$SL_3(\mathbb{F}_2)$-extensions of $\mathbb{Q}$ and arithmetic cohomology modulo 2

Avner Ash[1]
Boston College
Chestnut Hill, MA 02445
Avner.Ash@bc.edu

David Pollack
Wesleyan University
Middletown, CT 06457
dpollack@wesleyan.edu

Dayna Soares[1]
University of North Carolina
Durham, NC 27708
dsoares@email.unc.edu

May 5, 2004

1 Abstract

We generate extensions of $\mathbb{Q}$ with Galois group $SL_3(\mathbb{F}_2)$ giving rise to three-dimensional mod 2 Galois representations with sufficiently low level to allow the computational testing of a conjecture of Ash, Doud, Pollack, and Sinnott relating such representations to mod 2 arithmetic cohomology. We test the conjecture for these examples and offer a refinement of the conjecture that resolves ambiguities in the predicted weight.

2 Introduction and statement of the conjecture

The purpose of this paper is to test the main conjecture of [2] in characteristic 2. This conjecture (which we will refer to as the Ash-Doud-Pollack-Sinnott or ADPS conjecture) asserts the existence of Hecke cohomology eigenclasses in the mod p cohomology of certain arithmetic subgroups of GL_n attached to n-dimensional mod p representations of the absolute Galois group of $\mathbb{Q}$. The conjecture essentially boils down to Serre's conjecture if $n = 2$. In [2] the conjecture was tested in hundreds of three-dimensional examples with p an odd prime. Because the computer programs at that time couldn't handle it, the case of $p = 2$ was not treated in that paper.

[1]The first and third authors wish to thank the National Science Foundation for support of this research through NSF grant number DMS-0139287.

In an earlier paper [3], mod 2 cohomology was computed for GL_3 up to level 151, but only for trivial coefficient modules. All the Galois representations into $SL_3(\mathbb{F}_2)$ attached to these cohomology eigenclasses which we were able to find at that time had reducible image. Until the research reported upon here, it was an open question whether this would always be the case, at least for trivial coefficients. We now see that levels up to 151 were simply too small to provide examples of Galois representations with image $SL_3(\mathbb{F}_2)$.

In the current paper we restrict ourselves to Galois representations whose image is the full group $SL_3(\mathbb{F}_2)$. To generate examples of such representations, we searched through parameterized families of polynomials with Galois group equal to $SL_3(\mathbb{F}_2)$ (referred to from now on as $SL_3(\mathbb{F}_2)$-polynomials) published by Malle [6] to find those for which the ADPS conjecture predicts a corresponding Hecke cohomology class with a level small enough to allow feasible computations. In practice, this meant keeping the level below 500. To do this, we excluded representations that were wildly ramified outside 2.

In the end we tested 27 polynomials, including 7 that were suggested by the referee. Our results are tabulated in section 6 below. Concisely, one may say that the ADPS conjecture was again vindicated by the experimental evidence. In particular, we shall see that cohomology classes with trivial coefficients can be attached to irreducible $SL_3(\mathbb{F}_2)$-representations.

We now give the the precise setup of the ADPS conjecture in the special case of a Galois representation with irreducible image in $GL_n(\mathbb{F}_2)$:

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 $GL_n(\mathbb{Q})$ satisfying the same congruence condition and having positive determinant relatively prime to N.

Let $\mathcal{H}(N)$ denote the $\bar{\mathbb{F}}_2$-algebra of double cosets $\Gamma_0(N)S_N\Gamma_0(N)$. Then $\mathcal{H}(N)$ is a commutative algebra which acts on the cohomology and homology of $\Gamma_0(N)$ with coefficients in any $\bar{\mathbb{F}}_2[S_N]$ module. When a double coset is acting on cohomology or homology, we call it a Hecke operator. Clearly, $\mathcal{H}(N)$ contains all double cosets of the form $\Gamma_0(N)D(\ell,k)\Gamma_0(N)$, where ℓ is a prime not dividing N, $0 \le k \le n$, and

$$D(\ell,k) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \ell & & \\ & & & & \ddots & \\ & & & & & \ell \end{pmatrix}$$

is the diagonal matrix with the first $n-k$ diagonal entries equal to 1 and the last k diagonal entries equal to ℓ. When we consider the double coset generated by $D(\ell,k)$ as a Hecke operator, we call it $T(\ell,k)$.

Definition 1. *Let V be an $\mathcal{H}(2N)$-module, and suppose that $v \in V$ is a simultaneous eigenvector for all $T(\ell,k)$ and that $T(\ell,k)v = a(\ell,k)v$ with $a(\ell,k) \in \bar{\mathbb{F}}_2$*

for all $\ell \nmid 2N$ *prime and all* $0 \leq k \leq n$. *If*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{F}}_2)$$

is a representation unramified outside $2N$, *and*

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

for all $\ell \nmid 2N$, *then we say that* ρ *is attached to* v *(or that* v *corresponds to* ρ*).*

Now let

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{F}}_2)$$

be a continuous irreducible representation. We will define a level associated to ρ exactly as Serre does in [7].

For each prime $q \neq 2$ fix an embedding of $G_{\mathbb{Q}_q}$ into $G_{\mathbb{Q}}$ as the decomposition group of a prime above q and, for $i \geq 0$, let $g_i = |\rho(G_{q,i})|$ where the $G_{q,i}$ are the ramification subgroups of $G_{\mathbb{Q}_q}$ with the lower numbering. Let M be an n-dimensional $\bar{\mathbb{F}}_2$-vector space and choose a basis of M so that $G_{\mathbb{Q}}$ acts on M via ρ in the natural way. Define

$$n_q = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \dim M/M^{\rho(G_{q,i})}.$$

The sum defining n_q is actually a finite sum, since eventually the $\rho(G_{q,i})$ are trivial.

