PACIFIC JOURNAL OF MATHEMATICS
Vol. 181, No. 3, 1997

AN ELEMENTARY CASE OF SERRE'S CONJECTURE

David E. Rohrlich and Jerrold B. Tunnell

To the memory of Olga Taussky-Todd

The conjecture of Serre referred to in the title is the one relating Galois representations to modular forms [12]. Let $\overline{\mathbb{Q}}$ denote the field of algebraic numbers in $\mathbb{C}$ and $\overline{\mathbb{Z}}$ the subring of algebraic integers. Fix a prime number ℓ and a prime ideal $\mathfrak{l}$ of $\overline{\mathbb{Z}}$ lying over ℓ, and put $\overline{\mathbb{F}}_\ell = \overline{\mathbb{Z}}/\mathfrak{l}$. Given a cuspidal Hecke eigenform $f(z) = \sum_{n\geqslant 1} a(n)e^{2\pi inz}$ of level N, weight k, and character ϵ, we consider the continuous semisimple representation $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \overline{\mathbb{F}}_\ell)$ associated to f by the work of Shimura ($k = 2$), Deligne ($k \geqslant 2$), and Deligne-Serre ($k = 1$). It is characterized up to isomorphism by the formulas

$$\mathrm{tr}\ \rho_f(\sigma_p) = a(p) \bmod \mathfrak{l} \tag{1}$$

and

$$\det \rho_f(\sigma_p) = \epsilon(p)p^{k-1} \bmod \mathfrak{l}, \tag{2}$$

where p runs over primes not dividing $N\ell$ and $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is any Frobenius element corresponding to any prime ideal of $\overline{\mathbb{Z}}$ lying over p. Let $\sigma_\infty \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote the restriction to $\overline{\mathbb{Q}}$ of complex conjugation. In conjunction with the Chebotarev density theorem, formula (2) implies that $\det \rho_f(\sigma_\infty) = -1$. One says that ρ_f has "odd determinant." Serre's conjecture is a partial converse to this statement. It asserts that every continuous irreducible representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \overline{\mathbb{F}}_\ell)$ of odd determinant is isomorphic to ρ_f for some f, and it provides a choice of N, k, and ϵ for which the required eigenform f should exist.

The present note is devoted to a very special case of the conjecture. Let us call ρ dihedral if its image is a dihedral group. We consider the case where ρ is dihedral and $\ell = 2$. One curious feature of Serre's conjecture is that when $\ell = 2$ the requirement that ρ have odd determinant is vacuous, because $\det \rho(\sigma_\infty)$ is equal to ± 1 in any case, hence equal to -1 if $\ell = 2$. Thus the conjecture implies that *every* continuous irreducible representation

$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \overline{\mathbb{F}}_2)$ has the form ρ_f for some f. When ρ is dihedral this assertion is actually known (in the problematic case where ρ is induced from a real quadratic field the existence of f follows from a trick of Serre) and the only remaining issue is whether f can be chosen so that N, k, and ϵ are as predicted. Now for $\ell \geqslant 3$ it is precisely this sort of issue which has been tackled with great success in the work of Ribet [11] and Diamond [6]. However, the case $\ell = 2$ is largely untouched, and the present note is an attempt to obtain the correct N, k, and ϵ by *ad hoc* arguments in the case at hand.

Even this modest goal is more than we are able to achieve. A dihedral representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $\overline{\mathbb{F}}_2$ is induced from a uniquely determined quadratic field K, and we can exhibit a form f with the correct N, k, and ϵ only when the discriminant of K is either odd or divisible by 8. To some extent this outcome may be inevitable, because we look for f among classical modular forms rather than among the modular forms in characteristic ℓ defined by Katz [7], and there is an example of Serre showing that when ℓ is 2 or 3 the predicted choices of N, k, and ϵ cannot always be attained using classical modular forms alone. It should be added, however, that while Serre's example involves a representation of dihedral type (in the sense that the associated projective representation has dihedral image) the representation itself is not in fact dihedral.

This note is based on work done more than ten years ago. We would like to thank Serre for his guidance at the time and Dinakar Ramakrishnan for urging us to publish the result. It is an honor to dedicate the paper to the memory of Olga Taussky-Todd.

