Invent. math. 71, 193–205 (1983)

Inventiones mathematicae

Mod p Hecke Operators and Congruences Between Modular Forms

Kenneth A. Ribet*

University of Berkeley, Mathematics Department, Berkeley, CA. 94720, USA

1. This article is concerned with the general problem of "congruence primes." Let S be the $\mathbf{C}$-vector space of weight k cusp forms on $\Gamma_1(N)$, where $N \geqq 1$ and $k \geqq 2$ are integers. The classical Hecke operators T_n for $n \geqq 1$ act on S and preserve the space $S(\mathbf{Q})$ consisting of cusp forms whose Fourier coefficients are rational numbers. We suppose given a decomposition

$$S = X \oplus Y \tag{1.1}$$

of S as a direct sum of two subspaces, stable under the T_n, which is *rational* in the sense that it is obtained by extension of scalars to $\mathbf{C}$ from a decomposition of $S(\mathbf{Q})$. Here are two examples which immediately come to mind. First of all, we could take X to be the subspace of S spanned by a fixed newform f, together with all of its conjugates (or "companions"), taking Y to be the orthogonal complement to X under the Petersson inner product on S. This situation has been studied extensively by Doi-Hida [2] and by Hida [6–8]. Secondly, we could take X to be the "old part" and Y to be the "new part" of S in the theory of newforms on $\Gamma_1(N)$.

Our subject arises because the decomposition (1.1), while defined over $\mathbf{Q}$ by hypothesis, is not necessarily defined over $\mathbf{Z}$. More precisely, let M be the lattice in $S(\mathbf{Q})$ consisting of cusp forms with integral Fourier coefficients, and let M_X and M_Y be the two projections of M onto X and Y. We have $M \subseteq \tilde{M}$, where

$$\tilde{M} = M_X \oplus M_Y,$$

and the index $(\tilde{M}:M)$ is finite. A *congruence prime* is a prime number p which divides this index.

One sees immediately from the definition that p is a congruence prime if and only if there exist forms $f \in X$, $g \in Y$ which are integral (i.e., f, $g \in M$), not divisible by p (i.e., f, $g \notin pM$), and congruent mod p (i.e., $f - g \in pM$). Thus p is a congruence prime if and only if there is a non-trivial mod p congruence linking

* Research partially supported by the National Science Foundation

0020-9910/83/0071/0193/$02.60

X and Y. Alternately, one can show that p is a congruence prime if and only if there exist normalized eigenforms $f \in X$, $g \in Y$ for the Hecke operators T_n, together with a prime ideal $\mathfrak{p}$ dividing p in the ring of integers of the number field generated by the Fourier coefficients of f and g, such that the Fourier coefficients of f and g are congruent mod $\mathfrak{p}$. (See the proofs of Theorems 7.1 of [6] and [7].)

As mentioned above, much work on congruence primes has been carried out by K. Doi and by mathematicians working with him. In particular, Y. Maeda has made numerical calculations of congruence primes, some of which were cited in Table (8.11) of [6]. As a special example, we take $k=31$, $N=3$, and (1.1) as in the first of our two general examples, with f a suitable form with "complex multiplication" by $\mathbf{Q}(\sqrt{-3})$. Then the prime numbers 5, 53, 30842593 are congruence primes. Other numerical examples are contained in Doi-Ohta [3]. In this connection, we should point out that Mazur has shown, in the special case where $k=2$ and N is prime, that there are *always* congruence primes provided that X and Y are both non-zero [12, p. 98]. It would be extremely interesting to generalize this result to other situations. Meanwhile, no example of a decomposition (1.1) is *known* in the situation where N is 1.

In the first of his three recent articles cited above, Hida gave a useful sufficient condition for a prime p to be a congruence prime. Recall that the space S, viewed as a real vector space, has an interpretation (via the Shimura isomorphism) as a parabolic cohomology group with real coefficients [15, Chap. 8]. Let L be the image in S of the corresponding parabolic cohomology group made with *integral* coefficients. Thus L is a lattice in S viewed as a real vector space; its rank over $\mathbf{Z}$ is twice that of the lattice M.

Let $e \in \mathrm{End}(S)$ be the projection of S onto X along Y, i.e., that endomorphism which is the identity on X and 0 on Y. It is easy to see that e is a polynomial in the T_n with rational coefficients. [Indeed, if we consider the $\mathbf{Q}$-algebras A_S, A_X, A_Y generated by the T_n acting on S, X, and Y, then we have a tautologous inclusion

$$A_S \subseteq A_X \oplus A_Y.$$

By dimension considerations, we find that this inclusion is in fact an equality: (2.2) and its proof show that the algebras A_S, A_X, and A_Y have the same dimensions over $\mathbf{Q}$ as the spaces S, X, and Y over $\mathbf{C}$. Especially, the element e of the direct sum must belong to A_S.] Now since the T_n preserve L, the images of L in X and in Y must again be lattices in X and Y (viewed as real vector spaces). Hence, if we define $\tilde{L}$ to be the direct sum of these images, the index $(\tilde{L}:L)$ is finite.

