Wildly ramified Galois representations and a generalization of a conjecture of Serre

Darrin Doud
Brigham Young University
Department of Mathematics
292 TMCB
Provo, UT 84602

November 22, 2004

Abstract

Serre's conjecture relates two-dimensional odd irreducible characteristic p representations to modular forms. We discuss a generalization of this conjecture (due to Ash and Sinnott) to higher-dimensional Galois representations. In particular, we give a refinement of the conjecture in the case of wildly ramified Galois representations and we provide computational evidence for this refinement.

1 Introduction

In [4], Ash and Sinnott stated a conjecture which relates certain n-dimensional Galois representations with arithmetic cohomology classes. This conjecture is the beginning of a vast generalization of Serre's conjecture relating two-dimensional odd irreducible Galois representations defined over $\bar{\mathbb{F}}_p$ with mod p reductions of modular forms. Both Serre's conjecture and its generalization predict a weight for an object corresponding to a Galois representation. Serre's conjecture gives a precise prediction of the weight of a modular form corresponding to any odd irreducible two-dimensional Galois representation. On the other hand, in certain cases the conjecture of Ash and Sinnott asserts that at least one of several weights yields a cohomology eigenclass corresponding to an odd n-dimensional Galois representation. In this paper we discuss a refinement of the conjecture of Ash and Sinnott clarifying which of their predicted weights should actually contain an eigenclass corresponding to a given Galois representation and we present computational evidence for this refinement. We note that Ash and Sinnott only dealt with *niveau* one Galois representations—in [1] their conjecture is extended to more general Galois representations, but the ambiguity is not addressed. In this paper, we do not address the ambiguity in the case of higher niveau representations. The computational evidence in this paper all concerns niveau one representations in characteristic p with $5 \leq p \leq 17$. In addition, examples of wildly ramified Galois representations in characteristics two and three appear in [3] and [2]. The results of the computations done in these papers also support the refined conjecture.

2 The conjecture of Ash and Sinnott

2.1 Definitions

In this section, we give brief definitions of the objects relating to the conjecture of Ash and Sinnott. These definitions follow [4] and [1], and these papers should be consulted for more details.

2.1.1 Hecke operators

Let $\Gamma_0(N)$ be the subgroup of matrices in $SL_n(\mathbb{Z})$ whose first row is congruent to $(*, 0, \ldots, 0)$ modulo N. Define S_N to be the subsemigroup of integral matrices in $\mathrm{GL}_n(\mathbb{Q})$ satisfying the same congruence condition and having positive determinant relatively prime to N.

If we let $\mathcal{H}(N)$ be the $\bar{\mathbb{F}}_p$ algebra of double cosets $\Gamma_0(N)\backslash S_N/\Gamma_0(N)$, then $\mathcal{H}(N)$ is a commutative algebra that acts on the cohomology and homology of $\Gamma_0(N)$ with coefficients in any $\bar{\mathbb{F}}_p[S_N]$-module. We call this algebra of double cosets the Hecke Algebra and its elements Hecke operators. We single out certain Hecke operators related to diagonal matrices—namely, for a prime ℓ let $D(\ell, k)$ be the diagonal matrix with the first $n - k$ diagonal entries equal to 1 and the remaining k entries equal to ℓ. The Hecke operator (or double coset) corresponding to $D(\ell, k)$ will then be denoted by $T(\ell, k)$.

Definition 1. *Let V be an $\mathcal{H}(pN)$-module and suppose that $v \in V$ is a simultaneous eigenvector for all $T(\ell, k)$ such that $T(\ell, k)v = a(\ell, k)v$ with $a(\ell, k) \in \bar{\mathbb{F}}_p$ for all prime ℓ not dividing pN and all k between 0 and n inclusive. Let $\rho : G_{\mathbb{Q}} \to GL_n(\bar{\mathbb{F}}_p)$ be a representation unramified outside pN and assume that*

$$\sum_{k=0}^{n} (-1)^k \ell^{k(k-1)/2} a(\ell, k) X^k = \det(I - \rho(Frob_l)X)$$

for all ℓ not dividing pN. Then we say that ρ is attached to v or that v corresponds to ρ.

Note that in the definition of attached there is no explicit connection between ρ and v, except that there is a coincidence of eigenvalues and coefficients of the characteristic polynomial of the Frobenius elements. In addition, in all cases that we discuss, we will have $(N, p) = 1$.

2.1.2 Irreducible $\mathbf{GL}_n(\mathbb{F}_p)$-modules

In place of the weight in Serre's conjecture we use an irreducible $\mathrm{GL}_n(\mathbb{F}_p)$-module. Such modules are parametrized by certain n-tuples of integers.