1. A technical lemma.

Given positive integers N and k and a Dirichlet character χ modulo N, let $\mathrm{S}_k(N, \chi)$ denote the space of cusp forms of weight k for $\Gamma_1(N)$ with character χ. If χ is trivial then we also write $\mathrm{S}_k(N)$. We shall often identify an element of $\mathrm{S}_k(N, \chi)$ with its q-expansion, writing $f = \sum a(n)q^n$ if $f(z) = \sum_{n \geqslant 1} a(n)e^{2\pi inz}$, and we shall tolerate the slight abuse of notation inherent in an equation such as $g = f(dz)$, where d is a positive integer and $g = \sum a(n)q^{dn}$. Three points regarding the q-expansion need to be mentioned here. First, if $a(n) \in \overline{\mathbb{Q}}$ for all n and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ then the formal conjugate $f^\sigma = \sum a(n)^\sigma q^n$ is an element of $\mathrm{S}_k(N, \chi^\sigma)$, where $\chi^\sigma(n) = \chi(n)^\sigma$. Second, the action of the Hecke operator T_p on $\mathrm{S}_k(N, \chi)$ can be written

$$f|T_p = \sum a(pn)q^n + \chi(p)p^{k-1} \sum a(n)q^{pn},$$

with the understanding that if p divides N then $\chi(p) = 0$ in keeping with the usual convention for Dirichlet characters modulo N (in the literature,

the operator T_p is often denoted U_p when p divides N). Finally, if $a(n) \in \overline{\mathbb{Z}}$ for all n and $\sum b(n)q^n$ is an arbitrary element of $\overline{\mathbb{Z}}[[q]]$ then the notation $f \equiv \sum b(n)q^n \pmod{\mathfrak{l}}$ will mean that $a(n) \equiv b(n) \pmod{\mathfrak{l}}$ for all n. If $\sum b(n)q^n$ is actually the q-expansion of a cusp form g then we also write $f \equiv g \pmod{\mathfrak{l}}$.

Our primary tool in this note is the following standard application of the Deligne-Serre lemma ([5], Lemme 6.11). Let S be any set of prime numbers and $f \in \mathrm{S}_k(N, \chi)$ a cusp form with Fourier coefficients in $\overline{\mathbb{Z}}$. Suppose that for every prime $p \notin S$ there exists $\lambda_p \in \overline{\mathbb{Z}}$ with $f|T_p \equiv \lambda_p f \pmod{\mathfrak{l}}$. We assume also that $f \not\equiv 0 \pmod{\mathfrak{l}}$. Then there exists a nonzero cusp form $f' \in \mathrm{S}_k(N, \chi)$ and for each $p \notin S$ an element $\lambda'_p \in \overline{\mathbb{Z}}$ such that $f'|T_p = \lambda'_p f'$ and $\lambda'_p \equiv \lambda_p \pmod{\mathfrak{l}}$. To deduce this conclusion from [5] one may assume first of all that the λ_p lie in a sufficiently large number field K. One then takes the ring $\mathfrak{O}$ of [5] to be the localization at $\mathfrak{l} \cap K$ of the ring of integers of K, and one observes that in the present situation the eigenvalues λ'_p are *a priori* algebraic integers, as are the Fourier coefficients of some scalar multiple of f'.

Suppose that V is a finite-dimensional vector space over $\overline{\mathbb{F}}_\ell$ and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$ a continuous representation. For the purposes of Serre's conjecture, the correct way to define the conductor of ρ is to imitate the definition of the Artin conductor of a complex Galois representation but to omit the contribution at ℓ. Thus one chooses a finite Galois extension K of $\mathbb{Q}$ such that ρ factors through $\mathrm{Gal}(K/\mathbb{Q})$, and for each prime number $p \neq \ell$ one considers the sequence of ramification subgroups $I_0 \supset I_1 \supset I_2 \supset \dots$ of $\mathrm{Gal}(K/\mathbb{Q})$ at a prime ideal of K above p. The exponent of p in the conductor of ρ is the integer $a_p(\rho) \geqslant 0$ defined by

$$a_p(\rho) = \sum_{n \geqslant 0} [I_0 : I_n]^{-1} \dim V/V^{I_n},$$

where V^H denotes the subspace of H-invariants of a subgroup H of $\mathrm{Gal}(K/\mathbb{Q})$. The conductor of ρ is

$$N(\rho) = \prod_{p \neq \ell} p^{a_p(\rho)}.$$

If ρ is irreducible, two-dimensional, and of odd determinant, then the parameter N associated to ρ by Serre's conjecture is simply $N(\rho)$.

