**Proceedings of the International Congress of Mathematicians
August 16–24, 1983, Warszawa**

KENNETH A. RIBET*

Congruence Relations between Modular Forms

1. This article is concerned with the notion of *congruence primes* in the theory of modular forms, as in the work of Doi and Hida [1], Doi and Ohta [2], and Hida [3], [4], [5]. Our main aim is to point out how the explicit calculation of such primes, in a particular example involving forms of weight 2, leads to a non-trivial problem concerning finite subgroups of Jacobians of modular curves.

Let $k \geqslant 2$ and $N \geqslant 1$ be integers, and take S to be either the complex vector space of holomorphic modular forms or the vector space of holomorphic cusp forms of weight k on one of the classical modular groups $\Gamma_0(N)$ or $\Gamma_1(N)$. We denote by $S(\mathbf{Z})$ the lattice of forms in S with integral q-expansion, and by T_n (for $n \geqslant 1$) the n^{th} Hecke operator on S.

Suppose that we are given a direct sum decomposition

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

in which X and Y are both stable under the T_n and both generated by their intersections with $S(\mathbf{Z})$. A prime number p is a *congruence prime* relative to this decomposition if there is a non-trivial $\operatorname{mod} p$ congruence linking X to Y: there exist

$$f \in X \cap S(\mathbf{Z}), \quad g \in Y \cap S(\mathbf{Z})$$

such that

$$f \equiv g \operatorname{mod} pS(\mathbf{Z}), \quad f \not\equiv 0 \operatorname{mod} pS(\mathbf{Z}).$$

For example, taking S to be the space of weight-k modular forms on $\mathbf{SL}(2, \mathbf{Z})$, we may choose X (resp. Y) to be the space of Eisenstein series (resp. cusp forms) in S. The congruence primes are those prime numbers which divide the numerator of the constant term of the normali-

* Research partially supported by the National Science Foundation (USA).

zed Eisenstein series of weight k, i.e., the fraction $B_k/2k$, where B_k is the k^{th} Bernoulli number. Thus congruence primes are irregular primes, and the congruence link between X and Y may be used in studying the arithmetic of cyclotomic fields. Doi has asked whether, more generally, one can characterize congruence primes and interpret the link between X and Y in terms of arithmetic.

In his articles citied above, Hida discussed these questions of Doi, the first quite generally, and the second in reference to cusp forms with complex multiplication. Especially, the articles [3] and [4], together with the author's [10], give an interpretation of congruence primes in terms of parabolic cohomology. Here we assume that S is a space of cusp forms and use the well known Shimura isomorphism to realize S as a certain parabolic cohomology group V constructed with real coefficients. Via this isomorphism, S is endowed with a second integral lattice $V(\mathbf{Z})$, the image in V of the analogous cohomology group made with integral coefficients. Replacing $S(\mathbf{Z})$ by $V(\mathbf{Z})$ in the definition of "congruence prime", we obtain the alternate notion of *cohomology congruence prime.*

THEOREM 1.2 ([4], [10]). *Every cohomology congruence prime is a congruence prime. Conversely, if p is a congruence prime not dividing $(k-1)!N$, then p is a cohomology congruence prime.*

This theorem shows that the two notions of congruence prime are essentially equivalent. On the other hand, one feels that the set of cohomology congruence primes may be precisely calculated in certain contexts. (For example, Hida showed in some cases how the cohomology congruence primes are the prime divisors of a rational integer which may be interpreted as the "algebraic part" of a determinant of periods of forms in X.)

2. To test this idea, we are going to work out an explicit example. Since it is more pleasing to consider congruences between eigenforms for the Hecke operators, rather than congruences between arbitrary forms, we begin by reviewing the notion of *primes of fusion.* These will be maximal ideals of the Hecke ring associated to S whose residue characteristics are precisely the congruence primes.

