Multiplicities of p-finite mod p Galois representations in $J_o(Np)$

Kenneth A. Ribet

Department of Mathematics
University of California
Berkeley, CA 94720 USA

This article was prepared while the author was visiting the I.H.E.S., and is based partially on the author's lecture at I.M.P.A. during an algebraic geometry workshop in April, 1990. It is a pleasure to thank both institutes for their hospitality, as well as Professor B. Mazur for helpful suggestions. The author was partially supported by NSF contract DMS 88-06815.

1. Introduction.

Let $M \geq 1$ be an integer. Let $J_o(M)$ be the Jacobian $\mathrm{Pic}^o(X_o(M))$ of the modular curve $X_o(M)_{\mathbf{Q}}$. For all $n \geq 1$, let T_n be the n^{th} Hecke correspondence on $X_o(M)$. Write again T_n for the endomorphism T_n^* of $J_o(M)$ induced by the correspondence T_n. Let $\mathbf{T}_M = \mathbf{Z}[\ldots, T_n, \ldots]$ be the subring of $\mathrm{End}(J_o(M))$ generated by the T_n with $n \geq 1$. The ring $\mathbf{T}_M$ may be identified with the ring generated by the Hecke operators T_n acting on the complex vector space of weight-2 cusp forms on $\Gamma_o(M)$.

Suppose that $\mathfrak{p}$ is a maximal ideal of $\mathbf{T}_M$. The residue field $\mathbf{T}_M/\mathfrak{p}$ is a finite field k, whose characteristic will be denoted p. Attached to $\mathfrak{p}$ is a semisimple continuous representation

$$\rho_{\mathfrak{p}} \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, k),$$

unramified outside Mp, with the property that $\rho_{\mathfrak{p}}(\varphi_r)$ has characteristic polynomial $X^2 - T_r X + r \pmod{\mathfrak{p}}$ for each prime number r prime to Mp. (Here, φ_r denotes a Frobenius element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ for the prime number r.) The representation $\rho_{\mathfrak{p}}$ is well defined up to isomorphism.

Consider the group of p-division points

$$J_o(M)[\mathfrak{p}] := \left\{ x \in J_o(M)(\overline{\mathbf{Q}}) \;\middle|\; \lambda x = 0 \text{ for all } \lambda \in \mathfrak{p} \right\},$$

i.e., the "kernel of $\mathfrak{p}$ on $J_o(M)$." Assume:

i. The representation $\rho_{\mathfrak{p}}$ is irreducible over k.

ii. The prime number p is odd.

Then $\rho_{\mathfrak{p}}$ is an absolutely irreducible representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and a theorem of Boston, Lenstra, and the author [1] shows that $J_o(M)[\mathfrak{p}]$ is a direct sum of representations isomorphic to $\rho_{\mathfrak{p}}$. The associated *multiplicity* $\mu_{\mathfrak{p}}$ is the number of summands in the direct sum:

$$\mu_{\mathfrak{p}} = \frac{1}{2} \dim_k J_o(M)[\mathfrak{p}].$$

Since $J_o(M)[\mathfrak{p}]$ is non-zero, $\mu_{\mathfrak{p}}$ is a positive integer. Thus $J_o(M)[\mathfrak{p}]$ is "multiplicity free" (in the sense that $\mu_{\mathfrak{p}} \leq 1$) if and only if we have $\mu_{\mathfrak{p}} = 1$.

Using ideas of Mazur [4], the author proved that $\mu_{\mathfrak{p}} = 1$ whenever M is prime to p ([10], Theorem 5.2). In [5], Mazur and the author considered the case where p exactly divides M, i.e., where $M = Np$ for some integer $N \geq 1$ which is prime to p. The principal result of that article states that $\mu_{\mathfrak{p}} = 1$ provided that $\rho_{\mathfrak{p}}$ is not finite at p (in the sense of Serre [12], p. 189), or equivalently ([10], Theorem 6.1) provided that $\rho_{\mathfrak{p}}$ is not modular of level N. These results were motivated by applications to Serre's conjectures [12], and specifically are used in showing that certain mod p Galois representations which are known to be modular of some level are in fact modular of the conjectured level (see [10]).

In the present article, we explore the situation when p exactly divides M but $\rho_{\mathfrak{p}}$ is allowed to be finite. Although this situation does not appear in applications to Serre's conjectures, the author hopes that the present paper will shed light on the general problem of computing $\mu_{\mathfrak{p}}$.