Definition 2. *An n-tuple $(a_1, a_2, \ldots, a_n)$ of integers is said to be p-restricted if $0 \le a_n \le p-2$ and $0 \le a_i - a_{i+1} \le p-1$ for $1 \le i < n$.*

Theorem 3. *[9, p. 412] The collection of irreducible $GL_n(\mathbb{F}_p)$-modules is in one-to-one correspondence with the collection of p-restricted n-tuples.*

Definition 4. *Given a p-restricted n-tuple $(a_1, \ldots, a_n)$, we will denote the associated irreducible $GL_n(\mathbb{F}_p)$-module by $F(a_1, \ldots, a_n)$.*

We will also use an additional notation in stating the conjecture. For an n-tuple $(a_1, \ldots, a_n)$ of integers we will denote by $(a_1, \ldots, a_n)'$ the set of all n-tuples $(b_1, \ldots, b_n)$ such that $(b_1, \ldots, b_n)$ is p-restricted and $b_i \equiv a_i \pmod{p-1}$ for each i. We note that there may be several n-tuples which satisfy the condition to be in $(a_1, \ldots, a_n)'$. For example, working modulo 5, $(1, 0, 0)'$ will contain both $(1, 0, 0)$ and $(5, 4, 0)$. The set $(a_1, \ldots, a_n)'$ will contain more than one n-tuple whenever some $a_i \equiv a_{i+1} \pmod{p-1}$. The main point of this paper is to predict which elements of $(a_1, \ldots, a_n)'$ will satisfy the conjecture of Ash and Sinnott in certain cases. We will often denote by $F(a_1, \ldots, a_n)'$ the set of irreducible modules corresponding to n-tuples in $(a_1, \ldots, a_n)'$.

Definition 5. *A resolution of $(a_1, \ldots, a_n)'$ is any n-tuple $(b_1, \ldots, b_n)$ which is one of the n-tuples contained in $(a_1, \ldots, a_n)'$. A resolution of $F(a_1, \ldots, a_n)'$ is any module contained in $F(a_1, \ldots, a_n)'$.*

2.1.3 Level and nebentype

For a fixed prime q, fix an embedding of $G_{\mathbb{Q}_q} \to G_{\mathbb{Q}}$, and let $G_{q,i}$ be the resulting lower numbering filtration of ramification subgroups. With this notation, $G_{q,0}$ is an inertia group of q, and $G_{q,i}$ with $i > 0$ are wild ramification subgroups. We will often denote $G_{q,0}$ by I_q.

Given a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{F}}_p)$, we let $M = \bar{\mathbb{F}}_p^n$ be acted on by $G_{\mathbb{Q}}$ via ρ in the natural way. We define $g_{q,i} = |\rho(G_{q,i})|$. Then set

$$n_q = \sum_{i=0}^{\infty} \frac{g_{q,i}}{g_{q,0}} \dim M/M^{G_{q,i}}.$$

Note that this sum is finite, since eventually the images under ρ of the ramification groups are trivial. In addition, by the same reasoning used in [15] for two-dimensional representations, each n_q is a nonnegative integer, and $n_q = 0$ for all but finitely many primes q.

Definition 6. *With ρ as above, we define the level of ρ to be*

$$N(\rho) = \prod_{q \neq p} q^{n_q}$$

where the product runs over all primes q not equal to p.

To define the nebentype we factor $\det \rho = \omega^k \epsilon$, where ω is the cyclotomic character modulo p and $\epsilon : G_{\mathbb{Q}} \to \bar{\mathbb{F}}_p^{\times}$ is a character which is unramified at p. By class field theory, we may consider ϵ as a character

$$\epsilon : (\mathbb{Z}/N(\rho)\mathbb{Z})^{\times} \to \bar{\mathbb{F}}_p^{\times}$$

and then pull it back to S_N via

$$S_N \to (\mathbb{Z}/N(\rho)\mathbb{Z})^{\times} \to \bar{\mathbb{F}}_p^{\times},$$

where the first map takes a matrix in S_N to its (1,1) entry. We then define $\mathbb{F}_{\epsilon}$ to be the one-dimensional space $\bar{\mathbb{F}}_p$ considered as an S_N-module with the action given by ϵ.

Finally, if V is a $\mathrm{GL}_n(\mathbb{F}_p)$-module we define

$$V(\epsilon) = V \otimes \mathbb{F}_{\epsilon}.$$

2.2 The conjecture

We now state a version of the conjecture given by Ash and Sinnott [4]. Note that their conjecture is stronger than what is stated here, in that it deals not only with irreducible representations, but also with reducible representations.

Conjecture 7. *Let $\rho : G_{\mathbb{Q}} \to GL_n(\bar{\mathbb{F}}_p)$ be a continuous irreducible representation such that if p is odd, the image of complex conjugation is conjugate to a diagonal matrix with alternating 1's and (-1)'s on the diagonal. Assume that we can conjugate ρ so that*

$$\rho|_{I_p} = \begin{pmatrix} \omega^{a_1} & * & \cdots & * \\ & \omega^{a_2} & \cdots & * \\ & & \ddots & * \\ & & & \omega^{a_n} \end{pmatrix}.$$

Let N be the level of ρ and ϵ the nebentype, as defined above. Then for some resolution $(b_1, \ldots, b_n)$ of $(a_1 - (n-1), a_2 - (n-2), \ldots, a_{n-1} - 1, a_n)'$, and

$$V = F(b_1, \ldots, b_n)$$

ρ is attached to a cohomology eigenclass in

$$H^*(\Gamma_0(N), V(\epsilon)).$$

For evidence supporting this conjecture see [4] and [1]. Note that requiring $\rho|_{I_p}$ to have powers of the cyclotomic character on the diagonal when upper triangularized limits us to *niveau* one Galois representations. Higher *niveau* Galois representations are not considered in this paper. In addition, we remark that for $p = 2$, there is no condition on the image of complex conjugation.

