Modular Forms

Kenneth A. Ribet William A. Stein

November 17, 2003

Contents

1 Abelian Varieties Attached to Modular Forms **1**
1.1 Decomposition of the Hecke Algebra 1
1.1.1 The Dimension of L_f 2
1.2 Decomposition of $J_1(N)$ 3
1.2.1 Aside: Intersections and Congruences 4
1.3 Galois Representations Attached to A_f 4
1.3.1 The Weil Pairing 6
1.3.2 The Determinant 7
1.4 Remarks About the Modular Polarization 8

References **11**

1

Abelian Varieties Attached to Modular Forms

LECTURE NOTES FOR MATH 252, November 14, 2003, By William Stein

In this chapter we describe how to decompose $J_1(N)$, up to isogeny, as a product of abelian subvarieties A_f corresponding to Galois conjugacy classes of cusp forms f of weight 2. This was first accomplished by Shimura (see [6, Theorem 7.14]). We also discuss properties of the Galois representation attached to f.

In this chapter we will work almost exclusively with $J_1(N)$. However, everything goes through exactly as below with $J_1(N)$ replaced by $J_0(N)$ and $S_2(\Gamma_1(N))$ replaced by $S_2(\Gamma_0(N))$. Since, $J_1(N)$ has dimension much larger than $J_0(N)$, so for computational investigations it is frequently better to work with $J_0(N)$.

See Brian Conrad's appendix to [ribet-stein: Lectures on Serre's Conjectures] for a much more extensive exposition of the construction discussed below, which is geared toward preparing the reader for Deligne's more general construction of Galois representations associated to newforms of weight $k \geq 2$ (for that, see Conrad's book ...).

1.1 Decomposition of the Hecke Algebra

Let N be a positive integer and let

$$\mathbf{T} = \mathbf{Z}[\ldots, T_n, \ldots] \subset \mathrm{End}(J_1(N))$$

be the algebra of all Hecke operators acting on $J_1(N)$. Recall from Section **??** that the anemic Hecke algebra is the subalgebra

$$\mathbf{T}_0 = \mathbf{Z}[\ldots, T_n, \ldots : (n, N) = 1] \subset \mathbf{T}$$

of $\mathbf{T}$ obtained by adjoining to $\mathbf{Z}$ only those Hecke operators T_n with n relatively prime to N.

Remark 1.1.1. Viewed as $\mathbf{Z}$-modules, $\mathbf{T}_0$ need not be saturated in $\mathbf{T}$, i.e., $\mathbf{T}/\mathbf{T}_0$ need not be torsion free. For example, if $\mathbf{T}$ is the Hecke algebra associated to $S_2(\Gamma_1(24))$ then $\mathbf{T}/\mathbf{T}_0 \cong \mathbf{Z}/2\mathbf{Z}$. Also, if $\mathbf{T}$ is the Hecke algebra associated to $S_2(\Gamma_0(54))$, then $\mathbf{T}/\mathbf{T}_0 \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}$.

If $f = \sum a_n q^n$ is a newform, then the field $K_f = \mathbf{Q}(a_1, a_2, \ldots)$ has finite degree over $\mathbf{Q}$, since the a_n are the eigenvalues of a family of commuting operators with integral characteristic polynomials. The *Galois conjugates* of f are the newforms $\sigma(f) = \sum \sigma(a_n) q^n$, for $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. There are $[K_f : \mathbf{Q}]$ Galois conjugates of f.

As in Section **??**, we have a canonical decomposition

$$\mathbf{T}_0 \otimes \mathbf{Q} \cong \prod_f K_f, \tag{1.1.1}$$

where f varies over a set of representatives for the Galois conjugacy classes of newforms in $S_2(\Gamma_1(N))$ of level dividing N. For each f, let

$$\pi_f = (0, \ldots, 0, 1, 0, \ldots, 0) \in \prod K_f$$

be projection onto the factor K_f of the product (1.1.1). Since $\mathbf{T}_0 \subset \mathbf{T}$, and $\mathbf{T}$ has no additive torsion, we have $\mathbf{T}_0 \otimes \mathbf{Q} \subset \mathbf{T} \otimes \mathbf{Q}$, so these projectors π_f lie in $\mathbf{T}_{\mathbf{Q}} = \mathbf{T} \otimes \mathbf{Q}$. Since $\mathbf{T}_{\mathbf{Q}}$ is commutative and the π_f are mutually orthogonal idempotents whose sum is $(1, 1, \ldots, 1)$, we see that $\mathbf{T}_{\mathbf{Q}}$ breaks up as a product of algebras

