TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 270, Number 1, March 1982

CONGRUENCES BETWEEN SYSTEMS OF EIGENVALUES OF MODULAR FORMS

BY

NAOMI JOCHNOWITZ

ABSTRACT. We modify and generalize proofs of Tate and Serre in order to show that there are only a finite number of systems of eigenvalues for the Hecke operators with respect to $\Gamma_0(N)$ mod l. We also summarize results for $\Gamma_1(N)$.

Using these results, we show that an arbitrary prime divides the discriminant of the classical Hecke ring to a power which grows linearly with k. In this way, we find a lower bound for the discriminant of the Hecke ring. After limiting ourselves to cusp forms, we also find an upper bound.

Lastly we use the constructive nature of Tate and Serre's result to describe the structure and dimensions of the generalized eigenspaces for the Hecke operators mod l.

Introduction. Distinct eigenforms for the Hecke operators in characteristic zero often have congruent q-expansions modulo some prime. In fact, in the case of the full modular group, Atkin, Tate, and Serre proved that whereas there are infinitely many systems of eigenvalues for the Hecke operators in characteristic zero, there are only a finite number mod l. In particular, this implies that the Hecke operators are very nonsemisimple mod l. Tate and Serre's proof has been previously unpublished.

In this paper, we modify the proofs of Tate and Serre and generalize some of their results to the case of modular forms on the congruence subgroups $\Gamma_0(N)$. In particular, we show that there are only a finite number of systems of eigenvalues for the Hecke operators with respect to $\Gamma_0(N)$ mod l. Implicit in our proof is a bound for the number of such systems of eigenvalues. Later in the paper, we suggest a better bound, although our proof is only complete when the level is small. We also summarize the situation for $\Gamma_1(N)$.

Using the above-mentioned results, we obtain a lower bound for the discriminant of the Hecke ring in characteristic zero. In the process, we show that an arbitrary prime l divides the discriminant of the Hecke ring of weight k to a power which grows linearly with k. After limiting ourselves to cusp forms, we also use the Petersson conjecture to find an upper bound for the discriminant.

Lastly, we use the results about the finite number of systems of eigenvalues to derive information about the structure and dimension of the generalized eigenspaces for the Hecke operators mod l.

The author wishes to thank John Tate and David Kazhdan for their advice and concern, and especially Barry Mazur for his help and encouragement.

Received by the editors July 18, 1979 and, in revised form, February 6, 1981.
1980 *Mathematics Subject Classification.* Primary 10D12, 10D23.

0002-9947/81/0000-1034/$05.25

1. Background. Let N be a positive integer and let $A_k(N)$ (resp. $S_k(N)$) be the space of all modular forms (resp. all cusp forms) of weight k for the congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) | c \equiv 0 \pmod{N} \right\}.$$

We refer to $A_k(N)$ (resp. $S_k(N)$) as the space of modular (resp. cusp) forms of level N and weight k. By the q-expansion of a modular form f, we mean the q-expansion of f at infinity.

We recall the following formula which gives the action of the Hecke operator T_p (p a prime not dividing N) on the q-expansion of an element of $A_k(N)$:

$$T_p: \sum a_n q^n \mapsto \sum a_{np} q^n + p^{k-1} \sum a_n q^{np}.$$

More generally, if m is any integer relatively prime to N, we have

$$T_m: \sum_n a_n q^n \mapsto \sum_{d|m} d^{k-1} \sum_n a_{nm/d} q^{nd}.$$

For fixed weight k, each operator T_m can be expressed as a polynomial in the operators T_p. In this paper we deal exclusively with Hecke operators T_m where m is relatively prime to the level.

Fix a prime l not dividing N. Let $M_k(N)$ be the subset of $A_k(N)$ consisting of all forms whose q-coefficients at infinity are rational and l-integral.

DEFINITION 1.1. We define the space of modular forms mod l of weight k and level N, $\tilde{M}_k(N)$, to be the $\mathbf{F}_l$-vector space

$$\left\{ \tilde{f} = \sum \tilde{a}_n q^n | f = \sum a_n q^n \in M_k(N) \right\} \subseteq \mathbf{F}_l[[q]],$$

where the symbol $\tilde{a}_n$ denotes the reduction of a_n mod l.

Thus, according to this definition, a modular form mod l is identified with its q-expansion. Note that

$$\tilde{M}_k(N) \approx M_k(N)/lM_k(N) \approx M_k(N) \otimes \mathbf{F}_l.$$

Moreover, using the fact that $M_k(N)$ contains a basis for $A_k(N)$, one easily shows that $\dim_{\mathbf{F}_l} \tilde{M}_k(N) = \dim_{\mathbf{C}} A_k(N)$.

For the remainder of this paper, we assume that $l \geqslant 5$ unless otherwise specified. We define the space of all modular forms mod l of level N, $\tilde{M}(N)$, to be the subalgebra of $\mathbf{F}_l[[q]]$ which is the sum of the $\tilde{M}_k(N)$. This is not a direct sum since it can be shown that $\tilde{M}_k(N) \subseteq \tilde{M}_{k+l-1}(N)$ for all weights k. Conversely, $\tilde{M}_k(N)$ and $\tilde{M}_{k'}(N)$ have a nontrivial intersection if and only if $k \equiv k' \bmod l - 1$ ([**13**] and [**15**] for level one, [**7**] for arbitrary level).

DEFINITION 1.2. Given $f \in \tilde{M}_k(N)$, define the filtration of f, $w(f)$, to be the quantity $\inf\{j | f \in \tilde{M}_j(N)\}$.

DEFINITION 1.3. $W_k = (\tilde{M}_k(N) \otimes \bar{\mathbf{F}}_l)/(\tilde{M}_{k-l+1} \otimes \bar{\mathbf{F}}_l)$.

In other words, W_k is the quotient space of forms of weight k with coefficients in $\bar{\mathbf{F}}_l$, modulo the subvector space of all such forms of lower filtration.

The Hecke operators of weight k stabilize the set $M_k(N)$ and thus act on the space $\tilde{M}_k(N)$. The operator T_l coincides mod l with Atkin's U_l operator and is therefore

denoted by the letter U. Thus in terms of the q-expansion of a modular form mod l, we have the following formula:

$$U\colon \sum a_n q^n \mapsto \sum a_{nl} q^n.$$

Throughout this paper we write all operators on the right. We introduce two other operators on the space of modular forms mod l.

(a) $\theta = q(d/dq)\colon \sum a_n q^n \mapsto \sum n a_n q^n$,

(b) $V\colon \sum a_n q^n \mapsto \sum a_n q^{nl}$.

FACT 1.4. θ maps the space $\tilde{M}_k(N)$ to $\tilde{M}_{k+l+1}(N)$. In fact, $w(f|\theta) \leqslant w(f) + l + 1$ with equality if and only if l does not divide $w(f)$ ([**13**] and [**15**] for level one, [**8**] for higher levels).

COROLLARY 1.5. *If $\tilde{M}_k(N)$ contains no elements of filtration divisible by l, then θ is injective on it.*

FACT 1.6. $T_p \circ \theta = p\theta \circ T_p$.

Since for all $f \in \tilde{M}(N)$, $f|V = f^l$, the operator V clearly maps $\tilde{M}_k(N)$ to $\tilde{M}_{kl}(N)$. Moreover, we have the following equality.

FACT 1.7. $w(f|V) = lw(f)$.