In order to state our results, we introduce the p-old and p-new subvarieties A and B of $J_o(M)$. We assume that $M = Np$, and that p is prime to N. Recall [8] that the abelian varieties $J_o(N)$ and $J_o(Np)$ are connected by a natural "degeneracy map"

$$d\colon J_o(N) \times J_o(N) \longrightarrow J_o(Np),$$

whose kernel Σ is the finite group consisting of all pairs $(\sigma, -\sigma)$, where σ runs over the Shimura subgroup of $J_o(N)$, i.e., the kernel of the map $J_o(N) \to J_1(N)$ induced by the standard covering $X_1(N) \to X_o(N)$. The p-old subvariety of $J_o(Np)$ is the image A of d. The p-new subvariety of $J_o(Np)$ is the "orthogonal complement" B to A under the natural

autoduality $J_o(Np) \widetilde{\to} J_o(Np)^\vee$. In other words, the image of B in $J_o(Np)^\vee$ under the isomorphism $J_o(Np) \widetilde{\to} J_o(Np)^\vee$ is the kernel of the map $J_o(Np)^\vee \to A^\vee$ which is dual to the inclusion of A in $J_o(Np)$. One has $J_o(Np) = A + B$, and the group $\Delta := A \cap B$ is finite; this group was calculated in [8].

In the following discussion, we will write simply J for $J_o(Np)$. Also, we will let $A[\mathfrak{p}]$ and $B[\mathfrak{p}]$ be the analogues of $J_o(Np)[\mathfrak{p}]$ for A and B, respectively. When (i) and (ii) are satisfied, $A[\mathfrak{p}]$ and $B[\mathfrak{p}]$ are each direct sums of representations isomorphic to $\rho_{\mathfrak{p}}$. We say that $A[\mathfrak{p}]$ or $B[\mathfrak{p}]$ is *multiplicity free* if the corresponding direct sum has at most one term. Thus $B[\mathfrak{p}]$, for example, is multiplicity free if it is either zero, or else of dimension two over k. Finally, we write $J_o(N)^2$ for the product $J_o(N) \times J_o(N)$.

Assume that the above hypotheses (i) and (ii) are satisfied.

Proposition 1. *The representation $\rho_{\mathfrak{p}}$ is finite at p if and only if $A[\mathfrak{p}]$ is non-zero.*

Theorem 1. *If $A[\mathfrak{p}] = 0$, then $\mu_{\mathfrak{p}} = 1$.*

Proposition 1 results easily from known facts; its proof will be given in §2. Using the Proposition, we see immediately that Theorem 1 is a restatement of the result of [5] which was introduced above.

In this article, we shall prove the following complement:

Theorem 2. *Suppose that (i) and (ii) are satisfied. Then the group $J[\mathfrak{p}]$ is multiplicity free if and only if the group $B[\mathfrak{p}]$ is multiplicity free.*

As mentioned above, the condition that $J[\mathfrak{p}]$ be multiplicity free is equivalent to the equality $\mu_{\mathfrak{p}} = 1$. Hence Theorem 2 provides a means of verifying this equality even when the condition $A[\mathfrak{p}] = 0$ of Theorem 1 is not necessarily satisfied.

Corollary. *Suppose that (i) and (ii) are satisfied and that B is an elliptic curve. Then $J[\mathfrak{p}]$ is multiplicity free.*

The Corollary follows directly from the Theorem. Indeed, suppose that B is an elliptic curve. If $B[\mathfrak{p}]$ is non-zero, then $\mathfrak{p} \subset \mathbf{T}_{pN}$ generates a non-trivial ideal in the image of $\mathbf{T}_{pN}$ in $\operatorname{End} B$. Since this image is isomorphic to $\mathbf{Z}$, we have $B[\mathfrak{p}] = B[p]$, and the residue field

of $\mathfrak{p}$ is the prime field $\mathbf{F}_p$. Hence $B[\mathfrak{p}]$ is either 0, or else of dimension two over $\mathbf{F}_p$. In particular, $B[\mathfrak{p}]$ is multiplicity free.