Henceforth $\ell = 2$. Thus $\mathfrak{l}$ is a prime ideal of $\overline{\mathbb{Z}}$ of residue characteristic 2. The subset of $\mathrm{S}_k(N, \chi)$ consisting of primitive forms of conductor N (i.e. "normalized new forms of level N") will be denoted $\mathrm{Prim}_k(N, \chi)$, or simply $\mathrm{Prim}_k(N)$ if χ is trivial.

Lemma. *Let $g = \sum b(n)q^n$ be an element of $\mathrm{Prim}_1(2^\nu Nr, \chi)$, where $\nu \in \{0, 2, 3\}$, N is odd, r is either 1 or an odd prime not dividing N, and $\chi^2 = 1$. Assume that $N = N(\rho_g)$. Also, if $r \neq 1$ assume that $b(r) \not\equiv 1 \pmod{\mathfrak{l}}$; if $\nu = 2$ assume that $b(n) = 0$ whenever n is even; and if $\nu = 3$ assume that $b(2) \not\equiv 0 \pmod{\mathfrak{l}}$. Put $k = 2$ if $\nu \in \{0, 2\}$ and $k = 4$ if $\nu = 3$. Then there exists an element $f \in \mathrm{Prim}_k(N)$ such that $\rho_f \cong \rho_g$.*

Proof. The proof can be broken into three steps:

(i) There is a positive divisor M of N and an element $f = \sum a(n)q^n$ of $\mathrm{Prim}_k(M)$ such that $a(p) \equiv b(p) \pmod{\mathfrak{l}}$ for all p not dividing $2Nr$.

(ii) If f is as in (i) then $\rho_f \cong \rho_g$.

(iii) If M is as in (i) then $M = N$.

Step (ii) follows from the Chebotarev density theorem: Indeed the semisimple representations ρ_f and ρ_g are determined up to isomorphism by their characteristic polynomials, and referring to (1) and (2) we see that if $p \nmid 2Nr$ then

$$\mathrm{tr}\ \rho_f(\sigma_p) = a(p) \bmod \mathfrak{l} = b(p) \bmod \mathfrak{l} = \mathrm{tr}\ \rho_g(\sigma_p)$$

and

$$\det \rho_f(\sigma_p) = p^{k-1} \bmod \mathfrak{l} = \chi(p) \bmod \mathfrak{l} = \det \rho_g(\sigma_p).$$

As for (iii), a theorem of Carayol [3] implies that $N(\rho_f) \leqslant M$ (see Carayol [4] or Livné [9]). Since $N(\rho_f) = N(\rho_g)$ by (ii) and $N(\rho_g) = N$ by assumption, it follows that $N \leqslant M$, whence $M = N$ because M divides N.

It remains to prove (i). The proof is divided into cases according as $\nu = 0, 2$, or 3, but for the sake of efficiency we begin with an argument which is needed in all three cases. Suppose that $r \neq 1$. Put $N' = N$ or $N' = 2N$, and let $f_0 \in \mathrm{S}_2(N'r)$ be a nonzero eigenvector of the operators T_p for $p \neq 2$, with corresponding eigenvalues λ_p. Let $f = \sum a(n)q^n$ be the primitive form in $\mathrm{S}_2(N'r)$ such that $a(p) = \lambda_p$ for $p \nmid 2Nr$, and let M be the conductor of f, so that M divides $N'r$. We claim that if $\lambda_r \neq \pm 1$ then M divides N'. The proof is as follows. By the theory of new forms, f_0 is a linear combination of the cusp forms $f(dz)$, where d runs over divisors of $N'r/M$. If M does not divide N' then r divides M, and consequently d is prime to r. A standard calculation then shows that each $f(dz)$ is an eigenvector of T_r with eigenvalue $a(r)$, whence the same is true for f_0. But f_0 is by assumption an eigenvector of T_r with eigenvalue λ_r. Thus $\lambda_r = a(r)$, and in particular, $a(r) \neq \pm 1$. This is a contradiction, because $-a(r)$ is the eigenvalue of an involution on $\mathrm{S}_2(N'r)$, namely the Atkin-Lehner involution at the prime r ([1], p. 147, Thm. 3(iii)).

Put $\tau = \sigma_{\mathfrak{l}}^{-1}$, where $\sigma_{\mathfrak{l}} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is some fixed Frobenius element at $\mathfrak{l}$.

Case 1. $\nu = 0$.