PROOF. In level one, this is a trivial consequence of Lemma 1(b) of §2.2 of [**14**]. Moreover, using the notation of Katz, an element $f \in R_N^k$ has exact filtration k if and only if f is invertible at some zero of the Hasse invariant. (See §IV of [**8**].) This clearly implies the analogous lemma for higher levels. Q.E.D.

FACT 1.8. $V \circ T_p = T_p \circ V$ if $p \neq l$, $V \circ U = I$, $U \circ V = I - \theta^{l-1}$ where I is the identity map.

LEMMA 1.9. *$w(f|U) \leqslant (w(f) - 1)/l + l$ with equality if and only if $w(f) \equiv 1$ mod l. In particular, if $w(f) > l + 1$, U decreases the filtration.*

PROOF. By Fact 1.4, $w(f|\theta^{l-1}) \leqslant w(f) + l^2 - 1$ with equality if and only if $w(f) \equiv 1 \bmod l$. Since $f|UV = f - f|\theta^{l-1}$, we have $w(f|UV) = w(f|\theta^{l-1})$. Fact 1.7 concludes the proof. Q.E.D.

COROLLARY 1.10. *If $k > l + 1$, U annihilates the vector space W_k.*

COROLLARY 1.11. *If $w(f) \equiv 1 \bmod l$, then $f|U \neq 0$.*

REMARK. The operators θ, U, and V are related by the following exact sequence:

$$0 \to \tilde{M}(N) \xrightarrow{V} \tilde{M}(N) \xrightarrow{\theta} \tilde{M}(N) \xrightarrow{U} \tilde{M}(N) \to 0.$$

In particular, Kernel θ = Image V and Image θ = Kernel U.

PROPOSITION 1.12. *If k is sufficiently large, the Hecke operators do not act semisimply on $\tilde{M}_k(N)$.*

PROOF. One easily sees that when k is sufficiently large, $\tilde{M}_k(N)$ contains $f|V$ for some nonzero form f in the image of θ. But $f|V$ is annihilated by U^2 and not by U. Q.E.D.

In fact, one can show that the above conclusion is true whenever

$$k \geqslant \begin{cases} 2l^2 & \text{if } N > 1 \text{ or } l \geqslant 13, \\ 3l^2 - l & \text{if } N = 1 \text{ and } l = 11, 7, \\ 3l^2 + 3l & \text{if } N = 1 \text{ and } l = 5. \end{cases}$$

2. The finiteness of the number of systems of eigenvalues mod l. Fix a level N and a prime l such that $(l, 6N) = 1$.

DEFINITION 2.1. $\{\lambda_p\}_{(p,N)=1;\, p \text{ prime}}$ is called a system of eigenvalues of level N mod l if there exists a nonzero form $f \in \tilde{M}(N) \otimes \bar{\mathbf{F}}_l$ such that $f \mid T_p = \lambda_p f$ for all primes p not dividing N. To simplify notation, we sometimes write $\{\lambda_p\}$ to denote such a system.

The proof of the following theorem is a modification and generalization of a proof by Serre. The original proof was stated in the context of level one, but with a few adjustments extends to arbitrary level.

THEOREM 2.2. *There are only a finite number of systems of eigenvalues of level* N mod l.

PROOF. Let R be the subring of $\mathrm{End}_{\mathbf{F}_l} \tilde{M}(N)$ generated by the Hecke operators T_p where p is a prime not dividing N. We use the term Hecke module to mean a module over the ring R. Since the Hecke operators induce an action on the quotient space introduced in Definition 1.3, we can view W_k as a Hecke module.

DEFINITION 2.3. Let a be an integer with $1 \leqslant a \leqslant l - 1$ and define $W_k[a]$ to be the Hecke module $W_k \otimes F$, where F is a one-dimensional $\mathbf{F}_l$ vector space on which T_p acts as p^a.

The spaces $W_k[a]$ and W_k are clearly isomorphic as vector spaces. If $\{\lambda_p\}$ is a system of eigenvalues corresponding to W_k, then $\{p^a \lambda_p\}$ corresponds to $W_k[a]$. We refer to $W_k[a]$ (resp. to $\{p^a \lambda_p\}$) as a twist of W_k (resp. of $\{\lambda_p\}$). Each space W_k has only a finite number of twists.

The following theorem clearly suffices to prove Theorem 2.2.

THEOREM 2.4. *Any quotient* W_j *is isomorphic as a Hecke module to a twist of some* W_k *with* $0 \leqslant k \leqslant 2l$.

PROOF. We prove this theorem by showing that if $j > 2l$, W_j is isomorphic as a Hecke module to a twist of some W_m with $m < j$.

Case 1. $j \not\equiv 1 \pmod{l}$.

Fact 1.4 implies that θ induces a vector space embedding $\bar{\theta}$: $W_k \hookrightarrow W_{k+l+1}$ if l does not divide k.

LEMMA 2.5. *If* $k \geqslant l + 1$ *and* l *does not divide* k, *then the above embedding is a vector space isomorphism.*

PROOF. It suffices to show that W_k and W_{k+l+1} have the same dimension as $\bar{\mathbf{F}}_l$ vector spaces.

Using Theorem 2.23 of [**12**] one easily calculates

FORMULA 2.6. Let $k \geqslant l+1$, then

$$\begin{aligned}\dim_{\bar{\mathbf{F}}_l} W_k &= \dim_{\mathbf{F}_l} \tilde{M}_k(N) - \dim_{\mathbf{F}_l} \tilde{M}_{k-l+1}(N) \\ &= \dim_{\mathbf{C}} A_k(N) - \dim_{\mathbf{C}} A_{k-l+1}(N) \\ &= (l-1)(g-1) + (l-1)m/2 \\ &\quad + B([k/3] - [(k-l+1)/3]) \\ &\quad + C([k/4] - [(k-l+1)/4])\end{aligned}$$

where g is the genus of the Riemann surface corresponding to $\Gamma_0(N)$, m is the number of cusps, and B (resp. C) is the number of inequivalent elliptic points of order 2 (resp. 3).

Thus in order to prove the lemma, it suffices to show that

$$[k/3] - [(k-l+1)/3] \quad \text{and} \quad [k/4] - [(k-l+1)/4]$$

remain invariant when k is replaced by $k+l+1$. This is easily seen to be the case. Q.E.D.

Fact 1.6 and the above lemma imply that if $j > 2l$ and $j \not\equiv 1 \pmod{l}$, W_j is isomorphic to $W_{j-l-1}[1]$ as a Hecke module. This concludes Case 1 of the proof.

Case 2. $j \equiv 1 \pmod{l}$.

We complete the proof of Theorem 2.4 by showing that in this case W_j and $W_{(j-1)/l+l}$ are isomorphic as Hecke modules.

Lemma 1.9 implies that U induces a vector space embedding $\bar{U}$: $W_j \hookrightarrow W_{(j-1)/l+l}$ when $j \equiv 1 \pmod{l}$. Similarly, Fact 1.7 implies that V induces a vector space embedding $\bar{V}$: $W_{(j-1)/l+l} \hookrightarrow W_{j-1+l^2}$. Moreover, using Fact 1.8, we see that the composite map $\bar{U} \circ \bar{V}$: $W_j \hookrightarrow W_{j-1+l^2}$ equals the isomorphism $\bar{\theta}^{l-1}$. Thus $\bar{U}$ and $\bar{V}$ must each be vector space isomorphisms.

Furthermore, since U commutes with the other Hecke operators, the map $\bar{U}$ must be an isomorphism of Hecke modules. Q.E.D.