Theorem 2 is obtained as a consequence of two results proved below. Namely, in §2, we prove, under the hypotheses of Theorem 2, that $A[\mathfrak{p}]$ is multiplicity free (Theorem 3). In §3, we show that $B[\mathfrak{p}] = J[\mathfrak{p}]$ whenever $B[\mathfrak{p}]$ is non-zero (Theorem 4). These together imply Theorem 2 by an elementary argument, in which we consider separately the case where $B[\mathfrak{p}]$ is 0 and the case where it is non-zero. Indeed, suppose first that $B[\mathfrak{p}] = 0$. Then $B[\mathfrak{p}]$ is certainly multiplicity free, and Theorem 2 states that $J[\mathfrak{p}]$ is multiplicity free. However, $\Delta[\mathfrak{p}] = 0$, from which it follows that the p-divisible group $\cup_i J[\mathfrak{p}^i]$ is the direct sum of the analogous p-divisible groups for A and B. This gives, in particular, $J[\mathfrak{p}] = A[\mathfrak{p}] \oplus B[\mathfrak{p}]$, so that $J[\mathfrak{p}] = A[\mathfrak{p}]$, because $B[\mathfrak{p}]$ is 0. Theorem 3 then implies that $J[\mathfrak{p}]$ is multiplicity free, as desired. On the other hand, if $B[\mathfrak{p}]$ is non-zero, then Theorem 4 states that $J[\mathfrak{p}]$ and $B[\mathfrak{p}]$ are equal, so that one is multiplicity free if and only if the other is.

It is perhaps worth stressing that our results prove that $\mu_{\mathfrak{p}} = 1$ whenever one of $A[\mathfrak{p}]$ and $B[\mathfrak{p}]$ vanishes and the hypotheses (i) and (ii) are satisfied. Indeed, suppose this to be the case, and assume first that $A[\mathfrak{p}]$ vanishes. Then an argument analogous to that just given shows that $J[\mathfrak{p}] = B[\mathfrak{p}]$, so that Theorem 2 is trivially true (as is Theorem 4). By Theorem 1, we have $\mu_{\mathfrak{p}} = 1$; i.e., $J[\mathfrak{p}] = B[\mathfrak{p}]$ is multiplicity free. Next, assume that $B[\mathfrak{p}]$ vanishes. Then, as noted above, we have $A[\mathfrak{p}] = J[\mathfrak{p}]$. Also, $A[\mathfrak{p}]$ is multiplicity free by Theorem 3. Hence $\mu_{\mathfrak{p}} = 1$ in this case as well.

Assume now that both $A[\mathfrak{p}]$ and $B[\mathfrak{p}]$ are non-zero, and that (i) and (ii) are satisfied. Then our results give the relations

$$0 \subset A[\mathfrak{p}] \subseteq B[\mathfrak{p}] = J[\mathfrak{p}],$$

and show that $A[\mathfrak{p}]$ is multiplicity free. We have $\mu_{\mathfrak{p}} = 1$ in this situation if and only if all three groups $A[\mathfrak{p}]$, $B[\mathfrak{p}]$ and $J[\mathfrak{p}]$ coincide. By the Corollary above, these groups do in fact coincide if B is an elliptic curve, although perhaps not in general. (The author knows of no example where they fail to coincide.)

We close this Introduction with a numerical example. Take $N = 11$ and $p = 3$. The dimensions of $J_o(11)$ and $J_o(33)$ are respectively 1 and 3. Thus, A is isogenous to a product

of two copies of the elliptic curve $J_o(11)$, while B is an elliptic curve of conductor 33. By the Corollary to Theorem 2, $J[\mathfrak{p}]$ is multiplicity free for each prime $\mathfrak{p}$ of $\mathbf{T}_{33}$ which divides 3.

One can verify that there are in fact two $\mathfrak{p}$'s, and that $\rho_{\mathfrak{p}}$ is finite for each $\mathfrak{p}$. (In other words, Theorem 1 applies for neither of them.) To describe the two $\mathfrak{p}$, we let $E = J_o(11)$ and use the degeneracy map d to identify $A[3]$ with the product $E[3] \times E[3]$. The Hecke operator T_3 of J induces the operator $(x, y) \mapsto (-x, -x)$ on $E[3] \times E[3]$. Accordingly, the diagonal image V_1 of $E[3]$ in $E[3] \times E[3]$ is $\mathbf{T}_{33}$-stable, and $\mathbf{T}_{33}$ acts on V_1 via a homomorphism $\phi_1 \colon \mathbf{T}_{33} \to \mathbf{F}_3$ which maps T_3 to -1. If $\mathfrak{p}_1 = \ker \phi_1$, then Theorem 4 implies that $B[\mathfrak{p}_1] = J[\mathfrak{p}_1] = A[\mathfrak{p}_1] = V$. Similarly, if V_2 is the subspace $0 \oplus E[3]$ of $A[3]$, then $\mathbf{T}_{33}$ acts on V_2 via a homomorphism $\phi_2 \colon \mathbf{T}_{33} \to \mathbf{F}_3$ which maps T_3 to 0. If $\mathfrak{p}_2 = \ker \phi_2$, then $B[\mathfrak{p}_2] = 0$, and we have $J[\mathfrak{p}_2] = A[\mathfrak{p}_2] = V'$.