3 Refining the conjecture

We now give a refinement of the conjecture. This refinement allows us to predict which of the several possible weights given by the prime notation actually yield an eigenclass, rather than making the statement that at least one of several weights works. The refinement is derived from Serre's conjecture for two-dimensional representations and we will computationally test it for three-dimensional representations.

Let V be an n-dimensional $\bar{\mathbb{F}}_p$-vector space and let I_p act on V via ρ. Since $\rho|_{I_p}$ is upper-triangularizable, we may choose a basis $\{v_i\}_{1\leq i\leq n}$ with respect to which ρ has the form stated in the conjecture. Now, since $\rho|_{I_p}$ is upper triangular with respect to the basis $(v_1,\ldots,v_n)$, I_p acts on the space $V_i = \mathrm{span}(v_1,\ldots,v_i)$. For convenience, we will set V_0 to be the subspace of V consisting of only the zero vector. Now we have an I_p-stable filtration

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V.$$

Define $W_i = V_{i+1}/V_{i-1}$. Then I_p acts on W_i via ρ, and with respect to a basis consisting of the images of v_i and v_{i+1} in W_i the action of I_p on W_i is given by the two-dimensional representation

$$\rho_i = \begin{pmatrix} \omega^{a_i} & * \\ 0 & \omega^{a_{i+1}} \end{pmatrix}.$$

In the case where $a_i \not\equiv a_{i+1}+1 \pmod{p-1}$ the prime notation will not give multiple possibilities for the weights, and Conjecture 5 does not need to be refined. In the case where $a_i \equiv a_{i+1}+1 \pmod{p-1}$ we distinguish between three cases: ρ_i may be tamely ramified, *peu ramifiée*, or *très ramifiée*, according to the definitions of Serre [15, pg. 186]. We then choose an n-tuple $(b_1, b_2, \ldots, b_n)$ which is p-restricted, equal to $(a_1-(n-1), a_2-(n-2), \ldots, a_{n-1}-1, a_n)'$, and subject to the condition that

$$b_i - b_{i+1} = \begin{cases} p-1 & \text{if } \rho_i \text{ is } \textit{très ramifiée}; \\ \text{unrestricted} & \text{if } \rho_i \text{ is not } \textit{très ramifiée}. \end{cases} \tag{1}$$

Note that the case in which ρ_i is not *très ramifiée* includes both the *peu ramifiée* case and the case in which ρ_i is tamely ramified at p. We then replace the predicted weight(s) in the conjecture, namely

$$F(a_1-(n-1), a_2-(n-2), \ldots, a_{n-1}-1, a_n)'$$

by any

$$F(b_1, b_2, \ldots, b_n)$$

satisfying our more stringent requirement. Our conjecture is then:

Conjecture 8. *Let $\rho : G_{\mathbb{Q}} \to GL_n(\bar{\mathbb{F}}_p)$ be a continuous irreducible representation such that if p is odd, the image of complex conjugation is conjugate to a* *diagonal matrix with alternating 1's and (-1)'s on the diagonal. Assume that we can conjugate ρ so that*

$$\rho|_{I_p} = \begin{pmatrix} \omega^{a_1} & * & \cdots & * \\ & \omega^{a_2} & \cdots & * \\ & & \ddots & * \\ & & & \omega^{a_n} \end{pmatrix}.$$

Let N be the level of ρ and ϵ the nebentype, as defined above. Then for those resolutions $(b_1, b_2, \ldots, b_n)$ of $(a_1-(n-1), a_2-(n-2), \ldots, a_{n-1}-1, a_n)'$ satisfying condition (1) above, ρ is attached to a cohomology eigenclass in

$$H^*(\Gamma_0(N), F(b_1, \ldots, b_n)(\epsilon)).$$

We note [4, pg. 3] that for irreducible three-dimensional ρ we can show that if ρ is attached to any cohomology eigenclass, then it is attached to an eigenclass appearing in H^3. Hence, in our computational examples we just compute H^3 using the techniques of [1, Section 8]. In addition, it is easy to see that for irreducible two-dimensional ρ the refined conjecture is just the *niveau* one case of Serre's conjecture [15].

4 Computing wild ramification

We will use the following theorem to compute the depth of certain wild ramification filtrations:

Theorem 9. *Let p be a rational prime and let $L/\mathbb{Q}$ be a degree p extension of number fields with Galois closure $K/\mathbb{Q}$. Suppose that p is wildly ramified in $L/\mathbb{Q}$. Let $n = v_p(\Delta_{L/\mathbb{Q}})$. Let $g_{p,i}$ be the order of the image of $G_{p,i}$ in $\mathrm{Gal}(K/\mathbb{Q})$ under the standard projection from $G_{\mathbb{Q}}$ to $\mathrm{Gal}(K/\mathbb{Q})$. Then there are integers d and t such that*

$$g_{p,i} = \begin{cases} pt & \text{if } i = 0 \\ p & \text{if } 0 < i \le d \\ 1 & \text{if } i > d \end{cases},$$

with $n = (p-1)(1 + d/t)$ and $(d, t) = 1$.