Let $h = g^2$. Then $h \in \mathrm{S}_2(Nr)$ and $h \equiv \sum b(n)^2 q^{2n} \pmod{\mathfrak{l}}$. Consequently $h^\tau \equiv \sum b(n) q^{2n} \pmod{\mathfrak{l}}$. But $h^\tau \in \mathrm{S}_2(Nr)$ also, and a straightforward calculation shows that $h^\tau | T_p \equiv b(p) h^\tau \pmod{\mathfrak{l}}$ for $p \neq 2$. Hence the Deligne-Serre lemma provides a nonzero cusp form $f_0 \in \mathrm{S}_2(Nr)$ and for each $p \neq 2$ an element $\lambda_p \in \overline{\mathbb{Z}}$ such that $f_0 | T_p = \lambda_p f_0$ and $\lambda_p \equiv b(p) \pmod{\mathfrak{l}}$. Let $f = \sum a(n) q^n$ be the primitive form in $\mathrm{S}_2(Nr)$ such that $a(p) = \lambda_p$ for $p \nmid 2Nr$. If $r \neq 1$ then $b(r) \not\equiv 1 \pmod{\mathfrak{l}}$ by assumption, and consequently $\lambda_r \neq \pm 1$. Thus we can apply our preliminary remark with $N' = N$ to conclude that $f \in \mathrm{Prim}_2(M)$ for some divisor M of N. By construction, $a(p) \equiv b(p) \pmod{\mathfrak{l}}$ for $p \nmid 2Nr$.

Case 2. $\nu = 2$.

Certainly $g^2 \in \mathrm{S}_2(4Nr)$. We claim that in fact $g^2 \in \mathrm{S}_2(2Nr)$. To verify this, put

$$C = \begin{pmatrix} 1 & 0 \\ 2Nr & 1 \end{pmatrix}, \qquad D = \begin{pmatrix} 1 & -1/2 \\ 0 & 1 \end{pmatrix}, \qquad W = \begin{pmatrix} 0 & -1 \\ 4Nr & 0 \end{pmatrix},$$

so that

$$C = WDW^{-1}.$$

Since C is a representative of the nontrivial coset of $\Gamma_0(4Nr)$ in $\Gamma_0(2Nr)$ it suffices to see that

$$g|C = -g,$$

or equivalently, that

$$(g|W)|D = -(g|W). \tag{3}$$

In other words, we must check that the q-expansion of $g|W$ contains only odd powers of q. But g is a primitive form of conductor $4Nr$, and therefore $g|W = c\sum \overline{b(n)} q^n$ for some constant c ([**10**], p. 166, Thm. 4.6.15). Furthermore, if n is even then $b(n) = 0$ by assumption. Therefore (3) does hold, and consequently $g^2 \in \mathrm{S}_2(2Nr)$ as claimed.

Next choose integers a and b such that $4a + Nrb = 1$, and put

$$A = \begin{pmatrix} 2a & b \\ -Nr & 2 \end{pmatrix}.$$

Also put

$$B = \begin{pmatrix} 1 & 0 \\ Nr & 1 \end{pmatrix}$$

and let C be as in the previous paragraph. Then A, B, and C are representatives for the distinct right cosets of $\Gamma_0(2Nr)$ in $\Gamma_0(Nr)$. On the other hand, the matrices

$$W' = \begin{pmatrix} 0 & -1 \\ 2Nr & 0 \end{pmatrix}$$

and

$$W'' = \begin{pmatrix} 0 & 1 \\ -Nr & 0 \end{pmatrix}$$

normalize $\Gamma_0(2Nr)$ and $\Gamma_0(Nr)$ respectively. It follows that $g^2|W'(A+B+C)W'' \in \mathrm{S}_2(Nr)$. Now write $g^2 = \sum c(n)q^n$. A standard calculation gives

$$g^2|W'(A+B+C)W'' = \sum c(2n)q^n + 2^{-1}(g^2|J)(z/2) \tag{4}$$

where

$$J = \begin{pmatrix} 4 & 1 \\ -4Nrb & 4a \end{pmatrix}.$$

But $g^2|J = (g|J)^2$, and since J is the "W-operator" on $\mathrm{S}_1(4Nr, \chi)$ at the prime 2 we have $g|J = \lambda\check{g}$ with $\lambda \in \overline{\mathbb{Q}}^\times$ and $\check{g} \in \mathrm{Prim}_1(4Nr, \chi)$. (See [2], p. 224. The term "W-operator" refers to an operator of Atkin-Lehner type.) Put

$$h = 2\lambda^{-2}g^2|W'(A+B+C)W'' \in \mathrm{S}_2(Nr)$$

and write $\check{g} = \sum \check{b}(n)q^n$, so that (4) becomes

$$h = 2\lambda^{-2}\sum c(2n)q^n + \Big(\sum \check{b}(n)q_{\frac{1}{2}}^n\Big)^2 \tag{5}$$