Definition 2. *With* ρ *as above, define the level*

$$N(\rho) = \prod_{q \neq 2} q^{n_q}.$$

Note that this product is actually finite, since ρ is ramified at only finitely many primes and n_q is 0 at primes where ρ is unramified.

Before stating the conjecture, we note that there are exactly four irreducible representations of $\mathrm{GL}_3(\mathbb{F}_2)$ over $\bar{\mathbb{F}}_2$. These are the trivial representation, the three-dimensional standard representation and its dual, and the eight-dimensional Steinberg representation. When thought of as restrictions to $\mathrm{GL}_3(\mathbb{F}_2)$ of highest weight representations of $\mathrm{GL}_3(\bar{\mathbb{F}}_2)$ these are the representations with highest weights $(0,0,0), (1,0,0), (1,1,0)$, and $(2,1,0)$ respectively. We denote the representation with highest weight (a,b,c) by $F(a,b,c)$.

We may now state the ADPS conjecture for $p = 2$ where the image of ρ is $\mathrm{SL}_3(\mathbb{F}_2)$:

Conjecture 1. *Let* $\rho : G_{\mathbb{Q}} \to \mathrm{SL}_3(\mathbb{F}_2)$ *be a continuous surjective Galois representation. Further, let* $N = N(\rho)$ *be the level of* ρ. *Then for at least one irreducible representation* V *of* $\mathrm{GL}_3(\mathbb{F}_2)$, ρ *is attached to a cohomology eigenclass in* $H^*(\Gamma_0(N), V)$.

Given a Galois representation ρ, the full ADPS conjecture predicts not only a level but also a nebentype character and a collection of weights (i.e. irreducible coefficient modules). When ρ takes values over $\mathbb{F}_2$, however, the nebentype is automatically trivial, and the weight is completely undetermined because of the ambiguity of the "prime" notation (see [2] for the definitions of nebentype and "prime" notation, which we will not need again in this paper.) Below we discuss which weights are observed to provide the predicted cohomology, and we refine the conjecture in this context.

In practice, we can only check the equality of Hecke and characteristic polynomials that is required by the definition of "attached" for primes ℓ up to some bound. For this paper we checked all $\ell \leq 47$. When these polynomials coincide for all $\ell \leq 47$ we shall say that the Galois representation "appears" to be attached to the Hecke cohomology eigenclass.

Our paper is organized as follows: In section 3 we present our predictions regarding which of the four weights to expect for a given Galois representation. In section 4 we discuss Malle's parametrized families of $\mathrm{SL}_3(\mathbb{F}_2)$-polynomials and how we sifted through them to find ones that predicted small levels. In section 5 we discuss the methods used to compute the mod 2 arithmetic cohomology for $\Gamma_0(N) \subset \mathrm{GL}_3(\mathbb{Z})$. In section 6 we present our results.

We thank John Jones and David Roberts for providing their very useful local fields calculator and especially David Roberts for help in interpreting its output. We are also grateful to Gunter Malle for assistance in locating families of $\mathrm{PSL}_2(\mathbb{F}_7)$-polynomials and to Darrin Doud for his careful proofreading. Finally, it is a pleasure to thank the referee for pointing out how to simplify the computation of the level with Theorem 2 and for providing additional number fields on which to test our conjecture.

3 Refining the weight prediction

Given a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{SL}_3(\bar{\mathbb{F}}_2)$, the ADPS conjecture does not predict for which of the four possible weights we should find a corresponding Hecke eigenclass. After reviewing about half the data from our calculations, we saw how to adapt Serre's discussion of peu ramifée vs. très ramifée from [7] to refine the ADPS conjecture in the special case $\rho : G_{\mathbb{Q}} \to \mathrm{SL}_3(\mathbb{F}_2)$ to predict exactly which weights to expect, depending only on $\rho|I_2$. This refinement then correctly predicted the weights for the remaining data. There are, nonetheless, some cases of the refinement that did not occur in our data. We indicate which these are in our discussion below–our predictions for these cases remain unsupported guesses.

Let's arrange the four possible weights in a diamond pattern:

$$F(2,1,0)$$

$$F(1,1,0) \qquad F(1,0,0)$$

$$F(0,0,0)$$

Note that the two weights in the middle are isomorphic under the outer automorphism τ of $\mathrm{SL}_3(\mathbb{F}_2)$ given by the composition of transpose-inverse and the long Weyl element. (So τ preserves the Borel subgroup of upper triangular matrices.) The other two weights are self-dual. We set $\rho^\tau = \tau \circ \rho$.

It follows from a duality result [2, Theorem 3.10] that if either representation ρ or ρ^τ is attached to a cohomology class with weight $F(0,0,0)$ or $F(2,1,0)$ then the other representation is as well. Likewise if ρ or ρ^τ is attached to a cohomology class with weight $F(1,0,0)$ then the other representation is attached to a class with weight $F(1,1,0)$, and conversely.

When our refined conjecture predicts any weight it also predicts all the weights above it in the diamond. This seems to leave us with four possible sets of weights. Two of these, however, cannot be distinguished without differentiating between ρ and ρ^τ. While this can be achieved by comparing the traces of images of elements of order 7 in $G_\mathbb{Q}$, it would require making explicit our choice of ρ. Rather than do this (say by looking at actual permutations of the roots of the $\mathrm{SL}_3(\mathbb{F}_2)$-polynomial defining ρ) we consider ρ and ρ^τ together and make one of the following three predictions:

- I Both ρ and ρ^τ have a class attached with every possible weight.
- II ρ has a class attached with weight $F(1,0,0)$ or $F(1,1,0)$ and ρ^τ has a class attached with the other weight. Both ρ and ρ^τ have a class attached with weight $F(2,1,0)$.
- III ρ and ρ^τ have a class attached with weight $F(2,1,0)$.