Proof. See [10]. □

We note that this theorem allows us to determine the depth of the filtration of wild ramification subgroups just by examining the discriminant of an extension.

We next prove a theorem which indicates a relationship between the depth of the ramification filtration of the field cut out by a Galois representation and the type of wild ramification (*peu* or *très ramifiée*) occurring in that representation.

Theorem 10. *Let I_p be an inertia group above p in $G_{\mathbb{Q}_p}$ and let $\rho : I_p \to GL_2(\mathbb{F}_p)$ be a wildly ramified continuous representation of the form $\begin{pmatrix} \omega^{a+1} & * \\ & \omega^a \end{pmatrix}$.*

Then ρ cuts out a totally ramified Galois extension K of $\mathbb{Q}_p^{nr}$. If the ramification filtration of $K/\mathbb{Q}_p^{nr}$ has depth 1, then ρ is peu ramifiée. If the filtration has depth greater than 1, then ρ is très ramifiée.

Proof. Note that since ρ is wildly ramified, the $*$ in the upper right corner must be nonzero. Let v_K be the valuation of K, normalized so that a uniformizer of K has valuation 1. Set $K_0 = \mathbb{Q}_p^{nr}$ and let K_t be the maximal tamely ramified subextension of K/K_0. Then K_t/K_0 has degree $p-1$, and we see that $K_t = K_0(\zeta_p)$, where ζ_p is a primitive pth root of 1. We see easily that the degree of K/K_0 is $p(p-1)$. Also, from exercise 3 (page 72) of [14], we see that the depth of the ramification filtration of K/K_0 is at most p. The action of tame ramification on wild ramification [14, IV, §2, Prop. 9] forces the depth of the filtration to be either 1 or p.

Suppose that K/K_0 (and hence ρ) is *peu ramifiée*. Then from [15] we see that $K = K_t(x^{1/p})$ for some $x \in K_0$ with $v_p(x) \equiv 0 \pmod p$. Multiplying x by a power of a uniformizer we see that we may take $v_p(x) = 0$. Now $v_K(x^{1/p}) = 0$, so that for a nonidentity element $\sigma \in \mathrm{Gal}(K/K_t)$

$$v_K(x^{1/p} - \sigma(x^{1/p})) = v_K(x^{1/p}) + v_K(1 - \zeta_p^m) = 0 + p = p,$$

where $\zeta_p^m = \sigma(x^{1/p})/x^{1/p}$. Hence, $v_K(x^{1/p} - \sigma(x^{1/p})) < p+1$ so the pth ramification group of the extension K/K_0 is not all of $\mathrm{Gal}(K/K_t)$. Therefore, the pth ramification group is trivial, so the depth of the ramification filtration of K/K_0 is 1.

On the other hand, suppose that K/K_0 is *très ramifiée*. Then $K = K_t(x^{1/p})$ for some $x \in K_0$ such that $v_p(x) = n \not\equiv 0 \pmod p$. Choose a positive $k < p$ such that $nk \equiv 1 \pmod p$, and note that $K_t(x^{1/p}) = K_t((x^k)^{1/p})$. Adjusting by a pth power of a uniformizer of K_0, we may then take x to be a uniformizer of K_0.

We now set $\pi = (1-\zeta_p)^p/x \in K_t$. Note that π is a uniformizer of K_t, and that $K_t(\pi^{1/p}) = K_t(x^{1/p})$. However, by exercise 4(c), pg. 72 of [14], we then see that the depth of the ramification filtration is p, which is greater than 1. $\square$

We note that the combination of Theorems 9 and 10, together with the fact that an unramified base change does not affect the ramification filtration, allows us to determine whether ρ is *très ramifiée* merely by studying the discriminant of the extension cut out by ρ. We will give a number of examples. Note that all number field calculations in the examples which follow were carried out using the GP/PARI software package [17].

5 A tamely ramified example

Let $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^4 - x^3 + 6x^2 - 6x + 1$, and let L be the Galois closure of K. Then $\mathrm{Gal}(L/\mathbb{Q}) \cong S_4$, and we note that $L/\mathbb{Q}$ is ramified at 5 with ramification index 4, and at 103 with ramification index 2. One sees easily that the inertia group at 103 is generated by a two-cycle.

Let φ be the three-dimensional mod 5 representation of S_4 over $\mathbb{F}_5$ for which transpositions have trace 1. We may then define ρ to be the composition of the canonical projection $G_{\mathbb{Q}} \to \mathrm{Gal}(L/\mathbb{Q}) \cong S_4$ and φ. We see that since four-cycles have trace -1,

$$\rho|_{I_5} \sim \begin{pmatrix} \omega^3 & & \\ & \omega^2 & \\ & & \omega^1 \end{pmatrix}.$$

The level of ρ is 103 and the nebentype is the quadratic character ϵ_{103} ramified only at 103 (since the inertia at 103 is generated by a transposition). Our conjecture predicts weights of $F(1,1,1)'$ and, since there is no wild ramification (hence neither ρ_i is *très ramifiée*), we predict that all four resolutions should work. In fact, computations in weights $F(1,1,1)$, $F(5,1,1)$, $F(5,5,1)$, and $F(9,5,1)$ show that (at least for $\ell < 50$) the correct eigenvalues of $T(\ell,1)$ and $T(\ell,2)$ exist in the appropriate cohomology group.