2. Study of $A[\mathfrak{p}]$.

Let p be an odd prime, and suppose that N is a positive integer prime to p. Write $\mathbf{T}$ for the ring $\mathbf{T}_{Np}$. The p-old subvariety A of $J_o(pN)$ is $\mathbf{T}$-stable. We define the *p-old quotient of* $\mathbf{T}$ to be the image $\mathbf{T}_A$ of $\mathbf{T}$ in $\mathrm{End}(A)$. Similarly, we define a maximal ideal $\mathfrak{p}$ of $\mathbf{T}$ to be *p-old* if and only if it arises by pullback from a maximal ideal of $\mathbf{T}_A$. It is clear that $\mathfrak{p}$ is p-old if and only if $A[\mathfrak{p}]$ is non-zero. Thus, Proposition 1 states, for $\mathfrak{p}|p$ such that $\rho_{\mathfrak{p}}$ is irreducible, that $\rho_{\mathfrak{p}}$ is finite at p if and only $\mathfrak{p}$ is p-old.

We now prove this Proposition. Assume, first, that $\rho_{\mathfrak{p}}$ is finite at p. Theorem 6.1 of [10] then states that $\rho_{\mathfrak{p}}$ is "modular of level N." (The hypotheses of that theorem are satisfied because the residue characteristic of $\mathfrak{p}$, which is p, is not congruent to 1 mod p.) In fact, the argument given in [10] proves the apparently stronger fact that $\mathfrak{p}$ is p-old. Namely, under the finiteness assumption, the author constructs a certain subgroup $\mathcal{V}$ of the fiber at p of the Néron model for $J_o(Np)$. Write $\mathcal{J}_{\mathbf{F}_p}$ for this fiber. The discussion on pp. 470–471 of [10] shows that $\mathcal{V}$ cannot be a subgroup of the maximal torus T of $\mathcal{J}_{\mathbf{F}_p}$. Furthermore, the argument given to prove Lemma 6.3 of [10] shows then that $\mathcal{V}$ must map non-trivially to the product $J_o(N)_{\mathbf{F}_p} \times J_o(N)_{\mathbf{F}_p}$, which is the maximal abelian variety quotient of the connected component of the identity in $\mathcal{J}_{\mathbf{F}_p}$. Since $\mathcal{V}$ is annihilated by $\mathfrak{p}$, it follows from [10], Theorem 3.11 that $\mathfrak{p}$ is p-old.

Suppose, conversely, that $\mathfrak{p}$ is p-old. Then $A[\mathfrak{p}]$ is non-zero. Since $A[\mathfrak{p}]$ isomorphic to a direct sum of copies of the representation $\rho_{\mathfrak{p}}$, we may choose a two-dimensional $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-stable submodule V of $A[\mathfrak{p}]$ which is a model for the representation $\rho_{\mathfrak{p}}$. To show that $\rho_{\mathfrak{p}}$ is finite, we must produce a finite flat $\mathbf{T}/\mathfrak{p}$-vector space scheme $\mathcal{V}$ over $\mathbf{Z}_p$ such that $\mathcal{V}(\overline{\mathbf{Q}}_p)$ and V are isomorphic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. (We identify this latter Galois group with a decomposition group for p in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.) One has inclusions of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-modules $V \subseteq A[\mathfrak{p}] \subseteq A[p]$, and the latter group extends to a finite flat group scheme $\mathcal{S}$ of type $(p, \ldots, p)$ over $\mathbf{Z}_p$ because A has good reduction at p. Hence V extends to a finite flat group scheme $\mathcal{V}$ of this type: the Zariski closure of V in $\mathcal{S}$. Because $p > 2$, the action of $\mathbf{T}/\mathfrak{p}$ on V extends uniquely to $\mathcal{V}$ in view of Raynaud [6], 3.3.6. This completes the proof of Proposition 1.

Consider the subring R of $\mathbf{T}_N$ which is generated by all T_n with n prime to p. For each maximal ideal $\mathfrak{m}$ of R, we denote by $\rho_{\mathfrak{m}}$ the semisimple two-dimensional representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $R/\mathfrak{m}$ which is characterized by the property analogous to that given above for the $\rho_{\mathfrak{p}}$.