We explain below how to predict I, II, or III based on $\rho|_{I_2}$. In each case we've tested, the weights we've predicted turn out to be precisely those which have classes with the corresponding ρ or ρ^τ attached. In a number of cases these classes appeared with multiplicity greater than 1, but we have no explanation for this.

Recall that the niveau of ρ is defined to be the smallest integer m such that ρ on tame inertia factors through $\bar{\mathbb{F}}_2^\times \to \mathbb{F}_{2^m}^\times$. In our case, if the ramification index e of the prime 2 in the fixed field of the kernel of ρ factors as $2^b t$, with t odd, then the niveau is 1,2,3 when t is 1,3,7 respectively.

The representation ρ has niveau 1 if and only if $\rho(I_2)$ is a 2-group. If ρ does not have niveau 1 we predict case I. If ρ does have niveau 1 we will base our prediction on the nature of the ramification of certain quadratic extensions associated to ρ.

Let $E/\mathbb{Q}_2$ be an unramified extension, and let $E(\sqrt{b})/E$ be a ramified quadratic extension. We say $E(\sqrt{b})$ is "peu ramifée" if $v_2(b)$ is even, or equivalently if b can be taken to be a unit. We say it is "très ramifée" otherwise.

Let D_2 be a decomposition group at a prime above 2 and set K to be the fixed field of the kernel of $\rho|_{D_2}$, a finite extension of $\mathbb{Q}_2$. Let E be the maximal unramified subextension of $K/\mathbb{Q}_2$, so that the Galois group of K/E is $\rho(I_2)$ where $I_2 = G_{2,0}$.

Since the 2-Sylow subgroup of $\mathrm{SL}_3(\mathbb{F}_2)$ is isomorphic to the dihedral group D_4 of size 8, if $\rho(I_2)$ is a 2-group it must be isomorphic to a subgroup of D_4.

1. If $\rho(I_2) \cong C_2$ has size 2, then K itself is a ramified quadratic extension of E. We say that ρ is peu ramifée or très ramifée according to which K/E is. This case did not arise in any of our examples.

2. If $\rho(I_2) \cong C_4$ is cyclic of size 4 there is a unique quadratic subextension L of K/E. Then L/E is ramified and we say that ρ is peu ramifée or très ramifée according to which L/E is. Our only examples turned out to be très ramifée.

3. If $\rho(I_2) \cong V_4$ is isomorphic to the Klein four group then K/E has 3 quadratic subextensions, all of which are ramified. These extensions are obtained by adjoining the square roots of b_1, b_2, and b_1b_2 to E so they are either all peu ramifée or exactly two of them are très ramifée. In the former case we say that ρ is peu-peu ramifée and in the later case we say that ρ is peu-très ramifée. Our only example turned out to be peu-peu ramifée.

   We can get further information in this case by looking at $\rho(D_2)$ which can be isomorphic to S_4, A_4, D_4, or V_4. If $\rho(D_2) \cong S_4$ or A_4, then the three elements of order 2 in $\rho(I_2)$ are all conjugate in $\rho(D_2)$. Thus the three quadratic subextensions of K/E are all isomorphic (over $\mathbb{Q}_2$, but not over E). Thus if any of them are très ramifée they must all be très ramifée. This isn't possible, so we conclude that in this case ρ is peu-peu ramifée.

   If $\rho(D_2) \cong V_4$ then $E = \mathbb{Q}_2$. So the three ramified quadratic subextensions of K/E are actually quadratic extensions of $\mathbb{Q}_2$. The only peu ramifée extensions of $\mathbb{Q}_2$ are $\mathbb{Q}_2(\sqrt{3})$ and $\mathbb{Q}_2(\sqrt{7})$. If $K/\mathbb{Q}_2$ has these as subfields, then the third quadratic subfield must be $\mathbb{Q}_2(\sqrt{21}) = \mathbb{Q}_2(\sqrt{5})$ which is unramified. This contradicts the fact that $\mathbb{Q}_2 = K^{\rho(I_2)}$, and so we conclude that in this case ρ is peu-très ramifée.

   If $\rho(D_2) \cong D_4$ (unfortunate clash of notations) then ρ can be peu-peu ramifée or peu-très ramifée.

4. If $\rho(I_2) \cong D_4$ is isomorphic to the dihedral group of size 8 then since $\rho(I_2) \triangleleft \rho(D_2)$ but $D_4 \not\triangleleft S_4$ we see that $\rho(D_2) = \rho(I_2)$. Thus $E = \mathbb{Q}_2$. Now $\rho(I_2)$ has two subgroups isomorphic to V_4, these are conjugate under τ. Let L_1 and L_2 be the fixed fields of these two subgroups. So L_1 and L_2 are ramified quadratic extensions of $\mathbb{Q}_2$. If both $L_1/\mathbb{Q}_2$ and $L_2/\mathbb{Q}_2$ are peu ramifée then, as above, K would contain the unramified quadratic field $\mathbb{Q}_2(\sqrt{5})$. So at least one of L_1 and L_2 is très ramifée. We say ρ is peu-très ramifée if one of L_1/E and L_2/E is peu ramifée and the other is très ramifée, and ρ is très-très ramifée if both L_1/E and L_2/E are très ramifée. We have examples here of both types.