We may also adjust the order of the characters on the diagonal of ρ. Hence we have

$$\rho|_{I_5} \sim \begin{pmatrix} \omega^1 & & \\ & \omega^3 & \\ & & \omega^2 \end{pmatrix} \text{ and } \rho|_{I_5} \sim \begin{pmatrix} \omega^2 & & \\ & \omega^1 & \\ & & \omega^3 \end{pmatrix},$$

yielding predicted weights of $F(3,2,2)'$ and $F(0,0,3)'$. The resolutions of $F(3,2,2)'$ are $F(3,2,2)$ and $F(7,6,2)$, and the resolutions of $F(0,0,3)'$ are $F(4,4,3)$ and $F(8,4,3)$. Since there is no wild ramification the revised conjecture predicts that in both cases, both predicted weights should work. In fact, computations show that these four weights all yield cohomology eigenclasses with the correct eigenvalues (for $\ell < 50$) to have ρ attached.

Other permutations of the diagonal characters yield three more predictions for weights, namely $F(4,2,1)$, $F(5,4,2)$, and $F(7,5,3)$, none of which involve the ambiguity in which we are interested. Computations show that these weights also yield cohomology eigenclasses with the correct eigenvalues (for $\ell < 50$) to have ρ attached.

6 Computational examples with image isomorphic to S_5

We begin by exhibiting a subgroup of $\mathrm{GL}_3(\mathbb{F}_5)$ which is isomorphic to S_5. This subgroup is generated by

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 4 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 3 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 2 & 3 \\ 4 & 4 & 1 \\ 4 & 0 & 3 \end{pmatrix}$$

We note that A and B satisfy the relations $A^5 = B^4 = I$ and $BAB^{-1} = A^2$, so that A and B generate a Frobenius group of order 20. In addition, S_5 is isomorphic to the subgroup of $\mathrm{GL}_3(\mathbb{F}_5)$ generated by A, B, and C, so we may define an injection $\varphi : S_5 \to \mathrm{GL}_3(\mathbb{F}_5)$ via this isomorphism.

Let $f(x) \in \mathbb{Z}[x]$ be an irreducible degree five polynomial with Galois group S_5. Let $\alpha \in \mathbb{C}$ be a root of f, let $K = \mathbb{Q}(\alpha)$, and let L be a splitting field of f over $\mathbb{Q}$. We then get a continuous homomorphism

$$\rho : G_{\mathbb{Q}} \to \mathrm{Gal}(L/\mathbb{Q}) \cong S_5 \xrightarrow{\varphi} \mathrm{GL}_3(\mathbb{F}_5).$$

Assume now that $L/\mathbb{Q}$ is wildly ramified at 5. Then, up to conjugation, the image of an inertia group above 5 is contained in the subgroup of $\mathrm{GL}_3(\mathbb{F}_5)$ generated by A and B. By choosing the appropriate place above 5 we eliminate the ambiguity and say that the subgroup generated by A and B contains the image of inertia.

Suppose now that the inertia group above 5 in $L/\mathbb{Q}$ has order 20. Then it is a Frobenius group generated by σ of order 4 and τ of order 5 (where σ and τ correspond respectively to B and A), with $\langle\tau\rangle \lhd \langle\sigma, \tau\rangle$. Hence, $\sigma\tau\sigma^{-1} = \tau^k$ for some integer k. If we let d be the depth of the ramification filtration, we see easily [14, 10] that $\sigma\tau\sigma^{-1} = \tau^{\omega(\sigma)^d}$. Now since $BAB^{-1} = A^2$, we see that $\omega(\sigma)^d = 2$. We then note that

$$\rho|_{I_5} \sim \begin{pmatrix} \omega^d & * & * \\ & 1 & * \\ & & \omega^{-d} \end{pmatrix}.$$

There are now three cases possible. We could have $d = 1, 3$, or 5. If $d = 1$ or 5, then the conjecture of Ash and Sinnott predicts that at least one of the resolutions of $F(-1,-1,-1)' = F(3,3,3)'$ will work, or in other words, that at least one of the four weights $F(3,3,3)$, $F(7,3,3)$, $F(7,7,3)$ and $F(11,7,3)$ will yield the correct eigenvalues. On the other hand, if $d = 3$, the conjecture predicts a weight of $F(1,-1,1)' = F(5,3,1)$. Note that in the $d = 3$ case there is no ambiguity in the weight.