(1.2) **Proposition.** *Every prime number dividing $(\tilde{L}:L)$ is a congruence prime.*

This proposition is essentially elementary, as we will explain below. Its importance stems from the fact that the index $(\tilde{L}:L)$ tends to be more accessible than the index $(\tilde{M}:M)$. Suppose first that (1.1) has been defined by a newform f and its conjugates f_σ, as in the first of our two examples. In [6, § 7], Hida defined a certain integer $C(f)$ by taking the ratio of a certain period

determinant to the product of the Petersson inner products $\langle f_\sigma, f_\sigma \rangle$. He then proved:

(1.3) **Theorem.** *Suppose that p is a prime number satisfying $p \geqq k-1$ and $p \nmid 6N$. Then p divides $C(f)$ if and only if p divides $(\tilde{L}:L)$. Especially, if p divides $C(f)$, then p is a congruence prime.* (See, [6, Th. 7.1].)

In the second example of decompositions (1.1), that related to old and new forms, it is an interesting problem to try to describe the group $\tilde{L}/L$, or at least to compute its order. In the case $k=2$, this is related to the question (mentioned in [13]) of understanding the canonical isogeny between the new subvariety and the new optimal quotient of the Jacobian $J_1(N)$. A partial result for $J_0(N)$, where N is a product of two distinct primes, will be given in [14].

The purpose of this article is to present a converse to (1.2). We will say that a prime number is *large* provided that is prime to the level N and at least equal to the weight k. Prime numbers which are not large will be said to be small.

(1.4) **Theorem.** *Suppose that p is a large prime. Then p is a congruence prime if and only if p divides $(\tilde{L}:L)$.*

In view of the above discussion, we see that (1.3) has the following corollary, in the situation studied by Hida:

(1.5) *Suppose that p is a large prime which is different from 2 and 3. Then p is a congruence prime if and only if p divides the integer $C(f)$.*

Let $\mathbf{T}$ be the subring of $\mathrm{End}(S)$ generated by the Hecke operators T_n. Thus $\mathbf{T} \otimes \mathbf{Q}$ is the algebra A_S introduced above. Let $\mathfrak{o}_L$ be the *order* of the lattice L in A_S:

$$\mathfrak{o}_L = \{T \in A_S \mid T(L) \subseteq L\}.$$

Thus $\mathfrak{o}_L$ contains $\mathbf{T}$, and the index of $\mathbf{T}$ in $\mathfrak{o}_L$ is finite. We define $\mathfrak{o}_M$ similarly, replacing L by M. It is obvious from the definition of $\tilde{M}$ that congruence primes are precisely the primes p such that $e \notin \mathfrak{o}_M \otimes \mathbf{Z}_p$. Similarly, divisors of $(\tilde{L}:L)$ are the primes p for which $e \notin \mathfrak{o}_L \otimes \mathbf{Z}_p$. Hence knowing $\mathfrak{o}_L$ and $\mathfrak{o}_M$ is visibly related to the possibility of proving (1.2) and (1.4).

(1.6) *The order $\mathfrak{o}_M$ is equal to $\mathbf{T}$.*

(1.7) *The index of $\mathbf{T}$ in $\mathfrak{o}_L$ is divisible only by small primes.*

Despite the apparent similarly between (1.6) and (1.7), the two statements are not of equal difficulty. We will see in § 2 that (1.6) is essentially elementary; it is a consequence of a somewhat finer statement concerning the structure of the $\mathbf{T}$-module M which can be proved by completely classical methods. On the other hand, (1.7) is our main theorem; its proof, although simple in the case $k=2$, requires a large number of preliminaries in the general case. Many of our tools have been borrowed from Hida's article [7], where one finds a result analogous to (1.7) in which L has been replaced by its "ordinary" part. (Here the word "ordinary" is used in opposition to "supersingular.")

Notice that (1.6) and (1.7) give the following corollary:

(1.8) *The order* $\mathfrak{o}_M$ *is contained in* $\mathfrak{o}_L$. *The index* $(\mathfrak{o}_L:\mathfrak{o}_M)$ *is divisible only by small prime numbers.*

In view of the discussion above, we seen that the first assertion of (1.8) gives (1.2). Similarly, the second gives the Theorem (1.4).

