2005-06-03

Explicit Computations Supporting a Generalization of Serre's Conjecture

Brian Francis Hansen
Brigham Young University - Provo

EXPLICIT COMPUTATIONS SUPPORTING A GENERALIZATION OF SERRE'S CONJECTURE

by

Brian Hansen

A thesis submitted to the faculty of

Brigham Young University

in partial fulfillment of the requirements for the degree of

Master of Science

Department of Mathematics

Brigham Young University

August 2005

BRIGHAM YOUNG UNIVERSITY

GRADUATE COMMITTEE APPROVAL

of a thesis submitted by

Brian Hansen

This thesis has been read by each member of the following graduate committee and by majority vote has been found to be satisfactory.

Date	Darrin Doud, Chair
Date	David Cardon
Date	Chris Grant

BRIGHAM YOUNG UNIVERSITY

As chair of the candidate's graduate committee, I have read the thesis of Brian Hansen in its final form and have found that (1) its format, citations, and bibliographical style are consistent and acceptable and fulfill university and department style requirements; (2) its illustrative materials including figures, tables, and charts are in place; and (3) the final manuscript is satisfactory to the graduate committee and is ready for submission to the university library.

Date

Darrin Doud
Chair, Graduate Committee

Accepted for the Department

Tyler Jarvis
Graduate Coordinator

Accepted for the College

G. Rex Bryce, Associate Dean
College of Physical and Mathematical Sciences

ABSTRACT

EXPLICIT COMPUTATIONS SUPPORTING A GENERALIZATION OF SERRE'S CONJECTURE

Brian Hansen

Department of Mathematics

Master of Science

Serre's conjecture on the modularity of Galois representations makes a connection between two-dimensional Galois representations and modular forms. A conjecture by Ash, Doud, and Pollack generalizes Serre's to higher-dimensional Galois representations. In this paper we discuss an explicit computational example supporting the generalized claim. An ambiguity in a calculation within the example is resolved using a method of complex approximation.

Table of Contents

1 Introduction

Serre's conjecture on the modularity of Galois representations [11], or simply, "Serre's conjecture," makes a connection between modular forms and 2-dimensional Galois representations. It has played an important role in number theory for over three decades; recently Chandrasekhar Khare [7] has proven the level 1 case.

In [1], Serre's conjecture was generalized to include 3-dimensional representations. To date, little progress has been made in proving this generalized conjecture, though a considerable amount of computational evidence has been found.

One example in [1] was left incomplete due to an ambiguity in calculation caused by inability to compute the trace of a special generator of the inertia group. In this thesis, we resolve this ambiguity by computing the trace using a method of complex approximation. The trace is compared to a previously calculated eigenvalue in [1], providing more evidence for the generalized conjecture.

2 Modularity Conjectures concerning Galois representations

2.1 Modular Forms

In order to understand Serre's conjecture, we need an introduction to modular forms. Refer to [8, pp. 222-7] for more detail.

Let $k \in \mathbb{Z}$, and let $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ act on τ by $M\tau = \dfrac{a\tau + b}{c\tau + d}$.

Definition 1. Let $N \in \mathbb{Z}^+$, and let $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a homomorphism. An analytic function f on the upper half complex plane satisfying

$$f(M\tau) = (c\tau + d)^k \epsilon(d) f(\tau)$$

for all $M \in \Gamma_0(N) = \{\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in SL_2(\mathbb{Z}) \mid c \equiv 0 \bmod N\}$ is called an *unrestricted modular form of weight k, level N, and nebentype* (or *character*) ϵ.

Taking $M = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$, we have $f(\tau + 1) = f(\tau)$, so that each unrestricted modular form f is periodic. We therefore obtain the Fourier-, or q-expansion of f

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n q^n,$$

where $q = e^{2\pi i \tau}$.

Definition 2. If in the q-expansion of f we have $a_n = 0$ for $n < 0$, we say f is *holomorphic at* ∞ and is a *modular form.*

It is clear that sums, differences, and scalar multiples of modular forms are also modular forms of the same weight. Furthermore, it is easy to see that if k is odd, $f \equiv 0$: set $M = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$.

Proposition 1. *Let f and g be modular forms of weights k_1 and k_2, respectively, each having nebentype 1. Then fg is a modular form of weight $k_1 + k_2$.*

Proof. First note that products of holomorphic functions are holomorphic. Let $M \in SL_2(\mathbb{Z})$. Then

$$\begin{aligned} fg(M\tau) &= f(M\tau)g(M\tau) \\ &= (c\tau + d)^{k_1} f(\tau)(c\tau + d)^{k_2} g(\tau) \\ &= (c\tau + d)^{k_1+k_2} fg(\tau). \end{aligned}$$

fg is thus a modular form of weight $k_1 + k_2$. □

We now present some examples of modular forms. Define

$$G_{2k}(\tau) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau + n)^{2k}}.$$