The theorem is also true for the case of $l = 2$ or 3 and $N = 1$, since when $l = 2$ all of the Hecke operators are nilpotent and when $l = 3$ the only system of eigenvalues is $\{1 + p\}$.

3. The discriminant of the Hecke ring in characteristic zero. Theorem 2.2 has a significant application dealing with the discriminant of the Hecke ring in characteristic zero.

More specifically, fix a level N, and let $\mathbf{T}_k$ denote the subring of $\mathrm{End}_{\mathbf{C}} A_k(N)$ generated by the Hecke operators T_p for primes p not dividing N.

Let n be the number of distinct systems of eigenvalues belonging to $A_k(N)$. In particular, in level one, n equals the dimension of $A_k(1)$.

The ring $\mathbf{T}_k \otimes \mathbf{Q}$ is isomorphic to a direct product of totally real number fields, the sum of whose degrees over $\mathbf{Q}$ equals n. Moreover, $\mathbf{T}_k$ is isomorphic to an order in this product of number fields. One defines the discriminant of $\mathbf{T}_k$, $d(\mathbf{T}_k)$, in the usual manner. That is, $d(\mathbf{T}_k)$ is defined to be the determinant of the matrix $\mathrm{Tr}(\alpha_i \alpha_j)$ where $\alpha_1, \ldots, \alpha_n$ form a $\mathbf{Z}$-basis for $\mathbf{T}_k$.

Let l be an arbitrary prime not dividing N such that $l \neq 2, 3$ if $N \neq 1$. We show in this section that the power to which l divides $d(\mathbf{T}_k)$ grows linearly with k. The analogous result is true in the case of cusp forms and in this case, using other methods we also find an upper bound.

The ideal $l\mathbf{T}_k$ can be written as a product $\prod Q_i$ of primary ideals Q_i whose radicals are the distinct maximal ideals containing $l\mathbf{T}_k$. The ring $\mathbf{T}_k/l\mathbf{T}_k$ is isomorphic to the direct product $\prod \mathbf{T}_k/Q_i$ and each $\mathbf{T}_k/Q_i$ is a local ring which contains its residue field.

We introduce the usual indices e_i and f_i. Thus $\mathbf{F}_{l^{f_i}}$ is the residue field of $\mathbf{T}_k/Q_i$ and e_i is the dimension of $\mathbf{T}_k/Q_i$ as an $\mathbf{F}_{l^{f_i}}$ vector space. Then $\sum e_i f_i = \dim_{\mathbf{F}_l} \mathbf{T}_k/l\mathbf{T}_k = n$ where n is as above.

Let $\operatorname{ord}_l(X)$ signify the power to which l divides X, and let $\mathcal{O}_k$ denote the maximal order in $\mathbf{T}_k \otimes \mathbf{Q}$. Then in a manner analogous to the case of a single number field we can prove the following.

LEMMA 3.1.

$$\operatorname{ord}_l(d(\mathbf{T}_k)) \geqslant \sum (e_i f_i - f_i) + \operatorname{ord}_l[\mathcal{O}_k : \mathbf{T}_k] \geqslant n - \sum f_i.$$

We define the ring R_k to be the subring of $\operatorname{End}_{\mathbf{F}_l} \tilde{M}_k$ generated by the Hecke operators T_p for primes p not dividing N. There exists a natural surjection Ψ_k: $\mathbf{T}_k/l\mathbf{T}_k \twoheadrightarrow R_k$, which in the case of the full modular group is known to be an isomorphism [**11**].

LEMMA 3.2. *The kernel of the above surjection is nilpotent.*

PROOF. Choose a polynomial T in the Hecke operators T_p (p prime and not dividing N) whose image $\overline{T}$ in $\mathbf{T}_k/l\mathbf{T}_k$ is in the kernel of Ψ_k. Then T annihilates all modular forms mod l of weight k. In particular, T annihilates all eigenforms in $\tilde{M}_k \otimes \overline{\mathbf{F}}_l$. Since conjugates of eigenvalues are eigenvalues, it follows that the eigenvalues belonging to T of weight k are contained in all prime ideals lying over l in the ring of algebraic integers.

Using the canonical identification of $\mathbf{T}_k$ with an order in a product of number fields, one sees that $\overline{T}$ is thus contained in all maximal ideals of $\mathbf{T}_k/l\mathbf{T}_k$. Since $\mathbf{T}_k/l\mathbf{T}_k$ is an Artin ring, the lemma follows. Q.E.D.

LEMMA 3.3. *Let R be an Artin local ring whose residue field is of finite degree d over $\mathbf{F}_l$. Then $R \otimes \overline{\mathbf{F}}_l$ has d maximal ideals.*

PROOF. Let $\mathfrak{m}$ be the unique maximal ideal of the ring R. Since $\mathfrak{m}$ is nilpotent, so is $\mathfrak{m} \otimes \overline{\mathbf{F}}_l$. It thus suffices to prove that the quotient ring $R \otimes \overline{\mathbf{F}}_l$ modulo the image of $\mathfrak{m} \otimes \overline{\mathbf{F}}_l$ has d maximal ideals. But this ring is isomorphic to $(R/\mathfrak{m}) \otimes \overline{\mathbf{F}}_l$, which is easily seen to be isomorphic to the direct sum of d copies of $\overline{\mathbf{F}}_l$. Q.E.D.

LEMMA 3.4. *The number $\sum f_i$ equals the number of systems of eigenvalues* mod l *of weight k.*

PROOF. Since the systems of eigenvalues mod l of weight k are in one-to-one correspondence with the maximal ideals of $R_k \otimes \overline{\mathbf{F}}_l$, it suffices to show that $R_k \otimes \overline{\mathbf{F}}_l$ has precisely $\sum f_i$ maximal ideals.

By tensoring the homomorphism Ψ_k (introduced above) with the identity map, we obtain

$$\Psi_k \otimes 1 : \mathbf{T}_k/l\mathbf{T}_k \otimes \bar{\mathbf{F}}_l \to R_k \otimes \bar{\mathbf{F}}_l.$$

The map is still surjective and its kernel equals $(\operatorname{Ker} \Psi_k) \otimes \bar{\mathbf{F}}_l$, which by Lemma 3.2 is nilpotent. This implies that $R_k \otimes \bar{\mathbf{F}}_l$ and $\mathbf{T}_k/l\mathbf{T}_k \otimes \bar{\mathbf{F}}_l$ have the same number of maximal ideals.

It remains to show that this number equals Σf_i. The ith local component of $\mathbf{T}_k/l\mathbf{T}_k$ has residue field $\mathbf{F}_{l^{f_i}}$. Since tensor product commutes with direct sum, we are done by the previous lemma. Q.E.D.

We now present the main theorem of this section.

THEOREM 3.5. *Let l be a prime not dividing N such that $l \neq 2, 3$ if $N \neq 1$. Then* $\operatorname{ord}_l(d(\mathbf{T}_k))$ *grows linearly with k.*

PROOF. By Lemma 3.1, $\operatorname{ord}_l(d(\mathbf{T}_k)) \geq n - \Sigma f_i$. By Lemma 3.4 and the definition of n, this bound equals the number of systems of eigenvalues in characteristic zero of weight k minus the number of systems of eigenvalues mod l of weight k. The first of these grows linearly with k, whereas Theorem 2.2 and the remark following it imply that the second is bounded. Q.E.D.