Let us now briefly suppose that the level N is equal to 1 and mention a third lattice, which appears in the work of K. Hatada [4], [5]. Consider the involution on L which is induced by the matrix $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, and let L^+ be the subgroup of L consisting of elements left fixed by the involution (cf. [6, § 3]). The action of $\mathbf{T}$ on L^+ is easily seen to be faithful, and we define the order $\mathfrak{o}_{L^+}$ as above. One sees from the articles of Hatada that the index $(\mathfrak{o}_{L^+}:\mathbf{T})$ tends to be divisible by high powers of 2 and 3. By combining (1.7) with Theorem 3.2, Proposition 3.3 and (3.18_c) of [6], one shows:

(1.9) *The index* $(\mathfrak{o}_{L^+}:\mathbf{T})$ *is divisible only by small primes.*

In this case $N=1$, the algebra A_S is a product of totally real number fields (which in all known cases is in fact a single number field). The ring $\mathbf{T}$ is a subring of finite index of the product R of the integer rings of the factors. One knows from the work of *N.* Jochnowitz that the factor group $R/\mathbf{T}$ grows significantly as the weight k increases. (For example, let l be a prime number. Then [9, Th. 5.1] states that l divides the index $(R:\mathbf{T})$ for all k greater than a specific integer depending on l.) It is unknown whether either of the orders $\mathfrak{o}_L$, $\mathfrak{o}_{L^+}$ comes close to being equal to R.[1]

Returning to the case where $N \geqq 1$ is arbitrary, we would like to mention the relation between congruence primes and *primes of fusion* (as considered by Doi-Ohta and by Mazur). Let $\mathbf{T}_X$ and $\mathbf{T}_Y$ be the rings generated by the T_n acting on X and on Y, so that we have an inclusion

$$\mathbf{T} \subseteq \mathbf{T}_X \oplus \mathbf{T}_Y \tag{1.10}$$

with finite cokernel. Primes of fusion are simply prime ideals $\mathfrak{p}$ of $\mathbf{T}$ containing the conductor $\mathfrak{c}$ of the ring extension (1.10), which by definition is the annihilator of the $\mathbf{T}$-module $(\mathbf{T}_X \oplus \mathbf{T}_Y)/\mathbf{T}$. We have

$$\begin{aligned} \mathfrak{c} &= \{T \in \mathbf{T} \mid Te \in \mathbf{T}\} \\ &= \{T \in \mathbf{T} \mid Te(M) \subseteq M\} \\ &= \mathrm{Ann}_{\mathbf{T}}(\tilde{M}/M), \end{aligned}$$

where the middle equality follows from (1.6) and the first and third are trivial. It follows, then, that the primes of fusion are precisely the primes of $\mathbf{T}$ contained in the support of the finite $\mathbf{T}$-module $\tilde{M}/M$. The primes of fusion are therefore, in particular, maximal ideals of $\mathbf{T}$, and their various residue characteristics are precisely the congruence primes. Thus the notion of primes of fusion may be said to be refinement of that of congruence primes.

1 This problem was mentioned to the author by J-P. Serre

(1.11) **Proposition.** *The support of the* $\mathbf{T}$*-module* $\tilde{L}/L$ *is contained in the set of primes of fusion. Moreover, if* $\mathfrak{p}$ *is a maximal ideal of* $\mathbf{T}$ *whose residue characteristic is a large prime, then* $\mathfrak{p}$ *is a prime of fusion if and only if* $\mathfrak{p}$ *belongs to the support of* $\tilde{L}/L$.

Proof. We have

$$\mathrm{Ann}_{\mathbf{T}}(\tilde{L}/L)=\{T\in\mathbf{T}\,|\,Te(L)\subseteq L\};$$

by (1.8), it follows that $\mathrm{Ann}_{\mathbf{T}}(\tilde{L}/L)$ contains $\mathrm{Ann}_{\mathbf{T}}(\tilde{M}/M)$ and that the index of the latter in the former is divisible only by small primes. The proposition follows.

2. In this §, we shall prove (1.6) and begin our discussion of (1.7). In particular, we prove (1.1) in the special case $k=2$.

Let

$$a_n\colon M\to\mathbf{Z}\qquad(n\geqq 1)$$

be the map taking a form $f\in M$ to its n^{th} Fourier coefficient. Let

$$\iota\colon M\to\mathbf{Z}[\![q]\!]$$

be the map taking a form to its Fourier expansion. It is well known that this latter map is injective, and the definition of M is such that the cokernel of ι is torsion free. Also, one has the commutation formula

$$a_1\circ T_n=a_n, \tag{2.1}$$

cf. [15, Chap. 3].

Consider the $\mathbf{T}$-homomorphism

$$\varphi\colon M\to\mathrm{Hom}(\mathbf{T},\mathbf{Z})$$

defined by

$$\varphi(f)\colon T\mapsto a_1(f|T)$$

(as usual, we write $f|T$ for the image of f under T). The following theorem was proved by V. Miller in the case $N=1$. (See [11, p. 43].)