We let $\mathbf{T}$ be the subring of $\mathrm{End}(S)$ generated by the Hecke operators T_n acting on S, and we similarly define $\mathbf{T}_X$ and $\mathbf{T}_Y$ by replacing S by X and Y. Then $\mathbf{T}_X$ and $\mathbf{T}_Y$ are naturally quotients of $\mathbf{T}$, which in turn is a subring of the direct sum $\mathbf{T}_X \oplus \mathbf{T}_Y$. A *prime of fusion* is a prime ideal of $\mathbf{T}$ containing the conductor of the ring extension

$$\mathbf{T} \hookrightarrow \mathbf{T}_X \oplus \mathbf{T}_Y.$$

If $\mathscr{P}$ is such a prime, its image in $\mathbf{T}_X$ (resp. $\mathbf{T}_Y$) is a prime ideal $\mathscr{P}_X$ (resp. $\mathscr{P}_Y$) of $\mathbf{T}_X$ (resp. $\mathbf{T}_Y$). We again refer to $\mathscr{P}_X$ and $\mathscr{P}_Y$ as primes of fusion, and we note the canonical isomorphisms

$$\mathbf{T}_X/\mathscr{P}_X \simeq \mathbf{T}/\mathscr{P} \simeq \mathbf{T}_Y/\mathscr{P}_Y.$$

Especially, we view the isomorphism between extreme terms as a congruence between eigenvalues of the T_n on X and on Y (cf. [3], Th. 7.1).

Conversely, suppose that $f \in X$ and $g \in Y$ are eigenforms for the T_n, with eigenvalues a_n and b_n ($n \geqslant 1$) respectively. Let $\mathcal{O}$ be the ring of integers of the number field generated by all the a_n and b_n. Then there are unique homomorphisms

$$\phi_X\colon \mathbf{T}_X \to \mathcal{O}, \quad \phi_Y\colon \mathbf{T}_Y \to \mathcal{O}$$

such that $\phi_X(T_n) = a_n$ and $\phi_Y(T_n) = b_n$ for all n. Assume now that λ is a maximal ideal of O such that

$$a_n \equiv b_n \mod \lambda$$

for all n. Then one sees immediately that $\mathscr{P}_X = \phi_X^{-1}(\lambda)$ and $\mathscr{P}_Y = \phi_Y^{-1}(\lambda)$ are primes of fusion in $\mathbf{T}_X$ and $\mathbf{T}_Y$. The corresponding ideal $\mathscr{P}$ of $\mathbf{T}$ is obtained by pulling back either $\mathscr{P}_X$ or $\mathscr{P}_Y$ to $\mathbf{T}$.

If $\mathscr{P}_X$ is an ideal of $\mathbf{T}_X$ which one suspects to be a prime of fusion, one can prove that $\mathscr{P}_X$ is indeed such a prime by exhibiting a $\mathbf{T}_X$-module Ω, whose support contains $\mathscr{P}_X$, which satisfies the following condition: if we view Ω as a $\mathbf{T}$-module via the natural surjection $\mathbf{T} \to \mathbf{T}_X$, the resulting homomorphism

$$\mathbf{T} \to \mathrm{End}(\Omega)$$

factors through the surjection $\mathbf{T} \to \mathbf{T}_Y$ as well. In Proposition 1.11 of [10], the author showed that a certain $\mathbf{T}$-module $\tilde{L}/L$ detects in this way all primes of fusion which do not divide the level N of the space S. In other words, one can find essentially all primes of fusion by calculating the support of this module.

We now come to the specific problem alluded to above. We will consider only weight 2 cusp forms (and especially newforms) on groups of the form $\Gamma_0(N)$. We first take a newform

$$f = \sum a_n q^n$$

on $\Gamma_0(N)$ and then consider a prime number M which is prime to N. Suppose that λ is a prime ideal in the ring of integers of a sufficiently large finite extension of $\mathbf{Q}$ in $\bar{\mathbf{Q}}$ whose residue characteristic l is prime to

MN. Suppose that

$$g = \sum b_n q^n$$

is a weight 2 newform of level divisible by M and dividing NM for which we have the congruence

$$a_p \equiv b_p \bmod \lambda \tag{2.1}$$

for all prime numbers p in a set of primes of density 1. Then the mod λ representations of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ defined by f and g have isomorphic semi-simplifications. By considering the restrictions of these representations to the decomposition group $\mathrm{Gal}(\bar{\mathbf{Q}}_M/\mathbf{Q}_M)$ for M in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, we obtain the congruence

$$a_M \equiv b_M(1+M) \bmod \lambda.$$

Since b_M is either $+1$ or -1, we find

$$a_M^2 \equiv (1+M)^2 \bmod \lambda. \tag{2.2}$$

Our problem is to determine whether or not the converse holds: if the congruence (2.2) is verified for a specific prime $M \nmid N$, need there be a form g satisfying (2.1)?