$$\mathbf{T}_{\mathbf{Q}} \cong \prod_f L_f, \qquad t \mapsto \sum_f t\pi_f.$$

1.1.1 The Dimension of L_f

Proposition 1.1.2. *If f, L_f and K_f are as above, then $\dim_{K_f} L_f$ is the number of divisors of N/N_f where N_f is the level of the newform f.*

Proof. Let V_f be the complex vector space spanned by all images of Galois conjugates of f via all maps α_d with $d \mid N/N_f$. It follows from [Atkin-Lehner-Li theory – multiplicity one] that the images via α_d of the Galois conjugates of f are linearly independent. (Details: More generally, if f and g are newforms of level M, then by Proposition **??**, $B(f) = \{\alpha_d(f) : d \mid N/N_f\}$ is a linearly independent set and likewise for $B(g)$. Suppose some nonzero element f' of the span of $B(f)$ equals some element g' of the span of $B(g)$. Since T_p, for $p \nmid N$, commutes with α_d, we have $T_p(f') = a_p(f)f'$ and $T_p(g') = a_p(g)g'$, so $0 = T_p(0) = T_p(f' - g') = a_p(f)f' - a_p(g)g'$. Since $f' = g'$, this implies that $a_p(f) = a_p(g)$. Because a newform is determined by the eigenvalues of T_p for $p \nmid N$, it follows that $f = g$.) Thus the $\mathbf{C}$-dimension of V_f is the number of divisors of N/N_f times $\dim_{\mathbf{Q}} K_f$.

The factor L_f is isomorphic to the image of $\mathbf{T}_{\mathbf{Q}} \subset \mathrm{End}(S_k(\Gamma_1(N)))$ in $\mathrm{End}(V_f)$. As in Section **??**, there is a single element $v \in V_f$ so that $V_f = \mathbf{T}_{\mathbf{C}} \cdot v$. Thus the image of $\mathbf{T}_{\mathbf{Q}}$ in $\mathrm{End}(V_f)$ has dimension $\dim_{\mathbf{C}} V_f$, and the result follows. □

Let's examine a particular case of this proposition. Suppose q is a prime and $f = \sum a_n q^n$ is a newform of level N_f coprime to q, and let $N = N_f q$. We will show that

$$L_f = K_f[U]/(U^2 - a_q U + q),$$

hence $\dim_{K_f} L_f = 2$ which, as expected, is the number of divisors of $N/N_f = q$. The first step is to view L_f as the space of operators generated by the T_p acting on the span of the images $f(dz) = f(q^d)$ for $d \mid (N/N_f) = q$.

In our special case, T_p acts as the scalar a_p when $p \nmid N$. When $q \mid N$, the Hecke operator T_q acts as the operator also denoted U_q (see [...]). By Section **??**, we know that U_q corresponds to the matrix $\left(\begin{smallmatrix} a_q & 1 \\ -q & 0 \end{smallmatrix}\right)$ with respect to the basis $f(q), f(q^p)$. Thus U_q satisfies the relation $U_q^2 - a_q U + q$.

More generally, see [2, Lem. 4.4] (Diamond-Darmon-Taylor) for an explicit presentation of L_f as a quotient

$$L_f \cong K_f[\ldots, U_q, \ldots]/I$$

where I is an ideal and the U_q correspond to the prime divisors of N/N_f.

1.2 Decomposition of $J_1(N)$

Let f be a newform in $S_2(\Gamma_1(N))$ of level a divisor M of N, so $f \in S_2(\Gamma_1(M))_{\mathrm{new}}$ is a normalized eigenform for all the Hecke operators of level M. We associate to f an abelian subvariety A_f of $J_1(N)$, of dimension $[L_f : \mathbf{Q}]$, as follows. Recall that π_f is the fth projector in $\mathbf{T}_0 \otimes \mathbf{Q} = \prod_g K_g$. We can not define A_f to be the image of $J_1(N)$ under π_f, since π_f is only, a priori, an element of $\mathrm{End}(J_1(N)) \otimes \mathbf{Q}$. Fortunately, there exists a positive integer n such that $n\pi_f \in \mathrm{End}(J_1(N))$, and we let

$$A_f = n\pi_f(J_1(N)).$$

This is independent of the choice of n, since the choices for n are all multiples of the "denominator" n_0 of π_f, and if A is any abelian variety and n is a positive integer, then $nA = A$.