(2.2) **Theorem.** *The map* φ *is an isomorphism.*

Proof. It is certainly obvious that φ is injective with torsion free cokernel because of (2.1) and the analogous facts concerning ι. Since $\mathbf{T}$ and M are free finite rank $\mathbf{Z}$-modules, it suffices to show that the rank of $\mathbf{T}$ is at most that of M. Consider the transpose of φ, i.e., the map

$$\psi\colon\mathbf{T}\to\mathrm{Hom}(M,\mathbf{Z})$$

defined by

$$\psi(T)\colon f\mapsto a_1(f|T).$$

If T is in the kernel of ψ, we have for all $f\in M$ and all $n\geqq 1$ the equations

$$0=\psi(T)(f|T_n)=a_1(f|T_nT)=a_n(f|T).$$

By the injectivity of ι, it follows that $f|T=0$. Since this holds for all f, we have $T=0$, giving that ψ is injective. This injectivity implies, in particular, the required rank inequality.

Proof of (1.6). For each prime number p, it suffices to check that p is prime to the index $(\mathfrak{o}_M:\mathbf{T})$. One easily checks that this assertion amounts to the statement that the natural action of $\mathbf{T}/p\mathbf{T}$ on M/pM is *faithful*. In view of (2.2), we have

$$M/pM=\mathrm{Hom}_{\mathbf{F}_p}(\mathbf{T}/p\mathbf{T}, \mathbf{F}_p),$$

an equation which makes apparent that the statement is true.

Next, we consider (1.7) in the case $k=2$. The large primes are simply those prime to N. Let p be such a prime. We must show that the ring $\mathbf{T}/p\mathbf{T}$ acts faithfully on L/pL. To prove this, in view of (1.6), it suffices to show that any $T\in\mathbf{T}/p\mathbf{T}$ which annihilates L/pL must also annihilate M/pM.

Consider the modular curve $X_1(N)$ over the rational field $\mathbf{Q}$, and let $J=J_1(N)$ be its Jacobian. Since p is prime to N, we may consider the reduction $J_{/\mathbf{F}_p}$ of J modulo p. We make the standard identifications

$$L/pL=\mathrm{Hom}_{\mathbf{F}_p}(J[p], \mathbf{F}_p),$$
$$M/pM=\mathrm{Cot}(J_{/\mathbf{F}_p}),$$

where, in the former identification, $J[p]$ denotes the "physical" kernel of multiplication by p in $J(\mathbf{C})$. Further, we regard $\mathbf{T}$ as a subring of $\mathrm{End}_{\mathbf{Q}}(J)$ via Albanese functoriality, so that the above identifications become $\mathbf{T}$-equivariant.

Suppose that T annihilates L/pL. Then T annihilates $J[p]$, meaning that T is divisible by p in $\mathrm{End}_{\mathbf{Q}}(J)$. Then, *a fortiori*, T is divisible by p in $\mathrm{End}_{\mathbf{F}_p}(J_{/\mathbf{F}_p})$. Since multiplication by p induces the zero map on $\mathrm{Cot}(J_{/\mathbf{F}_p})$, we see that T annihilates $\mathrm{Cot}(J_{/\mathbf{F}_p})$ and thus that T annihilates M/pM.

We now begin to discuss the remaining case of (1.7), i.e., where we have

$$3\leqq k\leqq p.$$

Our idea is to fix a prime $p\nmid N$ and to treat all such weights simultaneously. Let $d(k)$ be the dimension of the space S (which of course depends on k), and set

$$d=d(3)+\cdots+d(p).$$

Write V_k for the module we have been calling L/pL, and set

$$V=V_3\oplus\cdots\oplus V_p.$$

Note that we now have

$$2d=\dim_{\mathbf{F}_p}(V).$$

For each k $(3\leqq k\leqq p)$, define R_k to be the subalgebra of $\mathrm{End}(V_k)$ generated by the T_n acting on V_k $(n\geqq 1)$, and define similarly R relative to V.

(2.3) **Theorem.** *We have* $\dim_{\mathbf{F}_p}(R)\geqq d$.

The proof of this theorem is the object of § 3 and § 4. For the moment, we observe that (2.3) implies the remaining case of (1.7). Indeed, (1.7) states that the natural map

$$i_k\colon \mathbf{T}_k/p\mathbf{T}_k \to \mathrm{End}(V_k)$$

is injective for each k, where $\mathbf{T}_k$ is the Hecke algebra earlier denoted $\mathbf{T}$. Since, by (2.2), the dimension of $\mathbf{T}_k/p\mathbf{T}_k$ is $d(k)$, we know *a priori* that the image of i_k has dimension at most $d(k)$, and (1.7) states that this image has dimension precisely $d(k)$. On the other hand, this image is by definition the algebra R_k, and we have, again by definition, an inclusion

$$R \subseteq \bigoplus_{k=3}^{p} R_k. \tag{2.4}$$

Therefore, (2.3) proves (1.7) for each k between 3 and p, and it shows incidentally that (2.4) is an equality.