REMARK. Another theorem of the author shows that in the case of the full modular group, $\operatorname{ord}_l([\mathcal{O}_k\colon \mathbf{T}_k])$ approaches infinity as k does [**4**]. However, the present theorem shows that $\operatorname{ord}_l(d(\mathbf{T}_k))$ approaches infinity at a much faster rate than that implied by the result about the index.

For the sake of simplicity, we now limit ourselves to level one. Then the results of the next section imply that there are at most $[(l^2 + l)/12] + 1$ systems of eigenvalues of weight $k \bmod l$ for any l. By combining this with the previous theorem, we obtain the following.

PROPOSITION 3.6. *In level one, $d(\mathbf{T}_k)$ is divisible by $\prod l^{m_l}$, where*

$$m_l = \max\bigl(0, [k/12] - \bigl[(l^2 + l)/12\bigr] - 1\bigr).$$

We continue to restrict ourselves to level one. We let $\mathbf{T}_k^0$ be the Hecke ring of weight k defined on the space of cusp forms and $d(\mathbf{T}_k^0)$ be its discriminant. In other words, $\mathbf{T}_k^0$ is the subring of $\operatorname{End}_{\mathbf{C}} S_k(1)$ generated by the operators T_p for all primes p.

Then by mimicking the proof of Theorem 3.5, we can show that $\operatorname{ord}_l(d(\mathbf{T}_k^0))$ is greater than or equal to the number of systems of eigenvalues for cusp forms in characteristic zero of weight k minus the number of systems of eigenvalues for cusp forms mod l of weight k. Moreover, the first of these values is at least $[k/12] - 1$ and the second is at most $[(l^2 + l)/12]$.

Thus Proposition 3.6 remains true when we replace $d(\mathbf{T}_k)$ by $d(\mathbf{T}_k^0)$ and gives us a lower bound for $d(\mathbf{T}_k^0)$. We conclude this section by providing an upper bound.

Let $f_1, \ldots, f_s$ be the normalized eigenforms which are cusp forms of weight k on $\mathrm{SL}_2(\mathbf{Z})$. For each i $(1 \leq i \leq s)$, let $\tau_i\colon \mathbf{T}_k^0 \to \mathbf{C}$ be the homomorphism sending T_n to

$a_n(f_i)$ for all $n \geq 1$. Since the s operators $T_1, \ldots, T_s$ form a $\mathbf{Z}$ basis for $\mathbf{T}_k^0$ [**10**, Theorem 4.4, Chapter III], it is easy to show that $d(\mathbf{T}_k^0)$ equals the square of the determinant of the matrix $(\tau_i T_j)$.

The Petersson conjecture, proven in [**2**], thus implies that $|\tau_i T_j| \leq 2^{\sigma_0(j)} j^{(k-1)/2}$, where $\sigma_0(j)$ is the number of distinct divisors of j.

Using the definition of determinant, one easily shows the following estimate.

ESTIMATE 3.7.

$$\begin{aligned} d(\mathbf{T}_k^0) &\leq (s!)^{k+1} 4^{\Sigma_{j=1}^{s} \sigma_0(j)} \\ &= (s!)^{k+1} 4^{\Sigma_{j=1}^{s} [s/j]} \leq (s!)^{k+1} 4^{s \Sigma_{j=1}^{s} 1/j} \\ &\leq (s!)^{k+1} 4^{s((\ln s)+1)} \leq (s!)^{k+1} s^{2s} 4^{s} \\ &\leq (k/12)^{k^2/12 - 3k/4 - 1} 4^{k/12}. \end{aligned}$$

4. A better bound for the number of systems of eigenvalues mod l. As before, let l be a prime not dividing N such that $l \neq 2, 3$ if $N \neq 1$. Theorem 2.4 implies that any system of eigenvalues of level N mod l is a twist of a system of weight less than or equal to $2l$. In the present section, we improve this bound for level one and certain other levels of low genus.

In level one the proof is due to Tate and Serre, and its generalization to the levels mentioned above is, for the most part, straightforward. The computations involved are significantly more complicated in those cases when the level is not square-free. The author believes the theorem to be true for all levels, but has not completed the proof for arbitrary level.

THEOREM 4.1. *Any system of eigenvalues of level $N \leq 17$ or $N = 19$ or 23 is a twist of a system of weight less than or equal to $l + 1$.*

PROOF. By Theorem 2.4, it suffices to show that any system of eigenvalues belonging to W_{j+l+1} with $2 \leq j \leq l - 1$ is a twist of a system belonging to W_j or W_{l+1-j}.

Let $\phi_1 = \bar{\theta}$: $W_j[1] \hookrightarrow W_{j+l+1}$ be the embedding introduced in §2. Since $j < l + 1$, this need not be an isomorphism. Let ϕ_2: $W_{l+1-j}[j] \hookrightarrow W_{j+l+1}$ be the embedding obtained by composing the map

$$\bar{V}\colon W_{l+1-j}[j] \to W_{(l+1-j)l}[j]$$

with the inverse of the isomorphism

$$\bar{\theta}^{l-j-1}\colon W_{j+l+1} \xrightarrow{\approx} W_{(l+1-j)l}[j].$$

It is shown in Appendix A that the image under ϕ_1 of the space spanned by the Eisenstein series in W_j coincides with the image under ϕ_2 of the span of the Eisenstein series in W_{l+1-j}.

It thus becomes handy to introduce the following notation. Let $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ denote the direct sum of the images of the two maps except that we identify those Eisenstein series whose images coincide. A precise definition of $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ is given in Appendix A.

We view both W_{j+l+1} and $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ as representations of R_{j+l+1}, the Hecke algebra mod l of weight $j + l + 1$. Since the dimensions of these two representations are equal, as a first attempt at proving the theorem, one might conjecture that they are isomorphic.

Unfortunately, as Tate pointed out, this is not the case in general, for the images of ϕ_1 and ϕ_2 may intersect in places other than the Eisenstein series. For example, when $l = 23$ and $j = 12$, $\phi_1(\tilde{\Delta})$ is a scalar multiple of $\phi_2(\tilde{\Delta})$.

However, we show in Lemma B.1 of Appendix B that even though the Hecke representations W_{j+l+1} and $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ may be nonisomorphic, they must have the same trace. We now make use of the following fact which is implied by the proof of Proposition 3, no. 1 of [**1**, §12].

FACT 4.2. If the traces of two finite-dimensional representations of a commutative $\mathbf{F}_l$-algebra are equal, then the multiplicities of each simple component of their semisimplifications are congruent to each other mod l.

In level one, since the dimensions of both of the above representations are less than l, Fact 4.2 and Lemma B.1 imply that they have isomorphic semisimplifications. In particular, we conclude that any system of eigenvalues belonging to W_{j+l+1} is a twist of a system of weight j or weight $l + 1 - j$, and thus prove the theorem in this case.

Unfortunately, as the level N increases, the dimensions of our two representations get arbitrarily large and we can no longer use the above argument. However, when the Riemann surface associated to $\Gamma_0(N)$ has low genus, the dimensions of our representations will be small.

We want to determine conditions sufficient for concluding that the two representations have isomorphic semisimplifications. It is clear, for example, that this will be true exactly as in level one, whenever the dimensions of both representations are less than l. Moreover, an elementary argument shows that we can make the above conclusion as long as the dimension of the intersection of image ϕ_1 with image ϕ_2, minus the dimension of the span of the Eisenstein series, is less than l. This is because in such a case, the multiplicities (in the two semisimplifications) of a simple component will be congruent mod l if and only if they are equal.