with $q_{\frac{1}{2}} = e^{\pi iz}$. The conductor of χ is either odd or an odd multiple of 4, and in the latter case $|b(2)| = 1$ ([10], p. 170, Thm. 4.6.17(1)). Since $b(2) = 0$ by assumption we deduce that χ has odd conductor. It follows that the W-operator defined by J is an involution of $\mathrm{S}_1(4Nr, \chi)$ ([2], p. 223, Prop. 1.1) and that $g = \check{g}$ ([2], p. 224, (1.1)), whence $\lambda = \pm 1$. Returning to (5), we find that $h \equiv \sum b(n)^2q^n \pmod{\mathfrak{l}}$ and consequently that $h^\tau \equiv \sum b(n)q^n \pmod{\mathfrak{l}}$. The Deligne-Serre lemma now provides a nonzero cusp form $f_0 \in \mathrm{S}_2(Nr)$ and for each $p \neq 2$ an element $\lambda_p \in \overline{\mathbb{Z}}$ such that $f_0|T_p = \lambda_p f_0$ and $\lambda_p \equiv b(p) \pmod{\mathfrak{l}}$. To complete the argument we simply repeat the last four sentences of Case 1.

Case 3. $\nu = 3$.

Write $g^2 = \sum c(n)q^n$ and put $h = \sum c(4n)q^n$. Then $g^2 \in \mathrm{S}_2(8Nr)$ and consequently $h \in \mathrm{S}_2(2Nr)$ ([8], p. 287). But $c(2n) \equiv b(n)^2 \pmod{\mathfrak{l}}$, whence $c(2n)^\tau \equiv b(n) \pmod{\mathfrak{l}}$. It follows that $h^\tau \equiv \sum b(2n)q^n \pmod{\mathfrak{l}}$, and then a straightforward calculation shows that $h^\tau|T_p \equiv b(p)h^\tau \pmod{\mathfrak{l}}$ for $p \neq 2$. Furthermore, h^τ is nonzero modulo $\mathfrak{l}$ because $b(2) \not\equiv 0 \pmod{\mathfrak{l}}$ by assumption. Hence by the Deligne-Serre lemma there is a nonzero form $f_0 \in \mathrm{S}_2(2Nr)$ and for each $p \neq 2$ an eigenvalue $\lambda_p \in \overline{\mathbb{Z}}$ such that $f_0|T_p = \lambda_p f_0$ and $\lambda_p \equiv b(p) \pmod{\mathfrak{l}}$. Let $g_1 = \sum b_1(n)q^n$ be the primitive form in $\mathrm{S}_2(2Nr)$ such that $b_1(p) = \lambda_p$ for $p \nmid 2Nr$, and let N_1 be the conductor of g_1. Then N_1 divides $2N$ (if $r \neq 1$ apply the preliminary remark with $N' = 2N$). Also $b_1(p) \equiv b(p) \pmod{\mathfrak{l}}$ for $p \nmid 2Nr$. We now consider cases, according as N_1 does or does not divide N.

First suppose that N_1 does divide N. Put $h_1 = g_1^2 \in \mathrm{S}_4(N_1)$, so that $h_1^\tau \equiv \sum b_1(n)q^{2n} \pmod{\mathfrak{l}}$. Applying the Deligne-Serre lemma once again, we obtain a nonzero cusp form $f_1 \in \mathrm{S}_4(N_1)$ and for each $p \neq 2$ an element $\lambda'_p \in \overline{\mathbb{Z}}$ such that $f_1|T_p = \lambda'_p f_1$ and $\lambda'_p \equiv b_1(p) \pmod{\mathfrak{l}}$. In particular, $\lambda'_p \equiv b(p) \pmod{\mathfrak{l}}$ for $p \nmid 2Nr$. If $f = \sum a(n)q^n$ is the primitive form determined by f_1 then $a(p) \equiv b(p) \pmod{\mathfrak{l}}$ for $p \nmid 2Nr$, and the conductor M of f divides N_1 and hence N.