We can now make our desired predictions:

1. If ρ is peu ramifée or peu-peu ramifée we predict case I.

2. If ρ is peu-très ramifée we predict case II.

3. If ρ is très ramifée or très-très ramifée we predict case III.

We conclude this section by explaining how we determined into which of these cases the Galois representations in our table fall. We will work through three examples, one with $\rho(I_2) \cong V_4$, one with $\rho(I_2) \cong C_4$ and one with $\rho(I_2) \cong D_4$. All of our niveau 1 examples can be handled using one of these three discussions. In these discussions we make use of the p-adic fields calculator on the Jones/Roberts web page [8], which we denote by J/R.

Example: The representation ρ corresponding to polynomial number 2, of level 181. We use the local fields calculator (J/R) to identify the field K as the splitting field over $\mathbb{Q}_2$ of the quartic polynomial $x^4 + 6x^2 + 10$. We thus see that $\rho(D_2) \cong D_4$. The calculator also tells us that $\rho(I_2) \cong D_4$ (so K is totally ramified). Further, we are given both the discriminant subfield of K and the unique quadratic subfield of the quartic extension of $\mathbb{Q}_2$ generated by a root of f. Looking at the subgroup lattice of D_4 and using some elementary Galois theory it is easy to see that these are the two quadratic extensions, called L_1 and L_2 above, which determine the type of ramification of ρ. In this case the two fields are $\mathbb{Q}_2(\sqrt{-1})$ and $\mathbb{Q}_2(\sqrt{10})$. Since one of these is peu ramifée and the other is très ramifée, ρ is peu-très ramifée. The eight other examples with $\rho(I_2) \cong D_4$ are handled in exactly the same manner.

Example: The representation ρ corresponding to polynomial number 12, of level 313. Here J/R tells us that K is the splitting field of $x^4 + 8x + 104$, that $\rho(D_2) \cong D_4$, and that $\rho(I_2) \cong C_4$ is cyclic of size 4. Of course, the field $E = K^{\rho(I_2)}$ must be $\mathbb{Q}_2(\sqrt{5})$ since it is an unramified quadratic extension of $\mathbb{Q}_2$. Further we are told by J/R that the fields L_1 and L_2 fixed by the two subgroups of D_4 isomorphic to V_4 are $\mathbb{Q}_2(\sqrt{-10})$ and $\mathbb{Q}_2(\sqrt{-2})$. Again looking at the subgroup lattice of D_4 we see that the quadratic subfield L of K/E is $L_1L_2{=}\mathbb{Q}_2(\sqrt{-10}, \sqrt{-2}) = \mathbb{Q}_2(\sqrt{5}, \sqrt{-2}) = E(\sqrt{-2})$. Thus K/E is très ramifée, and so ρ is très ramifée.

Example: The representation ρ corresponding to polynomial number 19, of level 383. This time J/R tells us that $\rho(D_2) \cong A_4$ and $\rho(I_2) \cong V_4$. Thus as we've seen above ρ must be peu-peu ramifée.

4 Finding examples

Our goal is to check the ADPS conjecture for $p = 2$ for Galois representations with image $\mathrm{SL}_3(\mathbb{F}_2)$. To do so, we need to produce polynomials over $\mathbb{Q}$ whose splitting fields have Galois group $\mathrm{SL}_3(\mathbb{F}_2)$. Noting that $\mathrm{SL}_3(\mathbb{F}_2) \cong \mathrm{PSL}_2(\mathbb{F}_7)$, we used the four parameterized families of septic polynomials in $\mathbb{Z}[x]$ with Galois group $\mathrm{PSL}_2(\mathbb{F}_7)$ found in Malle's paper [6]. We used PARI/GP and Theorem 2 below to search among these polynomials for ones with levels low enough for our computational methods (< 500).

Theorem 2 allows us to easily calculate the level of a tamely ramified representation. We also, however, computed the levels of several wildly ramified representations. Since wildly ramified primes tend to appear in the level with much higher exponents than tamely ramified primes, the wildly ramified representations we looked at all had levels much higher than 500. We therefore restricted our search to number fields ramified only at primes not equal to 3 or 7. This allowed us to use Theorem 2 and PARI's *nfdisc* command to determine the level and throw out those with level above 500.

In searching the polynomial families, for both three parameter families we varied all three parameters over the integers between -30 and 30, and for the four parameter family all four parameters varied over the integers between -20 and 20. Perhaps surprisingly, even large parameter values sometimes yielded levels less than 500, but the yield became sparser as the parameter values increased in absolute value. In fact, many different sets of parameter values, both from the same family and from different families, often gave different polynomials which generated the same field. The higher parameter values often just yielded repeats of fields already generated by polynomials with smaller parameter values. In the one parameter family, we ranged the parameters from $-10,000$ to $10,000$ and tried rational values of height ≤ 50 but no polynomials determining fields with levels ≤ 500 were found.

Since for each $\mathrm{SL}_3(\mathbb{F}_2)$-field there are two non-isomorphic septic subfields fixed by the two index 7 parabolic subgroups, there will always be two distinct degree 7 subfields with the same $\mathrm{SL}_3(\mathbb{F}_2)$ splitting field. This explains why we often found two distinct septic fields ramified at the same primes and, in fact, with the same splitting field. In other cases, our search did not locate the "twin." (Note that we've only listed one polynomial for each distinct splitting field in Table 3, but in Tables 1 and 2, we've included one polynomial for each distinct septic subfield.)

It seems likely that we would find even more fields if we expanded the parameter search space further. Indeed, the referee kindly suggested 7 additional polynomials whose levels are under 500, including one which is (tamely) ramified at 7. We have verified our refined conjecture for the corresponding representations, and include these polynomials in our tables.

Now let $\rho\colon G_{\mathbb{Q}} \to \mathrm{SL}_3(\mathbb{F}_2)$ be a surjective Galois representation, and suppose that ρ is not wildly ramified at any odd primes. We present the results that allow us to compute the level of ρ in terms of a degree seven subfield of the fixed field of ρ.