The natural map $\prod_f A_f \to J_1(N)$, which is induced by summing the inclusion maps, is an isogeny. Also A_f is simple if f is of level N, and otherwise A_f is isogenous to a power of $A'_f \subset J_1(N_f)$. Thus we obtain an isogeny decomposition of $J_1(N)$ as a product of $\mathbf{Q}$-simple abelian varieties.

Remark 1.2.1. The abelian varieties A_f frequently decompose further over $\overline{\mathbf{Q}}$, i.e., they are not absolutely simple, and it is an interesting problem to determine an isogeny decomposition of $J_1(N)_{\overline{\mathbf{Q}}}$ as a product of simple abelian varieties. It is still not known precisely how to do this computationally for any particular N.

This decomposition can be viewed in another way over the complex numbers. As a complex torus, $J_1(N)(\mathbf{C})$ has the following model:

$$J_1(N)(\mathbf{C}) = \mathrm{Hom}(S_2(\Gamma_1(N)), \mathbf{C})/H_1(X_1(N), \mathbf{Z}).$$

The action of the Hecke algebra $\mathbf{T}$ on $J_1(N)(\mathbf{C})$ is compatible with its action on the cotangent space $S_2(\Gamma_1(N))$. This construction presents $J_1(N)(\mathbf{C})$ naturally as $V/\mathcal{L}$ with V a complex vector space and $\mathcal{L}$ a lattice in V. The anemic Hecke algebra $\mathbf{T}_0$ then decomposes V as a direct sum $V = \bigoplus_f V_f$. The Hecke operators act on V_f and $\mathcal{L}$ in a compatible way, so $\mathbf{T}_0$ decomposes $\mathcal{L} \otimes \mathbf{Q}$ in a compatible way. Thus $\mathcal{L}_f = V_f \cap \mathcal{L}$ is a lattice in V_f, so we may $A_f(\mathbf{C})$ view as the complex torus $V_f/\mathcal{L}_f$.

Lemma 1.2.2. *Let $f \in S_2(\Gamma_1(N))$ be a newform of level dividing N and $A_f = n\pi_f(J_1(N))$ be the corresponding abelian subvariety of $J_1(N)$. Then the Hecke algebra $\mathbf{T} \subset \mathrm{End}(J_1(N))$ leaves A_f invariant.*

Proof. The Hecke algebra $\mathbf{T}$ is commutative, so if $t \in \mathbf{T}$, then

$$tA_f = tn\pi_f(J_1(N)) = n\pi_f(tJ_1(N)) \subset n\pi_f(J_1(N)) = A_f.$$

□

Remark 1.2.3. Viewing $A_f(\mathbf{C})$ as $V_f/\mathcal{L}_f$ is extremely useful computationally, since $\mathcal{L}$ can be computed using modular symbols, and $\mathcal{L}_f$ can be cut out using the Hecke operators. For example, if f and g are nonconjugate newforms of level dividing N, we can explicitly compute the group structure of $A_f \cap A_g \subset J_1(N)$ by doing a computation with modular symbols in $\mathcal{L}$. More precisely, we have

$$A_f \cap A_g \cong (\mathcal{L}/(\mathcal{L}_f + \mathcal{L}_g))_{\mathrm{tor}}.$$

Note that A_f depends on viewing f as an element of $S_2(\Gamma_1(N))$ for some N. Thus it would be more accurate to denote A_f by $A_{f,N}$, where N is any multiple of the level of f, and to reserve the notation A_f for the case $N = 1$. Then $\dim A_{f,N}$ is $\dim A_f$ times the number of divisors of N/N_f.