To prove (2.3), we exhibit a specific quotient of R having dimension d: the algebra generated by all T_n acting on a certain "primitive" subspace of the cotangent space of an Igusa curve in characteristic p. To do this, we recall the relation, essentially due to Shimura and Hida, between the space V and the group of p-division points on the Jacobian $J_1(pN)$.

3. Let X_1 be the modular curve $X_1(pN)$ (regarded as a curve over $\mathbf{Q}$), and let X_0 similarly denote the modular curve associated with the group $\Gamma_1(N)\cap\Gamma_0(p)$. The natural covering

$$\pi\colon X_1 \to X_0$$

induces by Pic functoriality a map

$$\alpha\colon J_0 \to J_1,$$

where J_0 and J_1 are the Jacobians of X_0 and X_1. We denote by Σ and by Q the kernel and the cokernel of α, respectively. The former is a finite subgroup of J_0 whose order divides $p-1$, while the latter is an abelian variety. We write

$$v\colon J_1 \to Q$$

for the structural map defining Q.

(3.1) **Proposition.** *The dimension of Q is $2d$.*

Proof. The dimension in question may be viewed simply as the difference between the dimensions of the spaces of weight-2 cusp forms for $\Gamma_1(pN)$ and for $\Gamma_0(p)\cap\Gamma_1(N)$. Thus what is asserted is a relation between dimensions of spaces of cusp forms of weight 2 and spaces of cusp forms of higher weight. Such relations may be verified by suitable trace formulas, as in Koike [10]. We leave to the reader the verification that the desired relation follows from [10, Th. 1].

Acting on J_0, J_1, and Q we have Hecke operators T_n ($n \geqq 1$) as usual. One has also an action of $(\mathbf{Z}/pN\mathbf{Z})^*$ on X_1 as a group of automorphisms, and a corresponding action of this group (induced by Albanese functoriality) on J_1. In fact, we shall be interested only in the action of the subgroup

$$\Delta = (\mathbf{Z}/p\mathbf{Z})^*$$

of $(\mathbf{Z}/pN\mathbf{Z})^*$ on J_1 and on X_1. For $a \in \Delta$, we write $\langle a \rangle$ for the corresponding automorphism of X_1 or of J_1. We set

$$\sigma = \sum_{a \in \Delta} \langle a \rangle.$$

Finally, we define as usual an Atkin-Lehner involution w of J_1 by choosing a primitive $(pN)^{\text{th}}$ root of 1 in $\bar{\mathbf{Q}}$ and by using the modular recipe given on page 15 of [9]. We let U be the Hecke operator T_p, and define

$$U' = wUw.$$

(3.2) **Proposition.** *We have the relations*

$$U'U = UU' = p$$

in End(Q).

Proof. We will prove the proposition in an especially long winded manner in order to introduce some notation and some facts which will be useful in the next §. Let $K \subset \bar{\mathbf{Q}}$ be the field of p^{th} roots of unity, and let $\mathfrak{p}$ be the unique prime of K lying over p. By a theorem of Deligne and Rapoport [1, V, 3.2], the abelian variety $Q_{/K}$ has good reduction at $\mathfrak{p}$. We denote by $\tilde{Q}$ the reduction of $Q_{/K}$ at $\mathfrak{p}$; thus $\tilde{Q}$ is an abelian variety over the residue field $\mathbf{F}_p$ of $\mathfrak{p}$. The quotient introduced above induces a map

$$v\colon \tilde{J}_1 \to \tilde{Q},$$

where $\tilde{J}_1$ is the connected component of 0 in the special fibre of the Néron model of $J_{1/K}$ at $\mathfrak{p}$. Let C and C' be the two Igusa curves $C_\infty^{(N)}$ and $C_0^{(N)}$ appearing in [16, Prop. 5.2], and let A and A' be their Jacobians. By the proposition of Wiles just cited, v must factor through the product $A \times A'$. Let

$$\mu\colon A \times A' \to \tilde{Q}$$

be the map induced v.