Theorem 1. *Let f be a degree seven monic integral polynomial. Let $F/\mathbb{Q}$ be the field extension generated by a root of f. Let K be the Galois closure of F, and assume $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{SL}_3(\mathbb{F}_2)$. Let q be an odd rational prime, tamely ramified in K. Let $\rho : G_{\mathbb{Q}} \to \mathrm{SL}_3(\mathbb{F}_2)$ be a Galois representation whose fixed field is K. Let ν_q be the exponent of q in the Serre conductor of ρ and let N be the level predicted by the ADPS conjecture. If $e = |I_q|$, then ν_q, and therefore the exact power of q dividing N, can be determined as follows.*

1. *If $e = 2$, then $\nu_q = 1$. Hence $q \parallel N$.*
2. *If $e = 3$, then $\nu_q = 2$. Hence $q^2 \parallel N$.*

3. *If* $e = 4$*, then* $\nu_q = 2$*. Hence* $q^2 \parallel N$*.*

4. *If* $e = 7$*, then* $\nu_q = 3$*. Hence* $q^3 \parallel N$*.*

Proof. Recall that for $p = 2$, the level predicted by the ADPS conjecture is

$$N = \prod_{\substack{q \neq 2 \\ q | disc(F)}} q^{\nu_q},$$

where

$$\nu_q = \sum_{k=0}^{\infty} \frac{|I_k|}{|I_0|}(3 - \dim(\mathbb{F}_2^3)^{I_k}).$$

Here $I_0 = I_q \supset I_1 \supset I_2 \supset \cdots$ are the higher inertia groups. In the tame case, $I_k = 0$ if $k > 0$, so

$$\nu_q = (3 - \dim(\mathbb{F}_2^3)^{I_q}).$$

Therefore, to find ν_q we only need to find the dimension of the fixed space of I_q (i.e., the dimension of the 1-eigenspace of a generator g of I_q) for each possible inertial degree e.

1. Assume $e = 2$. Up to conjugation, $g = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ in $\mathrm{SL}_3(\mathbb{F}_2)$. So the dimension of the fixed space of I_q is 2, and therefore $\nu_q = 1$, and $q \parallel N$.

2. Assume $e = 4$. Up to conjugation, $g = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ in $\mathrm{SL}_3(\mathbb{F}_2)$. So the dimension of the fixed space of I_q is 1, and therefore $\nu_q = 2$, and $q^2 \parallel N$.

3. Assume $e = 3$. Up to conjugation, $g = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ in $\mathrm{SL}_3(\mathbb{F}_2)$. So the dimension of the fixed space of I_q is 1, and therefore $\nu_q = 2$, and $q^2 \parallel N$.

4. Assume $e = 7$. An element of order 7 in $\mathrm{SL}_3(\mathbb{F}_2)$ has seventh roots of unity as eigenvalues. After base change to $\mathbb{F}_8/\mathbb{F}_2$ and letting σ generate the Galois group of $\mathbb{F}_8/\mathbb{F}_2$, we find that $g = \begin{pmatrix} \zeta_7 & 0 & 0 \\ 0 & \sigma(\zeta_7) & 0 \\ 0 & 0 & \sigma^2(\zeta_7) \end{pmatrix}$, for some nontrivial seventh root of unity ζ_7. The group generated by this element has trivial fixed space on $\mathbb{F}_8^3$, so $\nu_q = 3$. Hence, $q^3 \parallel N$.

□

The following theorem was pointed out to us by the referee; we are grateful for his help.

Theorem 2. *Let f,F,K, and ρ be as in Theorem 1, and suppose ρ is not wildly ramified at any odd primes. Then the level $N(\rho)$ of ρ predicted by the ADPS conjecture is the square root of the odd part of the discriminant $d(F)$.*

Proof. Let q be an odd rational prime which is ramified in K. Then since q is tamely ramified the inertia group $I_q \subset \mathrm{Gal}(K/\mathbb{Q})$ is cyclic. Let σ be a generator of I_q, and let $l_1, \ldots, l_n$ be sizes of the orbits of σ on the roots of f. It is well known that the precise power of q dividing $d(F)$ is $\sum_{i=1}^{n}(l_i - 1)$.

Moreover, the sizes of the orbits of σ on the roots of f are determined by the order e of σ. We have

1. If $e = 2$ then σ has two orbits of size 2 and three fixed points. Thus $q^2 \parallel d(F)$.
2. If $e = 3$ then σ has two orbits of size 3 and one fixed point. Thus $q^4 \parallel d(F)$.
3. If $e = 4$ then σ has one orbit of size 4, one orbit of size 2, and one fixed point. Thus $q^4 \parallel d(F)$.
4. If $e = 7$ then σ has a single orbit, of size 7. Thus $q^6 \parallel d(F)$.

Comparing this with theorem 1 we see that the exact power of q dividing $d(F)$ is the square of the exact power of q dividing $N(\rho)$. This proves the theorem. □

5 Computing the cohomology

Our computations of the mod 2 arithmetic cohomology of the $\Gamma_0(N)$ were carried out using programs based on those written for the calculations in [2]. We will review the basic approach taken by the original programs (see [2, Sect. 8] for more details) and then mention a few of the particular adaptations we made in the new version.

In actual fact, we do not compute cohomology groups at all, but rather work with the homology groups $H_*(\Gamma_0(N), M)$ to which they are naturally dual. Moreover, we only compute H_3. This is simpler than computing H_1 or H_2 since the virtual cohomological dimension of $\mathrm{SL}_3(\mathbb{Z})$ is 3. Since we are only interested in irreducible Galois representations here, testing our conjecture for H_3 is equivalent to testing it for H_* [4]. Finally, as explained below, what we actually compute is the $\Gamma_0(N)$-invariants in $H_3(\Delta, M)$, where Δ is a torsion-free normal subgroup of finite index in $\Gamma_0(N)$.

