Experimental Indications of Three-dimensional Galois Representations from the Cohomology of SL(3, Z)

Avner Ash and Mark McConnell

CONTENTS

Conjecturally, any "algebraic" automorphic representation on $\mathrm{GL}(n)$ should have an n-dimensional Galois representation attached. Many examples of algebraic automorphic representations come from the cohomology over $\mathbf{C}$ of congruence subgroups of $\mathrm{GL}(n,\mathbf{Z})$. On the other hand, the first author has conjectured that for any Hecke eigenclass in the mod p cohomology of a congruence subgroup of $\mathrm{GL}(n,\mathbf{Z})$ there should be an attached n-dimensional Galois representation.

By computer, we found Hecke eigenclasses in the mod p cohomology of certain congruence subgroups of $\mathrm{SL}(3,\mathbf{Z})$. In a range of examples, we then found a Galois representation (uniquely determined up to isomorphism by our data) that seemed to be attached to the Hecke eigenclass.

INTRODUCTION

The method of attaching Galois representations to holomorphic modular forms for $\mathrm{GL}(2)$ has provided many examples of two-dimensional representations of the absolute Galois group of $\mathbf{Q}$. The idea has been expanded to become part of the Langlands philosophy, so that, conjecturally, any "algebraic" automorphic representation on $\mathrm{GL}(n)$ should have an n-dimensional Galois representation attached.

Many examples of automorphic representations come from the cohomology over $\mathbf{C}$ of congruence subgroups $\Gamma \subseteq \mathrm{SL}(n,\mathbf{Z})$. On the other hand, the first author has made conjectures about the mod p cohomology that parallel the ones for complex cohomology. In particular, Conjecture 1 in Section 1 would attach a three-dimensional Galois representation to any Hecke eigenclass in the mod p cohomology of a congruence subgroup of $\mathrm{SL}(3,\mathbf{Z})$. For further discussion of these conjectures and of

Ash's research was partially supported by NSF Grant DMS-8919696.

1058-6458/92 $0.50 per page

their relationship, with references to the history, see [Ash 1992a,b] and [Ash et al. 1991].

In the summer of 1991, we wrote and ran computer programs to find Hecke eigenclasses in the mod p cohomology of certain congruence subgroups of $\mathrm{SL}(3, \mathbf{Z})$. We then chose a variety of examples, of different degrees of difficulty, for which the search for the attached three-dimensional Galois representation seemed feasible. In each example, we did find a Galois representation (uniquely determined up to isomorphism by our data) that seemed to be attached to the Hecke eigenclass. We say "seemed" because all we could do was check the conjecture at a finite number of primes l and at infinity. (We computed Hecke eigenvalues for T_l, $l \leq 97$.) All the cases we could handle involved reducible Galois representations. Nevertheless, they provide striking evidence for the conjecture, since the cohomology classes they are based on are in no obvious way "reducible" to GL(2)-classes.

Two desiderata remain. First, in any example, we would like to prove that the Galois representation we found is really attached; that is, we would like to verify the conjecture for all l. Secondly, when $p = 3$, 7, 17 or 23, our data predict Galois representations whose image is the full group $\mathrm{SL}(3, \mathbf{Z}/p)$. We would like to find these representations with large nonsolvable image.

Serre's conjecture [Serre 1987] would give an approach to the first problem in the reducible case, where the Galois representation has an odd two-dimensional component. The modular form predicted by Serre's conjecture could be found, and the appropriate relations could be proved between its Fourier coefficients mod p and the Hecke eigenvalues of the GL(3)-cohomology class in question. Alternatively, one might be able to prove a congruence mod p between our given class and an Eisenstein cohomology class. We have few approaches to suggest for the second problem, of finding representations with image $\mathrm{SL}(3, \mathbf{Z}/p)$.

In Section 1, we recall the mod p conjecture in the form in which we tested it by computer, and we discuss its significance. In Section 2, we discuss the algorithms we used to compute the mod p cohomology of congruence subgroups of $\mathrm{SL}(3, \mathbf{Z})$ as a Hecke module. In Section 3, we summarize the output of our programs and discuss the reliability of our computations. In Section 4, we explain how we found the attached Galois representations (when we could). We summarize our results in tables throughout the paper.

In 1986, Philip Green (unpublished) computed the mod p cohomology of certain congruence subgroups of $\mathrm{SL}(3, \mathbf{Z})$ (without the Hecke action) on an IBM PC. These computations assured us that we would obtain interesting results, and we thank him for sharing his data with us. We will discuss his work in more detail in Section 3. We thank Nicole Schulte for sharing tables of quartic and cubic number fields. We also thank B. Gross, B. Mazur, J.-P. Serre and D. Wright for helpful comments and suggestions.

1. REVIEW OF THE CONJECTURE

We state all definitions and conjectures in terms adapted to this paper. For the statements in the case of general congruence subgroups of $\mathrm{GL}(n)$ for any $n \geq 2$ and for general coefficients, see [Ash 1992a,b].

We start with a brief review of the definition of the Hecke algebra and its action on cohomology classes. A *Hecke pair* is a pair (Γ, S), where Γ is a subgroup of $\mathrm{SL}(3, \mathbf{Z})$ and $S \supset \Gamma$ is a subsemigroup of $\mathrm{GL}(3, \mathbf{Q})^+$. The Hecke algebra of integral linear combinations of double cosets $\Gamma s \Gamma$, for $s \in S$, will be denoted $H(\Gamma, S)$, or just H if no confusion is likely. We shall use the notation T_s for the double coset $\Gamma s \Gamma$ in $H(\Gamma, S)$.

For example, if N is an integer, let $S_0(N;3)$ be the set of $\gamma \in \mathrm{GL}(3, \mathbf{Q})^+ \cap M(3, \mathbf{Z})$ whose top row is of the form $(*, 0, 0) \pmod N$ and which satisfy $(\det \gamma, N) = 1$. Let $\Gamma_0(N;3) = S_0(N;3) \cap \mathrm{SL}(3, \mathbf{Z})$. Then $H(\Gamma_0(N;3), S_0(N;3))$ is a Hecke algebra; we call it $H(N)$ for short.

Now we define the action of $H(\Gamma, S)$ on cohomology with trivial coefficients A. For any $s \in S$, set $\Gamma(s) = s^{-1}\Gamma s \cap \Gamma$. We have two morphisms i, j of $\Gamma(s)$ into Γ, given by $i(x) = x$ and $j(x) = sxs^{-1}$. For each $\beta \in H^*(\Gamma, A)$, define

$$T_s(\beta) = i_* j^*(\beta),$$

where i_* is the transfer with respect to i and j^* is the pullback with respect to j.

Recall that $H(N)$ is a polynomial ring over $\mathbf{Z}$ generated by the elements

$$T(l, k) = \Gamma_0(N, 3)\, \mathrm{diag}(1, \ldots, 1, \underbrace{l, \ldots, l}_{k \text{ times}}) \Gamma_0(N, 3),$$

where $k = 1, 2, 3$ and l runs over all primes not dividing N. We set $T(l, 0) = 1$ for all l.

Suppose $\alpha \neq 0$ and $T(l, k)\alpha = a(l, k)\alpha$ for all k. Then the Hecke polynomial attached to α at l is defined to be

$$P(\alpha, l) = \sum_{k=0}^{3} (-1)^k l^{k(k-1)/2} a(l, k) X^k.$$

For each l unramified in an extension E of $\mathbf{Q}$, we write Frob_l for the geometric Frobenius element in the Galois group of $E/\mathbf{Q}$ (defined up to conjugacy). Thus Frob_l^{-1} acts on the residue field of a prime above l by raising to the l-th power. Also, let c be the complex conjugation element in $\mathrm{Gal}(E/\mathbf{Q})$ (defined up to conjugacy).

Let $G_{\mathbf{Q}}$ denote $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Take $N \geq 1$. We have the following conjecture:

Conjecture 1. *Let $(\Gamma, S) = (\Gamma_0(N; 3), S_0(N; 3))$. Let p be a prime and $\mathbf{F}$ a finite field of characteristic p. Suppose $\beta \in H^i(\Gamma, \mathbf{F})$ is an eigenclass for the action of the Hecke algebra $H(N)$, with eigenvalues $a(l, k)$ in $\mathbf{F}$. Then there exists a semisimple continuous representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(3, \mathbf{F})$, unramified outside pN, such that*

$$\det(I - \rho(\mathrm{Frob}_l)^{-1} X) = P(\beta, l)$$

for all primes l not dividing pN. Furthermore, $\rho(c)$ has eigenvalues 1, 1 and -1.

We refer to [Ash 1992b] for discussion of the conjecture and of some cases in which it can be proved. In particular, theorems of Eichler and Shimura [Shimura 1971, Theorem 7.11] and of Deligne [1971] show that the analogous conjecture for GL(2) holds true. Conversely, Serre [1987] conjectured that all odd irreducible representations of $G_{\mathbf{Q}}$ into $\mathrm{GL}(2, \mathbf{F})$ arise this way.

The purpose of this paper is to investigate Conjecture 1 when the level N is prime.

2. ALGORITHMS

For this whole section, we refer to [Ash et al. 1984] for background. Let $\Gamma = \Gamma_0(N; 3)$ and $H = H(N)$ for some prime level N. Let X be the symmetric space for $\mathrm{SL}(3, \mathbf{R})$, where Γ acts on X on the right. Let A be a trivial coefficient module for Γ. Rather than compute $H^i(\Gamma, A)$, we will compute $H_i(X/\Gamma, A)$. We view all homology and cohomology groups (with their Hecke structure) as AH-modules.