We can rephrase this problem in terms of primes of fusion by considering a suitable decomposition (1.1) of the space S of weight 2 cusp forms on $\Gamma_0(NM)$. Namely, we take X to be the subspace of old forms of S which is associated to $\Gamma_0(N)$, so that X is naturally isomorphic to the direct sum of two copies of the space of cusp forms of weight 2 on $\Gamma_0(N)$. We then take Y to be the orthogonal complement to X under the Petersson inner product on S. Thus Y is the intersection of the kernels of the two natural trace maps from S to the space of weight 2 cusp forms on $\Gamma_0(N)$. Our problem will be to show, under hypothesis (2.2), that a certain ideal $\mathscr{P}_X$ of $\mathbf{T}_X$ is a prime of fusion.

To define $\mathscr{P}_X$, our inclination would be to proceed as before, using f to define a homomorphism ϕ_X, and using ϕ_X to pull back λ to $\mathbf{T}_X$. A technical complication arises, however: f is no longer an eigenform for the Hecke operator T_M acting on X. To surmount this, assuming that we have

$$a_M \equiv \pm(1+M) \bmod \lambda,$$

we introduce

$$f' = \sum a_n q^n \mp M \sum a_n q^{Mn} \in X.$$

Then f' is a mod λ eigenform for T_M with eigenvalue ± 1; it is also an eigenform for the T_n such that $(n, M) = 1$, with eigenvalue a_n. Thus f' defines a homomorphism $\mathbf{T}_X \to \mathbf{F}$, where $\mathbf{F}$ is the residue field of λ, such that the image of T_n for each $n \geqslant 1$ is the eigenvalue of T_n acting on f', modulo λ. Its kernel is a prime ideal $\mathscr{P}_X$ of $\mathbf{T}_X$; pulling back to $\mathbf{T}$ we obtain a prime ideal $\mathscr{P}$ of T.

The problem stated above now amounts to determining whether or not $\mathscr{P}$ and $\mathscr{P}_X$ are primes of fusion. We will write η for the operator $T_M^2 - 1$, viewed either as an element of $\mathbf{T}$ or an element of $\mathbf{T}_X$. Then we wish to study

PROBLEM 2.3. Suppose that $\mathscr{P}_X$ is a prime ideal of $\mathbf{T}_X$ which contains η. Is $\mathscr{P}_X$ necessarily a prime of fusion?

It is easy to see that the answer to this problem is, in general, negative. For example, taking $N = 11$ and $M = 7$, one can prove that the ideal $(T_M + 1)$ of $\mathbf{T}_X$ is a prime ideal containing $T_M^2 - 1$ which is *not* a prime of fusion. In this case, the residue field of our ideal is the field with 5 elements. We will see, however, that Problem 2.3 has an affirmative solution if we impose on $\mathscr{P}_X$ a suitable additional condition, for example that $\mathscr{P}_X$ be prime to the order of the *Shimura subgroup* $\mathbf{S}$ of $J_0(N)$ (as defined in § 4 below). If N is a prime number, this group has order $n = \mathrm{num}\left(\frac{N-1}{12}\right)$ (cf. [7], Ch. II, § 11); if $N = 11$, this group has order 5. Notice especially that the Shimura subgroup of $J_0(N)$ depends only on N, and not on the prime number M.

3. Our result arises from the study of a certain $\mathbf{T}_X$-module Ω, which is closely related to the group $\tilde{L}/L$ mentioned above. Its support contains only primes of fusion, and in fact contains all such primes which do not divide the integer NM. We shall exhibit a $\mathbf{T}_X$-module Δ, whose support consists precisely of the primes containing η, which is furnished with a filtration

$$\Delta = M_0 \supset M_1 \supset M_2 \supset M_3 = 0$$

such that M_1/M_2 is isomorphic to Ω and such that the quotients M_0/M_1 and M_2/M_3 have the same cardinality as $\mathbf{S}$. Any prime ideal of $\mathbf{T}_X$ which contains η and which is prime to the cardinality of $\mathbf{S}$ is consequently in the support of Ω and is therefore a prime of fusion.