We use the SL_3 variant of Theorem 2.1 of [1] to identify the $\Gamma_0(N)$-invariants of $H_3(\Delta, M)$ with the subspace of all $v \in V$ such that

1. $v \cdot d = v$ for all diagonal matrices $d \in \mathrm{SL}_3(\mathbb{Z})$
2. $v \cdot z = -v$ for all monomial matrices of order 2 in $\mathrm{SL}_3(\mathbb{Z})$
3. $v + v \cdot h + v \cdot (h^2) = 0$,

where

$$h = \begin{pmatrix} 0 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

This is the space on which we act our Hecke operators and look for suitable eigenclasses.

In [2, Sect. 8] we explain in detail the models we use for the modules V that arise, as well as our methods for solving the linear algebra problem above. Since we are working in characteristic 2 we are no longer able to use a projection operator to find the solutions to equations (1) and (2), but instead use the same approach for these as we do for equation (3).

Although the linear algebra involved is abstractly a simple row reduction, the size of the matrices involved has prompted us to balance the concerns of memory usage against run time. For instance, in the course of computing with $N = 443$ and $M = F(2, 1, 0)$ we needed to find the kernel of a $1,573,544 \times 66,009$ matrix. This is far too large for us to store in resident memory, especially since the matrix becomes less sparse as the row reduction proceeds. As explained in [2] our programs make use of disk storage and swap parts of the matrix in and out of resident memory as the calculation proceeds. The new versions of the program expand on this idea and also use the disk to store bases for subspaces that arise during the calculation of the kernel (c.f. [2, pg. 575]). We have also adjusted some of our algorithms to cut down on the number of disk swaps required and more efficiently access the data structures in which the resident portions of the matrix are being stored.

The computation of the actions of the Hecke operators on the homology group is done exactly as in [2], except that as a final optimization in all of the programs we have taken advantage of the fact that our coefficients are numbers modulo 2 to hardcode the field arithmetic and reduce storage size.

6 Results

The following tables contain the results of our calculations. Table 1 describes the $\mathrm{SL}_3(\mathbb{F}_2)$-polynomials we found that give feasible levels, indicating how these polynomials arise from the families in [6] and giving the decomposition of the primes 2 and N (the level) in the septic extension of $\mathbb{Q}$ defined by the polynomial. Table 2 gives the actual coefficients of these polynomials, as well as of seven addition polynomials suggested by the referee. Both tables list the predicted level of the corresponding Galois representation.

Table 3 contains one row for each of the distinct $\mathrm{SL}_3(\mathbb{F}_2)$-fields we investigated. Each such field corresponds to two Galois representations, called ρ and ρ^τ above. For each field, we list the inertia group at 2 and the common niveau of ρ and ρ^τ, and indicate the common peu ramifée/très ramifée nature of ρ and ρ^τ. We also list the weights for which we observed a cohomology eigenclass apparently attached to ρ or ρ^τ.

As we described in section 3 if either ρ or ρ^τ is attached to a cohomology class with weight $F(0,0,0)$ or $F(2,1,0)$ then the other representation is as well. Likewise if ρ or ρ^τ is attached to a cohomology class with weight $F(1,0,0)$ then the other representation is attached to a class with weight $F(1,1,0)$, and conversely. Our data bears this out in every case, so that for example when the first entry in Table 3 indicates that the observed weights are $F(1,0,0), F(1,1,0)$, and $F(2,1,0)$ we are saying that both ρ and ρ^τ appear for weight $F(2,1,0)$, one of ρ and ρ^τ appears for weight $F(1,0,0)$, and the other appears for $F(1,1,0)$.

We stress again that when we say a class appears to be attached to a Galois representation, we mean that the corresponding Hecke and Frobenius polynomials agree for $\ell \leq 47$.