It is obvious that the endomorphism $(p-1-\sigma)$ of J_1 vanishes on J_0/Σ and therefore induces a homomorphism

$$\tau\colon Q \to J_1$$

such that $v \circ \tau = p-1$. By reducing mod $\mathfrak{p}$ we obtain a map

$$\tilde{\tau}\colon \tilde{Q} \to \tilde{J}_1;$$

combining this map with the canonical quotient

$$\tilde{J}_1 \to A \times A',$$

we obtain a map

$$\beta\colon \tilde{Q} \to A \times A'$$

with the property that

$$\mu \circ \beta = p-1.$$

Especially, β has finite kernel; its image is an abelian subvariety B of $A \times A'$, isogenous to $\tilde{Q}$, which is killed by the endomorphism of $A \times A'$ induced by σ. Using the Eichler-Shimura relation of Wiles [16, Th. 5.3] (cf. [7, (4.11)]), we obtain the factorizations

$$p = UU' = U'U$$

in End(B), and therefore in End(Q) as desired.

(3.3) **Corollary.** *The kernels of U and of U' in Q are contained in the group $Q[p]$ of p-division points on Q, and they each have order $p^{\dim(Q)} = p^{2d}$. If we regard U and U' as endomorphisms of the finite group $Q[p]$, we have the relations*

$$\text{Image}(U) = \text{Kernel}(U'),$$
$$\text{Image}(U') = \text{Kernel}(U).$$

Proof. Since U and U' are conjugate by w, their kernels have the same order. By (3.2), the common order must be p^{2d}, and the kernels are contained in $Q[p]$. Finally, the indicated kernel-image relations follow from the fact that all four groups have the same order, together with the obvious inclusions of the left-hand groups in the right-hand groups.

We now let

$$G = \text{Hom}_{\mathbf{F}_p}(Q[p], \mathbf{F}_p)$$

be the $\mathbf{F}_p$-dual of the group of p-division points on Q. If T is an endomorphism of Q, we will again write T for the endomorphism of G induced by T.

(3.4) **Theorem.** *There are T_n-equivariant maps*

$$\iota\colon V \to G, \qquad \pi\colon G \to V$$

such that $\iota \circ \pi = U$ on G.

Proof. This result is simply a variant of some facts proved in § 3 of [7]. Let ω denote the identity map

$$\Delta \to \mathbf{F}_p^*,$$

viewed as an $\mathbf{F}_p^*$-valued character of the finite group Δ. For each $k \geqq 2$, let G_k denote the eigenspace of G corresponding to the character ω^{k-2} under the action of Δ on G:

$$G_k = \{g \in G \mid \delta g = \omega^{k-2}(\delta) \cdot g \text{ for all } \delta \in \Delta\}.$$

Since σ annihilates Q, it is clear that $G_2 = 0$, so that we have

$$G = \bigoplus_{k=3}^{p} G_k.$$

For each k, we wish to exhibit maps

$$\iota_k\colon V_k \to G_k, \qquad \pi_k\colon G_k \to V_k,$$

T_n-equivariant, such that $\iota_k \circ \pi_k$ is the restriction of U to G_k.

In [7, (3.8)], such maps are constructed with the group G_k replaced by a cohomology group denoted

$$H^1_P(\bar{\Phi}_1, \Lambda_1(k-2)),$$

whose precise definition will not be recalled here. The T_n-equivariance of these maps follows from Theorem 3.1 of [7] for n prime to p and from Theorem 3.2 of [7] for n a power of p. Further, the latter theorem furnishes also the desired relation $\iota_k \circ \pi_k = U$. Now in [7, (3.14_a)] we find an identification between the above cohomology group and the ω^{k-2} eigenspace of the $\mathbf{F}_p$-dual $J_1[p]^\vee$ of the group of p-division points on J_1. Finally, this eigenspace is easily seen to be identified with G_k by the natural map $J_1 \to Q$, since the action of Δ on J_0/Σ is trivial.

(3.5) **Corollary.** *The map ι induces an isomorphism between V and the kernel $G[U']$ of U' acting on G.*

Proof. The formula $\iota \circ \pi = U$ shows that the image of ι is contained in the image of U. Since the image of U has the same cardinality as the group V (because of (3.3)), ι induces an isomorphism between V and the image of U. By (3.3) again, this image is alternately the kernel of U'.

From now on, we let $\mathbf{T}$ be the subring of $\mathrm{End}(Q)$ generated by the endomorphisms T_n of Q. Since U' commutes with the T_n, $\mathbf{T}$ operates on the group $G[U']$, so that we obtain a homomorphism

$$\varphi\colon\ T \to \mathrm{End}(G[U']).$$

Using ι to identify $G[U']$ with V, we see that the image of φ may be identified with the algebra R defined near the end of § 2, i.e., with the algebra generated by the T_n acting on V. Therefore, (2.5) becomes a statement about the image of φ.