1.2.1 Aside: Intersections and Congruences

Suppose f and g are not Galois conjugate. Then the intersection $\Psi = A_f \cap A_g$ is finite, since $V_f \cap V_g = 0$, and the integer $\#\Psi$ is of interest. This cardinality is related to congruence between f and g, but the exact relation is unclear. For example, one might expect that $p \mid \#\Psi$ if and only if there is a prime $\wp$ of the compositum $K_f.K_g$ of residue characteristic p such that $a_q(f) \equiv a_q(g) \pmod{\wp}$ for all $q \nmid N$. If $p \mid \#\Psi$, then such a prime $\wp$ exists (take $\wp$ to be induced by a maximal ideal in the support of the nonzero $\mathbf{T}$-module $\Psi[p]$). The converse is frequently true, but is sometimes false. For example, if N is the prime 431 and

$$\begin{aligned} f &= q - q^2 + q^3 - q^4 + q^5 - q^6 - 2q^7 + \cdots \\ g &= q - q^2 + 3q^3 - q^4 - 3q^5 - 3q^6 + 2q^7 + \cdots, \end{aligned}$$

then $f \equiv g \pmod 2$, but $A_f \cap A_g = 0$. This example implies that "multiplicity one fails" for level 431 and $p = 2$, so the Hecke algebra associated to $J_0(431)$ is not Gorenstein (see [Lloyd Kilford paper] for more details).

1.3 Galois Representations Attached to A_f

It is important to emphasize the case when f is a newform of level N, since then A_f is $\mathbf{Q}$-simple and there is a compatible family of 2-dimensional ℓ-adic representations attached to f, which arise from torsion points on A_f.

Proposition 1.1.2 implies that $L_f = K_f$. Fix such an f, let $A = A_f$, let $K = K_f$, and let

$$d = \dim A = \dim_{\mathbf{Q}} K = [K : \mathbf{Q}].$$

Let ℓ be a prime and consider the $\mathbf{Q}_\ell$-adic Tate module $\mathrm{Tate}_\ell(A)$ of A:

$$\mathrm{Tate}_\ell(A) = \mathbf{Q}_\ell \otimes \varprojlim_{\nu>0} A[\ell^\nu].$$

Note that as a $\mathbf{Q}_\ell$-vector space $\mathrm{Tate}_\ell(A) \cong \mathbf{Q}_\ell^{2d}$, since $A[n] \cong (\mathbf{Z}/n\mathbf{Z})^{2d}$, as groups.

There is a natural action of the ring $K \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ on $\mathrm{Tate}_\ell(A)$. By algebraic number theory

$$K \otimes_{\mathbf{Q}} \mathbf{Q}_\ell = \prod_{\lambda \mid \ell} K_\lambda,$$

where λ runs through the primes of the ring $\mathcal{O}_K$ of integers of K lying over ℓ and K_λ denotes the completion of K with respect to the absolute value induced by λ. Thus $\mathrm{Tate}_\ell(A)$ decomposes as a product

$$\mathrm{Tate}_\ell(A) = \prod_{\lambda \mid \ell} \mathrm{Tate}_\lambda(A)$$

where $\mathrm{Tate}_\lambda(A)$ is a K_λ vector space.

Lemma 1.3.1. *Let the notation be as above. Then for all λ lying over ℓ,*

$$\dim_{K_\lambda} \mathrm{Tate}_\lambda(A) = 2.$$

Proof. Write $A = V/\mathcal{L}$, with $V = V_f$ a complex vector space and $\mathcal{L}$ a lattice. Then $\mathrm{Tate}_\lambda(A) \cong \mathcal{L} \otimes \mathbf{Q}_\ell$ as K_λ-modules (not as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules!), since $A[\ell^n] \cong \mathcal{L}/\ell^n\mathcal{L}$, and $\varprojlim_n \mathcal{L}/\ell^n\mathcal{L} \cong \mathbf{Z}_\ell \otimes \mathcal{L}$. Also, $\mathcal{L} \otimes \mathbf{Q}$ is a vector space over K, which must have dimension 2, since $\mathcal{L} \otimes \mathbf{Q}$ has dimension $2d = 2\dim A$ and K has degree d. Thus

$$\mathrm{Tate}_\lambda(A) \cong \mathcal{L} \otimes K_\lambda \approx (K \oplus K) \otimes_K K_\lambda \cong K_\lambda \oplus K_\lambda$$

has dimension 2 over K_λ. □

Now consider $\mathrm{Tate}_\lambda(A)$, which is a K_λ-vector space of dimension 2. The Hecke operators are defined over $\mathbf{Q}$, so $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $\mathrm{Tate}_\ell(A)$ in a way compatible with the action of $K \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$. We thus obtain a homomorphism

$$\rho_\ell = \rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}_{K\otimes\mathbf{Q}_\ell} \mathrm{Tate}_\ell(A) \approx \mathrm{GL}_2(K \otimes \mathbf{Q}_\ell) \cong \prod_\lambda \mathrm{GL}_2(K_\lambda).$$