Recall ([8], § 2a) the two natural "degeneracy" maps

$$B_1, B_M\colon X_0(NM) \to X_0(N)$$

which correspond, respectively to the identity map and the map $\tau \mapsto M\tau$ on the Poincaré upper half plane. By Pic functoriality they induce maps

$$B_1^*, B_M^*: J_0(N) \to J_0(NM)$$

from which we obtain a homomorphism

$$\alpha: J_0(N) \times J_0(N) \to J_0(NM)$$

by adding these two maps together. The kernel of α is a ceratin finite subgroup Σ of $J_0(N)^2$, which we will study below. The image of α is an abelian subvariety A of $J_0(NM)$ which naturally corresponds to the subspace X of S. For example, when we view $\mathbf{T}$ as a subring of End $(J_0(NM))$ in the usual way we find that $\mathbf{T}$ preserves A and that its action on A factors through $\mathbf{T}_X$.

Similarly, we consider the transpose

$$\alpha': J_0(NM) \to J_0(N) \times J_0(N)$$

of α; it corresponds to the two degeneracy maps induced by B_1 and B_M using Albanese functoriality of the Jacobian. Its kernel is not necessarily connected; in fact, it is an extension of a finite group, canonically isomorphic to the Cartier dual of Σ, by an abelian subvariety B of $J_0(NM)$. The variety B analogously corresponds to Y, so that the action of $\mathbf{T}$ on B factors through $\mathbf{T}_Y$. The intersection

$$\Omega = A \cap B$$

is a finite subgroup of $J_0(NM)$, stable under $\mathbf{T}$, such that the action of $\mathbf{T}$ on Ω factors through both rings $\mathbf{T}_X$ and $\mathbf{T}_Y$. Therefore any prime in the support of Ω is a prime of fusion; and as mentioned above one can show that all primes of fusion occur in the support of Ω, with the possible exceptions of those whose residue fields are of characteristic dividing NM.

Now let L be the line bundle on A arising from the canonical "theta divisor" on $J_0(NM)$ and the inclusion ι of A in $J_0(NM)$. Then L induces an isogeny

$$\phi_L: A \to A^\vee,$$

where $A^\vee$ denotes the abelian variety dual to A. We will denote by $K(L)$ the kernel of this map. It is easy to check the equality

$$\Omega = K(L). \tag{3.1}$$

Indeed, B is quickly seen to be the kernel of the composite $\iota^\vee \circ \phi$, where ϕ is the canonical autoduality of the Jacobian $J_0(NM)$. This gives that Ω

is the kernel of

$$\iota^{\vee} \circ \phi \circ \iota,$$

which is just another way of writing ϕ_L. From (3.1) we obtain a slightly different way of viewing Ω, as follows. Let β denote the isogeny

$$J_0(N) \times J_0(N) \to A$$

for which $\alpha = \iota \circ \beta$. Pulling L back to $J_0(N)^2$ via β, we obtain a line bundle $\beta^* L$, whence a finite subgroup $K(\beta^* L)$ of $J_0(N)^2$. This subgroup, which we call Δ, contains Σ and is endowed with a canonical non-degenerate alternating $\mathbf{G}_m$-valued pairing. Let $\Sigma^{\perp}$ be the orthogonal to Σ relative to this pairing; this subgroup of Δ contains Σ, and we have the formula

$$\Omega = \Sigma^{\perp}/\Sigma, \tag{3.2}$$

in view of [9], § 23, Lemma 2.

On the other hand, we can check that Δ is just the kernel of $\alpha' \circ \alpha$. Viewing this endomorphism of $J_0(N)^2$ as a 2×2 matrix of endomorphisms of $J_0(N)$, we find the formula

$$\alpha' \circ \alpha = \begin{bmatrix} M+1 & \tau \\ \tau & M+1 \end{bmatrix},$$

where τ is the usual Hecke operator T_M on $J_0(N)^2$. In other words, we have

$$\Delta = \{(x, y) \in J_0(N)^2 \mid \tau x = -(M+1)y \text{ and } \tau y = -(M+1)x\}.$$