Next suppose that N_1 does not divide N. Write $N_1 = 2L$, where L divides N. Thus $g_1 \in \mathrm{Prim}_2(2L)$. We now argue as in Case 2, but with N replaced by L. More precisely, choose integers a and b such that $4a + Lb = 1$, and put

$$A = \begin{pmatrix} 2a & b \\ -L & 2 \end{pmatrix}.$$

Also put

$$B = \begin{pmatrix} 1 & 0 \\ L & 1 \end{pmatrix}, \qquad W' = \begin{pmatrix} 0 & -1 \\ 2L & 0 \end{pmatrix}, \qquad W'' = \begin{pmatrix} 0 & 1 \\ -L & 0 \end{pmatrix},$$

and

$$J = \begin{pmatrix} 2 & 1 \\ -2Lb & 4a \end{pmatrix},$$

and set $C = B^2$. Since A, B, and C represent the distinct right cosets of $\Gamma_0(2L)$ in $\Gamma_0(L)$, and $g_1^2 \in \mathrm{S}_4(2L)$, we have $g_1^2|W'(A + B + C)W'' \in \mathrm{S}_4(L)$. But $g_1^2|W'AW'' = g_1^2|J = (g_1|J)^2$, and the action of J on $\mathrm{S}_2(2L)$ defines the Atkin-Lehner involution at 2. As $g_1 \in \mathrm{Prim}_2(2L)$ we deduce that $g_1|J = \pm g_1$ and hence that $g_1^2|W'AW'' = g_1^2$. On the other hand, if we write $g_1^2 = \sum c_1(n)q^n$ then a straightforward calculation gives $2g_1^2|W'(B+C)W'' =$

$\sum c_1(2n)q^n$. Put $h_1 = 2g_1^2|W'(A+B+C)W'' \in \mathrm{S}_4(L)$. Then

$$h_1 = \sum c_1(2n)q^n + 2\sum c_1(n)q^n.$$

But the equation $g_1^2 = \sum c_1(n)q^n$ also gives $\sum c_1(n)q^n \equiv \sum b_1(n)^2 q^{2n} \pmod{\mathfrak{l}}$. It follows that $c_1(2n) \equiv b_1(n)^2 \pmod{\mathfrak{l}}$, whence $h_1^\tau \equiv \sum b_1(n)q^n \pmod{\mathfrak{l}}$. A final appeal to the Deligne-Serre lemma yields a nonzero cusp form $f_1 \in \mathrm{S}_4(L)$ and for each $p \neq 2$ an element $\lambda_p' \in \overline{\mathbb{Z}}$ such that $f_1|T_p = \lambda_p' f_1$ and $\lambda_p' \equiv b_1(p) \pmod{\mathfrak{l}}$. To complete the proof we now repeat the last two sentences of the previous paragraph, with N_1 replaced by L. □

2. Dihedral representations.

A consideration of Jordan normal forms shows that an element of even order in $\mathrm{GL}(2,\overline{\mathbb{F}}_2)$ is the product of an involution and an element of the center, the latter necessarily of odd order. On the other hand, a dihedral group contains no nontrivial central elements of odd order. Thus an element of even order in a dihedral subgroup of $\mathrm{GL}(2,\overline{\mathbb{F}}_2)$ is an involution, and therefore the order of such a subgroup, if at least 6, is twice an odd integer. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2,\overline{\mathbb{F}}_2)$ be an irreducible representation with dihedral image. It follows from the preceding remarks that ρ has the form $\rho = \mathrm{ind}_{K/\mathbb{Q}}\varphi$, where K is a quadratic field and $\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \overline{\mathbb{F}}_2^\times$ a character of odd order. Let $\tilde{\varphi}$ be the unique complex-valued character of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ which has the same order as φ and satisfies $\varphi(\sigma) = \tilde{\varphi}(\sigma) \bmod \mathfrak{l}$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. The complex representation $\tilde{\rho} = \mathrm{ind}_{K/\mathbb{Q}}\tilde{\varphi}$ is a lift of ρ which preserves the dimension of the 1-eigenspace of $\rho(\sigma)$ for each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Hence the parameter $N = N(\rho)$ in Serre's conjecture is simply the Artin conductor of $\tilde{\rho}$ with the factor at 2 omitted. In other words,

$$|D|\,\mathbf{N}\mathfrak{f}(\tilde{\varphi}) = 2^\nu N,$$

where D is the discriminant of K, $\mathfrak{f}(\tilde{\varphi})$ the conductor of $\tilde{\varphi}$, and ν a nonnegative integer.