Thus ρ_ℓ is the direct sum of ℓ-adic Galois representations ρ_λ where

$$\rho_\lambda : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{End}_{K_\lambda}(\mathrm{Tate}_\lambda(A))$$

gives the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $\mathrm{Tate}_\lambda(A)$.

If $p \nmid \ell N$, then ρ_λ is unramified at p (see [5, Thm. 1]). In this case it makes sense to consider $\rho_\lambda(\varphi_p)$, where $\varphi_p \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is a Frobenius element at p. Then $\rho_\lambda(\varphi_p)$ has a well-defined trace and determinant, or equivalently, a well-defined characteristic polynomial $\Phi(X) \in K_\lambda[X]$.

Theorem 1.3.2. *Let $f \in S_2(\Gamma_1(N), \varepsilon)$ be a newform of level N with Dirichlet character ε. Suppose $p \nmid \ell N$, and let $\varphi_p \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be a Frobenius element at p. Let $\Phi(X)$ be the characteristic polynomial of $\rho_\lambda(\varphi_p)$. Then*

$$\Phi(X) = X^2 - a_p X + p \cdot \varepsilon(p),$$

where a_p is the pth coefficient of the modular form f (thus a_p is the image of T_p in E_f and $\varepsilon(p)$ is the image of $\langle p \rangle$).

Let $\varphi = \varphi_p$. By the Cayley-Hamilton theorem

$$\rho_\lambda(\varphi)^2 - \mathrm{tr}(\rho_\lambda(\varphi))\rho_\lambda(\varphi) + \det(\rho_\lambda(\varphi)) = 0.$$

Using the Eichler-Shimura congruence relation (see) we will show that $\mathrm{tr}(\rho_\lambda(\varphi)) = a_p$, but we defer the proof of this until ....

We will prove that $\det(\rho_\lambda(\varphi)) = p$ in the special case when $\varepsilon = 1$. This will follow from the equality

$$\det(\rho_\lambda) = \chi_\ell, \tag{1.3.1}$$

where χ_ℓ is the ℓth cyclotomic character

$$\chi_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_\ell^* \subset K_\lambda^*,$$

which gives the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on μ_{ℓ^∞}. We have $\chi_\ell(\varphi) = p$ because φ induces induces pth powering map on μ_{ℓ^∞}.

It remains to establish (1.3.1). The simplest case is when A is an elliptic curve. In [7,], Silverman shows that $\det(\rho_\ell) = \chi_\ell$ using the Weil pairing. We will consider the Weil pairing in more generality in the next section, and use it to establish (1.3.1).

1.3.1 The Weil Pairing

Let $T_\ell(A) = \varprojlim_{n\geq 1} A[\ell^n]$, so $\mathrm{Tate}_\ell(A) = \mathbf{Q}_\ell \otimes T_\ell(A)$. The Weil pairing is a non-degenerate perfect pairing

$$e_\ell : T_\ell(A) \times T_\ell(A^\vee) \to \mathbf{Z}_\ell(1).$$

(See e.g., [3, §16] for a summary of some of its main properties.)

Remark 1.3.3. Identify $\mathbf{Z}/\ell^n\mathbf{Z}$ with μ_{ℓ^n} by $1 \mapsto e^{-2\pi i/\ell^n}$, and extend to a map $\mathbf{Z}_\ell \to \mathbf{Z}_\ell(1)$. If $J = \mathrm{Jac}(X)$ is a Jacobian, then the Weil pairing on J is induced by the canonical isomorphism

$$T_\ell(J) \cong \mathrm{H}^1(X, \mathbf{Z}_\ell) = \mathrm{H}^1(X, \mathbf{Z}) \otimes \mathbf{Z}_\ell,$$

and the cup product pairing

$$\mathrm{H}^1(X, \mathbf{Z}_\ell) \otimes_{\mathbf{Z}_\ell} \mathrm{H}^1(X, \mathbf{Z}_\ell) \xrightarrow{\cup} \mathbf{Z}_\ell.$$