Remark. $H_i(X/\Gamma, A)$ and $H_i(\Gamma, A)$ are isomorphic except in characteristics 2 and 3. In those characteristics, the equivariant homology spectral sequence relates the two, and the classes we compute below in $H_i(X/\Gamma, A)$ actually live also in $H_i(\Gamma, A)$. We don't verify this claim here, since our position is that any Hecke eigenclass, whether in $H_i(X/\Gamma, A)$ or in $H_i(\Gamma, A)$, should have a Galois representation attached.

The homology for $i = 3$, together with the homology of the Borel–Serre boundary of X/Γ, determines all the homology groups as AH-modules. Therefore we concentrate on finding $H_3(X/\Gamma, A)$.

If $A = \mathbf{F}$ is a field, $H_3(X/\Gamma, \mathbf{F})$ and $H^3(X/\Gamma, \mathbf{F})$ are dual to each other as $\mathbf{F}H$-modules, so Conjecture 1 applies as well to $H_3(X/\Gamma, \mathbf{F})$. In fact, we will be testing the conjecture using H_3 rather than H^3. What is more, by the universal coefficient theorem, we are at the same time testing the analogous conjecture for p-torsion classes in the integral homology and cohomology. For instance, $H_3(X/\Gamma, \mathbf{Z})$ is torsion-free, but the cokernel of $H_3(X/\Gamma, \mathbf{Z}) \otimes \mathbf{F} \to H_3(X/\Gamma, \mathbf{F})$ is isomorphic to the torsion in $H_2(X/\Gamma, \mathbf{Z})$.

From [Ash et al. 1984, § 3], we recall the following method of computing $H_3(\Gamma, A)$ for any prime level N and trivial coefficient module A. Although the result is stated there for complex coefficients, it works just as well for any A.

Let $W(N, A)$ denote the A-module of functions $f : (\mathbf{Z}/N)^3 \to A$ that satisfy

$$\begin{aligned} &f(x, y, z) = f(ax, ay, az) \quad \text{for } a \neq 0 \text{ in } \mathbf{Z}/N; \\ &f(x, y, z) = -f(-y, x, z); \\ &f(x, y, z) = f(y, z, x); \\ &f(x, y, z) + f(-y, x - y, z) + f(y - x, -x, z) = 0. \end{aligned} \tag{2.1}$$

The module $W(N, A)$ is isomorphic to $H_3(X/\Gamma, A)$. The Hecke action can be computed using the Ash–Rudolph algorithm for GL(3)-modular symbols, exactly as explained in [Ash et al. 1984, §§ 4, 6(B)].

Solving the set of linear equations (2.1) for the unknowns $f(x, y, z)$ is easy using standard Gaussian elimination, once the equations are set up. Let

$G_1 \subset GL(3, \mathbf{Z}/N)$ be generated by the scalars,

$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

G_1 acts on $(\mathbf{Z}/N)^3$, and the first three equalities in (2.1) are relations holding within each G_1-orbit separately. We use those three equalities to reduce the number of unknowns to one for each G_1-orbit, and we construct a conversion table correlating the representative of each orbit with any given (x, y, z), keeping track of the sign in the second equality. We then set up the last equality as a system in these unknowns and solve by row reduction.

Although the system is initially sparse, we didn't use special sparse matrix methods. (If we wished to extend the range of N, these methods might become useful.) Since we are working with $A = \mathbf{Z}/p$, we used exact integers and didn't have to worry about numerical stability.

This part of the calculation is relatively quick, even for $N \approx 200$, and even though we have approximately $\frac{1}{24}N^2$ unknowns and $\frac{1}{12}N^2$ equations. The bulk of the time is taken later, in the calculation of the Hecke operators on the homology.

The sketch just given differs from our actual procedure in one way. Before solving the initial system, we added some equations (2.2) designed to remove a portion of the solution space whose Hecke eigenvalues we knew to be uninteresting. Then, before computing the Hecke operators, we changed bases in the solution space so that the matrix representation of the Hecke operators would be block upper triangular, with the first block consisting again of uninteresting eigenvalues. In the rest of this section we explain this in more detail.

We denote by Y the Borel–Serre compactification of X/Γ, and by B the boundary of Y. We let $W^*(N, A)$ be the image of $H_3(B, A)$ in $H_3(Y, A)$, viewed as a submodule of $W(N, A)$. A description of $W^*(N, A)$ is given in [Ash et al. 1984, Theorem 3.19] in the case $A = \mathbf{C}$, and it works as well for $A = \mathbf{Z}/p$ unless $N - 1$ is a multiple of p. A simple modification of that theorem and its proof[1] leads to the following construction.

Let $V(N)$ denote the $\mathbf{Z}$-module of functions $\Phi : (\mathbf{Z}/N)^2 \to \mathbf{Z}$ that satisfy

$$\begin{aligned} &\Phi(x, y) = \Phi(ax, ay) \qquad \text{for } a \neq 0 \text{ in } \mathbf{Z}/N; \\ &\Phi(1, 0) = 0; \\ &\Phi(x, y) = \Phi(-x, y); \\ &\Phi(x, y) = -\Phi(y, x); \\ &\Phi(x, y) + \Phi(-y, x - y) + \Phi(y - x, -x) = 0. \end{aligned}$$

Given Φ in $V(N)$, we define $\alpha\Phi \in W(N, \mathbf{Z}/p)$ and $\beta\Phi \in W(N, \mathbf{Z}/p)$ as follows. Let D denote the greatest common divisor of the elements $\Phi(x, y) + \Phi(y, z) + \Phi(z, x)$, where x, y, z range over $\mathbf{Z}/N$, with $xyz \neq 0$. (It can be shown that $D = 1$ whenever $N - 1$ is prime to p.) If $xyz \neq 0$, we set $\alpha\Phi(x, y, z)$ equal to the reduction modulo p of

$$(\Phi(x, y) + \Phi(y, z) + \Phi(z, x))/D;$$

if not, we set $\alpha\Phi(x, y, z) = 0$. We define $\beta\Phi$ by

$$\begin{aligned} &\beta\Phi(x, y, z) = 0 \qquad \text{if } xyz \neq 0; \\ &\beta\Phi(0, y, z) = \Phi(y, z); \\ &\beta\Phi(x, y, 0) = \Phi(x, y); \\ &\beta\Phi(x, 0, z) = \Phi(z, x). \end{aligned}$$

Then $W^*(N, \mathbf{Z}/p)$ consists of the span of the images of α and β.

As explained in [Ash and Stevens 1986], $W^*(N, \mathbf{Z}/p)$ is a Hecke submodule of $W(N, \mathbf{Z}/p)$, and the Hecke eigenvalues can be written in terms of Hecke eigenvalues of classical holomorphic modular forms of weight 2 (corresponding to the Φ's). Since Conjecture 1 holds in the classical case, when $n = 2$, we conclude that it holds also for the eigenclasses in $W^*(N, \mathbf{Z}/p)$. Hence we call these eigenclasses uninteresting (for our present purposes).

We can construct a complement to the image of β in $W(N, \mathbf{Z}/p)$ by imposing on $W(N, \mathbf{Z}/p)$ the further conditions

$$f(x, y, z) = 0 \qquad \text{if } xyz = 0. \tag{2.2}$$

These are the extra equations alluded to above, the ones we use before beginning Gaussian elimination. They simply set some of our variables equal to 0. We take them into account in the programs by throwing out the corresponding variables, taking care when setting up the third set of equalities in (2.1) to replace by 0 any term of the form $f(x, y, z)$ if $xyz = 0$.

[1] We note here an error in the proof of Theorem 3.19 in [Ash et al. 1984]. On p. 422, f' should be defined by the same formula as f'' except with P_2 replaced by ${}^tP_2$. In the third paragraph on that page, $\nu(m)$ should equal 1, not 3. This error does not affect the result, which is correctly stated in the theorem.

We could try to construct a complement to the image of α as in [Ash et al. 1984], by requiring $\sum_z f(x,y,z) = 0$ for all x, y. However, these are $O(N^2)$ additional nonsparse equations, and they are not respected by the Hecke operators. It is far more efficient and "Hecke-equivariant" to deal with the image of α in the following way.

If $h(\xi, \eta, \zeta)$ is any function of three variables, let $\Delta_x h(\xi,\eta,\zeta) = h(\xi+1,\eta,\zeta) - h(\xi,\eta,\zeta)$. Define Δ_y, Δ_z similarly. After we solve equations (2.1)–(2.2), getting a basis for the solution space W', we impose the linear conditions $\Delta_x\Delta_y\Delta_z f(\xi,\eta,\zeta) = 0$ for some values of ξ, η, ζ. These conditions for all $1 \le \xi, \eta, \zeta \le \frac{1}{2}(N-1)$ cut out a linear subspace of f's that contains the image of α. In practice, for $N \le 251$, using these conditions just for all $1 \le \xi, \eta, \zeta \le 8$ gave a basis for exactly the image of α. (Because of the first condition, these are only 64 additional equations.) We then extended this to a basis for W' by randomly adjoining $\dim W' - \dim \operatorname{Im} \alpha$ elements from the previously found basis of W', testing for linear independence, and repeating as needed.