The determination of ν is a straightforward exercise in class field theory. Viewing $\tilde{\varphi}$ as a ray class character of odd order, one finds that if 2 splits or ramifies in K then $\mathbf{N}\mathfrak{f}(\tilde{\varphi})$ is odd, while if 2 remains prime in K then $\mathbf{N}\mathfrak{f}(\tilde{\varphi})$ is either odd or an odd multiple of 4. Hence there are four possibilities:

(i) D and $\mathbf{N}\mathfrak{f}(\tilde{\varphi})$ are both odd.

(ii) $D \equiv \pm 5 \pmod 8$ and $\mathbf{N}\mathfrak{f}(\tilde{\varphi}) \equiv 4 \pmod 8$.

(iii) $D \equiv 4 \pmod 8$ and $\mathbf{N}\mathfrak{f}(\tilde{\varphi})$ is odd.

(iv) $D \equiv 0 \pmod 8$ and $\mathbf{N}\mathfrak{f}(\tilde{\varphi})$ is odd.

We see that $\nu = 0$ in case (i), $\nu = 2$ in cases (ii) and (iii), and $\nu = 3$ in case (iii). Furthermore, according to Serre's recipe the parameters ϵ and k associated to ρ are as follows: ϵ is the trivial character in all cases and k is 2 or 4 according as $\nu \in \{0, 2\}$ or $\nu = 3$ (cf. [**12**], p. 188). We shall verify Serre's conjecture in cases (i), (ii), and (iv):

Theorem. *Suppose that D is either odd or divisible by 8. Then there exists $f \in \mathrm{Prim}_k(N)$ such that $\rho \cong \rho_f$.*

Proof. The argument is the same as in [**12**] (p. 218, Prop. 10) but with the additional input of the technical lemma. We consider the cases $D < 0$ and $D > 0$ separately.

First suppose that $D < 0$. Write $L(s, \tilde{\varphi}) = \sum_{n \geqslant 1} b(n) n^{-s}$ and put $g = \sum b(n) q^n$. Then $g \in \mathrm{Prim}_1(2^\nu N, \chi)$, where χ is the Kronecker symbol at D viewed as a Dirichlet character modulo $2^\nu N$. Also $\rho_g \cong \rho$, whence $N(\rho_g) = N$. Now if $\nu = 2$ then we are in case (ii) above, so that $\tilde{\varphi}$ is ramified at the unique prime of K above 2. Therefore $b(n) = 0$ for n even. On the other hand, if $\nu = 3$ then we are in case (iv) above, so that $\tilde{\varphi}$ is unramified at the unique prime $\mathfrak{p}$ of K above 2. Therefore the coefficient $b(2) = \tilde{\varphi}(\mathfrak{p})$ is nonzero, hence a root of unity, hence nonzero modulo $\mathfrak{l}$. Applying the lemma, we obtain $f \in \mathrm{Prim}_k(N)$ with $\rho_f \cong \rho_g$. This is the desired result, because $\rho_g \cong \rho$.

Next suppose that $D > 0$. Let ∞_1 and ∞_2 denote the two infinite places of K. We claim that there is a prime ideal $\mathfrak{r}$ of K, relatively prime to $2N$ and of degree one, together with a quadratic Hecke character ξ of K, ramified precisely at ∞_1 and $\mathfrak{r}$, such that $\tilde{\varphi}(\mathfrak{r}) \neq 1$. Granting this claim temporarily, we complete the proof as follows. Write $L(s, \tilde{\varphi}\xi) = \sum_{n \geqslant 1} b(n) n^{-s}$ and put $g = \sum b(n) q^n$ and $r = \mathbf{N}\mathfrak{r}$. Then $g \in \mathrm{Prim}_1(2^\nu N r, \chi)$, where χ is the product of the Kronecker symbol at D and the Legendre symbol at r, viewed as a Dirichlet character modulo $2^\nu N r$. Since ξ is quadratic we still have $\rho_g \cong \rho$ and hence $N(\rho_g) = N$. Also $b(r) \equiv \tilde{\varphi}(\mathfrak{r}')$, where $\mathfrak{r}'$ is the conjugate of $\mathfrak{r}$ under the nontrivial automorphism of K over $\mathbb{Q}$. Since the representation induced by $\tilde{\varphi}$ is dihedral we have $\tilde{\varphi}(\mathfrak{r}') = \tilde{\varphi}(\mathfrak{r})^{-1}$; on the other hand, $\tilde{\varphi}(\mathfrak{r})$ is a nontrivial root of unity of odd order and is therefore not congruent to 1 modulo $\mathfrak{l}$. Hence $b(r) \not\equiv 1 \pmod{\mathfrak{l}}$. Furthermore, just as in the case $D < 0$, if $\nu = 2$ then $b(n) = 0$ for n even and if $\nu = 3$ then $b(2) \neq 0$. Thus the hypotheses of the lemma are satisfied, and it remains only to check that a quadratic character ξ with the required properties exists. Let C be the narrow ray class group of K modulo $4\mathfrak{f}(\tilde{\varphi})$, and let $c \in C$ be the class consisting of all principal fractional ideals (γ) such that γ is negative at ∞_1, positive at ∞_2, and congruent to 1 modulo $4\mathfrak{f}(\tilde{\varphi})$. Then c has order 1 or 2. On the other hand, let C' be the wide ray class group of K modulo $\mathfrak{f}(\tilde{\varphi})$, and