Proposition 2. *The index of R in $\mathbf{T}_N$ is finite and prime to p.*

To prove the Proposition, we can (and shall) assume that $N \geq 11$, since otherwise $\mathbf{T}_N = 0$. This enables us to apply a result of N. Katz [3] concerning the operator $\theta = q\frac{d}{dq}$ on weight-k mod p modular forms, for which the assumption $N \geq 3$ is made. The result proved by Katz had been proved by Serre and Swinnerton-Dyer (see [11], [14]) in the case $N = 1$.

Let S be the space of weight-2 cusp forms on $\Gamma_o(N)$ with coefficients in $\mathbf{F}_p$. For each $f \in S$, let $\sum_{n\geq 1} a_n(f)q^n \in \mathbf{F}_p[[q]]$ be the q-expansion of f. As is well known (cf. [7], §2), an argument due to Shimura ([13], Chapter 3) shows that the pairing

$$\mathbf{T}_N/p\mathbf{T}_N \times S \longrightarrow \mathbf{F}_p, \qquad (T, f) \mapsto a_1(f|T)$$

is perfect. Let $\mathcal{A}$ be the subring of $\mathbf{T}_N/p\mathbf{T}_N$ generated by the T_n with n prime to p. Suppose that f is orthogonal to $\mathcal{A}$ in the sense that $a_1(f|T_n) = 0$ for all n prime to p. Since $a_1(f|T_n) = a_n(f)$, the power series $\sum_{n\geq 1} a_n(f)q^n$ is then annihilated by θ. By the theorem of Katz, the sum $\sum_{n\geq 1} a_n(f)q^n$ vanishes. (The point is that $\sum_{n\geq 1} a_n(f)q^n$,

viewed as the mod p modular form f, otherwise has filtration $w(f) = 2$. Since 2 is prime to p, the filtration of θf is then $2 + p + 1$. This contradicts the vanishing of θf.) The subspace of S orthogonal to $\mathcal{A}$ is then 0, which proves that $\mathcal{A} = \mathbf{T}_N/p\mathbf{T}_N$. The Proposition now follows immediately, since $\mathbf{T}_N$ is free of finite rank over $\mathbf{Z}$, and since $\mathcal{A}$ is the image of R in $\mathbf{T}_N/p\mathbf{T}_N$.

Corollary. *Let $\mathfrak{p}$ be a maximal ideal of $\mathbf{T}_N$ of residue characteristic p. Let $\mathfrak{m} = R \cap \mathfrak{p}$. Then the natural inclusion $R/\mathfrak{m} \hookrightarrow \mathbf{T}_N/\mathfrak{p}$ is an isomorphism, and we have $J_o(N)[\mathfrak{p}] = J_o(N)[\mathfrak{m}]$.*

The first statement is an immediate consequence of the Proposition, since the index of $R/\mathfrak{m}$ in $\mathbf{T}_N/\mathfrak{p}$ is simultaneously a power of p and a divisor of the index $i = (\mathbf{T}_N : R)$ of R in $\mathbf{T}_N$. For the second, we must show that a point x of $J_o(N)$ which is annihilated by $\mathfrak{m}$ is automatically annihilated by $\mathfrak{p}$. Let λ be an element of $\mathfrak{p}$. Then $i\lambda \in \mathfrak{m}$. Hence x in annihilated by $i\lambda$, and it is also annihilated by $p\lambda$, since $p \in \mathfrak{m}$. Thus x is annihilated by λ, since $(i, p) = 1$.

Proposition 3. *Let $\mathfrak{m}$ be a maximal ideal of R of residue characteristic p. Suppose that the associated representation $\rho_{\mathfrak{m}}$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is irreducible. Then $J_o(N)[\mathfrak{m}]$ has dimension two over $R/\mathfrak{m}$.*

By a theorem of Cohen-Seidenberg, we may find a maximal ideal $\mathfrak{p}$ of $\mathbf{T}_N$ such that $\mathfrak{m} = \mathfrak{p} \cap R$. The Proposition follows from the above Corollary, together with the fact that $J_o(N)[\mathfrak{p}]$ has dimension two over $\mathbf{T}_N/\mathfrak{p}$ ([10], Theorem 5.2b).

Remark: Proposition 2 becomes false if we allow the case $p = 2$. Indeed, if $N = 23$, then $\mathbf{T}_N$ is isomorphic to the ring of integers of the quadratic field $\mathbf{Q}(\sqrt{5})$. Let R be the subring of $\mathbf{T}_N$ which is generated by the T_n with n odd. Then the index of R in $\mathbf{T}_N$ is divisible by 2. For more details concerning this example, see [2], §4. (The author wishes to thank G. Shimura for pointing out this example to him some years ago.)