With respect to this new basis, we computed the Hecke operators $T(l,1)$ and $T(l,2)$ for $l \ne N$ in exactly the way explained in [Ash et al. 1984]. The matrix of $T(l,k)$ with respect to this new basis was in upper triangular block form, since we arranged α in such a way that $T(l,k)$ would preserve its image. By focussing on the interesting diagonal block, we got the matrix for $T(l,k)$ acting on the quotient space of W that has the interesting Hecke eigenvalues. We call this quotient space W^{qc}, for quasicuspidal. It is isomorphic as a Hecke module to the quotient W/W^*. (If our coefficients had been $\mathbf{C}$ as opposed to $\mathbf{Z}/p$, then W/W^* would have been dual to the cuspidal cohomology of Γ; hence our terminology.)

Our computer output consists of the Hecke matrices on a fixed basis of W^{qc}. The advantage of splitting off W^{qc} is that W^* is generally quite big, whereas W^{qc} is usually much smaller.

	p (characteristic)								
N	2	3	5	7	11	13	17	19	23
29	1								
37	1								
41	1								
43	1								
∗53	2	2	2	2	2	2	2	2	2
59	1								
∗61	2	2	2	2	2	2	2	2	2
67	2								
71	2								
73	2								
∗79	3	2	2	2	2	2	2	2	2
83	4								
∗89	3	2	2	2	2	2	2	2	2
97	3								
101	4								
103	2								
107	5								
109	6								
113	6								
127	5	2							
131	5								
137	7	2							
139	6								
149	10								
151	7	2							
157	6								2
163	8		2						
167	6			2					
173	9								
179	9								
181	9								
191	8						2		
193	11	6							
197	14		4						
199	8								
211	15	6	2						
∗223	12	2	2	2	2	2	2	2	2
227	13		4		–	–	–	–	–
229	15		2		–	–	–	–	–
233	15	10			–	–	–	–	–
239	11				–	–	–	–	–
241	13	4			–	–	–	–	–
251	??			2	–	–	–	–	–

TABLE 1. Dimension $D(N,p)$ of the quasicuspidal cohomology of $\Gamma_0(N)$ with coefficients in $\mathbf{F}_p$, for prime $N \le 251$ and $p \le 23$. Blank entries and omitted values of N indicate that $D(N,p) = 0$. A dash indicates that the calculation was not performed, and ?? indicates that the size of the kernel overran our program. The starred values of N are special: see next page. Results for $p = 37$ and $p = 691$ are the same as for $p = 11, 13, 19$.

3. COHOMOLOGY RESULTS. CONSISTENCY TESTS

Our results fall into two parts. First, we computed a basis for $W^{\mathrm{qc}}(N, \mathbf{Z}/p)$ for every prime $N \le 223$ and every $p \le 23$, and for a few larger pairs (N,p). Table 1 shows the dimension $d(N,p)$ of $W^{\mathrm{qc}}(N, \mathbf{Z}/p)$.

It is striking that $d(N, p)$ was always found to be even, except when $p = 2$. We have no explanation for this.

For $N = 53$, 61, 79 and 89, there exists a pair of linearly independent classes in $H^3_{\mathrm{cusp}}(\Gamma, \mathbf{C})$, by [Ash et al. 1984]. The same is almost certainly true for $N = 223$, as our data shows, although the computation for $N = 223$ with coefficients in $\mathbf{C}$ has not been performed.

We also computed $d(N, 37)$ and $d(N, 691)$ for $N \leq 223$. In these cases the result is 0, except for the five values of N in the previous paragraph, where it is 2.

The second type of computation is as follows. Whenever $d(N, p) \neq 0$, we computed the Hecke matrices with respect to our basis of $W^{\mathrm{qc}}(N, \mathbf{Z}/p)$, for the Hecke operators $T(l, 1)$ for all $l \leq 97$ and $T(l, 2)$ for all $l \leq 19$.

The Hecke operators $T(l, 2)$ for $19 < l \leq 97$ ($l \neq N$) can be deduced from these data as follows. The automorphism φ of GL(3) that sends g to the conjugate of ${}^t g^{-1}$ by $\mathrm{diag}(N, 1, 1)$ preserves Γ and switches $\mathrm{diag}(1, 1, l)$ with $\mathrm{diag}(1, l, l)$ modulo scalar matrices. Hence φ acts on the homology of Γ and intertwines $T(l, 1)$ and $T(l, 2)$. Therefore, the Hecke matrices for $T(l, 1)$ and $T(l, 2)$ have the same characteristic polynomial. Moreover, from the Hecke matrices for the first few l, we can in practice determine a simultaneous Hecke eigenbasis and then observe the relationship between $T(l, 1)$ and $T(l, 2)$—whether they are always equal, or at least have the same semisimplification, or are transposes of each other. In every case coming from our data, we can then determine $a(l, 2)$ from $a(l, 1)$ for all $l \leq 97$ ($l \neq N$).

In Section 4 we supply lists of the computed Hecke eigenvalues for the quasicuspidal classes we discuss.

Both parts of the computation were performed in Fortran on a Sun SPARCstation 2 and other Suns at the Ohio State University.

Here are some compelling reasons for believing the output of our computations:

- Every computation was in exact integer arithmetic or arithmetic mod p.
- Each algorithm was checked by hand on small examples.
- Each matrix whose nullspace we were computing had many more rows than columns. The fact that this nullspace was always nonzero is a very strong indication that the matrices were set up properly.
- The dimension of the nullspace was always at least $\dim \mathrm{Im}\, \alpha$, which is the genus of the modular curve $X_0(N) = g(N)$.
- The Hecke operators as computed always left the nullspace stable and acted on it in block diagonal form, with blocks of sizes $g(N)$ and $d(N, p) - g(N)$ with respect to the new basis, as described near the end of Section 2.
- Spot checking showed that the matrices of the Hecke operators acting on our new basis commuted with one another.
- $T(l, 1)$ and $T(l, 2)$ always had the same characteristic polynomial for $l \leq 19$.
- In all cases we attempted, we found Galois representations compatible with Conjecture 1 and the computed values of the Hecke eigenvalues (Section 4).
- Our tabulation of $d(N, p)$ agrees with the unpublished 1986 computations of Philip Green for all $p \leq 7$ and all $N \leq 223$, with the exception of $d(197, 5)$, which we computed to be 4 and Green reported to be 2. We believe Green made an error in the letter in which he communicated his results to us.

4. GALOIS REPRESENTATIONS

In this section we describe our efforts to find the Galois extensions of $\mathbf{Q}$ and the representations of the Galois groups predicted by Conjecture 1. After some preliminary comments, we discuss our results, grouping them by common values of the coefficient characteristic p; see Table 2 for a summary.

As before, let $\mathbf{F}$ be a finite field of characteristic p. Suppose we have a representation ρ as in Conjecture 1. Then $\det \rho(\mathrm{Frob}_l)^{-1} = l^3$ for each l outside pN. Let $\omega : G_{\mathbf{Q}} \to \mathbf{F}_p^\times$ be the reduction mod p of the cyclotomic character, which satisfies $\omega(\mathrm{Frob}_l^{-1}) = l$ for each l not dividing p. If we replace ρ with the twist $\rho' = \omega^{-1}\rho$, then ρ' takes values in $\mathrm{SL}(3, \mathbf{F})$. (Here we use a special feature of $n = 3$.) This change makes it slightly easier to discuss our results. Thus we can rephrase the conjecture in terms of this twist and the usual characteristic polynomial:

N	q	$\mathrm{Im}\,\rho'$	$f(x)$
characteristic $p=2$			
29	2	S	x^3+2x+4
37	2	S	x^3-4x+2
41	2	$\{1\}$	x
43	2	S	x^3+4x+4
53	2	S	x^3-x^2-4x+8
59	2	S	x^3+2x+1
61	2	S	x^3+x+6
67	4	A	$x^5+2x^3+4x^2+6x+4$
71	2	S	$x^3-10x-8$
73	4	A	$x^5+2x^3+4x^2-2x-4$
79	2	S	x^3-7x+2
83	2	S	x^3+8x+1
89	2	S	x^3-7x+8
97	8	$\subset \mathrm{SO}(3)$	
101	2	S	x^3-8x+4
101	8	$\subset \mathrm{SO}(3)$	
103	4	A	$x^5+x^4-4x^3-6x^2-2x+18$
149	2	S	$x^3+13x+50$
197	2	S	x^3-x^2-7x-3
223	2	S	$x^3-x^2-8x+10$

N	q	$\mathrm{Im}\,\rho'$	$f(x)$
characteristic $p=3$			
61	3	$\{1\}\times\mathrm{SL}(2)$	see [Ash et al. 1991]
79	3	$\{1\}\times\mathrm{SL}(2)$	see text
127	3	$\{1\}\times\mathrm{SL}(2)$	see text
137	3	$\mathrm{SL}(3)$	
151	9	$\subset \mathrm{SU}(3)$	
characteristic $p=5$			
163	5	$\subset \mathrm{GL}(1)\times\mathrm{GL}(2)$	
197	625		
211	5	C_4	$x^4+x^3+x^2+x+1$
characteristic $p=7$			
167	7	$\mathrm{SL}(3)$	
characteristic $p=17$			
191	17	$\mathrm{SL}(3)$	
characteristic $p=23$			
157	23	$\mathrm{SL}(3)$	

TABLE 2. Summary of the information obtained about Galois representations seemingly attached to quasicuspidal cohomology of arithmetic subgroups of $\mathrm{SL}(3,\mathbf{Z})$. Each row is devoted to a single Hecke eigenclass; p and N are as in Table 1, but certain combinations don't appear here because our Hecke operator programs ran into machine limitations. The column labeled q gives the number of elements in the field $\mathbf{F}$ generated over the prime field by the Hecke eigenvalues. The next column gives information about the image of ρ' (see Conjecture 1$'$). The image is predicted to be the whole listed group, unless it is prefixed by $\subset$. We use the abbreviations S for $O(3,\mathbf{F}_2)$, which is isomorphic to the symmetric group S_3, and A for $O(3,\mathbf{F}_4)$, which is isomorphic to the alternating group A_5. (Note that, in characteristic 2, the orthogonal groups are not irreducible.) C_4 denotes a subgroup of the diagonal matrices isomorphic to $\mathbf{F}_5^\times$. The last column gives a polynomial $f(x)$ whose splitting field is the fixed field of the kernel of ρ'.