Now, in the $d = 1$ or 5 cases we need to examine the local subrepresentations. Let ρ_1 and ρ_2 be the two representations described in section 3 constructed from ρ. Then we see that

$$\rho_1(\tau) = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \quad \rho_1(\sigma) = \begin{pmatrix} 2 & 4 \\ & 1 \end{pmatrix}$$

and

$$\rho_2(\tau) = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \quad \rho_2(\sigma) = \begin{pmatrix} 1 & 3 \\ & 3 \end{pmatrix}.$$

Hence, we see that the image of inertia under both ρ_1 and ρ_2 has order 20. Further, it is easy to see that $\ker \rho|_{I_5} \subseteq \ker \rho_i$, so that the fixed field of ρ_i is contained in the fixed field of $\rho|_{I_5}$. From these two facts we may deduce that the ramification filtration of ρ_i is identical to that of ρ and, in fact, is identical to the filtration of ramification subgroups in $L/\mathbb{Q}$. This filtration is easy to compute by Theorem 9. If the discriminant of K is exactly divisible by 5^5 then $d = 1$, and each ρ_i is *peu ramifiée*. If the discriminant of K is divisible by 5^9 then $d = 5$ and each ρ_i is *très ramifiée*. In the *peu ramifiée* case the refined conjecture predicts that all four of the weights $F(3,3,3), F(7,3,3), F(7,7,3)$ and $F(11,7,3)$ should contain eigenvalues corresponding to ρ. In the *très ramifiée* case the only one of these weights that should contain the correct eigenvalues is $F(11,7,3)$. We proceed to give examples of each of these cases.

Example 11. Let $f(x) = x^5 - 80x + 160 \in \mathbb{Q}[x]$, let α be a root of f, and let $K = \mathbb{Q}(\alpha)$. The discriminant of $K/\mathbb{Q}$ is $5^5 41$ and the Galois group of f is S_5. Hence, f yields an S_5-extension as above with $d = 1$. One checks easily that the level associated to ρ is 41^2, and the nebentype is trivial. This level is too large to allow us to compute the relevant cohomology, so we twist ρ by the quadratic character ϵ_{41} ramified only at 41. Then $\rho \otimes \epsilon_{41}$ has level 41 and nebentype ϵ_{41}. Note that since ϵ_{41} is trivial on inertia at 5 this twist does not affect the predicted weights. Hence, eigenvalues corresponding to ρ should exist in the cohomology in the four weights predicted above. Computation with these weights, level 41, and nebentype ϵ_{41} shows that (at least for $\ell < 50$), these eigenvalues do appear.

Example 12. Let $f(x) = x^5 - 25x^2 + 55$, let α be a root of f, and let $K = \mathbb{Q}(\alpha)$. Then the discriminant of $K/\mathbb{Q}$ is $-5^9 11$, so that $d = 5$ and we are in the *très ramifiée* case. The level of ρ is easily seen to be 11^2, and its nebentype is trivial. Twisting as above, we see that $\rho \otimes \epsilon_{11}$ has level 11 and nebentype ϵ_{11}. The refined conjecture then indicates that the correct eigenvalues should appear in the cohomology with weight $F(11,7,3)$, level 11, and nebentype ϵ_{11}, but not in the cohomology for the other weights permitted by Ash and Sinnott. Computation shows that (for $\ell < 50$) this is the case.

In Table 1 we give several examples of Galois representations, along with cohomology calculations that support the conjecture. Most of the polynomials defining these representations were obtained from the online tables of Jones and Roberts [12]. Each row of the table contains a quintic polynomial defining an S_5-extension of $\mathbb{Q}$. The Galois representations that we study are constructed as above, by composing the natural projection of $G_\mathbb{Q}$ onto S_5 defined by the polynomial with the given three-dimensional representation. In some cases, the level of this Galois representation is lowered by twisting by a character, as in Example 9. In all such cases, the nebentype of the twisted representation is the same as the character by which the representation was twisted—this character is indicated in the column labeled $\epsilon(\rho)$. The discriminant of the S_5-extension (which allows us to predict the weights) and the level of the final Galois representation are also indicated. Finally, we list the weights predicted by the refined conjecture. With four exceptions (each denoted by an asterisk), computations show that all the weights listed in the table work; namely, in that cohomology with that weight and the corresponding level and nebentype the appropriate eigenvalues exist (for $\ell < 50$) to correspond to the given Galois representation. The exceptions are not counterexamples to the conjecture—they are merely examples for which the size of the cohomology calculations exceeded our available computer resources. We include them because the weights with which we were able to calculate give additional evidence that the smaller resolution of the prime notation does work in the *peu ramifiée* case. We note also that in the *très*

Δ_K	$N(\rho)$	$\epsilon(\rho)$	Weights	Defining polynomial
$5^5 41$	41	ϵ_{41}	$F(3,3,3), F(7,3,3)$ $F(7,7,3), F(11,7,3)$	$x^5 - 80x + 160$
$5^5 73$	73	ϵ_{73}	$F(3,3,3), F(7,3,3)$ $F(7,7,3), F(11,7,3)$	$x^5 + 40x + 5$
$5^5 13^3$	13^2	1	$F(3,3,3), F(7,3,3)$ $F(7,7,3), F(11,7,3)^*$	$x^5 + 5x^3 - 15x^2 - 15x - 49$
$5^5 17^4$	17^2	1	$F(3,3,3), F(7,3,3)^*$ $F(7,7,3)^*, F(11,7,3)^*$	$x^5 - 85x - 153$
$5^9 2^2$	2^2	1	$F(11,7,3)$	$x^5 + 25x - 10$
$5^9 3^4$	3^2	1	$F(11,7,3)$	$x^5 + 75x + 105$
$5^9 7^2$	7	ϵ_7	$F(11,7,3)$	$x^5 - 100x^2 - 100x - 55$
$5^9 7^4$	7^2	1	$F(11,7,3)$	$x^5 - 175x^2 - 1050x - 3640$
$-5^9 11$	11	ϵ_{11}	$F(11,7,3)$	$x^5 - 25x^2 + 55$
$5^9 17^2$	17	ϵ_{17}	$F(11,7,3)$	$x^5 - 50x^2 + 100x - 65$

Table 1: S_5-representations with predicted weights and levels

ramifiée cases weights permitted by the conjecture of Ash and Sinnott, but not predicted by the refined conjecture, do not yield eigenvalues corresponding to the given representation.