Recall now that the subring of $\mathbf{T}_A$ generated by the Hecke operators T_n with n prime to p may be identified with the ring $R \subseteq \mathbf{T}_N$ which appears above. Indeed, $\mathbf{T}_N$ is a subring of the ring of endomorphisms of $J_o(N)$, which acts diagonally on the product

$J_o(N)^2 = J_o(N) \times J_o(N)$. This gives a natural action of $\mathbf{T}_N$ on $J_o(N)^2$. This action preserves the finite subgroup Σ of $J_o(N)^2$, and so descends to a faithful action of $\mathbf{T}_N$ on the quotient A. If n is prime to p, the operator T_n of $\mathbf{T}_N$ induces the operator labeled T_n in $\mathbf{T}_A$. Hence the subring R of $\mathbf{T}_N$ generated by such T_n maps isomorphically onto the indicated subring of $\mathbf{T}_A$. Note, however, that the p^{th} Hecke operator in $\mathbf{T}_N$ maps to an endomorphism of A which is not necessarily an element of $\mathbf{T}_A$. Let τ denote this element of $\mathbf{T}_N$. Then, with our conventions, the operator $T_p \in \mathbf{T}_A$ is induced by the endomorphism $(x, y) \mapsto (\tau x + py, -x)$ of $J_o(N)^2$, which we regard as the matrix $\begin{pmatrix} \tau & p \\ -1 & 0 \end{pmatrix}$ of endomorphisms of $J_o(N)$.

Theorem 3. *Let $\mathfrak{p}$ be a maximal ideal of $\mathbf{T}$ with residue characteristic p. Assume that $\rho_{\mathfrak{p}}$ is irreducible, and that $A[\mathfrak{p}]$ is non-zero. Then $A[\mathfrak{p}]$ is of dimension two over $\mathbf{T}/\mathfrak{m}$.*

Since $A[\mathfrak{p}]$ is non-zero, the maximal ideal $\mathfrak{p}$ is p-old. By abuse of notation, we consider that $\mathfrak{p}$ is a maximal ideal of $\mathbf{T}_A$. Set $\mathfrak{m} = R \cap \mathfrak{p}$. Considering first the action of R on $J_o(N)$, we find that $J_o(N)[\mathfrak{m}]$ has dimension two over $R/\mathfrak{m}$ (Proposition 3). The kernel Σ of the quotient map $J_o(N)^2 \to A$ is Eisenstein [9], and therefore prime to $\mathfrak{m}$ (cf. [10], Theorem 5.2c). Therefore, $A[\mathfrak{m}]$ may be identified with $J_o(N)[\mathfrak{m}]^2$, and in particular has dimension four over $R/\mathfrak{m}$.

We have $\mathbf{T}_A/\mathfrak{p} \supseteq R/\mathfrak{m}$ and $A[\mathfrak{m}] \supseteq A[\mathfrak{p}]$. Also, the dimension of $A[\mathfrak{p}]$ over $\mathbf{T}_A/\mathfrak{p}$ is a multiple of 2. Hence, this dimension is either 2 or 4, with the latter case occurring if and only if we have both $A[\mathfrak{p}] = A[\mathfrak{m}]$ and $\mathbf{T}_A/\mathfrak{p} = R/\mathfrak{m}$. However, if these equalities are satisfied, then $T_p \in \mathbf{T}_A$ operates on $J_o(N)[\mathfrak{m}]^2$ as a scalar, i.e., as an element of $R/\mathfrak{m}$. This is impossible, since the operation of T_p is given by the matrix $\begin{pmatrix} \tau & 0 \\ -1 & 0 \end{pmatrix}$, which is clearly not a scalar because of the -1 in the lower-left corner. (The element τ of $\mathbf{T}_N$ is not in R; however τ preserves $J_o(N)[\mathfrak{m}]$ and acts on $J_o(N)[\mathfrak{m}]$ as a scalar, in view of the corollary to Proposition 2.) The Theorem is therefore proved.