Conjecture 1$'$. *Let*

$$(\Gamma, S) = (\Gamma_0(N;3), S_0(N;3)).$$

Let p be a prime and $\mathbf{F}$ a finite field of characteristic p. Suppose $\beta \in H^i(\Gamma,\mathbf{F})$ is an eigenclass for the action of the Hecke algebra $H(N)$, with eigenvalues $a_l = a(l,1)$ and $b_l = a(l,2)$ in $\mathbf{F}$. Then there exists a semisimple continuous representation $\rho' : G_{\mathbf{Q}} \to \mathrm{SL}(3,\mathbf{F})$, unramified outside pN, such that

$$\det(X-\rho'(\mathrm{Frob}_l)^{-1}) = X^3 - a_l l^{-1}X^2 + b_l l^{-1}X - 1 \tag{4.1}$$

for all primes l not dividing pN. Furthermore, $\rho'(c)$ has eigenvalues 1, -1 and -1.

The rest of this paper involves examples of ρ' for Conjecture 1$'$, with one exception: when $p=3$ and $N=127$, we do not twist ρ by the cyclotomic character, but instead work with Conjecture 1. The reason is that, in this case, twisting would obscure the fact that the field cut out by the two-dimensional component π of ρ (see discussion preceding (4.2)) is totally real.

Definition. If we have β and ρ' as in Conjecture 1$'$ such that condition (4.1) holds for every $l \le 97$ not dividing pN, we say that ρ' *seems to be attached to* β, or to the corresponding system of Hecke eigenvalues $\{a_l, b_l\}$. If (4.1) holds for all l not dividing pN, and if the statement about $\rho'(c)$ holds, we shall say ρ' *is attached to* β, or to the system of eigenvalues.

Suppose that ρ' is attached to β. If

$$X^3 - aX^2 + bX - 1$$

is the characteristic polynomial of a matrix g, then $X^3 - bX^2 + aX - 1$ is the characteristic polynomial of g^{-1}. Now suppose σ is either an involution of $\mathbf{F}$ or the identity map, and that $a_l = \sigma(b_l)$ for all l not dividing pN. It follows by the Tchebetarov density theorem and the Brauer–Nesbitt theorem that ρ' is equivalent to $\sigma({}^t\rho'^{-1})$; that is, for some invertible matrix M, we have $M\rho'(x) = \sigma({}^t\rho'(x^{-1}))M$ for every x in $G_{\mathbf{Q}}$. It follows that the nondegenerate sesquilinear form corresponding to M (bilinear if $\sigma = 1$) is preserved by $\operatorname{Im}\rho'$. The same is true for $\sigma({}^tM)$, and hence for $M + \sigma({}^tM)$. If this sum is nonzero, it is a nonzero symmetric sesquilinear form preserved by $\operatorname{Im}\rho'$; if the sum is 0, M itself is a nondegenerate antisymmetric sesquilinear form preserved by $\operatorname{Im}\rho'$. These statements still hold if $\operatorname{char}\mathbf{F} = 2$, but the notions of symmetry and antisymmetry coincide.

Thus, if $a_l = \sigma(b_l)$ for all l not dividing pN, either ρ' is reducible or its image lies in the corresponding unitary or orthogonal group. In the examples below, wherever we find a ρ' that seems to be attached to β, it will turn out that $a_l = \sigma(b_l)$ for some σ (for all the l for which we have data), and ρ' will be reducible. We shall comment on several examples where ρ' must be surjective (and hence irreducible) if it exists, but we do not know how to look for ρ' in those cases, because $\operatorname{Im}\rho'$ is then (conjecturally) a very large almost simple group.

If the package of Hecke eigenvalues for β were congruent mod p to another package coming from a cohomology class $\tilde\beta$ for a Γ of level $\tilde N$ (e.g., $\tilde N = Np^k$ for some k), and if $\tilde\beta$ were the reduction of a nontorsion class in the integral cohomology, then Conjecture 4.1 in [Clozel 1990], applied to the automorphic representation corresponding to $\tilde\beta$, would lead us to include the condition at infinity in Conjectures 1 and 1′ (see [Ash 1992a]). In all of the examples we have calculated, $\rho'(c)$ does possess the desired eigenvalues. The conjecture for $\rho'(c)$ has no content, of course, when $p = 2$; in these cases, sometimes c lies in the kernel of ρ' and sometimes it does not.

We now describe our computations in more detail.

Classes in Characteristic $p = 2$

Here we have many examples. We have looked at all systems of Hecke eigenvalues occurring for $N \le 103$, and we have done spot-checking for $N = 149$, 197 and 223, where we looked at all systems that lie in the prime field. In all these cases, $a_l = b_l$ for all l not dividing $2N$, so that we may take $\sigma = \mathrm{id}$. (We do not know whether this is a general rule when $p = 2$.) In all these cases, except $N = 97$ and one system for $N = 101$, the field generated by Hecke eigenvalues is $\mathbf{F}_2$ or $\mathbf{F}_4$, and we have found the Galois representation that seems to be attached to each system. When $N = 97$ or 101, the field generated by Hecke eigenvalues is $\mathbf{F}_8$, and we haven't attempted to find the Galois representation.

As explained above, since $a_l = b_l$, the image of the attached ρ' (if it exists) must stabilize a nontrivial symmetric bilinear form. But in characteristic 2, the stabilizer of any nontrivial symmetric bilinear form is reducible. (If the form is nondegenerate, this can be checked directly. Otherwise, $\operatorname{Im}\rho'$ is contained in a parabolic subgroup; since the representation is semisimple, the image must be contained in $\mathrm{GL}(1) \times \mathrm{GL}(2)$.)

We ask whether the Galois representations attached to Hecke eigenclasses in characteristic 2 are always reducible, or even whether a_l always equals b_l in these cases. Both conjectures are compatible with the data in this paper and in [Ash et al. 1984].

Hence we are looking for ρ' of the form $\pi \oplus \chi$, where π is two-dimensional and χ is a character. In all our examples, the data forces $\chi = 1$, so that π maps to the special linear group. We end up then searching for a semisimple, continuous representation $\pi : G_{\mathbf{Q}} \to \mathrm{SL}(2, \mathbf{F})$, unramified outside $2N$ and such that

$$\operatorname{Tr}\pi(\mathrm{Frob}_l)^{-1} = \frac{a_l}{l} - 1 \qquad \text{for } l \ne 2, N. \tag{4.2}$$

Now $\mathrm{SL}(2, \mathbf{F}_2)$ is isomorphic to the symmetric group S_3, and $\mathrm{SL}(2, \mathbf{F}_4)$ is isomorphic to the alternating group A_5. It is easy to see that, in all but one of our cases, π is surjective. (In the exceptional case, we have $N = 41$, all the $a_l = 1$, and π is the trivial representation.) Finding π is equivalent to finding the fixed field M of $\ker\pi$; this M will be an $\mathrm{SL}(2, \mathbf{F})$-extension of $\mathbf{Q}$, unramified outside $2N$.

When $\mathbf{F} = \mathbf{F}_2$, M will be the splitting field of an irreducible cubic polynomial over $\mathbf{Q}$ with nonsquare discriminant divisible by at most 2 and N. We searched for the polynomial either by looking in the tables of [Delone and Faddeev 1964], by looking in tables sent to us by Nicole Schulte (unpublished), or by searching the space of cubics using Mathematica on a Macintosh SE/30. When $\mathbf{F} = \mathbf{F}_4$, M will be the splitting field of an irreducible quintic polynomial over $\mathbf{Q}$ with square discriminant divisible by at most 2 and N. We searched for the polynomial either by looking in the tables of [Buhler 1978] or by searching the space of quintics using Mathematica on a Sun SPARCstation 2 at the Ohio State University. With a polynomial in hand, we tested the conjecture by computing the splitting of prime ideals in the splitting field of the polynomial. We continued the search until we found a polynomial that seemed to satisfy the conjecture. Usually it was the first polynomial we tried.

When $\mathbf{F} = \mathbf{F}_4$, there is an additional check to perform: we can distinguish between the two conjugacy classes of elements of order 5 in A_5, using a simple test involving the discriminant. We did the test using Mathematica on a Macintosh SE/30. Since the computation becomes rather lengthy as l increases, we only checked the first five values of l in each example for which $\pi(\mathrm{Frob}_l)$ has order 5. This gave four independent checks, and they always worked correctly.

We give one example of each type.