choose a class $b' \in C'$ of odd order such that $\tilde{\varphi}(\mathfrak{b}) \neq 1$ for $\mathfrak{b} \in b'$. Choose a class $b \in C$ of odd order which is a preimage of b' under the natural map $C \to C'$. Finally, let $\mathfrak{r}$ be a prime ideal of degree one, relatively prime to $2N$, which belongs to the class bc. Then $\mathfrak{r}^2 \in b^2$ and consequently $\tilde{\varphi}(\mathfrak{r}) \neq 1$. If n is the order of b then $\mathfrak{r}^n$ belongs to the ray class c and therefore has a generator ρ which is negative at ∞_1, positive at ∞_2, and congruent to 1 modulo 4. The quadratic Hecke character ξ associated to the extension $K(\sqrt{\rho})/K$ is then ramified precisely at ∞_1 and $\mathfrak{r}$. □

Remarks. 1) The "trick of Serre" alluded to in the introduction is the replacement of $\tilde{\varphi}$ by $\tilde{\varphi}\xi$ in the case $D > 0$. Since ξ is chosen to have mixed signature the representation $\mathrm{ind}_{K/\mathbb{Q}}\,\tilde{\varphi}\xi$ has odd determinant and so corresponds to a modular form of weight one rather than to a Maass form.

2) It is easy to pinpoint where the argument breaks down in case (iii) above: In this case $\tilde{\varphi}$ is unramified at the unique prime ideal of K above 2, and consequently the Fourier coefficient $b(2)$ of g is nonzero. This violates a hypothesis of the technical lemma, namely that when $\nu = 2$ the Fourier coefficients $b(n)$ are zero for even n. Without this assumption formula (3) in the proof of the lemma is false.

3) We lack examples or counterexamples bearing on the possible validity of our theorem in case (iii). As we have mentioned in the introduction, Serre's counterexample does not quite match our situation.

References

[1] A.O.L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann., **185** (1970), 134-160.

[2] A.O.L. Atkin and W. Li, *Twists of newforms and pseudo-eigenvalues of* W*-operators*, Invent. Math., **48** (1978), 221-243.

[3] H. Carayol, *Sur les représentations* ℓ*-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. Ec. Norm. Sup., **19** (1986), 409-468.

[4] H. Carayol, *Sur les représentations galoisiennes modulo* ℓ *attachées aux formes modulaires*, Duke Math. J., **59** (1989), 785-801.

[5] P. Deligne and J-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. Ec. Norm. Sup., **7** (1974), 507-530.

[6] F. Diamond, *The refined conjecture of Serre*, in 'Elliptic Curves, Modular Forms, and Fermat's Last Theorem' (ed. J. Coates and S.T. Yau), International Press, Cambridge, Mass., (1995), 22-37.

[7] N. Katz, *p-adic properties of modular schemes and modular forms*, in 'Modular Functions of One Variable III', Springer-Verlag, Lecture Notes in Math., **350** (1973), 69-190.

[8] W. Li, *Newforms and functional equations*, Math. Ann., **212** (1975), 285-315.

[9] R. Livné, *On the conductors of* mod ℓ *Galois representations coming from modular forms*, J. Number Theory, **31** (1989), 133-141.

[10] T. Miyake, *Modular Forms*, Springer-Verlag, 1989.

[11] K.A. Ribet, *Report on* mod ℓ *representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, in 'Motives' (ed. U. Jannsen, S. Kleiman and J-P. Serre), Proc. Symp. Pure Math., **55**(**2**), Amer. Math. Soc., Providence, (1994), 639-676.

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

Boston University
Boston, MA 02215
E-mail address: rohrlich@math.bu.edu

and

Rutgers University
New Brunswick, NJ 08903
E-mail address: tunnel@math.rutgers.edu