Remark: The example of level 23 mentioned above shows that Theorem 3 becomes false if the prime $p = 2$ is not excluded. Indeed, suppose that $p = 2$ and that $N = 23$. Let A again be the p-old subvariety of $J_o(pN) = J_o(46)$. The group $A[2]$ is naturally isomorphic to $J_o(23)[2] \oplus J_o(23)[2]$, since the kernel of the degeneracy map d has order $11 = \text{num}\left(\frac{22}{12}\right)$,

which is prime to 2. For n odd, the action of T_n on $A[2]$ is the diagonal action of T_n coming from the action of $\mathbf{T}_{23}/2\mathbf{T}_{23}$ on $J_o(23)[2]$. The ring $\mathbf{T}_{23}/2\mathbf{T}_{23}$ is the field with 4 elements, because 2 remains prime in $\mathbf{Q}(\sqrt{5})$. The T_n with n odd map to elements of the prime field $\mathbf{F}_2$, since they lie in the order of $\mathbf{T}_{23}$ having index 2 in $\mathbf{T}_{23}$. The element T_2 of $\mathbf{T}_{46}$ induces on $J_o(23)[2] \oplus J_o(23)[2]$ the map $(x, y) \mapsto (\tau x, -x)$, where τ is the automorphism of $J_o(23)[2]$ coming from the Hecke operator T_2 of $\mathbf{T}_{23}$. It follows that all $T_n \in \mathbf{T}_{46}$ act as elements of $\mathbf{F}_2$ on $0 \oplus J_o(23)[2]$, with T_2 acting as 0. If $\mathfrak{p} \subseteq \mathbf{T}_{46}$ is the kernel of the map $\mathbf{T}_{46} \to \mathbf{F}_2$ representing this action, then $A[\mathfrak{p}]$ contains $0 \oplus J_o(23)[2]$, and therefore has dimension ≥ 4 over $\mathbf{T}_{46}/\mathfrak{p} = \mathbf{F}_2$. The associated 2-dimensional representation $\rho_{\mathfrak{p}}$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is irreducible as follows from [4], Chapter II, Proposition 14.1. This representation is an $\mathbf{F}_2$-model for $J_o(23)[2]$, considered as a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\mathbf{F}_4$.

3. Study of $B[\mathfrak{p}]$.

In this §, N is again a positive integer, and p a prime which is prime to N. We do not make the assumption $p > 2$. The p-old and p-new subvarieties of $J = J_o(Np)$ are again denoted A and B, respectively. Their intersection is a finite subgroup Δ of J. Consider a maximal ideal $\mathfrak{p}$ of $\mathbf{T} = \mathbf{T}_{Np}$ for which $\rho_{\mathfrak{p}}$ is irreducible. (We do not assume that the residue characteristic of $\mathfrak{p}$ is p.)

Theorem 4. *If $B[\mathfrak{p}] \neq 0$, then $B[\mathfrak{p}] = J[\mathfrak{p}]$.*

We have an exact sequence

$$0 \to \Delta \to A \times B \to J \to 0,$$

where Δ is embedded "diagonally" in $A \times B$, and where this product is mapped to J by $(x, y) \mapsto x - y$. View $J[\mathfrak{p}]$ as the group $\mathcal{R}/\Delta$, where

$$\mathcal{R} = \{\, (x, y) \in A(\overline{\mathbf{Q}}) \times B(\overline{\mathbf{Q}}) \mid (\lambda x, \lambda y) \in \Delta \text{ for all } \lambda \in \mathfrak{p} \,\}.$$

Let $\pi\colon \mathcal{R} \to A$ be the projection $(x, y) \mapsto x$. We may identify $\ker \pi$ with $B[\mathfrak{p}]$. Further, since $\mathcal{R}$ contains the diagonal image of Δ, the image $\pi(\mathcal{R})$ of π contains Δ, regarded

as a subgroup of A. From this perspective, it is clear that the theorem amounts to the statement that $\pi(\mathcal{R})$ coincides with Δ in A.

Let $I \subseteq \mathbf{T}$ be the annihilator of B in $\mathbf{T}$, i.e., the kernel of the natural map $\mathbf{T} \to \operatorname{End} B$. The hypothesis $B[\mathfrak{p}] \neq 0$ is equivalent to the statement that $\mathfrak{p}$ contains I. For $\lambda \in I$ and $(x, y) \in \mathcal{R}$, we then have $\lambda x = 0$, since $(\lambda x, \lambda y)$ is necessarily the 0-element of Δ. In other words, we have $\Delta \subseteq \pi(\mathcal{R}) \subseteq A[I]$. To conclude the proof, we will show that the quotient $A[I]/\Delta$ involves only "Eisenstein primes" of $\mathbf{T}$. This gives the desired equality $\Delta = \pi(\mathcal{R})$, since $\pi(\mathcal{R})/\Delta$ is killed by $\mathfrak{p}$ and since $\rho_{\mathfrak{p}}$ is irreducible.

