_m = \mathcal{O}_m$, so in particular $\mathfrak{a}_\sigma \subseteq \mathcal{O}_m$. Then $[\mathcal{O}_m : \mathfrak{a}_\sigma] = [\mathcal{O}_m\mathfrak{a}_\sigma : \mathcal{O}_m] = l$; the latter equality is valid for any invertible $\mathcal{O}_n$-submodule of K. Using the above expression for the Heegner point x_n, this shows that the first coordinates of $Tr_l x_n$ are $\sum_{\sigma \in G_l} j(E_n)^\sigma = \sum_{\sigma \in G_l} j(\mathbb{C}/\mathfrak{a}_\sigma)$ and that $\mathbb{C}/\mathfrak{a}_\sigma$ is an order p overlattice of $C/\mathcal{O}_m$, so by the discussion at the end of Section 2 we have equality of first coordinates in the divisors $T(l)x_m$ and $Tr_l x_n$. But now writing $Tr_l x_n = \sum(j(\mathbb{C}/\mathcal{O}_n), j(\mathbb{C}/\mathcal{N}_n^{-1}))$, observe that since $\mathbb{C}/\mathcal{N}_n^{-1}$ is also an $\mathcal{O}_n$-CM curve, the Galois action is still given by multiplication by the ideal $\mathfrak{a}_\sigma$: $Tr_l x_n = \sum_{(} j(\mathbb{C}/\mathfrak{a}_\sigma), j(\mathbb{C}/\mathcal{N}_n^{-1}\mathfrak{a}_\sigma))$, it follows that since each kernel of the N-isogeny linking the respective j-invariants, namely $\mathcal{N}_n^{-1}\mathfrak{a}_\sigma/\mathfrak{a}_\sigma$, surjects onto $\mathcal{N}_m^{-1}/\mathcal{O}_m$, the second coordinates of the divisors match as well.

Proposition 8 *(Gross' 3.7) Recall $y_n = \phi(x_n)$, where $\phi : X_0(N) \to E$ is our modular parameterization. Then*

a) $Tr_l y_n = a_l y_m$ in $E(K_m)$.
b) Each prime factor λ_m of l in K_m lies under a unique prime λ_n of K_n, and $y_n \equiv \mathrm{Frob}(\lambda_m/l)(y_m)$ (λ_n).

Proof: a) We have $Tr_l x_n = T(l)x_m$. Apply ϕ to both sides, noting as we

have that the Hecke operators $T(l)$ act as the L-series coefficients a_l; the result is then immediate.
b) Observe that the prime λ (the unique prime lying over l in K) is principal and generated by an integer l prime to the conductor m, i.e. it lies in the kernel of the Artin map for K_m/K and thus splits completely in K_m. On the other hand, the factors λ_m of λ in K_m are totally ramified in K_n – indeed, the l-ray classfield is totally ramified over the Hilbert classfield at l; and we have $\lambda_m = \lambda_n^{l+1}$. In particular, the residue field F_{λ_n} equals the residue field F_λ; both have l^2 elements. Again we exploit the identity $T(l)x_m = Tr_l x_n$, by noting that the total ramification at λ_m implies that $Tr_l x_n = \sum_{\sigma \in G_l} x_n^\sigma \equiv (l+1)x_n(\lambda_n)$, i.e. we have equality in the residue field. Note that $\mathrm{Frob}(\lambda_m/l) \equiv \mathrm{Fr}_l(\lambda_n)$, whereas Fr_l itself has order 2 on the quadratic extension, F_λ/F_l, i.e. is self-inverse. Thus Eichler-Shimura for K_m-valued divisors reads $T(l) \equiv (l+1)\,\mathrm{Fr}_l$ (remember that Fr_l' has order l as a correspondence). So we have

$$(l+1)x_n \equiv Tr_l x_n \equiv T(l)x_m \equiv (l+1)\,\mathrm{Frob}(\lambda_m/l)(x_m)(\lambda_n)$$

whence we may certainly conclude $x_n \equiv \mathrm{Frob}(\lambda_m/l)(x_m)(\lambda_n)$, and pushing everything forward by ϕ, we get the desired result.

7 Comments on References

The material of Section 1 on Hecke operators occurs in many places; our treatment is taken from Knapp's *Elliptic Curves* (Chapter IX) and Milne's *Modular Functions and Modular Forms* (available on the web at www.jmilne.org). Miyake's *Modular Forms* and Shimura's *Introduction to the Arithmetic of Automorphic Forms* give more complete treatments, although Miyake is rather dry. Sections 2 through 4 are taken from Milne's notes – in fact Alex Ghitza and I have reproduced almost everything he has to say there about $X_0(N)$ as a moduli variety and the Eichler-Shimura congruence. As for the material in Section 5, Knapp has a leisurely, readable treatment of most of our Theorem 4, and his discussion can be well-supplemented by Milne's notes (circa p. 110). Neither of these sources gives a complete discussion on the subject, however – I for one would like to know of a more comprehensive reference. Finally, Gross' paper *Heegner Points on* $X_0(N)$ (cited in Gross' survey article) is a good reference for the title topic.