polynomial	*parameters*	*decomposition at* 2	*decomposition at* N	N
3 parameter family (1)				
5	-2,2,2	$(6,1),(1,1)$	$(2,2),(1,1),(1,1),(1,1)$	251
6	1,-1,-8	$(4,1),(3,1)$	$(2,1),(2,1),(1,2),(1,1)$	251
15	-1,1,1	$(7,1)$	$(2,2),(1,1),(1,1),(1,1)$	317
18	8,4,8	$(2,3),(1,1)$	$(2,2),(1,1),(1,1),(1,1)$	383
24	-1,-1,-17	$(7,1)$	$(2,2),(1,2),(1,1)$	443
27	-1,-1,-10	$(4,1),(3,1)$	$(2,1),(2,1),(1,1),(1,1),(1,1)$	487
31	4,4,-16	$(4,1),(2,1),(1,1)$	$(2,2),(1,2),(1,1)$	499
32	2,2,4	$(4,1),(2,1),(1,1)$	$(2,2),(1,2),(1,1)$	499
3 parameter family (2)				
12	2,-2,4	$(4,1),(2,1),(1,1)$	$(2,2),(1,2),(1,1)$	313
13	2,-2,-4	$(4,1),(2,1),(1,1)$	$(2,2),(1,2),(1,1)$	313
14	-2,1,-1	$(7,1)$	$(2,1),(2,1),(1,2),(1,1)$	317
19	-3,-1,-4	$(4,1),(1,3)$	$(2,1),(2,1),(1,2),(1,1)$	383
22	4,-2,4	$(4,1),(2,1),(1,1)$	$(2,1),(2,1),(1,1),(1,1),(1,1)$	443
23	2,-1,1	$(7,1)$	$(2,2),(1,2),(1,1)$	443
25	0,-1,7	$(7,1)$	$(2,1),(2,1),(1,2),(1,1)$	457
29	1,-2,4	$(4,1),(3,1)$	$(2,2),(1,2),(1,1)$	491
30	-1,1,1	$(6,1),(1,1)$	$(2,2),(1,2),(1,1)$	491
4 parameter family				
1	-4,0,1,20	$(4,1),(2,1),(1,1)$	$(2,2),(1,2),(1,1)$	181
2	4,0,1,-2	$(4,1),(2,1),(1,1)$	$(2,2),(1,2),(1,1)$	181
3	-1,-4,2,2	$(4,1),(2,1),(1,1)$	$(2,2),(1,2),(1,1)$	227
4	-4,-4,-2,0	$(4,1),(2,1),(1,1)$	$(2,2),(1,1),(1,1),(1,1)$	239
7	-4,0,2,4	$(4,1),(2,1),(1,1)$	$(2,1),(2,1),(1,2),(1,1)$	257
8	-2,0,1,-2	$(4,1),(2,1),(1,1)$	$(2,2),(1,1),(1,1),(1,1)$	257
9	-4,0,2,-4	$(4,1),(3,1)$	$(2,2),(1,2),(1,1)$	277
10	-2,0,1,0	$(6,1),(1,1)$	$(2,2),(1,2),(1,1)$	277
11	-2,-4,2,8	$(4,1),(2,1),(1,1)$	$(2,2),(1,2),(1,1)$	307
16	-4,0,1,12	$(6,1),(1,1)$	$(2,1),(2,1),(1,2),(1,1)$	331
17	-1,-4,1,4	$(4,1),(3,1)$	$(2,2),(1,1),(1,1),(1,1)$	331
20	-4,8,4,-16	$(4,1),(2,1),(1,1)$	$(2,1),(2,1),(1,1),(1,1),(1,1)$	389
21	1,2,2,17	$(4,1),(2,1),(1,1)$	$(2,1),(2,1),(1,2),(1,1)$	421
26	-2,0,1,8	$(6,1),(1,1)$	$(2,1),(2,1),(1,2),(1,1)$	461
28	-8,0,4,16	$(6,1),(1,1)$	$(2,1),(2,1),(1,1),(1,1),(1,1)$	487

Table 1: One polynomial for each distinct septic subfield, keyed by number to the polynomials listed in Table 2. The families are listed in the order they appear in [6], the numberings to distinguish between the three parameter families being our own. Polynomials 33-39 were provided by the referee and do not appear in this table.

	polynomial	*field discriminant*	N
1	$x^7 - x^6 - 4x^5 + 6x^4 - 2x^3 + -6x^2 + 8x - 4$	$2^{12} * 181^2$	181
2	$x^7 - x^6 - 2x^5 - 2x^4 + x^3 + 3x^2 + 6x + 2$	"	181
3	$x^7 - x^6 - 4x^5 + 4x^4 - x^3 + x^2 + 6x + 2$	$2^{14} * 227^2$	227
4	$x^7 - 3x^6 + 12x^4 - 15x^3 - 7x^2 + 24x - 8$	$2^{12} * 239^2$	239
5	$x^7 - 2x^6 - 3x^5 + 10x^4 - 9x^3 + 2x^2 + 5x - 2$	$2^{10} * 251^2$	251
6	$x^7 - 3x^6 + x^5 + 3x^4 - 2x^3 + 2x^2 - 2x - 2$	"	251
7	$x^7 - x^6 + x^5 + 11x^4 - 24x^3 + 32x^2 - 20x + 4$	$2^{14} * 257^2$	257
8	$x^7 - x^6 - 5x^5 + 9x^4 + 5x^3 - 21x^2 + 3x + 1$	"	257
9	$x^7 - x^6 - 5x^5 + 7x^4 - 7x^3 + 3x^2 - x - 1$	$2^{10} * 277^2$	277
10	$x^7 - 3x^6 + 4x^5 - 2x^4 - 8x^3 + 16x^2 + 2x - 2$	"	277
11	$x^7 - 3x^6 + 2x^5 - 6x^4 - 3x^3 - 3x^2 - 6x - 2$	$2^{12} * 307^2$	307
12	$x^7 - 3x^6 + 6x^5 - 14x^4 + 13x^3 - 15x^2 + 24x - 4$	$2^{14} * 313^2$	313
13	$x^7 - 3x^6 + 6x^5 - 6x^4 - 11x^3 + 9x^2 + 16x - 4$	"	313
14	$x^7 - 2x^6 + 2x^4 - 2x^3 + 2x^2 - 2$	$2^6 * 317^2$	317
15	$x^7 - 3x^6 + 3x^5 - x^4 - 5x^3 + 5x^2 + 3x - 1$	"	317
16	$x^7 - x^6 - 4x^5 + 6x^4 - 8x^2 + 6x - 2$	$2^{10} * 331^2$	331
17	$x^7 - 2x^6 + 2x^5 - 2x^4 - 2x^3 + 4x^2 - 4x - 4$	"	331
18	$x^7 - x^6 + 2x^5 + 2x^4 - 5x^3 + 7x^2 - 5x + 1$	$2^6 * 383^2$	383
19	$x^7 - x^6 - x^5 - 5x^4 + 2x^3 + 4x^2 + 6x + 2$	"	383
20	$x^7 - 2x^6 + x^5 - 8x^3 + 12x^2 - 14x + 16$	$2^{12} * 389^2$	389
21	$x^7 - x^6 + 2x^5 - 11x^3 + 7x^2 - 16x + 2$	$2^{12} * 421^2$	421
22	$x^7 - 3x^6 - 2x^5 + 14x^4 - 7x^3 - 15x^2 + 6x + 10$	$2^{12} * 443^2$	443
23	$x^7 - 3x^6 + 3x^5 + x^4 - 3x^3 + x^2 - x - 1$	$2^6 * 443^2$	443
24	$x^7 - 3x^6 + x^5 + 3x^4 - x^3 + x^2 - 3x - 1$	"	443
25	$x^7 - 2x^6 - 2x^5 + 6x^4 - 4x^3 - 2x^2 + 4x - 2$	$2^6 * 457^2$	457
26	$x^7 - x^6 - 5x^5 + 9x^4 - 5x^3 - 11x^2 + 13x - 9$	$2^{10} * 461^2$	461
27	$x^7 - 3x^6 - x^5 + 9x^4 - 2x^3 - 10x^2 + 2x + 2$	$2^{10} * 487^2$	487
28	$x^7 - 3x^5 - 8x^4 + 11x^3 + 12x^2 - 15x - 8$	"	487
29	$x^7 - 3x^6 - x^5 + 9x^4 - 12x^2 + 4$	$2^6 * 491^2$	491
30	$x^7 - 3x^6 + 7x^5 - 5x^4 + x^3 + 7x^2 - 3x - 1$	"	491
31	$x^7 - x^6 - 6x^5 + 18x^4 - 34x^3 + 42x^2 - 28x + 4$	$2^{14} * 499^2$	499
32	$x^7 + 2x^6 - 10x^5 - 12x^4 + 34x^3 + 4x^2 - 28x + 8$	"	499
33	$x^7 - 3x^6 + 10x^5 - 10x^4 + 7x^3 - 13x^2 + 4$	$2^{14} * 5^2 * 67^2$	335
34	$x^7 - 7x^5 - 2x^4 + 20x^3 - 4x^2 - 18x + 4$	$2^{12} * 353^2$	353
35	$x^7 - 3x^6 - 4x^5 + 20x^4 - 10x^3 - 26x^2 + 16x + 16$	$2^{14} * 383^2$	383
36	$x^7 - 3x^6 - 3x^5 + 9x^4 + 4x^3 - 8x^2 + 12x + 20$	$2^{12} * 401^2$	401
37	$x^7 - x^6 - 5x^5 + 9x^4 + x^3 - 17x^2 + 7x - 3$	$2^{14} * 7^2 * 61^2$	427
38	$x^7 - 3x^6 - 4x^5 + 28x^4 - 15x^3 - 35x^2 + 38x - 2$	$2^{14} * 431^2$	431
39	$x^7 - x^6 - 2x^5 + 2x^4 - 6x^3 - 2x^2 + 20x - 4$	$2^{14} * 487^2$	487