We now claim that $\mathbf{T}_X$ acts on $J_0(N)^2$ as a subring of endomorphisms of this abelian variety. By this we mean that, for each each $n \geqslant 1$, the quantity

$$T'_n = \beta^{-1} \circ T_n \circ \beta,$$

a priori an endomorphism of $J_0(N)^2$ up to isogeny, is in fact a genuine endomorphism of $J_0(N)^2$. This assertion is clear indeed if n is prime to M; in that case, T'_n is nothing but the usual Hecke operator T_n on $J_0(N)$, acting "diagonally" on the product $J_0(N)^2$. Thus the general case follows from the explicit formula

$$T'_M = \begin{bmatrix} \tau & M \\ -1 & 0 \end{bmatrix}.$$

In what follows, we will omit the superscript $'$ and write T_n for T'_n.

PROPOSITION 3.3. *The group Δ is the kernel of the endomorphism $\eta = T_M^2 - 1$ of $J_0(N)^2$.*

This proposition is proved by a short calculation, which we omit; the reader can verify that we have more precisely the identity

$$\eta = \begin{bmatrix} -1 & \tau \\ 0 & -1 \end{bmatrix} \circ (\alpha' \circ \alpha).$$

Because of (3.3), we can view Δ as a $\mathbf{T}_X$-module. Its *support* consists of all prime ideals of $\mathbf{T}_X$ which contain the annihilator I of Δ in $\mathbf{T}_X$. We have

$$I = \{T \in \mathbf{T}_X |\ T = \varepsilon\eta \text{ for some } \varepsilon \in \mathrm{End}(J_0(N)^2)\},$$

i.e.,

$$I = R\eta \cap \mathbf{T}_X,$$

where

$$R = (\mathbf{T}_X \otimes \mathbf{Q}) \cap \mathrm{End}(J_0(N)^2).$$

Now R is a finitely generated abelian group, so certainly finitely generated as a $\mathbf{T}_X$-module. Hence if $\mathscr{P}_X$ is a maximal ideal of $\mathbf{T}_X$ we have

$$\mathscr{P}_X = R\mathscr{P}_X \cap \mathbf{T}_X.$$

This formula shows that we have $\mathscr{P}_X \supseteq I$ if and only if $\mathscr{P}_X$ contains η. Hence we get:

PROPOSITION 3.4. *The support of Δ consists precisely of those primes of $\mathbf{T}_X$ which contain η.*

This proposition may be viewed as a partial solution to Problem 2.3. It fails to be a complete solution because of the group Σ, which is the obstruction to the equality between Δ and Ω. We will determine Σ in the next section.

4. Our analysis of Σ is based on results contained in Ihara's article [6].[1] We will find, in studying Σ, that the analogue of this group is 0 in the situation where $\Gamma_0(N)$ is replaced by either of its subgroups $\Gamma_1(N)$ or $\Gamma(N)$. For definiteness in what follows, we shall regard these groups as subgroups of $\mathbf{PSL}(2, \mathbf{Z})$, rather than $\mathbf{SL}(2, \mathbf{Z})$. We will let $X_1(N)$ and $X(N)$ be the modular curves associated with these groups and let $J_1(N)$ and $J(N)$ be, as usual, the Jacobians of these curves.

---

[1] The author wishes to thank J.-P. Serre for bringing Ihara's results to his attention.

The inclusions $\Gamma(N) \subset \Gamma_1(N)$ and $\Gamma_1(N) \subset \Gamma_0(N)$ correspond to coverings of curves

$$\sigma\colon X(N) \to X_1(N), \quad \pi\colon X_1(N) \to X_0(N).$$

From these maps we obtain, by Pic functoriality, maps

$$\pi^*\colon J_0(N) \to J_1(N), \quad \sigma^*\colon J_1(N) \to J(N).$$

The kernel of π^* is a finite subgroup $\mathbf{S}$ of $J_0(N)$ which is known as the *Shimura subgroup* of $J_0(N)$. It is isomorphic to the $\mathbf{G}_m$-dual of the covering group of the maximal abelian unramified covering of $X_0(N)$ which is intermediate to $X_1(N) \to X_0(N)$. The kernel of σ^* is trivial, because there are no unramified coverings of $X_1(N)$ intermediate to $X(N) \to X_1(N)$: the standard cusp "∞" of $X_1(N)$ is totally ramified in this covering.