Consider the element $\gamma := T_p^2 - 1$ of $\mathbf{T}$. By (3.7) and (3.10) of [10], T_p coincides with the negative of the Atkin-Lehner involution on B. Therefore, $\gamma = 0$ on B, so that $\gamma \in I$. Accordingly, we have $A[I] \subseteq A[\gamma]$. Let τ again denote the p^{th} Hecke operator on $J_o(N)$. Since the restriction to A of T_p is induced by the endomorphism $\begin{pmatrix} \tau & p \\ -1 & 0 \end{pmatrix}$ of $J_o(N)^2$, γ restricts to the endomorphism of A induced by the product $\begin{pmatrix} -1 & \tau \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1+p & \tau \\ \tau & 1+p \end{pmatrix}$. Abusing notation, we will again refer to this product as γ.

The main theorem of [8] relates Δ to the kernel Ω of $\begin{pmatrix} 1+p & \tau \\ \tau & 1+p \end{pmatrix}$ on $J_o(N)^2$. Firstly, Ω contains the kernel Σ of the quotient $J_o(N)^2 \to A$. Secondly, we have $\Delta = \tilde{\Delta}/\Sigma$, where $\tilde{\Delta}$ is a subgroup of Ω such that the quotient $\Sigma^* := \Omega/\tilde{\Delta}$ is naturally dual to Σ. Both groups Σ and Σ^* are Eisenstein in the sense that the relation $T_l = 1 + l$ holds on each of them, for all primes l prime to pN. The group Ω is also the kernel of γ on $J_o(N)^2$, since $\begin{pmatrix} -1 & \tau \\ 0 & -1 \end{pmatrix}$ is visibly an automorphism of $J_o(N)^2$.

We claim that $Q := A[\gamma]/\Delta$ is an extension of Σ by Σ^*. To see this, apply the Snake Lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \to & \Sigma & \to & J_o(N)^2 & \to & A & \to & 0 \\ & & \uparrow 0 & & \uparrow \gamma & & \uparrow \gamma & & \\ 0 & \to & \Sigma & \to & J_o(N)^2 & \to & A & \to & 0 \end{array}$$

to obtain a 4-term exact sequence $0 \to \Sigma \to \Omega \to A[\gamma] \to \Sigma \to 0$. Equivalently, this gives a 3-term exact sequence $0 \to \Omega/\Sigma \to A[\gamma] \to \Sigma \to 0$. Then Q maps to $\Sigma = A[\gamma]/(\Omega/\Sigma)$ with kernel $(\Omega/\Sigma)/(\tilde{\Delta}/\Sigma)$. The latter group is $\Omega/\tilde{\Delta} = \Sigma^*$.

The claim implies that the support of Q contains only primes which divide the ideal generated by all $T_l - (1 + l)$. It follows that $\mathfrak{p}$ is not in the support of Q, cf. [10], 5.2c. A

fortiori, $\mathfrak{p}$ is not in the support of $A[I]/\Delta$. As noted above, this proves that $\pi(\mathcal{R}) = \Delta$, and concludes the proof of the Theorem.

References.

1. N. Boston, H. W. Lenstra, Jr., K. A. Ribet, *Quotients of group rings arising from two-dimensional representations*, CRAS (Paris). To appear.
2. K. Doi, H. Naganuma, *On the jacobian varieties of the fields of elliptic functions II*, J. Math. Kyoto Univ. **6** (1967), 177–185.
3. N. M. Katz, *A result on modular forms in characteristic p*, Lecture Notes in Math. **601** (1977), 53–61.
4. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977) 33–186.
5. B. Mazur, K. A. Ribet, *Two-dimensional representations in the arithmetic of modular curves*, Astérisque. To appear.
6. M. Raynaud, *Schémas en groupes de type* $(p, ..., p)$, Bull SMF **102** (1974) 241–280.
7. K. A. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), 193–205.
8. K. A. Ribet, *Congruence relations between modular forms*, Proc. Int. Cong. of Mathematicians (1983) 503–514.
9. K. A. Ribet, *On the Component Groups and the Shimura Subgroup of* $J_o(N)$, Sém. Th. Nombres, Université Bordeaux (1987–88) exposé 6.
10. K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990) 431–476.
11 J-P. Serre, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]*, Sém. Bourbaki n° 416 (1971/72), Lecture Notes in Math. **317** (1973), 319–338.
12. J-P. Serre, *Sur les représentations modulaires de degré 2 de Gal*$(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987) 179–230.
13. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton 1971.
14. H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for modular forms*, Lecture Notes in Math. **350** (1973), 1–55.