• $N = 29$: This is the lowest level with nontrivial quasicuspidal cohomology, and the quasicuspidal cohomology group is one-dimensional. We are looking for a semisimple, continuous representation $\pi : G_{\mathbf{Q}} \to \mathrm{SL}(2, \mathbf{F}_2)$, unramified outside $2 \cdot 29$ and such that

$$\mathrm{Tr}\,\pi(\mathrm{Frob}_l)^{-1} = \frac{a_l}{l} - 1 = a_l + 1$$

for $l \neq 2, 29$. The values of a_l are

$$\begin{aligned} a_l &= 0 \quad \text{for } l = 3, 5, 11, 13, 31, 43, 47, 53, 79;\\ a_l &= 1 \quad \text{for } l = 2, 7, 17, 19, 23, 37, 41, 59,\\ &\qquad\qquad 61, 67, 71, 73, 83, 89, 97. \end{aligned}$$

So we need to have $\mathrm{Tr}\,\pi(\mathrm{Frob}_l)^{-1} = 0$ if $a_l = 1$, and $\mathrm{Tr}\,\pi(\mathrm{Frob}_l)^{-1} = 1$ if $a_l = 0$.

We list the six elements in $\mathrm{SL}(2, \mathbf{F}_2)$ and find that we need $\pi(\mathrm{Frob}_l)$ to have order 1 or 2 if $a_l = 1$, and order 3 if $a_l = 0$. Since our list contains both 0 and 1 as values for a_l, we know the image of π must be cyclic of order 3 or all of $\mathrm{SL}(2, \mathbf{F}_2)$. It's easy to find the cyclic extensions of order 3 of $\mathbf{Q}$ that are unramified outside $2 \cdot 29$ and to see that they don't fit the data.

Hence we are looking for a degree-6 extension K of $\mathbf{Q}$ that is the splitting field of some irreducible cubic $f(x)$ with rational coefficients, which factors mod l if $a_l = 1$ and stays irreducible mod l if $a_l = 0$. We can find K by using class field theory on $\mathbf{Q}(\sqrt{d})$, where $d = (-1)^a 2^b 29^c$, trying various values of $a, b, c = 0, 1$. Or, more easily, we search the tables of cubics $x^3 + bx + c$ with integer b, c as found in [Delone and Faddeev 1964]. We find that K is uniquely determined by our requirements and happens to be the splitting field of $x^3 + 2x + 4$.

• $N = 103$: In this case, the cohomology is two-dimensional and the Hecke eigenvalues lie in $\mathbf{F}_4$. We obtain a pair of conjugate Hecke eigenclasses and study one of them. We are looking for a semisimple, continuous representation

$$\rho' : G_{\mathbf{Q}} \to \mathrm{SL}(3, \mathbf{F}_4),$$

unramified outside $2 \cdot 103$ and such that

$$\mathrm{Tr}\,\rho'(\mathrm{Frob}_l)^{-1} = \frac{a_l}{l} = a_l$$

for each $l \neq 2, 103$. The values of a_l are

$$\begin{aligned} a_l &= 0 \quad \text{for } l = 3, 7, 31, 37, 43, 67;\\ a_l &= 1 \quad \text{for } l = 11, 23, 29, 41, 89, 97;\\ a_l &= j \quad \text{for } l = 19, 53, 61, 83;\\ a_l &= j' \quad \text{for } l = 2, 5, 13, 17, 47, 59, 71, 73, 79 \end{aligned}$$

(where j and j' denote the roots of $x^2 + x + 1$).

Since the image of ρ' preserves a nonzero symmetric bilinear form over $\mathbf{F}_4$, it must lie in

$$[\mathrm{GL}(2, \mathbf{F}_4) \times \mathrm{GL}(1, \mathbf{F}_4)] \cap \mathrm{SL}(3, \mathbf{F}_4).$$

This is isomorphic to $\mathrm{SL}(2, \mathbf{F}_4) \times \mathrm{GL}(1, \mathbf{F}_4)$ by the map $(M, \lambda) \to (\lambda M, \lambda)$. Write $\rho' \cong \pi \oplus \chi$. If $\chi \neq 1$, the kernel of χ has as fixed field L the unique cyclic cubic extension of $\mathbf{Q}$ unramified outside $2 \cdot 103$. From [Gras 1975], we see that L is the splitting field of $x^3 + x^2 - 34x - 61$.

We list the characteristic polynomials of the elements of $\mathrm{SL}(3, \mathbf{F}_4)$ and find that we need $\rho'(\mathrm{Frob}_l)$ to have order 3 if $a_l = 0$; 1 or 2 if $a_l = 1$; and 5 if $a_l = j, j'$. From our list of Hecke eigenvalues, we see that $\chi(\mathrm{Frob}_5)$ must equal 1. Since 5 does not split in L, this implies that the image of ρ' must lie in $\mathrm{SL}(2, \mathbf{F}_4) \times \{I\}$. It is easy to see that ρ' must be surjective. So we are looking for an A_5-extension K of $\mathbf{Q}$, the splitting field of some quintic, unramified outside $2 \cdot 103$, and such that the order of Frob_l in $\mathrm{SL}(2, \mathbf{F}_4)$ depends on a_l in the way just specified.

We searched the space of quintics $f(x) = x^5 + ax^4 + bx^3 + cx^2 + dx + e$ for $a = 0, 1, 2$ and $-20 \le b, c, d, e \le 20$ using Mathematica, looking for those with square discriminant divisible by at most 2 and 103. After discarding those whose discriminants were divisible by primes other than 2 and 103, we still had several candidates. One of them, namely $f(x) = x^5 + x^4 - 4x^3 - 6x^2 - 2x + 18$, matched our data: it factors mod l into two linear terms and one cubic term when $a_l = 0$, it factors mod l into one linear and two quadratic terms when $a_l = 1$, and it stays irreducible mod l when $a_l = j$ or j'.

We were also able to discriminate between the two conjugacy classes of elements of order 5 in A_5 and to check that they matched up properly with j versus j'. The method is attributed to Serre by Buhler [Buhler 1974]. Let D be the discriminant of f, which equals $2^6 \cdot 103^2$. Choose a square root δ of D by fixing an ordering of the roots $\alpha_1, \dots, \alpha_5$ of f and setting $\delta = \prod_{i<j}(\alpha_i - \alpha_j)$. If $z = \mathrm{Frob}_l$ in $\mathrm{Gal}(K/\mathbf{Q})$ has order 5, compute

$$d_l = \prod_{i<j}(z^i\alpha_1 - z^j\alpha_1) \mod l.$$

If z induces a permutation of the roots conjugate to (12345), this number d_l is congruent to δ mod l; if z is in the other conjugacy class, $d_l \equiv -\delta$ mod l.

We chose δ to be the positive square root of D. One can't a priori distinguish j from j', so we used Frob_5 to fix the correspondence so that j' occurred when $d_l \equiv \delta$ mod l. We then checked the consistency for the next four l's, namely $l = 11, 13, 17, 19$: $a_l = j'$ when $d_l \equiv \delta$ mod l, and $a_l = j$ when $d_l \equiv -\delta$ mod l.

Classes in Characteristic $p = 3$

• $N = 127$. We concentrate on this case, which among the examples we looked at involved the most intensive computing.

The quasicuspidal cohomology has dimension 2, but the Hecke operators do not act semisimply on it. Thus we have just one package of Hecke eigenvalues, lying in $\mathbf{F}_3$:

$$\begin{aligned} a_l = 0 \quad & \text{for } l = 2, 5, 13, 47, 53, 59, 71, 79, 97, 101; \\ a_l = 1 \quad & \text{for } l = 17, 19, 31, 41, 43, 67, 73, 103; \\ a_l = 2 \quad & \text{for } l = 3, 7, 11, 23, 29, 37, 61, 83, 89, 107, \\ & \qquad 109, 113. \end{aligned}$$

Here $a_l = b_l$. We carried the computations beyond $l = 97$ because of our special interest in this example.

Considerations such as those in [Ash et al. 1991, §§3.1–3.3] (the role played there by $\mathbf{Q}(\sqrt{-3})$ is played here by $\mathbf{F}_3$, since these are the fields of definition of the Hecke eigenvalues in the respective papers) tell us that the nonzero bilinear form fixed by the image of ρ is alternating, and hence that ρ is reducible, of the form $\pi \oplus \chi$. As mentioned at the beginning of this section, we work here with the untwisted ρ, so $\det \rho$ is the cube of the cyclotomic character ω mod 3, that is, $\det \rho = \omega$. Thus, π takes values in $\mathrm{SL}(2, \mathbf{F}_3)$, since it fixes a nondegenerate alternating form, and $\chi = \omega$. In sum, we are looking for a semisimple, continuous representation $\pi : G_{\mathbf{Q}} \to \mathrm{SL}(2, \mathbf{F}_3)$, unramified outside $3 \cdot 127$ and such that

$$\mathrm{Tr}\, \pi(\mathrm{Frob}_l)^{-1} = a_l - l$$

for all $l \ne 3, 127$.

It's not hard to see that if π exists it must be surjective. Thus, finding π is equivalent to finding the fixed field M of $\ker \pi$; this M will be an $\mathrm{SL}(2, \mathbf{F}_3)$-extension of $\mathbf{Q}$, unramified outside $3 \cdot 127$. We have indeed obtained an M that seems to be attached to the given package of Hecke eigenvalues, as we will explain shortly. As usual, the extension is uniquely determined, even highly overdetermined, by the data.

Remarks. (a) M is totally real, and the inertia at 127 has order 3. As mentioned before, these facts are consonant with Conjecture 4.1 in [Clozel 1990]. So we wonder if there is a characteristic 0 object whose Hecke eigenvalues are congruent mod 3 to those we are studying here.