Table 2: One polynomial for each distinct septic subfield that met our criteria, along with the field discriminant and level.

polynomial	*level*	*niveau*	I_2	*peu/très*	*observed weights*
2	181	1	D_4	*pt*	b, c, d
3	227	1	D_4	*tt*	d
4	239	1	D_4	*pt*	b, c, d
5	251	2	A_4	–	a, b, c, d
8	257	1	D_4	*tt*	d
10	277	2	A_4	–	a, b, c, d
11	307	1	D_4	*pt*	b, c, d
12	313	1	C_4	*t*	d
15	317	3	C_7	–	a, b, c, d
17	331	2	A_4	–	a, b, c, d
19	383	1	V_4	*pp*	a, b, c, d
20	389	1	D_4	*pt*	b, c, d
21	421	1	D_4	*pt*	b, c, d
22	443	1	D_4	*pt*	b, c, d
23	443	3	C_7	–	a, b, c, d
25	457	3	C_7	–	a, b, c, d
26	461	2	A_4	–	a, b, c, d
27	487	2	A_4	–	a, b, c, d
30	491	2	A_4	–	a, b, c, d
32	499	1	D_4	*tt*	d
33	335	1	D_4	*tt*	d
34	353	1	D_4	*pt*	b, c, d
35	383	1	D_4	*tt*	d
36	401	1	D_4	*pt*	b, c, d
37	427	1	C_4	*t*	d
38	431	1	D_4	*tt*	d
39	487	1	D_4	*tt*	d

Table 3: One polynomial for each distinct splitting field, keyed by number to the polynomials listed in Table 2, along with the level, niveau, inertia at 2, the peu ramifée/très ramifée classification of ramification at 2, and the observed weights. The peu ramifée/très ramifée ramification possibilities are abbreviated as: *pp* = peu-peu, *pt* = peu-très, *t* = très, *tt* = très-très. The weights are abbreviated as follows: $a = F(0,0,0)$, $b = F(1,0,0)$, $c = F(1,1,0)$, $d = F(2,1,0)$

References

[1] Gerald Allison, Avner Ash, and Eric Conrad. Galois representations, Hecke operators, and the mod-p cohomology of $\mathrm{GL}(3, \mathbf{Z})$ with twisted coefficients. *Experiment. Math.*, 7(4):361–390, 1998.

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

[3] Avner Ash and Mark McConnell. Experimental indications of three-dimensional Galois representations from the cohomology of $\mathrm{SL}(3, \mathbf{Z})$. *Experiment. Math.*, 1(3):209–223, 1992.

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

[5] Avner Ash and Glenn Stevens. Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues. *J. Reine Angew. Math.*, 365:192–220, 1986.

[6] Gunter Malle. Multi-parameter polynomials with given Galois group. *J. Symbolic Comput.*, 30(6):717–731, 2000. Algorithmic methods in Galois theory.

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

[8] John Jones and David Roberts. Web page located at http://hobbes.la.asu.edu/LocalFields.