For more details see the discussion on pages 210–211 of Conrad's appendix to [4], and the references therein. In particular, note that $\mathrm{H}^1(X, \mathbf{Z}_\ell)$ is isomorphic to $\mathrm{H}_1(X, \mathbf{Z}_\ell)$, because $\mathrm{H}_1(X, \mathbf{Z}_\ell)$ is self-dual because of the intersection pairing. It is easy to see that $\mathrm{H}_1(X, \mathbf{Z}_\ell) \cong T_\ell(J)$ since by Abel-Jacobi $J \cong T_0(J)/\mathrm{H}_1(X, \mathbf{Z})$, where $T_0(J)$ is the tangent space at J at 0 (see Lemma 1.3.1).

Here $\mathbf{Z}_\ell(1) \cong \varprojlim \mu_{\ell^n}$ is isomorphic to $\mathbf{Z}_\ell$ as a ring, but has the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ induced by the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $\varprojlim \mu_{\ell^n}$. Given $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, there is an element $\chi_\ell(\sigma) \in \mathbf{Z}_\ell^*$ such that $\sigma(\zeta) = \zeta^{\chi_\ell(\sigma)}$, for every ℓ^nth root of unity ζ. If we view $\mathbf{Z}_\ell(1)$ as just $\mathbf{Z}_\ell$ with an action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then the action of $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $\mathbf{Z}_\ell(1)$ is left multiplication by $\chi_\ell(\sigma) \in \mathbf{Z}_\ell^*$.

Definition 1.3.4 (Cyclotomic Character). The homomorphism

$$\chi_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_\ell^*$$

is called the *ℓ-adic cyclotomic character.*

If $\varphi : A \to A^\vee$ is a polarization (so it is an isogeny defined by translation of an ample invertible sheaf), we define a pairing

$$e_\ell^\varphi : T_\ell(A) \times T_\ell(A) \to \mathbf{Z}_\ell(1) \tag{1.3.2}$$

by $e_\ell^\varphi(a,b) = e_\ell(a, \varphi(b))$. The pairing (1.3.2) is a skew-symmetric, nondegenerate, bilinear pairing that is $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivariant, in the sense that if $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then

$$e_\ell^\varphi(\sigma(a), \sigma(b)) = \sigma \cdot e_\ell^\varphi(a,b) = \chi_\ell(\sigma) e_\ell^\varphi(a,b).$$

We now apply the Weil pairing in the special case $A = A_f \subset J_1(N)$. Abelian varieties attached to modular forms are equipped with a canonical polarization called the *modular polarization.* The canonical principal polarization of $J_1(N)$ is an isomorphism $J_1(N) \xrightarrow{\sim} J_1(N)^\vee$, so we obtain the modular polarization $\varphi = \varphi_A : A \to A^\vee$ of A, as illustrated in the following diagram:

$$\begin{tikzcd}
J_1(N) \arrow[r, "\text{autoduality} \cong"] & J_1(N)^\vee \arrow[d] \\
A \arrow[u] \arrow[r, "\text{polarization } \varphi_A"] & A^\vee
\end{tikzcd}$$

Consider (1.3.2) with $\varphi = \varphi_A$ the modular polarization. Tensoring over $\mathbf{Q}$ and restricting to $\mathrm{Tate}_\lambda(A)$, we obtain a nondegenerate skew-symmetric bilinear pairing

$$e : \mathrm{Tate}_\lambda(A) \times \mathrm{Tate}_\lambda(A) \to \mathbf{Q}_\ell(1). \tag{1.3.3}$$

The nondegeneracy follows from the nondegeneracy of e_ℓ^φ and the observation that

$$e_\ell^\varphi(\mathrm{Tate}_\lambda(A), \mathrm{Tate}_{\lambda'}(A)) = 0$$

when $\lambda \neq \lambda'$. This uses the Galois equivariance of e_ℓ^ϕ carries over to Galois equivariance of e, in the following sense. If $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and $x, y \in \mathrm{Tate}_\lambda(A)$, then

$$e(\sigma x, \sigma y) = \sigma e(x,y) = \chi_\ell(\sigma) e(x,y).$$

Note that σ acts on $\mathbf{Q}_\ell(1)$ as multiplication by $\chi_\ell(\sigma)$.