(b) As in [Ash et al. 1991], we find a posteriori that there should be a congruence of Hecke eigenvalues mod 3 between our torsion class of level 127 and an Eisenstein series built from a Maass form on GL(2). We see no way of predicting its existence a priori, and no way of verifying Conjecture 1 for this class at all values of l.

We follow the method of [Ash et al. 1991], explaining where our current task became considerably more difficult because of large class numbers.

There is a filtration of $\mathrm{SL}(2, \mathbf{F}_3)$ with successive quotients C_2, $C_2 \times C_2$ and C_3. So if π exists, and if we let M be the fixed field of $\ker \pi$, we obtain a diagram of fields

$$\begin{array}{l} M \\ \mid {\scriptstyle C_2} \\ L \\ \mid {\scriptstyle C_2\times C_2} \quad , \\ K \\ \mid {\scriptstyle C_3} \\ \mathbf{Q} \end{array}$$

where K, L and M should be Galois over $\mathbf{Q}$ with Galois groups C_3, A_4 and $\mathrm{SL}(2,\mathbf{F}_3)$, respectively. All the fields should be unramified outside 3 and 127 (we will see below that M/K is also unramified at 127).

We found K, L and M in succession. We began by looking for a Galois cubic extension K of $\mathbf{Q}$, unramified outside $3\cdot 127$ and such that the splitting of primes in K is compatible with the conjecture. There are four Galois cubic fields unramified outside $3\cdot 127$: those inside the 9th and 127th roots of unity, and two fields of conductor $9\cdot 127$. As in [Ash et al. 1991], one checks that the K we want is determined uniquely by the Hecke data. We have $K = \mathbf{Q}(\theta)$, where θ is a root of the polynomial $\theta^3 - 381\theta - 127 = 0$.

Let σ be a generator of $\mathrm{Gal}\, K/\mathbf{Q}$. By [Gras 1975], the ring of integers $\mathcal{O}_K$ is $\mathbf{Z}[1,\theta,\theta^\sigma]$, the class number of K is 12, and the fundamental units are ε and ε^σ, where $\varepsilon = 19+\theta+2\theta^\sigma$. One checks that $\mathfrak{L}_3 = (3, 1-\theta)$ and $\mathfrak{L}_{127} = (\theta)$ are the unique prime ideals of $\mathcal{O}_K$ over 3 and 127, respectively.

By studying the group structure of $\mathrm{SL}(2,\mathbf{F}_3)$, one can show for primes $l \neq 3, 127$ that, if π exists, the way (l) splits in L and in M is determined by the trace $\mathrm{Tr}\,\pi(\mathrm{Frob}_l)^{-1} = a_l - l$ and by the way l splits in K. The precise results are summarized in Table 3.

$\mathrm{Tr}\,\pi(\mathrm{Frob}_l)^{-1}$	in K	in L	in M
-1	1	4	8
-1	3	12	24
0	3	6	6
1	1	4	4
1	3	12	12

TABLE 3. Number of primes in the factorization of (l) over the fields K, L, M (see text for notation).

We now look for L. Since L/K is a $C_2\times C_2$ Galois extension with $K/\mathbf{Q}$ cubic Galois and $L/\mathbf{Q}$ nonabelian, we must have

$$L = L_x = K(\sqrt{x}, \sqrt{x^\sigma}, \sqrt{x^{\sigma\sigma}})$$

for some squarefree $x \in \mathcal{O}_K$ such that the norm $N_{K/\mathbf{Q}}(x)$ is a square in $\mathbf{Z}$. To study the ramification in L/K, we cannot proceed as in [Ash et al. 1991], since K has class number greater than 1. Instead, we use a lemma, whose proof we omit.

Lemma. *Let E/F be a quadratic extension of number fields with $E = F(\sqrt{\xi})$ for $\xi \in F$. If $\mathfrak{l}$ is a prime ideal of $\mathcal{O}_F$ not dividing 2, then E/F is unramified over $\mathfrak{l}$ if and only if the prime ideal factorization of the principal ideal $(\xi) \subset \mathcal{O}_F$ contains $\mathfrak{l}$ to an even power. E/F is unramified at the primes over 2 if and only if ξ is the product of a nonzero square in F and an element of $1+4\mathcal{O}_F$.*

If $L = L_x$ exists, the lemma implies that the principal ideal (x) is of the form $\mathfrak{L}_3^i\mathfrak{L}_{127}^j\mathfrak{A}^2$, where $i,j \geq 0$ and $\mathfrak{A}$ is an ideal of $\mathcal{O}_K$ not divisible by $\mathfrak{L}_3$ or $\mathfrak{L}_{127}$. Since $N_{K/\mathbf{Q}}(x)$ must be a square, i and j must be even. Furthermore, we are free to alter x by squares in K. Dividing by θ^2 as often as necessary, we may assume $j = 0$. Dividing by 9 as often as necessary, we may assume $i = 0$, 2 or 4. Dividing by other squares, we may assume $\mathfrak{A}$ runs through a set of representatives of the ideal class group of $\mathcal{O}_K$, which we may take to be prime to $2\cdot 3\cdot 127$.

So, to find L, it suffices to enumerate the ideals

$$\mathfrak{L}_3^i\mathfrak{A}^2 \tag{4.3}$$

that are principal, where $i = 0,2,4$ and $\mathfrak{A}$ runs through a set of representatives of the ideal class group of $\mathcal{O}_K$. It suffices to look at only one ideal of this form in a given $\mathrm{Gal}(K/\mathbf{Q})$-orbit. Let $y \in \mathcal{O}_K$ be a generator of the ideal. Consider only the cases where y is not a square in $\mathcal{O}_K$, but where the norm $N_{K/\mathbf{Q}}(y)$ is a square in $\mathbf{Z}$. Let $x = \varepsilon^{k_1}(\varepsilon^\sigma)^{k_2}y$, where k_1, k_2 run through the set $\{0,1\}$. Ignore the x's that are not in $((\mathcal{O}_K/4\mathcal{O}_K)^\times)^2$. Then if our L exists, it is of the form $L = L_x$ for one of the x we have just enumerated.

To enumerate the ideals of the form (4.3), one must understand the ideal class group of K. We factored many principal ideals $(a-b\theta)$ into primes of $\mathcal{O}_K$ in order to get relations in the class group. Since we already knew the class number, it was straightforward to show that the class group is $C_6 \times C_2$ (generated by the ideals $(11, 2+\theta)$ and $(19, 5+\theta)$ of orders 6 and 2), and to find where a given prime $\mathfrak{L}$ of $\mathcal{O}_K$ lies in the group.

To find y, one must be able to find elements of given norm in a given ideal. We used the very fast algorithm in [Pohst and Zassenhaus 1989, pp. 338–343].

The computations described in the last few paragraphs were done in TI Scheme on the second author's Compaq 80286-based machine. From this point on, however, we worked with Mathematica on a SPARCstation 1+ at Oklahoma State University.

For each x enumerated above, we computed the minimal polynomial f_x for the primitive element $\sqrt{x} + \sqrt{x^\sigma}$ of $L_x/\mathbf{Q}$. We factored f_x mod l for all l for which we had Hecke data; as long as l did not divide the discriminant of f_x, the factorization mod l of the polynomial determined how the ideal (l) split in L_x. Comparing the results with the table of splitting behavior given above, we found there was exactly one field $L = L_x$ that met all our conditions, and that this L was highly overdetermined by the Hecke data. Here $x = 22 - 2\theta - \theta^\sigma$; we have $(x) = (19, 2+\theta)^2$, the square of a prime of K. Note that L/K is unramified outside 3; in particular, it is unramified over 2 because x is the square of $1 + \theta + \theta^\sigma$ in $(\mathcal{O}_K/4\mathcal{O}_K)^\times$.

We remark that the discriminant of f_x (for the specific x above) was divisible by 11, 13 and 19 and by no other primes $l \le 113$, $l \ne 3$. Replacing the primitive element $\sqrt{x} + \sqrt{x^\sigma}$ with $\sqrt{x} + k\sqrt{x^\sigma}$ for various $k \in \mathbf{Z}$, we found primitive elements of $L/\mathbf{Q}$ whose minimal polynomials did not have discriminant divisible by 11 or 19; we could then check that L matched our Hecke data for 11 and 19. Also, L is the splitting field over $\mathbf{Q}$ of $g(\nu) = \nu^4 - 33\nu^2 - 19\nu + 195$, where $\nu = \sqrt{x} + \sqrt{x^\sigma} + \sqrt{x^{\sigma\sigma}} \in \mathcal{O}_L$ is a root of $g(\nu)$. The discriminant of $g(\nu)$ is not divisible by 13, and g splits into linear factors mod 13; this implies that 13 is unramified and splits completely in L, as predicted by our Hecke data.

Next, we looked for a quadratic extension $M = L(\delta')$ for $\delta' \in \mathcal{O}_L$, with M/L unramified outside 3 and such that $\mathrm{Gal}(M/\mathbf{Q}) \cong \mathrm{SL}(2, \mathbf{F}_3)$. A theorem of Serre [1984] gives a criterion for an A_4-extension L of $\mathbf{Q}$ to be liftable to an $\mathrm{SL}(2, \mathbf{F}_3)$-extension. A theorem of Crespo [1989] says that if L is liftable, all the extensions must be of the form $L(\sqrt{q\delta})$, where $q \in \mathbf{Q}$ and δ is an element of L that can be computed explicitly. In our case, we found that L does lift to $\mathrm{SL}(2, \mathbf{F}_3)$-extensions of $\mathbf{Q}$, and we computed δ using Crespo's procedure.