(3.6) **Proposition.** *Let T be an element of $\mathbf{T}$. We have $\varphi(T)=0$ if and only if T may be written in the form $U'\eta$ for some $\eta \in \mathrm{End}_{\mathbf{Q}}(Q)$.*

Proof. If T may be so written, then we have the opposite relation

$$T = \eta U'$$

in $\mathrm{End}(G)$, and therefore $\varphi(T)=0$. Conversely, if T annihilates $G[U']$, then the endomorphism UT of Q acts as 0 on G and is therefore divisible by p in $\mathrm{End}_{\mathbf{Q}}(Q)$. Writing $p = UU'$ and using that U is invertible in $(\mathrm{End}_{\mathbf{Q}}(Q)) \otimes \mathbf{Q}$, we obtain the desired result.

4. We return now to the discussion begun in the course of the proof of (3.2). The relation

$$\mu \circ \beta = p - 1$$

shows that the map

$$\alpha^*\colon\ \mathrm{Cot}(\tilde{Q}) \to \mathrm{Cot}(A) \oplus \mathrm{Cot}(A')$$

is injective. Since $\sigma = 0$ on Q, the image of α^* lies in the direct sum of the eigenspaces of $\mathrm{Cot}(A) \oplus \mathrm{Cot}(A')$ corresponding to the non-trivial characters of Δ. We refer to this direct sum as the *primitive* part of $\mathrm{Cot}(A) \oplus \mathrm{Cot}(A')$.

(4.1) **Lemma.** *The map* α^* *induces an isomorphism between* $\mathrm{Cot}(\tilde{Q})$ *and the primitive part of* $\mathrm{Cot}(A)\oplus\mathrm{Cot}(A')$.

Proof. We establish this lemma by a simple dimension argument. We note that the two Igusa coverings over $\mathbf{F}_p$

$$C \to X_1(N)_{/\mathbf{F}_p}, \qquad C' \to X_1(N)_{/\mathbf{F}_p}$$

have degree prime to p. They consequently induce injections

$$\mathrm{Cot}(J_1(N)_{/\mathbf{F}_p}) \hookrightarrow \mathrm{Cot}(A), \qquad \mathrm{Cot}(J_1(N)_{/\mathbf{F}_p}) \hookrightarrow \mathrm{Cot}(A').$$

It follows that the trivial eigenspace in $\mathrm{Cot}(A)\oplus\mathrm{Cot}(A')$ for the action of Δ has dimension at least equal to $2\dim(J_1(N))$. Therefore, to prove the lemma it suffices to check the equality

$$\dim(A \times A') = \dim(Q) + 2\dim(J_1(N)).$$

We know that the left-hand side represents the dimension of the maximal abelian variety quotient of the connected component of 0 in the fibre over $\mathbf{F}_p$ of the Néron model for $J_{1/K}$ [16, (5.2)]. We have already remarked that the abelian variety $Q_{/K}$ has good reduction at $\mathfrak{p}$ because of [1, V, 3.2]. On the other hand, the abelian variety J_0, up to isogeny, is a product of two copies of $J_1(N)$ (abelian varieties which have good reduction at p) and an abelian variety which generalizes $J_0(p)$ and has in particular toric reduction at p, cf. [1, VI, Th. 6.9]. Hence, up to isogeny, J_1 is the product of a "potentially good"

$$Q \times J_1(N) \times J_1(N)$$

and an abelian variety which has toric reduction at p and therefore at $\mathfrak{p}$.

(4.2) **Corollary.** *The intersection*

$$W = \mathrm{Cot}(A) \cap \alpha^* \mathrm{Cot}(\tilde{Q}),$$

computed in $\mathrm{Cot}(A)\oplus\mathrm{Cot}(A')$ *is the primitive part of* $\mathrm{Cot}(A)$. *We have*

$$\dim_{\mathbf{F}_p}(W) = d.$$

Proof. By (4.1), $\alpha^*\mathrm{Cot}(\tilde{Q})$ is the primitive part of $\mathrm{Cot}(A)\oplus\mathrm{Cot}(A')$, which is just the direct sum of the primitive parts of the two factors. Therefore, the indicated intersection is indeed the primitive part of the first factor. Since the dimension of Q is $2d$ by (3.1), the second statement of (4.2) means that the primitive parts of $\mathrm{Cot}(A)$ and of $\mathrm{Cot}(A')$ have the same dimension, since the sum of these dimensions is the dimension of Q. In fact, from the discussion at the beginning of the proof of (4.1), the two dimensions in question are respectively the differences

$$\dim(A) - \dim(J_1(N)), \qquad \dim(A') - \dim(J_1(N));$$

therefore, we need know only that A and A' have the same dimensions, i.e., that the Igusa curves C and C' have the same genus. This is the case because they are permuted by the Atkin-Lehner involution w of $X_1(pN)$, as is apparent from the discussion in § 5 of [16].