Since, when $N > 1$, $\dim S_k(N)$ is an increasing function of k, the above remarks imply that Theorem 4.2 is true whenever the dimension of the space of cusp forms of weight $2[(l + 1)/4]$ is less than l. Using Theorem 2.24 of [**12**], it can be shown that this is so whenever $N \leqslant 17$ or when $N = 19$ or 23 as well as in some other cases when l is small.

5. Modular forms for $\Gamma_1(N)$. Let N be a fixed integer and $l \neq 2, 3$ a prime not dividing N. Let $A_1(N, k)$ be the space of all modular forms of weight k for the group

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid a \equiv d \equiv 1 \pmod{N} \right\}.$$

The group $(\mathbf{Z}/N\mathbf{Z})^* \approx \Gamma_0(N)/\Gamma_1(N)$ acts on the space $A_1(N, k)$ in a canonical manner. More precisely, if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ and $f \in A_1(N, k)$, the form $f|_k\gamma$,

defined by

$$f|_k\gamma(z) = f\left(\frac{az+b}{cz+d}\right)(cz+d)^{-k},$$

depends only on the image of d in $(\mathbf{Z}/N\mathbf{Z})^*$ and is denoted by $f|R_d$. The operators R_d commute with the Hecke operators.

If p is a prime not dividing N, the formula for the action of the Hecke operator T_p on the q-expansion at infinity of an element of $A_1(N, k)$ is given by

FORMULA 5.1.

$$T_p\colon \sum a_n(f)q^n \mapsto \sum a_{np}(f)q^n + p^{k-1}\sum a_n(f|R_p)q^{np}.$$

The Hecke ring $\mathbf{T}_1(N, k)$ is defined to be the commutative subring of $\mathrm{End}_{\mathbf{C}} A_1(N, k)$ generated by the operators R_d for $d \in (\mathbf{Z}/N\mathbf{Z})^*$ and T_p for primes p not dividing N. The ring $\mathbf{T}_1(N, k) \otimes \mathbf{Q}$ is well known to be a product of number fields and $\mathbf{T}_1(N, k)$ is an order in this product.

Let $M_1(N, k)$ be the set of all $f \in A_1(N, k)$ such that the q-expansions at infinity of all of the forms $f|R_d$ have rational and l-integral coefficients. We define the space of modular forms mod l, $\tilde{M}_1(N, k)$, to be the $\mathbf{F}_l$ vector space $M_1(N, k)/lM_1(N, k) \approx M_1(N, k) \otimes \mathbf{F}_l$. It is easy to check that $\dim_{\mathbf{F}_l} \tilde{M}_1(N, k) = \dim_{\mathbf{C}} A_1(N, k)$.

The canonical homomorphism $\tilde{M}_1(N, k) \to \mathbf{F}_l[[q]]$ defined by sending f to the reduction mod l of its q-expansion at infinity may no longer be an embedding. However, there is a canonical embedding of $\tilde{M}_1(N, k)$ into $\mathbf{F}_l[[q]]^{\phi(N)}$ obtained by considering the q-expansions of all of the forms $f|R_d$.

The operators R_d and T_p stabilize $\tilde{M}_1(N, k)$, and the formula for the action of the Hecke operators on each of the $\phi(N)$ components of a modular form f is given by the reduction of Formula 5.1. The operator T_l is again denoted by the letter U. The concept of filtration generalizes and it is clear that $w(f|R_d) = w(f)$ for any f and d.

The definitions of θ and V extend to this case. For example, if $(\sum a_{n,1}q^n, \ldots, \sum a_{n,\phi(N)}q^n)$ is the $\phi(N)$-tuple of q-expansions corresponding to a form f, then $(\sum na_{n,1}q^n, \ldots, \sum na_{n,\phi(N)}q^n)$ corresponds to $f|\theta$. Both θ and V commute with the operators R_d and the following facts follow from the work of Katz [7], [8].

FACT 5.2. $w(f|\theta) \leqslant w(f) + l + 1$ with equality if and only if $l \nmid w(f)$.

FACT 5.3. $w(f|V) = lw(f)$.

It is then straightforward to prove the following two theorems.

THEOREM 5.4. *There are only a finite number of systems of eigenvalues for* $\Gamma_1(N)$ mod l. *In fact, any such system of eigenvalues is a twist of a system of weight less than or equal to* $2l$.

PROOF. The proof is similar to that of Theorem 2.2.

THEOREM 5.5. *The power of* l *dividing the discriminant of* $\mathbf{T}_1(N, k)$ *grows linearly with* k.

PROOF. The proof is analogous to that of Theorem 3.5.

Moreover, it is natural to conjecture the following.

CONJECTURE 5.6. Any system of eigenvalues for $\Gamma_1(N)$ of even (resp. odd) weight is a twist of a system of weight less than or equal to $l + 1$ (resp. $l + 2$).

REMARK. In approaching this conjecture the author has considered square-free levels and has proven this conjecture for $N = 1, 2, 3, 5$ and 6. The proof for these levels is analogous to that of Theorem 4.2, except that in the case of $\Gamma_1(N)$, one must consider the operators $T_m R_d$ in addition to the operators T_m. The computation involving the trace goes through for all square free N, but as in §4 only proves the theorem when the dimensions are small.

6. The structure and dimensions of the generalized eigenspaces mod l. For purposes of simplicity, we restrict ourselves to level one in this section, although similar results can be obtained for other levels. We fix a prime $l \neq 2, 3$. We have already seen that the operator $U = T_l$ annihilates the vector space W_j whenever $j \geqslant l + 1$. In particular, whenever $j \geqslant l + 1$, W_j can have a nonzero eigenspace associated to the system of eigenvalues $\{\lambda_p\}$ only if $\lambda_l = 0$.

For each system of eigenvalues $\{\lambda_p\}$ such that $\lambda_l = 0$, we are interested in determining which W_j contain a nonzero eigenspace associated to $\{\lambda_p\}$. We are also interested in determing the dimensions of the corresponding generalized eigenspaces.[1] These questions are answered by Theorems 6.3 and 6.6 below.

Certain steps in the proofs of these theorems rely on computations carried out in the author's Ph.D. thesis [**6**], and we have decided not to reproduce them in full detail. Thus, we will give what should be regarded merely as an outline of the proof.

DEFINITION 6.1. Let $\{\delta_p\}$, $\{\gamma_p\}$ be systems of eigenvalues. We say that $\{\delta_p\}$ is an l-prime twist of $\{\gamma_p\}$ if $\delta_p = p^a \gamma_p$ for some a and all $p \neq l$.

The following lemma is helpful in understanding the results of this section.

LEMMA 6.2. *Let $\{\delta_p\}$ be a system of eigenvalues of filtration $4 \leqslant k \leqslant l + 1$. Then:*

(1) *If $\delta_l = 0$, $\{p^{l+1-k}\delta_p\}$ is a system of eigenvalues of filtration $l + 3 - k$ and no other system of eigenvalues of filtration $4 \leqslant k' \leqslant l + 1$ is an l-prime twist of $\{\delta_p\}$.*

(2) *If $\delta_l \neq 0$ and $k \neq l + 1$, there may exist a system of eigenvalues $\{\gamma_p\}$ of filtration $l + 1 - k$ such that $\gamma_p = p^{l-k}\delta_p$ when $p \neq l$, and no other system of eigenvalues of filtration $4 \leqslant k' \leqslant l + 1$ is an l-prime twist of $\{\delta_p\}$.*

(3) *If $k = l + 1$, no other system of eigenvalues of filtration $4 \leqslant k' \leqslant l + 1$ is an l-prime twist of $\{\delta_p\}$.*

PROOF. The proof involves a straightforward application of Tate's θ cycles. This theory is presented in [**5**]. Q.E.D.