1.3.2 The Determinant

There are two proofs of the theorem, a fancy proof and a concrete proof. We first present the fancy proof. The pairing e of (1.3.3) is a skew-symmetric and bilinear form so it determines a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivarient homomorphism

$$\bigwedge_{K_\lambda}^2 \mathrm{Tate}_\lambda(A) \to \mathbf{Q}_\ell(1). \tag{1.3.4}$$

It is not *a priori* true that we can take the wedge product over K_λ instead of $\mathbf{Q}_\ell$, but we can because $e(tx, y) = e(x, ty)$ for any $t \in K_\lambda$. This is where we use that A is attached to a newform with trivial character, since when the character is nontrivial, the relation between $e(T_p x, y)$ and $e(x, T_p y)$ will involve $\langle p \rangle$. Let $D = \bigwedge^2 \mathrm{Tate}_\lambda(A)$ and note that $\dim_{K_\lambda} D = 1$, since $\mathrm{Tate}_\lambda(A)$ has dimension 2 over K_λ.

There is a canonical isomorphism

$$\mathrm{Hom}_{\mathbf{Q}_\ell}(D, \mathbf{Q}_\ell(1)) \cong \mathrm{Hom}_{K_\lambda}(D, K_\lambda(1)),$$

and the map of (1.3.4) maps to an isomorphism $D \cong K_\lambda(1)$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. Since the representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on D is the determinant, and the representation on $K_\lambda(1)$ is the cyclotomic character χ_ℓ, it follows that $\det \rho_\lambda = \chi_\ell$.

Next we consider a concrete proof. If $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then we must show that $\det(\sigma) = \chi_\ell(\sigma)$. Choose a basis $x, y \in \mathrm{Tate}_\lambda(A)$ of $\mathrm{Tate}_\lambda(A)$ as a 2 dimensional K_λ vector space. We have $\sigma(x) = ax + cy$ and $\sigma(y) = bx + dy$, for $a, b, c, d \in K_\lambda$. Then

$$\begin{aligned}
\chi_\ell(\sigma)e(x, y) &= \langle \sigma x, \sigma y \rangle \\
&= e(ax + cy, bx + dy) \\
&= e(ax, bx) + e(ax, dy) + e(cy, bx) + e(cy, dy) \\
&= e(ax, dy) + e(cy, bx) \\
&= e(adx, y) - e(bcx, y) \\
&= e((ad - bc)x, y) \\
&= (ad - bc)e(x, y)
\end{aligned}$$

To see that $e(ax, bx) = 0$, note that

$$e(ax, bx) = e(abx, x) = -e(x, abx) = -e(ax, bx).$$

Finally, since e is nondegenerate, there exists x, y such that $e(x, y) \neq 0$, so $\chi_\ell(\sigma) = ad - bc = \det(\sigma)$.

1.4 Remarks About the Modular Polarization

Let A and φ be as in Section 1.3.1. The degree $\deg(\varphi)$ of the modular polarization of A is an interesting arithmetic invariant of A. If $B \subset J_1(N)$ is the sum of all modular abelian varieties A_g attached to newforms $g \in S_2(\Gamma_1(N))$, with g not a Galois conjugate of f and of level dividing N, then $\ker(\varphi) \cong A \cap B$, as illustrated in the following diagram:

$$\begin{tikzcd}
 & \ker(\varphi_B) \arrow[d, "\cong"] \arrow[dr] & & \\
\ker(\varphi_A i) \arrow[r, "\cong"] \arrow[dr] & A \cap B \arrow[r] \arrow[d] & B \arrow[d] \arrow[dr] & \\
 & A \arrow[r] \arrow[dr, "\varphi"] & J_1(N) \arrow[r] \arrow[d] & B^\vee \\
 & & A^\vee &
\end{tikzcd}$$

Note that $\ker(\varphi_B)$ is also isomorphic to $A \cap B$, as indicated in the diagram.

In connection with Section **??**, the quantity $\ker(\varphi_A) = A \cap B$ is closely related to congruences between f and eigenforms orthogonal to the Galois conjugates of f.