We now study the action of the Hecke operators T_n on W; we may view these T_n, for instance, as being induced by the action of the Hecke algebra

$$\mathbf{T} \subseteq \mathrm{End}(Q)$$

on $\mathrm{Cot}(\tilde{Q})$ by transport of structure. In this optic, we obtain a homomorphism

$$\varphi' : \mathbf{T} \to \mathrm{End}_{\mathbf{F}_p}(W),$$

whose image R' is the algebra generated by the T_n acting on W. We wish to compare φ' and R' with the homomorphism φ and its image R which we introduced at the end of § 3. As explained in § 3, the main result (2.5) amounts to the inequality

$$\dim_{\mathbf{F}_p}(R) \overset{?}{\geqq} d.$$

This inequality clearly results from the following two assertions.

(4.3) *We have* $\ker(\varphi) \subseteq \ker(\varphi')$. (Therefore R' is naturally a quotient of R.)

Proof. In view of (3.6), it suffices to show that the operator U' induces the 0-map on W. By the Eichler-Shimura formula of Wiles [16] (see [7, 4.11]), this is certainly the case.

(4.4) *The* $\mathbf{F}_p$*-dimension of* R' *is at least* d.

Proof. This assertion follows by the proof of (2.1). Indeed, we may view $\mathrm{Cot}(A)$ as $H^0(C, \Omega^1)$ and exploit the fact that there is a natural injective q-expansion map

$$H^0(C, \Omega^1) \hookrightarrow \mathbf{F}_p[\![q]\!], \qquad f \mapsto \Sigma a_n(f) q^n$$

which satisfies the usual formula

$$a_1 \circ T_n = a_n.$$

(See [16, § 6] and the proof of Corollary 5.3 of [7].)

Remark. Serre (for $N = 1$) and Katz (for general N) have established an isomorphism

$$H^0(C, \Omega^1)(\omega^{k-2}) \simeq S_k$$

for all $k = 2, \ldots, p$, where S_k denotes the space of cusp forms of weight k on $\Gamma_1(N)$ with coefficients in $\mathbf{F}_p$. Therefore W may be viewed as a space of mod p modular forms. Although this fact was not used in the above proof, it motivated consideration of W.

The author wishes to thank Professors Hida, Katz, Mazur, and Serre for helpful conversations and correspondence. During the time this article was first written, the author was first a visitor at the Tata Institute for Fundamental Research and then a fellow of the Japanese Society for the Promotion of Science. This article was revised during a visit to the I.H.E.S. in Bures. The author wishes to thank these institutions, as well as the universities of Hokkaido and Tokyo, for their hospitality.

References

1. Deligne, P., Rapoport, M.: Schémas de modules de courbes elliptiques, Lecture Notes in Math., vol. 349, pp. 143–174. Berlin-Heidelberg-New York: Springer 1973
2. Doi, K., Hida, H.: On a certain congruence of cusp forms and the special values of their Dirichlet series. Unpublished manuscript, 1979
3. Doi, K., Ohta, M.: On some congruences between cusp forms on $\Gamma_0(N)$. Lecture Notes in Math., vol. 601, pp. 91–105. Berlin-Heidelberg-New York: 1977
4. Hatada, K.: Eigenvalues of Hecke operators on $\mathbf{SL}(2, \mathbf{Z})$. Math. Ann. **239**, 75–96 (1979)
5. Hatada, K.: Congruences for eigenvalues of Hecke operators on $\mathbf{SL}_2(\mathbf{Z})$. Manuscripta Math. **34**, 305–326 (1981)
6. Hida, H.: Congruences for cusp forms and special values of their zeta functions. Invent. Math. **63**, 225–261 (1981)
7. Hida, H.: On congruence divisors of cusp forms as factors of the special values of their zeta functions. Invent. Math. **64**, 221–262 (1981)
8. Hida, H.: Kummer's criterion for the special values of Hecke L-functions of imaginary quadratic fields and congruences among cusp forms. Invent. Math. **66**, 415–459 (1982)
9. Jochnowitz, N.: A study of the local components of the Hecke algebra mod l. Trans. AMS. **270**, 253–267 (1982)
10. Koike, M.: A note on modular forms mod p. Proc. Japan Acad. Ser. A **55**, 313–315 (1979)
11. Lang, S.: Introduction to Modular Forms. Berlin-Heidelberg-New York: Springer 1976
12. Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. I.H.E.S. **47**, 33–186 (1977)
13. Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)
14. Ribet, K.: Congruences between modular forms on $\Gamma_0(p\,q)$. Proceedings ICM 1983. In preparation
15. Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions, Princeton: Princeton University Press 1971
16. Wiles, A.: Modular curves and the class group of $\mathbf{Q}(\zeta_p)$. Invent. Math. **58**, 1–35 (1980)

Oblatum 9-XI-1981 & 14-VI-1982