Statement of first result. Introductory notation. Let $\{\lambda_p\}$ be a fixed system of eigenvalues with $\lambda_l = 0$. By Theorem 4.1 we can choose a system of eigenvalues $\{\delta_p\}$ of filtration $4 \leqslant m \leqslant l + 1$ such that $\{\lambda_p\} = \{p^B \delta_p\}$ for some $B = 0, \ldots, l - 1$. As Lemma 6.2 implies, the choice of m and B is not always unique. When $\delta_l = 0$, we normalize our choice so that $B \leqslant l - m$.

We then choose integers A and k according to the following rule.

(1) If $B \leqslant l - m$ or $m = l + 1$, set $k = m$ and $A = B$.

(2) Otherwise set $k = l + 1 - m$ and $A = B - l + m$.

---

[1] DEFINITION. The generalized eigenspace corresponding to $\{\lambda_p\}$ in W_j is defined to be the maximal subspace of W_j which is annihilated by some power of the operators $T_p - \lambda_p$ for each prime p.

THEOREM 6.3. *Keep the above notation. Then the quotient space W_j contains a nonzero eigenspace for $\{\lambda_p\}$ if and only if one of the following is true for some positive integer n.*

(a) $j = k + A(l+1) + n(l^2-1)$.

(b) $j = kl + A(l+1) + n(l^2-1)$.

(c) $j = k + l - 1 + A(l+1) + n(l^2-1)$ *and* $\delta_l = 0$.

(d) $j = kl - l + 1 + A(l+1) + n(l^2-1)$ *and* $\delta_l = 0$.

Outline of the proof.

LEMMA 6.4. *Let $j > l+1$; then the semisimplification of W_j is isomorphic to that of W_{j+l^2-1} as a Hecke module.*

PROOF. If $j \equiv 1 \bmod l$, Lemma 2.5 and Corollary 1.10 imply that W_j is itself isomorphic to W_{j+l^2-1}. The case where $j \not\equiv 1 (\bmod l)$ is proven by repeated applications of the various maps introduced in §2. For details see XIII.2 of [**6**]. Q.E.D.

Lemma 6.4 reduces the proof of the theorem to determining which spaces W_j, with $j \leqslant l^2 + l$, have nonzero eigenspaces corresponding to $\{\lambda_p\}$. The proof is then concluded by making use of the constructive nature of the proofs of Theorems 2.4 and 4.1. For details see XIII.4 of [**6**]. Q.E.D.

Second result. The analogous procedure is used to determine the dimensions of the generalized eigenspaces corresponding to $\{\lambda_p\}$. Details can be found in XIII.9 of [**6**]. The results are listed below.

Notation. Let $\{\lambda_p\}$ and $\{\delta_p\}$ be as above. Thus $\{\lambda_p\} = \{p^B\delta_p\}$ where $\{\delta_p\}$ is of filtration $4 \leqslant m \leqslant l+1$.

DEFINITION 6.5. (a) Let S_δ be the generalized eigenspace in W_m corresponding to the system $\{\delta_p\}$.

(b) If $\delta_l \neq 0$ and $m \neq l+1$ let P_δ be the generalized eigenspace in W_{l+1-m} corresponding to an l-prime twist of $\{\delta_p\}$. According to Lemma 6.2, P_δ may be trivial.

(c) If $\delta_l = 0$, let Q_δ be the generalized eigenspace in W_{l+3-m} corresponding to $\{p^{l+1-m}\delta_p\}$. According to Lemma 6.2, Q_δ is never trivial.

THEOREM 6.6. *Keep the above notation and suppose that W_j has a nonzero eigenspace corresponding to the system of eigenvalues $\{\lambda_p\}$. Then*:

(1) *If $m = l+1$, the generalized eigenspace in W_j corresponding to $\{\lambda_p\}$ has the same dimension as S_δ.*

(2) *If $m \neq l+1$ and $\delta_l \neq 0$, then the dimension of the generalized eigenspace in W_j corresponding to $\{\lambda_p\}$ equals*

$$\dim S_\delta + \dim P_\delta - \begin{cases} 1 & \text{if } \{\delta_p\} = \{1 + p^{m-1}\}, \\ 0 & \text{otherwise.} \end{cases}$$

(3) *If $\delta_l = 0$, then the generalized eigenspace in W_j corresponding to $\{\lambda_p\}$ has the same dimension as S_δ in cases* (a) *and* (b) *of Theorem* 6.3 *and the same dimension as Q_δ in cases* (c) *and* (d).

Appendix A: The image of the span of the Eisenstein series. Keep the definitions and notations of §4. We claimed there that the image under ϕ_1 of the space spanned by the Eisenstein series in W_j coincides with the image under ϕ_2 of the span of the Eisenstein series in W_{l+1-j}. We now prove this claim and use this proof to make precise the definition of the representation $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ introduced in §4.

Level one. For simplicity, we first treat the case of level one. Then when $j = 2$ or $l - 1$, the claim is vacuously true since there are no nonzero Eisenstein series in either W_j or W_{l+1-j}. Otherwise, if G_k denotes the Eisenstein series of weight k normalized so that $a_1(G_k) = 1$, a direct examination of the q-expansions shows that $G_j \mid \theta^{l-j} = G_{l+1-j} \mid \theta^{l-1}$. By Fact 1.8, this implies that

$$G_j \mid \theta \mid \theta^{l-j-1} = G_{l+1-j} \mid \theta^{l-1} = G_{l+1-j} - G_{l+1-j} \mid UV = G_{l+1-j} - G_{l+1-j} \mid V$$

and, hence, that $-G_j \mid \theta \mid \theta^{l-j-1}$ and $G_{l+1-j} \mid V$ have equivalent images in the quotient space $W_{(l+1-j)l}$. It then follows directly from the definitions of ϕ_1 and ϕ_2 that $\phi_2(G_{l+1-j}) = -\phi_1(G_j)$.

We can now make the definition of $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ explicit in level one.

DEFINITION A.1 (LEVEL ONE). Let $\mathcal{V}_j$ be the direct sum of $\phi_1(W_j)$ and $\phi_2(W_{l+1-j})$. If $j \neq 2$ or $l - 1$, let $\mathcal{E}_j$ be the subspace of $\mathcal{V}_j$ spanned by $\phi_2(G_{l+1-j}) + \phi_1(G_j)$, and if $j = 2$ or $l - 1$, let $\mathcal{E}_j$ be the zero vector space. Then $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ is defined to be the quotient space $\mathcal{V}_j/\mathcal{E}_j$.

Arbitrary level N. The idea in the general case is essentially the same, although the Eisenstein series involved look more complicated. Let χ be a primitive character of conductor f such that f^2 divides N. In particular, when N is square-free we only consider the trivial character.