7 Computational examples arising from elliptic curves

Three-dimensional Galois representations can also be obtained as adjoint representations of torsion-point representations on elliptic curves. We do one example in detail and specify the curve and computational results for several other examples.

Let E be the elliptic curve defined by the equation

$$y^2 + xy = x^3 - 4x - 1.$$

This curve has conductor 21 [6]. Let $\varphi : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_7)$ be a seven-division-point representation, and let $L/\mathbb{Q}$ be the fixed field of φ. We note that E has multiplicative reduction at both 3 and 7, hence, by [8, Prop. 2.12] and [16, Prop. V.6.1], we see that

$$\varphi|_{I_7} \sim \begin{pmatrix} \omega & * \\ & 1 \end{pmatrix}$$

and

$$\varphi|_{I_3} \sim \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix},$$

and that for both restrictions the $*$ in the upper right corner is nonzero. (Note that the seventh cyclotomic character is trivial on I_3 [8, pg. 44].)

Further, by [13, Cor. 1, pg. 308] we see that the image of φ is isomorphic to all of $GL_2(\mathbb{F}_7)$.

We now let $\rho = \mathrm{Ad}^0(\varphi)$. Then $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_3(\mathbb{F}_7)$ is a Galois representation, and the image of ρ is easily seen to be isomorphic to $\mathrm{PGL}_2(\mathbb{F}_7)$.

We have that

$$\rho|_{I_7} \sim \begin{pmatrix} \omega & * & * \\ & 1 & * \\ & & \omega^{-1} \end{pmatrix}$$

and

$$\rho|_{I_3} \sim \begin{pmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{pmatrix}$$

One then checks easily that the level predicted for ρ is $3^2 = 9$ and its nebentype is trivial.

Finally, we see that the predicted weight for ρ is $F(1-2, 0-1, -1)' = F(5,5,5)'$. The conjecture of Ash and Sinnott then predicts that at least one of the four weights

$$F(5,5,5),\ F(11,5,5),\ F(11,11,5),\ F(17,11,5)$$

will yield an eigenclass corresponding to ρ. We now need to determine which of these weights are predicted by the refined conjecture.

We note that $\varphi|_{I_7}$ must be *très ramifiée*, by [8, Prop 2.12(d)] and the fact that $v_7(j_E) = -2$ is not divisible by 7. Each of the subrepresentations ρ_1 and ρ_2 can be seen to have the same kernel as the restriction of φ to inertia, so each of them must also be *très ramifiée*. Hence, we see that the only predicted weight for ρ is the weight with the larger resolution in both positions, namely $F(17,11,5)$.

Computation shows that in weight $F(17,11,5)$, level 9, and trivial nebentype, there is a unique eigenclass having the correct eigenvalues (for $\ell < 50$). On the other hand, in the other three weights no such eigenclass exists. Hence, the refinement of the conjecture of Ash and Sinnott is justified in this case.

Other examples in which similar computations work are the curves of conductor 33 and 39. These yield three-dimensional representations of level 9 modulo 11 and modulo 13 for which both ρ_1 and ρ_2 are *très ramifiée*. As above, only one of the four predicted weights yields an eigenclass with the correct eigenvalues, and in each case it is the one predicted by the refined conjecture. In the case of the representation modulo 11, the conjecture of Ash and Sinnott predicts the weights $F(9,9,9)'$ and the refined conjecture predicts the weight $F(29,19,9)$. Computation shows that the only resolution of $F(9,9,9)'$ which yields the correct eigenvalues is $F(29,19,9)$. In the case of the representation modulo 13, the predicted weights are $F(11,11,11)'$, the refined conjecture predicts that only $F(35,23,11)$ will work, and the only resolution which yields the correct eigenvalues is $F(35,23,11)$.