The problem was now to choose q such that $M = L(\sqrt{q\delta})$ matched our Hecke data. We found that the norm $N_{L/\mathbf{Q}}(\delta) = 2^{24}3^6 13^6 19^{12} 127^8$. By the lemma above, M can be unramified outside 3 only if $|q|$ is a squarefree product of primes from the set $\{2, 3, 13, 19, 127\}$. If any prime of L over 13 occurred to an odd power in the ideal factorization of (δ), all the primes over 13 would occur in (δ) to an odd power (since $M/\mathbf{Q}$ is Galois). Since 13 splits completely in L, this would imply 13^{12} divides $N_{L/\mathbf{Q}}(\delta)$, a contradiction. This proves that $L(\sqrt{\delta})$ is unramified over 13. So $M = L(\sqrt{q\delta})$ can be unramified outside 3 only if

$$q = (-1)^{i_1} 2^{i_2} 3^{i_3} 19^{i_4} 127^{i_5}$$

for some $i_1, \dots, i_5 \in \{0, 1\}$.

For the 32 values of q in the preceding paragraph, we found the minimal polynomial of $\sqrt{q\delta}$ over $\mathbf{Q}$ and factored it mod l (for l not dividing the polynomial's discriminant). We found that only for the case $q = 2 \cdot 3 \cdot 19 = 114$ did $M = L(\sqrt{q\delta})$ seem to match our Hecke data. For this reason we set $\delta' = 114\delta$, $M = L(\delta')$ from now on. Let $f_{\delta'}$ be the minimal polynomial of δ' over $\mathbf{Q}$.

Of the primes $l \le 113$, $l \ne 3$, only 2, 5, 13, 17 and 19 divided the discriminant of $f_{\delta'}$. The cases $l = 5$, 13, 17, 19 are handled as follows. Since 5 is inert in K, it must split into four or eight primes of M. If it split into eight primes, $f_{\delta'}$ would factor over $\mathbf{Z}/5$ as a product of (not necessarily distinct) cubics; but instead, it factors into sextics over $\mathbf{Z}/5$. Hence 5 splits into four primes in M, as predicted by the Hecke data. The cases of 13 and 17 are handled similarly. The number $\delta'/19^2$ is an integer of L whose minimal polynomial has discriminant prime to 19; this allowed us to check that M matched our Hecke data at 19.

To show that 2 splits in $M/\mathbf{Q}$ as predicted by the Hecke data, we proceed as follows. 2 is inert in K and splits into four primes $\mathfrak{T}_1, \dots, \mathfrak{T}_4$ in L. We must show that M/L is unramified at 2 and that the $\mathfrak{T}_j$ do not split in M. (This last requirement comes from Table 3, since $\mathrm{Tr}\,\mathrm{Frob}_2^{-1} = a_2 - 2 = 1$.) First, $\frac{1}{4}\delta'$ is an integer of L; we may write $M = L(\sqrt{\delta'/4})$ to check the ramification of M

$$
\begin{aligned}
&t^{24} - 29708856t^{22} + 367756718678640t^{20} - 2509261723108363425984t^{18} + 10493414013632298034200374016t^{16} \\
&\quad - 28231091051345399970505044540776448t^{14} + 498264315929779520273097949446668587499 52t^{12} \\
&\quad - 5771804355521178174862417926755609645976 0943104t^{10} \\
&\quad + 432089608366905408327182201179736534530084010115 07200t^{8} \\
&\quad - 20229808135005646521374508186867852379514853356997205819392t^{6} \\
&\quad + 557265459338991639389034533776557272502035141554585017520226 3040t^{4} \\
&\quad - 796761793283233463108285449803241699225351432742561065212688050683904t^{2} \\
&\quad + 4260285786445539295308037872686242947152377112867878301807783285257509 2736
\end{aligned}
$$

Minimal polynomial of a generator of the extension $M/\mathbf{Q}$ that seems to be attached to our cohomology class for $p = 3$, $N = 127$.

at 2. Second, as above, L is the splitting field over $\mathbf{Q}$ of $g(\nu) = \nu^4 - 33\nu^2 - 19\nu + 195$. There are four embeddings of L into $\bar{\mathbf{Q}}_2$, the algebraic closure of the local field $\mathbf{Q}_2$; they are given by mapping the roots of g in L to the roots of g in $\bar{\mathbf{Q}}_2$ in a Galois-compatible way. Let $\Lambda_1, \ldots, \Lambda_4 \subset \bar{\mathbf{Q}}_2$ be the images of these embeddings. We explicitly found all four Λ_j, representing elements of $\bar{\mathbf{Q}}_2$ as polynomials with coefficients in $\mathbf{Z}/2^i\mathbf{Z}$ for sufficiently large i (we used $i = 5$). We showed that the image of $\frac{1}{4}\delta'$ in Λ_1 was 0 mod 16, and that its image in Λ_j ($j = 2, 3, 4$) was a square and a unit in $\mathcal{O}_{\Lambda_j}/4\mathcal{O}_{\Lambda_j}$. A norm check shows that $(\frac{1}{4}\delta')$ is divisible by exactly the fourth power of $\mathfrak{T}_1$ and by no other $\mathfrak{T}_j$. A local version of the lemma above then shows that M/L is unramified at 2. We also showed that $\frac{1}{4}\delta'$ is not a square mod $8\mathcal{O}_{\Lambda_j}$ in $\mathcal{O}_{\Lambda_j}$ for $j = 2, 3, 4$, which implies that the corresponding $\mathfrak{T}_j$ (and hence $\mathfrak{T}_1$, by Galois symmetry) remain inert in M.

This proves that there is a unique $\mathrm{SL}(2, \mathbf{F}_3)$-extension $M/\mathbf{Q}$ that is unramified outside 3 and 127 and seems to be attached to our Hecke data for all primes $l \leq 113$, $l \neq 3$. A primitive element for this extension is $\sqrt{\delta'}$, whose minimal polynomial over $\mathbf{Q}$ is given in the sidebar above.

A Sturm sequence calculation shows M is totally real. Also, θ^2 divides δ'; this means $N_{L/\mathbf{Q}}(\delta'/\theta^2)$ is prime to 127, implying M/L is unramified at 127. Hence the inertia group of a prime of M over 127 is a 3-group.

- $N = 79$. We have also found the $\mathrm{SL}(2, \mathbf{F}_3)$-extension of $\mathbf{Q}$ that seems to be attached to the reduction mod 3 of the nontorsion class of level 79, a task left undone in [Ash et al. 1991]. It is generated by the element δ' whose minimal polynomial over $\mathbf{Q}$ is given in the sidebar below.

We have also checked that the extension found in [Ash et al. 1991] for the class mod 3 of level 61 fits the conjecture for all $l \leq 97$. (The data used in [Ash et al. 1991] only went up through $l \leq 29$.)

Another interesting example for $p = 3$ is discussed at the end of this section.

Classes in Characteristic $p = 5$

- $N = 211$. This was the only example we treated. The cohomology is two-dimensional, but the Hecke operators do not act semisimply. For the unique

$$
\begin{aligned}
&t^{24} - 585282103380t^{22} + 142731308557048753093500t^{20} - 19024710548794458071527989093462840t^{18} \\
&\quad + 1533435092622632409189133072771812461476126230t^{16} - 782489260987564269959346775679784209231909213573055333 60t^{14} \\
&\quad + 25749679721119220638301196373433081427446490831651304115638374099 00t^{12} \\
&\quad - 545919588471504800632662627019638536543703098893274624244154785981635114365 20t^{10} \\
&\quad + 7310251403888240479054756320403975745936927053256442840093290989113046162119478069612 65t^{8} \\
&\quad - 590655677286632381959881126553999613264773206030375223307455876066140466744817245052708201144 4060t^{6} \\
&\quad + 260574495666110870173113404681631329613062130674320652521004886674445231611997990852539128123777064549181 60t^{4} \\
&\quad - 479270051088840461452907758163101333419713597273889681082418840278119688933438356753905 02\ldots \\
&\qquad\qquad 974510245280538620760600320t^{2} \\
&\quad + 2034938395039721847573157332828492336421579445881074153118158166649010022457516050619778 3\ldots \\
&\qquad\qquad 5906691614496073810999490796097536
\end{aligned}
$$

Minimal polynomial of a generator of the extension of $\mathbf{Q}$ that seems to be attached to the reduction modulo 3 of the cohomology class for $N = 79$ in [Ash et al. 1991].

Hecke eigenclass we get this table of Hecke eigenvalues for $a_l = b_l$:

$$\begin{aligned} a_l &= 1 \quad \text{for } l = 5, 19, 29, 59, 79, 89; \\ a_l &= 2 \quad \text{for } l = 2, 7, 17, 37, 47, 67, 97; \\ a_l &= 3 \quad \text{for } l = 3, 11, 13, 23, 31, 41, 43, 53, \\ &\qquad\qquad 61, 71, 73, 83. \end{aligned}$$

In this case, we find that the image of ρ' must be diagonal. In fact, by factoring the Hecke polynomial $X^3 - a_l l^{-1} X^2 + a_l l^{-1} X - 1$, we see that ρ' must be isomorphic to the representation $1 \oplus \omega \oplus \omega^3$, where ω is the cyclotomic character of $\mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q})$. This fits our data for all $l \leq 97$.