If Γ is one of the three groups $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$, we will let Γ' be the intersection of Γ with $\Gamma_0(M)$. We use the symbol $'$ in writing the corresponding modular curves and their Jacobians. Thus $J_0'(N)$, for instance, is $J_0(NM)$. We then have a pair of commutative diagrams

$$\begin{array}{ccc} J(N)^2 & \xrightarrow{\gamma} & J'(N) \\ {\scriptstyle\sigma^*}\uparrow & & \uparrow \\ J_1(N) & \xrightarrow{\beta} & J_1'(N) \end{array} \qquad \begin{array}{ccc} J_1(N)^2 & \xrightarrow{\beta} & J_1'(N) \\ {\scriptstyle\pi^*}\uparrow & & \uparrow \\ J_0(N)^2 & \xrightarrow{\alpha} & J_0'(N) \end{array}$$

in which the horizontal maps are the obvious degeneracy maps. We shall admit for the moment the following result:

THEOREM 4.1. *The kernel of γ is trivial.*

Then, by the above discussion, we certainly have:

COROLLARY 4.2. *The kernel of β is trivial. The kernel Σ of α is a subgroup of* $\mathbf{S} \times \mathbf{S}$.

More precisely, we will prove

THEOREM 4.3. *The group Σ is the subgroup*

$$T = \{(x, y) \in \mathbf{S} \times \mathbf{S} \mid x + y = 0\}$$

of $\mathbf{S} \times \mathbf{S}$.

To prove Theorem 4.3 we first will show that Σ contains T. Let

$$B\colon J_0(N) \to J_0(NM)$$

be the degeneracy map B_1^*. Then the degeneracy map B_M^* is the composition $W_M \circ B$, where W_M is the indicated Atkin–Lehner involution of $J_0(NM)$. The inclusion $\Sigma \supseteq T$ thus means that W_M acts on the group $B(\mathbf{S})$ by multiplication by $+1$. Now the Atkin–Lehner involution W_N on $J_0(N)$ acts on $\mathbf{S}$ by multiplication by -1 (cf. [7], Chapter II, Proposition 11.7), which gives that the Atkin–Lehner involution W_N of $J_0(NM)$ acts on $B(\mathbf{S})$ by multiplication by -1. But since $B(\mathbf{S})$ is a subgroup of the Shimura subgroup of $J_0(NM)$, we find that W_{NM} acts on $B(\mathbf{S})$ by multiplication by -1. Since $W_M = W_{NM} \circ W_N$, we get that Σ contains T.

In view of this inclusion, the assertion $\Sigma = T$ amounts to the injectivity of B on $\mathbf{S}$. In fact, B has kernel 0 because the covering B_1: $X_0(NM) \to X_0(N)$ is ramified and such that there is no non-trivial covering of $X_0(N)$, other than B_1, which is intermediate to B_1.

Proof of Theorem 4.1. We must show, for all prime numbers l, the injectivity of the map

$$H^1(X(N), \mathbf{Z}/l\mathbf{Z}) \oplus H^1(X(N), \mathbf{Z}/l\mathbf{Z}) \to H^1(X'(N), \mathbf{Z}/l\mathbf{Z})$$

resulting from the two degeneracy coverings $X'(N) \rightrightarrows X(N)$. We may view $H^1(X(N), \mathbf{Z}/l\mathbf{Z})$ as classifying unramified Galois coverings of $X(N)$ with structural group $\mathbf{Z}/l\mathbf{Z}$, and the problem is to show that there is no non-trivial pair of such coverings which become equal after pullback to $X'(N)$ by the two different degeneracy maps. However, this is just a special case of Lemma 3.2 of Ihara [6], which asserts that the system

$$\begin{array}{ccc} & X'(N) & \\ \swarrow & & \searrow \\ X(N) & & X(N) \end{array}$$

is "simply connected". (See also the remarks at the beginning of § 3.4 of [6].)