When A has dimension 1, we may alternatively view A as a quotient of $X_1(N)$ via the map

$$X_1(N) \to J_1(N) \to A^\vee \cong A.$$

Then $\varphi_A : A \to A$ is pullback of divisors to $X_1(N)$ followed by push forward, which is multiplication by the degree. Thus $\varphi_A = [n]$, where n is the degree of the morphism $X_1(N) \to A$ of algebraic curves. The *modular degree* is

$$\deg(X_1(N) \to A) = \sqrt{\deg(\varphi_A)}.$$

More generally, if A has dimension greater than 1, then $\deg(\varphi_A)$ has order a perfect square (for references, see [3, Thm. 13.3]), and we define the *modular degree* to be $\sqrt{\deg(\varphi_A)}$.

Let f be a newform of level N. In the spirit of Section 1.2.1 we use congruences to define a number related to the modular degree, called the congruence number. For a subspace $V \subset S_2(\Gamma_1(N))$, let $V(\mathbf{Z}) = V \cap \mathbf{Z}[[q]]$ be the elements with integral q-expansion at ∞ and $V^\perp$ denotes the orthogonal complement of V with respect to the Petersson inner product. The *congruence number* of f is

$$r_f = \# \frac{S_2(\Gamma_1(N))(\mathbf{Z})}{V_f(\mathbf{Z}) + V_f^\perp(\mathbf{Z})},$$

where V_f is the complex vector space spanned by the Galois conjugates of f. We thus have two positive associated to f, the congruence number r_f and the modular degree m_f of of A_f.

Theorem 1.4.1. $m_f \mid r_f$

Ribet mentions this in the case of elliptic curves in [ZAGIER, 1985] [8], but the statement is given incorrectly in that paper (the paper says that $r_f \mid m_f$, which is wrong). The proof for dimension greater than one is in [AGASHE-STEIN, Manin constant...]. Ribet also subsequently proved that if $p^2 \nmid N$, then $\mathrm{ord}_p(m_f) = \mathrm{ord}_p(r_f)$.

We can make the same definitions with $J_1(N)$ replaced by $J_0(N)$, so if $f \in S_2(\Gamma_0(N))$ is a newform, $A_f \subset J_0(N)$, and the congruence number measures congruences between f and other forms in $S_2(\Gamma_0(N))$. In [**?**, Ques. 4.4], they ask whether it is always the case that $m_f = r_f$ when A_f is an elliptic curve, and m_f and r_f are defined relative to $\Gamma_0(N)$. I implemented an algorithm in MAGMA to compute r_f, and found the first few counterexamples, which occur when

$$N = 54, 64, 72, 80, 88, 92, 96, 99, 108, 120, 124, 126, 128, 135, 144.$$

For example, the elliptic curve A labeled 54B1 in [1] has $r_A = 6$ and $m_A = 2$. To see directly that $3 \mid r_A$, observe that if f is the newform corresponding to E and g is the newform corresponding to $X_0(27)$, then $g(q) + g(q^2)$ is congruent to f modulo 3. This is consistent with Ribet's theorem that if $p \mid r_A/m_A$ then $p^2 \mid N$. There seems to be no absolute bound on the p that occur.

It would be interesting to determine the answer to the analogue of the question of Frey-Mueller for $\Gamma_1(N)$. For example, if $A \subset J_1(54)$ is the curve isogeneous to 54B1, then $m_A = 18$ is divisible by 3. However, I do not know r_A in this case, because I haven't written a program to compute it for $\Gamma_1(N)$. *If somebody would like to work with me on this for a final project, let me know. The final project would involve: (1) reading relevant literature (I'll tell you the papers), (2) summarizing it, and (3) I'll code a program to compute r_A and m_A for $\Gamma_1(N)$, and you'll orchestrate running it.*

WEDNESDAY: Description of the Eichler-Shimura Congruence Relation I'll describe the relationship between T_p and Frobenius in characteristic p and use this relationship to prove that $\mathrm{tr}(\rho(\mathrm{Frob}_p)) = a_p$. In particular, this will finally explain why if E is an elliptic curve $p + 1 - \#E(\mathbf{F}_p)$ is the coefficient of p of the corresponding newform!

References

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

[2] 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.

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

[4] 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

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

[6] 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.

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

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