The other example feasible to check would be $N = 163$, where we expect ρ' to be reducible and to give an icosahedral representation of $G_{\mathbf{Q}}$.

Examples Where ρ' Will Have Maximal Image

Here we have four examples; in each case, the cohomology is two-dimensional, and $a_l \neq b_l$ in general. We take each example in turn, and explain why ρ' should have maximal image $\mathrm{SL}(3, \mathbf{F}_p)$. The first case is the model, and the others differ only slightly. Let $g_l = \rho'(\mathrm{Frob}_l)^{-1}$.

• $p = 3$, $N = 137$. According to our data, g_2 has irreducible characteristic polynomial over $\mathbf{F}_3$. Hence the order of g_2 divides $1 + p + p^2 = 13$, the number of elements in $\mathbf{F}_{p^3}^{\times}$ that have norm 1; this means g_2 has order 13. Now [Mitchell 1911] (see also [Bloom 1967]) gives the complete classification of subgroups of $\mathrm{PSL}(3, \mathbf{F})$ for any finite field $\mathbf{F}$ of characteristic $\neq 2$, and moreover $\mathrm{PSL}(3, \mathbf{F}_p) = \mathrm{SL}(3, \mathbf{F}_p)$ whenever $p \not\equiv 1 \pmod 3$. It follows from the classification that the only proper subgroup of $\mathrm{PSL}(3, \mathbf{F}_3)$ with order divisible by 13 is the normalizer of a nonsplit Cartan, which is a subgroup of order 39. So to show ρ' has maximal image, it suffices to exhibit an l for which g_l has order not a divisor of 39. The characteristic polynomial of g_7 splits over $\mathbf{F}_3$ into a linear and a quadratic factor, so this element has order 4 or 8, and we are done.

• $p = 23$, $N = 157$. Since g_3 has irreducible characteristic polynomial $x^3 + 14x^2 + 19x - 1$, its order divides $1+23+23^2 = 7 \cdot 79$. If ρ' does not have maximal image, it follows from [Mitchell 1911] that the image must lie either in the normalizer of a nonsplit Cartan, a group of order $3 \cdot 7 \cdot 79$, or in a

	$p=3$	$p=7$	$p=17$	$p=23$
$T(2,1)$	$\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&6\\4&12\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}19&13\\21&15\end{smallmatrix}\right)$
$T(2,2)$	$\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}12&11\\13&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}15&10\\2&19\end{smallmatrix}\right)$
$T(3,1)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}6&1\\0&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&3\\2&10\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}3&11\\16&12\end{smallmatrix}\right)$
$T(3,2)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}3&6\\0&6\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}10&14\\15&4\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}12&12\\7&3\end{smallmatrix}\right)$
$T(5,1)$	$\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2&3\\0&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&6\\4&16\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}11&5\\1&13\end{smallmatrix}\right)$
$T(5,2)$	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&4\\0&2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}16&11\\13&4\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}13&18\\22&11\end{smallmatrix}\right)$
$T(7,1)$	$\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&5\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}10&5\\9&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}19&0\\0&19\end{smallmatrix}\right)$
$T(7,2)$	$\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}5&6\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}3&12\\8&10\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}19&0\\0&19\end{smallmatrix}\right)$
$T(11,1)$	$\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}11&16\\5&9\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}19&15\\3&2\end{smallmatrix}\right)$
$T(11,2)$	$\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}9&1\\12&11\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2&8\\20&19\end{smallmatrix}\right)$
$T(13,1)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}3&3\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}14&7\\16&11\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}17&21\\18&7\end{smallmatrix}\right)$
$T(13,2)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&4\\0&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}11&10\\1&14\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}7&2\\5&17\end{smallmatrix}\right)$
$T(17,1)$	$\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}6&2\\0&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}6&12\\8&13\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}21&18\\22&19\end{smallmatrix}\right)$
$T(17,2)$	$\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&5\\0&6\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}13&5\\9&6\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}19&5\\1&21\end{smallmatrix}\right)$
$T(19,1)$	$\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}6&0\\0&6\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2&6\\4&14\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}19&10\\2&0\end{smallmatrix}\right)$
$T(19,2)$	$\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}6&0\\0&6\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}14&11\\13&2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&13\\21&19\end{smallmatrix}\right)$
$T(23,1)$	$\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}8&6\\15&15\end{smallmatrix}\right)$

TABLE 4. Hecke matrices for ρ' that have maximal image $\mathrm{SL}(3, \mathbf{F}_p)$.

certain subgroup of order 168. But g_3 is conjugate over $\mathbf{F}_{23}$ to its rational canonical form

$$g_3' = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -19 \\ 0 & 1 & -14 \end{pmatrix}.$$

We check that $(g_3')^7 \neq I$, which rules out the group of order 168. Next, the characteristic polynomial of g_2 splits as $(x+5)(x^2+19x+9)$. Since -5 is of order $11 \pmod{23}$, g_2 cannot lie in a group of order $3 \cdot 7 \cdot 79$.

• $p = 7$, $N = 167$. Since g_{13} has irreducible characteristic polynomial, its order is 19 or 57. As before, if the image of ρ' in $\mathrm{PSL}(3, \mathbf{F}_7)$ were not maximal, it would be contained in the normalizer $\mathcal{N}$ of a nonsplit Cartan, a group of order $3 \cdot 19$. The image of ρ' in $\mathrm{SL}(3, \mathbf{F}_7)$ would be contained in the lift of $\mathcal{N}$ to SL, a group of order $3^2 \cdot 19$. On the other hand, the characteristic polynomial of g_2 splits into a linear and a quadratic factor, and calculations like those above show g_2 must have even order.

- $p = 17$, $N = 191$. This is like the first two cases: g_2 has irreducible characteristic polynomial, and g_3 splits into a linear and a quadratic factor.

We have few ideas on how to find ρ'. We list in Table 4 the Hecke matrices for $l \leq 23$. (We have on file all the $T(l,1)$'s for $l \leq 97$.)

REFERENCES

[Ash 1992a] A. Ash, "Galois representations and cohomology of $\mathrm{GL}(n,\mathbf{Z})$", in *Séminaire de Théorie des Nombres, Paris, 1989–90* (edited by S. David), Birkhäuser, Boston, 1992.

[Ash 1992b] A. Ash, "Galois representations attached to mod p cohomology of $\mathrm{GL}(n,\mathbf{Z})$", *Duke Math. J.* **65** (1992), 235–255.

[Ash et al. 1984] A. Ash, D. Grayson and P. Green, "Computations of cuspidal cohomology of congruence subgroups of $\mathrm{SL}(3,\mathbf{Z})$", *J. Number Theory* **19** (1984), 412–436.

[Ash et al. 1991] A. Ash, R. Pinch and R. Taylor, "An $\hat{A}_4$ extension of $\mathbf{Q}$ attached to a nonselfdual automorphic form on GL(3)", *Math. Ann.* **291** (1991), 753–766.

[Ash and Stevens 1986] A. Ash and G. Stevens, "Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues", *J. Reine Angew. Math.* **365** (1986), 192–220.

[Bloom 1967] D. Bloom, "The subgroups of $\mathrm{PSL}(3,q)$ for odd q", *Trans. Amer. Math. Soc.* **127** (1967), 150–178.

[Buhler 1978] J. Buhler, *Icosahedral Galois Representations*, Lecture Notes in Math. **654**, Springer-Verlag, New York, 1978.

[Clozel 1990] L. Clozel, "Motifs et formes automorphes: applications du principe de fonctorialité", pp. 77–159, in *Automorphic Forms, Shimura Varieties and L-functions. Proceedings of the Ann Arbor Conference*, vol. I (edited by L. Clozel and J. S. Milne), Academic Press, New York, 1990.

[Crespo 1989] T. Crespo, "Explicit construction of $\tilde{A}_n$-type fields", *J. Algebra* **127** (1989), 452–461.

[Deligne 1971] P. Deligne, "Formes modulaires et représentations l-adiques", pp. 139–186 in *Séminaire Bourbaki* **355** (1968/69), Lecture Notes in Math. **179**, Springer-Verlag, New York, 1971.

[Delone and Faddeev 1964] B. Delone and D. Faddeev, *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monographs **10**, Amer. Math. Soc., Providence, RI, 1964.

[Gras 1975] M. Gras, "Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbf{Q}$", *J. Reine Angew. Math.* **277** (1975), 89–116.

[Mitchell 1911] H. H. Mitchell, "Determination of the ordinary and modular ternary linear groups", *Trans. Amer. Math. Soc.* **12** (1911), 207–242.

[Pohst and Zassenhaus 1989] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Encyc. of Math. and Its Applications, Cambridge University Press, Cambridge, 1989.

[Serre 1984] J.-P. Serre, "L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$", *Comment. Math. Helvetici* **59** (1984), 651–676.

[Serre 1987] J.-P. Serre, "Sur les représentations modulaires de degré 2 de $\mathrm{Gal}\,\bar{\mathbf{Q}}/\mathbf{Q}$", *Duke Math. J.* **54** (1987), 179–230.

[Shimura 1971] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, 1971.

Avner Ash, Department of Mathematics, The Ohio State University, Columbus, OH 43210 (ash@function.mps.ohio-state.edu)

Mark McConnell, Department of Mathematics, Oklahoma State University, Stillwater, OK 74078-0613 (mmcconn@hardy.math.okstate.edu)

Received March 30, 1992; revised May 22; accepted September 10