For any integer ν let

$$\sigma_\nu(\chi, n) = \sum_{t \mid n} \chi(t)\bar{\chi}\left(\frac{n}{t}\right)t^\nu,$$

and for any positive even integer k, let b_k be the kth Bernoulli number. Let

$$G_k(\chi) = \begin{cases} \dfrac{-b_k}{2k} + \displaystyle\sum_{n=1}^{\infty} \sigma_{k-1}(\chi, n)q^n & \text{if } \chi \text{ is trivial,} \\ \displaystyle\sum_{n=1}^{\infty} \sigma_{k-1}(\chi, n)q^n & \text{otherwise.} \end{cases}$$

For any integer d, let B_d be the operator which takes $\sum a_n q^n$ to $\sum a_n q^{nd}$.

Then we define

$$G_k(\chi, d) = \begin{cases} G_2(\chi) - dG_2(\chi) \mid B_d & \text{if } k = 2 \text{ and } \chi \text{ is trivial,} \\ d(G_{l-1}(\chi) - G_{l-1}(\chi) \mid B_d) & \text{if } k = l - 1 \text{ and } \chi \text{ is trivial,} \\ G_k(\chi) \mid B_d & \text{otherwise.} \end{cases}$$

The space of Eisenstein series in W_k is spanned by those series of the form $G_k(\chi, d)$ where χ is primitive of conductor f and $f^2 d$ divides N. Note that when χ is

the trivial character and $d = 1$, we can obviously omit the series $G_2(\chi, d) = 0 = G_{l-1}(\chi, d)$.

By comparing q-expansions, one easily sees that

$$d^{j-1}G_j(\bar{\chi}, d) \mid \theta^{l-j} = G_{l+1-j}(\chi, d) \mid \theta^{l-1}.$$

Since $G_{l+1-j}(\chi, d)$ is an eigenvector for the operator U with eigenvalue $\bar{\chi}(l)$, then by Fact 1.8,

$$\begin{aligned} G_{l+1-j}(\chi, d) \mid \theta^{l-1} &= G_{l+1-j}(\chi, d) - G_{l+1-j}(\chi, d) \mid UV \\ &= G_{l+1-j}(\chi, d) - \bar{\chi}(l)G_{l+1-j}(\chi, d) \mid V. \end{aligned}$$

By combining the above two equations, we see that $-\chi(l)d^{j-1}G_j(\bar{\chi}, d) \mid \theta^{l-j}$ and $G_{l+1-j}(\chi, d) \mid V$ have equivalent images in the quotient space $W_{(l+1-j)l}$. It then directly follows from the definitions of ϕ_1 and ϕ_2 that

$$\phi_2\big(G_{l+1-j}(\chi, d)\big) = -\chi(l)d^{j-1}\phi_1\big(G_j(\bar{\chi}, d)\big).$$

We now define $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ in the general case.

DEFINITION A.1 (ARBITRARY LEVEL). Let $\mathfrak{V}_j$ be the direct sum of $\phi_1(W_j)$ and $\phi_2(W_{l+1-j})$ and let $\mathfrak{S}_j$ be the subspace of $\mathfrak{V}_j$ spanned by the elements $\phi_2(G_{l+1-j}(\chi, d)) + \chi(l)d^{j-1}\phi_1(G_j(\bar{\chi}, d))$ where χ and d are as above. Then $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ is defined to be the quotient space $\mathfrak{V}_j/\mathfrak{S}_j$.

Appendix B. A calculation involving the Selberg trace formula. Keep the definitions and notations of §4 and recall that we reduced the proof of Theorem 4.1 to that of the following proposition.

PROPOSITION B.1. *W_{j+l+1} and $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ have the same trace when considered as representations of R_{j+l+1}.*

PROOF. Any $T \in R_{j+l+1}$ can be written as an $\mathbf{F}_l$-linear combination of operators of the form T_m for integers m prime to N. Thus it suffices to prove that the trace of T_m is the same on both representations.

To do this we use the Eichler-Selberg trace formula, which gives us a method for evaluating the trace of T_m on the space of cusp forms of fixed weight in characteristic zero.

We will use a version of this formula which is found in IV.8.4 of [**9**].[2]

For integers n, u let $S(n, u)$ be as defined in IV.1.10 of [**9**], let $\omega(n)$ be the number of prime divisors of n, let

$$\Psi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right) \quad \text{and} \quad \sigma_1(n) = \sum_{d \mid n} d.$$

[2] In the square-free case, see also [**3**, Chapter III, §7] and [**9**, Remark 1, p. 127].

Then the trace of the operator T_m on the space $S_k(N)$ is given by

FORMULA B.2.

$$\begin{aligned}\text{Trace } T_m = &\sum_{\alpha} H_\alpha \frac{\alpha^{k-1} - \bar{\alpha}^{k-1}}{\alpha - \bar{\alpha}} \\ &-2^{\omega(N)-1} \sum_{\substack{uv=m \\ u>0}} \min(u, v)^{k-1} S(N, v-u) \\ &+ \begin{cases} \sigma_1(m) & \text{if } k = 2, \\ 0 & \text{otherwise,} \end{cases} \\ &+ \begin{cases} \frac{1}{12}\Psi(N) m^{k/2-1}(k-1) & \text{if } m \text{ is a square,} \\ 0 & \text{otherwise,} \end{cases}\end{aligned}$$

where the elements $\alpha, \bar{\alpha}$ run through all complex numbers of absolute value m such that $\mathbf{Q}(\alpha)$ is a quadratic imaginary field. For our purposes, it suffices to note that H_α is some quantity which depends only on α and, in particular, is independent of the weight. Note that $\alpha = \sqrt{m}\lambda$ in the notation of [**9**].

LEMMA B.3.

$$2^{\omega(n)} S(n, u) = \sum_{\substack{f^2 | n \\ f | u}} 2^{\omega(n/f^2)} \phi(f).$$

PROOF. Both sides of the equation are multiplicative in u and n and agree on powers of primes. (See [**9**, IV.1.11].) Q.E.D.

For the rest of this section, in order to simplify our presentation, we assume that $j \neq 2$ and $j \neq l-1$. We write $\mathcal{E}_j(N)$ to be the subspace spanned by the Eisenstein series in $A_j(N)$. We want to show that T_m has the same trace in $\phi_1(W_j) \oplus_* \phi_2(W_{l+1-j})$ as in W_{l+1+j}.

Equivalently, we must show

CONGRUENCE B.4.

$$\begin{aligned}m\big(\text{Trace } T_m \text{ on } S_j(N)\big) + m^j\big(\text{Trace } T_m \text{ on } S_{l+1-j}(N)\big) + m\big(\text{Trace } T_m \text{ on } \mathcal{E}_j(N)\big) \\ \equiv \text{Trace } T_m \text{ on } S_{j+l+1} - \text{Trace } T_m \text{ on } S_{j+2} \pmod{l}.\end{aligned}$$

This congruence follows by a direct computation after applying the following two lemmas, the first of which is due to Tate.

LEMMA B.5 (TATE). *Let* $F_k(X, Y) = X^{k-2} + X^{k-3}Y + \cdots + Y^{k-2}$ *and let* $\alpha, \bar{\alpha}$ *be roots of the quadratic polynomial* $x^2 - rx + m = 0$. *Then modulo any prime lying above* l, *we have the following equality.*

$$F_{j+l+1}(\alpha, \bar{\alpha}) = F_{j+2}(\alpha, \bar{\alpha}) + mF_j(\alpha, \bar{\alpha}) + m^j F_{l+1-j}(\alpha, \bar{\alpha}).$$

PROOF. Break the polynomial $F_{j+l+1}(\alpha, \bar{\alpha})$ into the following three groupings.

Grouping I. $\alpha^{j+l-1} + \cdots + \alpha^l \bar{\alpha}^{j-1}$.