Alternatively, we may obtain a slightly more direct proof of Theorem 4.1 from the ingredients used in the proof of Ihara's Lemma 3.2. Here we view Theorem 4.1 as asserting the surjectivity of the natural map

$$H_1(X'(N), \mathbf{Z}) \to H_1(X(N), \mathbf{Z}) \oplus H_1'(X(N), \mathbf{Z}).$$

In terms of subgroups of $\mathbf{PSL}(2, \mathbf{Q})$, we have corresponding inclusions of the group

$$\Delta = \Gamma(N) \cap \Gamma_0(N)$$

in the two groups

$$G_1 = \Gamma(N), \quad G_2 = \begin{bmatrix} M & 0 \\ 0 & 1 \end{bmatrix}^{-1} \Gamma(N) \begin{bmatrix} M & 0 \\ 0 & 1 \end{bmatrix};$$

we wish to prove the surjectivity of

$$H_1(A, \mathbf{Z}) \to H_1(G_1, \mathbf{Z})/\mathrm{Pb}(G_1) \oplus H_1(G_2, \mathbf{Z})/\mathrm{Pb}(G_2). \tag{4.4}$$

(Here $\mathrm{Pb}(G_i)$ denotes the subgroup of $H_1(G_i, \mathbf{Z})$ generated by the set of parabolic elements of the group G_i, for $i = 1, 2$.)

Let Γ be the principal congruence subgroup of level N (i.e., the analogue of $\Gamma(N)$) in $\mathbf{PSL}(2, \mathbf{Z}[1/M])$. Then the inclusions of G_1 and G_2 in Γ are well known to induce an isomorphism of the amalgamated product $G_1 *_A G_2$ with Γ (see, e.g., [11], Ch. II, § 1.4). Accordingly, by the exact sequence of Lyndon (see, e.g., [*loc. cit.*], page 169), the cokernel of the map

$$H_1(A, \mathbf{Z}) \to H_1(G_1, \mathbf{Z}) \oplus H_1(G_2, \mathbf{Z})$$

may be identified with $H_1(\Gamma, \mathbf{Z})$. Let Δ be the subgroup of Γ generated by the commutator subgroup of Γ and by the parabolic elements of G_1 and G_2. Then the cokernel of the map (4.4) may be identified with the quotient Γ/Δ.

Since Γ is generated by its parabolic elements, the surjectivity of (4.4) thus means that all parabolic elements of Γ lie in Δ. As on page 178 of [6], we now note that if γ is a parabolic element of Γ, then γ^{M^n} lies in G_1 for some positive integer n. It is easy to deduce from this that γ lies in Δ (*loc. cit.*).

References

[1] Doi K. and Hida H., *On a Certain Congruence of Cusp Forms and the Special Values of Their Dirichlet Series*, Unpublished manuscript, 1979.

[2] Doi K. and Ohta M., *On Some Congruences Between Cusp Forms on $\Gamma_0(N)$*, Lecture Notes in Math. 601, pp. 91–105, Springer, Berlin–Heidelberg–New York, 1977.

[3] Hida H., Congruences for Cusp Forms and Special Values of Their Zeta Functions, *Invent. Math.* **63** (1981), pp. 225–261.

[4] Hida H., On Congurence Divisors of Cusp Forms as Factors of the Special Values of Their Zeta Functions, *Invent. Math.* **64** (1981), pp. 221–262.

[5] Hida H., Kummer's Criterion for the Special Values of Hecke L-Functions of Imaginary Quadtratic Fields and Congruences Among Cusp Forms, *Invent. Math.* **66** (1982), pp. 415–459.

[6] Ihara Y., On Modular Curves Over Finite Fields, *Proceedings of the International Colloquium on Discrete Subgroups of Lie Groups and Applications to Moduli*, Bombay, January 1973, pp. 161–202.

[7] Mazur B., Modular Curves and the Eisenstein Ideal, *Publ. Math. IHES* **47** (1977), pp. 33–186.
[8] Mazur B., Rational Isogenies of Prime Degree, *Invent. Math.* **44** (1978), pp. 129–162.
[9] Mumford D., *Abelian Varieties,* Oxford University Press, London, 1970.
[10] Ribet K., Mod p Hecke Operators and Congruences Between Modular Forms, *Invent. Math.* **71** (1983), pp. 193–205.
[11] Serre J.-P., Arbres, Amalgames, SL_2, *Astérisque* **46**, Société Mathématique de France, Paris, 1977.

U.C. BERKELEY MATH. DEPARTMENT,
BERKELEY, CA.
94720 USA