One may also construct similar examples which are *peu ramifiée* by using elliptic curves with good ordinary reduction at p. As examples, we begin with the elliptic curve E defined by $y^2 + y = x^3 - x^2 - 10x - 20$ of conductor 11 [6]. We choose a prime $p > 5$ for which E has good ordinary reduction and let $\varphi : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ be the p-division point representation. Then by [8, Prop. 2.11(c)],

$$\varphi|_{I_p} \sim \begin{pmatrix} \omega & * \\ & 1 \end{pmatrix}.$$

Further, E has multiplicative reduction at 11, so we see, as above, that

$$\varphi|_{I_{11}} \sim \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix},$$

with the $*$ nonzero. If we now let $\rho = \mathrm{Ad}^0(\varphi)$, then we see, as above, that

$$\rho|_{I_p} \sim \begin{pmatrix} \omega & * & * \\ & 1 & * \\ & & \omega^{-1} \end{pmatrix},$$

and that both subrepresentations ρ_1 and ρ_2 are *peu ramifiée*, since φ is. Hence, the predicted weights for ρ are all the resolutions of $F(-1,-1,-1)'$, or in other words

$$F(p-2,p-2,p-2),\ F(2p-3,p-2,p-2),\ F(2p-3,2p-3,p-2),\ F(3p-4,2p-3,p-2).$$

As in the previous examples, the level of ρ is easily seen to be 11^2, and the nebentype is trivial. Hence, we wish to find an eigenclass with the appropriate eigenvalues in $H^3(\Gamma_0(11^2), V)$, where V is any one of the four weights given above.

The curve E has good ordinary reduction at the primes 7, 13, and 17. For $p = 7$, we have checked computationally that the correct eigenvalues (for $\ell < 50$) to correspond to ρ appear in weights $F(5,5,5)$, $F(11,5,5)$, and $F(11,11,5)$. The other predicted weight, $F(17,11,5)$ is to large for us to work with. For $p = 13$ and $p = 17$, we have checked computationally that the correct eigenvalues (for $\ell < 50$) to correspond to ρ appear in weight $F(p-2,p-2,p-2)$, and the other weights are too large for us to work with. Nevertheless, these computations give evidence that in the *peu ramifiée* case at least the smallest of the resolutions works, as predicted by the refined conjecture. We remark that choosing $p = 5$ would have yielded a reducible representation [7, pg. 140], to which the refined conjecture would not apply.

We note that using the main theorem of [11], one could prove that the ρ derived here as symmetric squares of torsion point representations of elliptic curves are in some sense modular. However, it is not clear how to use this to prove the correspondence described by the refined conjecture. In [5] certain symmetric square representations are shown to be attached to cohomology eigenclasses, but the cases dealt with there are level 1 representations, and the examples given here have higher level. Hence, proving that these symmetric square representations are attached to the given cohomology eigenclasses seems to be nontrivial.

8 Conclusion

In many cases, Ash and Sinnott predict that one of several predicted weights yields a cohomology eigenclass attached to a certain Galois representation. All the computational evidence to date supports this conjecture fully. In addition, we have presented computational evidence that the refinement to Ash and Sinnott's original conjecture described in this paper correctly predicts which of these several weights actually do give rise to the correct systems of eigenvalues.

9 Acknowledgments

The author thanks David Pollack and Avner Ash for helpful conversations and advice on this paper. He also thanks the referees for their comments.

References

[1] Avner Ash, Darrin Doud, and David Pollack. Galois representations with conjectural connections to arithmetic cohomology. *Duke Math. J.*, 112(3):521–579, 2002.

[2] Avner Ash, David Pollack, and Warren Sinnott. A_6-extensions of $\mathbb{Q}$ and the mod p cohomology of $\mathrm{GL}_3(\mathbb{Z})$. *preprint*, 2003.

[3] Avner Ash, David Pollack, and Dayna Soares. $\mathrm{SL}_3(\mathbb{F}_2)$-extensions of $\mathbb{Q}$ and arithmetic cohomology modulo 2. *Experiment. Math.*, 13:297–307, 2004. to appear.

[4] Avner Ash and Warren Sinnott. An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod p cohomology of $\mathrm{GL}(n,\mathbb{Z})$. *Duke Math. J.*, 105(1):1–24, 2000.

[5] Avner Ash and P. Tiep. Modular representations of $\mathrm{GL}(3, \mathbb{F}_p)$, symmetric squares, and mod- p cohomology of $\mathrm{GL}(3, \mathbb{Z})$. *J. Algebra*, 222(2):376–399, 1999.

[6] John Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 2 edition, 2000.

[7] Henri Darmon. Serre's conjectures. In *Seminar on Fermat's Last Theorem, CMS Con. Proc. 17*, pages 135–153. American Math. Soc., Providence, 1995.

[8] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In J. Coates and S. T. Yau, editors, *Elliptic Curves, Modular Forms, and Farmat's Last Theorem*, pages 2–140. International Press, 1997.

[9] Stephen R. Doty and Grant Walker. The composition factors of $F_p[x_1, x_2, x_3]$ as a $\mathrm{GL}(3, p)$-module. *Journal of Algebra*, 147:411–441, 1992.

[10] Darrin Doud. Wild ramification in number field extensions of prime degree. *Arch. Math.(Basel)*, 81:646–649, 2003.

[11] Stephen Gelbart and Hervé Jacquet. A relation between automorphic representations of GL(2) and GL(3). *Ann. Sci. École Norm. Sup. (4)*, 11(4):471–542, 1978.

[12] John Jones and David Roberts. Tables of number fields with prescribed ramification. Online, 2001. available at `http://math.la.asu.edu/~jj/numberfields/`.

[13] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[14] Jean-Pierre Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979.

[15] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[16] Joseph Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[17] The PARI-Group, Bordeaux. *PARI/GP, Version 2.1.5*, 2000. available from `http://www.parigp-home.de`.