Grouping II. $\alpha^{l-1}\bar{\alpha}^j + \cdots + \alpha^j \bar{\alpha}^{l-1}$.

Grouping III. $\alpha^{j-1}\bar{\alpha}^l + \cdots + \bar{\alpha}^{j+l-1}$.

Note that Grouping II can be rewritten as $m^j F_{l+1-j}(\alpha, \bar{\alpha})$.

Let P be a prime lying above l. The remainder of this proof is a straightforward exercise involving rewriting Groupings I and III mod P. It is divided into two different cases depending on whether the Frobenius map leaves α alone or maps it to its conjugate. Thus in Case A, $\alpha^l = \alpha$ and $\bar{\alpha}^l = \bar{\alpha} \bmod P$, whereas in Case B, $\alpha^l = \bar{\alpha}$ and $\bar{\alpha}^l = \alpha \bmod P$. The details are left to the reader. Q.E.D.

LEMMA B.6. *Let m be any integer relatively prime to N, then*

$$m2^{\omega(N)-1} \sum_{\substack{uv=m \\ u>0}} \min(u, v)^{j-1} S(N, v-u) + m^j 2^{\omega(N)-1} \sum_{\substack{uv=m \\ u>0}} \min(u, v)^{l-j} S(N, v-u) \equiv m\big(\text{Trace } T_m \text{ on } \mathfrak{S}_j(N)\big) \mod l.$$

PROOF. We first rewrite the left-hand side of the above congruence. Using the fact that $S(N, v-u) = S(N, u-v)$ and the fact that $m^j t^{l-j} \equiv m(m/t)^{j-1} \bmod l$, one shows this side is congruent to

$$m\left(2^{\omega(N)} \sum_{t|m} t^j S\left(N, t - \frac{m}{t}\right)\right).$$

It remains to calculate the trace of T_m on $\mathfrak{S}_j(N)$. The modular forms $G_j(\chi, d)$ introduced in Appendix A form a basis for $\mathfrak{S}_j(N)$. Moreover, the $G_j(\chi, d)$ are eigenforms for the operator T_m with eigenvalues $\Sigma_{t|m} \chi(t)\bar{\chi}(m/t)t^{j-1}$. Since m is relatively prime to the conductor of χ, we can write this in the form $\Sigma_{t|m} \chi(t^2/m)t^{j-1}$. Note that the eigenvalues associated to $G_j(\chi, d)$ are independent of d.

To compute the trace of T_m on $\mathfrak{S}_j(N)$, we sum over the above eigenvalues, making sure to count each one with the appropriate multiplicity. More precisely, let $\sigma_0(n)$ be the number of divisors of n. Then if χ is of conductor f where $f^2 \mid N$, the value $\Sigma_{t|m} \chi(t^2/m)t^{j-1}$ appears in the sum with multiplicity $\sigma_0(N/f^2)$.

Therefore,

$$\big(\text{Trace } T_m \text{ on } \mathfrak{S}_j(N)\big) = \sum_{\chi, f} \sigma_0\left(\frac{N}{f^2}\right) \sum_{t|m} \chi\left(\frac{t^2}{m}\right) t^{j-1},$$

where the sum is taken over all integers f, such that $f^2 \mid N$, and all characters χ of conductor f.

Using an elementary combinatorial argument, we can rewrite the above expression in the form

$$\sum_{\chi, f}{}' 2^{\omega(N/f^2)} \sum_{t|m} \chi\left(\frac{t^2}{m}\right) t^{j-1},$$

where the symbol $\Sigma'_{\chi, f}$ means that now for each f whose square divides N, the sum is taken over all characters χ defined mod f. Note that such characters χ need not be primitive mod f.

Keeping this grouping of the characters χ, we thus have the following equation.

$$\begin{aligned}\left(\text{Trace } T_m \text{ on } \mathcal{E}_j(N)\right) &= \sum_{t|m} t^{j-1} \sum_{f^2|N} 2^{\omega(N/f^2)} \sum_{\chi \bmod f} \chi\left(\frac{t^2}{m}\right) \\ &= \sum_{t|m} t^{j-1} \sum_{f^2|N} 2^{\omega(N/f^2)} \times \begin{cases} \phi(f) & \text{if } t^2/m \equiv 1 \bmod f \\ 0 & \text{otherwise} \end{cases} \\ &= \sum_{t|m} t^{j-1} \sum_{\substack{f^2|N \\ f|t-m/t}} 2^{\omega(N/f^2)} \phi(f).\end{aligned}$$

By Lemma B.3 this last expression equals

$$2^{\omega(N)} \sum_{t|m} t^{j-1} S\left(N, t - \frac{m}{t}\right). \quad \text{Q.E.D.}$$

REMARK. In order to simplify our presentation we omitted the cases $j = 2$ and $j = l - 1$. The proof in these cases is similar to the above except that there is one less Eisenstein series to be considered. In checking for the desired congruence, the missing series is compensated for by the extra term $\sigma_1(m)$ in Formula B.2.

REFERENCES

1. N. Bourbaki, *Algèbre*, Chap. 8.

2. P. Deligne, *La conjecture de Weil*. I, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–306.

3. M. Eichler, *The basis problem for modular forms and the traces of the Hecke operators*, Lecture Notes in Math., vol. 320, Springer-Verlag, Berlin and New York, 1973, pp. 75–151.

4. N. Jochnowitz, *The index of the Hecke ring* $\mathbf{T}_k$ *in the ring of integers of* $\mathbf{T}_k \otimes \mathbf{Q}$, Duke Math. J. **46** (1979), 861–869.

5. _____, *A study of the local components of the Hecke algebra* mod l, **Trans. Amer. Math. Soc. 270 (1982), 253–267.**

6. _____, *Congruences between systems of eigenvalues and implications for the Hecke algebra*, Harvard Ph.D. Thesis, November, 1976.

7. N. Katz, *p-adic properties of modular schemes and modular forms*, Lecture Notes in Math., vol. 350, Springer-Verlag, Berlin and New York, 1973, pp. 69–190.

8. _____, *A result on modular forms in characteristic p*, Lecture Notes in Math., vol. 601, Springer-Verlag, Berlin and New York, 1976, pp. 53–61.

9. P. G. Kluit, *Hecke operators on* $\Gamma^*(N)$ *and their traces*, Academisch Proefschrift, Vrije Universiteit te Amsterdam, Krips Repro Meppel, 1979.

10. S. Lang, *Introduction to modular forms*, Springer-Verlag, Berlin and New York, 1976.

11. V. Miller, *Diophantine and p-adic analysis of elliptic curves and modular forms*, Ph.D. Thesis, Harvard, June 1975.

12. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten, Tokyo; Princeton Univ. Press, Princeton, N. J., 1971.

13. J-P. Serre, *Congruences et formes modulaires (d'apres Swinnerton-Dyer)*, Sém. Bourbaki, Exp. 416, Lecture Notes in Math., vol. 317, Springer-Verlag, Berlin and New York, 1973 pp. 319–338.

14. _____, *Formes modulaires et fonctions zêta p-adiques*, Lecture Notes in Math., vol. 350, Springer-Verlag, Berlin and New York, 1973, pp. 191–268.

15. H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms*, Lecture Notes in Math., vol. 350, Springer-Verlag, Berlin and New York, 1973, pp. 1–55.

DEPARTMENT OF MATHEMATICS, BROWN UNIVERSITY, PROVIDENCE, RHODE ISLAND 02912