We show that if $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in SL_2(\mathbb{Z})$, then $G_{2k}(M\tau) = (c\tau + d)^{2k} G_{2k}(\tau)$, i.e., G_{2k} is a modular form of weight $2k$:

$$\begin{aligned} G_{2k}(M\tau) &= \sum_{(m,n)\neq(0,0)} \frac{1}{(m(\frac{a\tau+b}{c\tau+d}) + n)^{2k}} \\ &= (c\tau + d)^{2k} \sum_{(m,n)\neq(0,0)} \frac{1}{(m(a\tau + b) + n(c\tau + d))^{2k}}, \end{aligned}$$

which can be written

$$G_{2k}(M\tau) = (c\tau + d)^{2k} \sum_{(m,n)\neq(0,0)} \frac{1}{((ma + nc)\tau + (mb + nd))^{2k}}.$$

Since $M \in SL_2(\mathbb{Z})$, we have that $[m, n]M = [m', n']$ is a bijective transformation, so that

$$\sum_{(m,n)\neq(0,0)} \frac{1}{((ma + nc)\tau + (mb + nd))^{2k}} = \sum_{(m',n')\neq(0,0)} \frac{1}{(m'\tau + n')^{2k}}.$$

Therefore, $G_{2k}(M\tau) = (c\tau + d)^{2k} G_{2k}(\tau)$. Also, from [8, p. 225],

$$G_{2k}(\tau) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n,$$

where $\sigma_\ell(n) = \sum_{d|n, d>0} d^\ell$.

Define the *Eisenstein Series* by $E_{2k}(\tau) = \frac{G_{2k}(\tau)}{2\zeta(2k)}$, and let $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$. By Proposition 1, Δ is a modular form of weight 12. It is also a cusp form, i.e., the constant term in its q-expansion is 0. To see this, recall that $\zeta(4) = \frac{\pi^4}{90}$ and $\zeta(6) = \frac{\pi^6}{945}$ [8, p. 227]. By direct substitution we obtain

$$\Delta(\tau) = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + ...,$$

so that $\Delta(\tau)$ is a cusp form.

Definition 3. A *normalized* modular form has 1 as its first nonzero Fourier coefficient. A modular form is said to be an *eigenform* if it is a simultaneous eigenvector for Hecke operators T_p; see [8, p. 280].

2.2 Statement of Serre's Conjecture

In this section we introduce Serre's conjecture; see [4]. Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Let ρ be a two-dimensional Galois representation, i.e., a continuous homomorphism $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$, where $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and $\mathbb{F}$ is a finite field of characteristic p. If the determinant of the matrix to which the complex conjugation map is sent is 1, the representation is called even; otherwise, the representation is said to be odd.

In the following definition, the *Frobenius* element Frob_ℓ of $G_\mathbb{Q}$ exists for any prime ℓ which is unramified for ρ. The Frobenius will be described in more detail in Section 4.1.

Definition 4. If there exists a normalized eigenform f of weight $k \geq 2$, level N, and character ϵ with Fourier coefficients a_n in $\mathbb{F}$ (and $a_1 = 1$) such that for all ℓ which are unramified for ρ and do not divide Np, the characteristic polynomial of $\rho(\text{Frob}_\ell)$ is $x^2 - a_\ell x + \ell^{k-1}\epsilon(\ell)$, then ρ is said to be *modular*, and ρ and f are *associated*.

It should be noted that the level N is an integer divisible only by ramified primes of ρ not equal to p. Therefore, when ρ is ramified at a single prime, we have $N = 1$, which forces ϵ to be the trivial character.

It has been previously shown by Eichler, Shimura, and Deligne that any eigenform f gives rise to an associated representation ρ. The general idea of Serre's conjecture is that the converse holds also: any odd irreducible representation ρ as above is modular.

Conjecture 1 (Serre's Conjecture). There exists a normalized mod p eigenform of level $N(\rho)$, weight $k(\rho)$, and (when char $\mathbb{F} > 3$) character $\epsilon(\rho)$ which is associated to ρ, where $N(\rho)$, $k(\rho)$, and $\epsilon(\rho)$ are defined by a formula of Serre. [4, p. 3]

Serre's conjecture gives a valuable way to study algebraic number fields using analytic methods. In 1995, Andrew Wiles used proven cases of Serre's conjecture to complete the proof of Fermat's Last Theorem. In specific, and perhaps more importantly due to its implications, it was used to help prove the modularity of elliptic curves.

factorization of $f(x)$ mod ℓ	order of $\pi(\text{Frob}_\ell)$	$\text{Tr}(\rho(\text{Frob}_\ell))$
three linear factors	1	2
one linear, one quadratic	2	0
irreducible	3	-1

Table 1: Calculation of $\text{Tr}(\rho(\text{Frob}_\ell))$ according to factorization of $f(x)$

As an example of Serre's conjecture, consider the splitting field K of $f(x) = x^3 - x + 1$. We have $\text{Gal}(K/\mathbb{Q}) \cong S_3$. Let $\sigma : S_3 \to GL_2(\mathbb{F}_{23})$ be the homomorphism defined by

$$\sigma((1\ 2)) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ \sigma((1\ 2\ 3)) = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

We then have a Galois representation

$$\rho : G_{\mathbb{Q}} \xrightarrow{\pi} \text{Gal}(K/\mathbb{Q}) \cong S_3 \xrightarrow{\sigma} GL_2(\mathbb{F}_{23}),$$

where π is the natural projection map. For all primes $\ell \neq 23$, the order of the image of the Frobenius element Frob_ℓ under the projection π depends on the factorization of $f(x)$ modulo ℓ, therefore so does $\text{Tr}(\rho(\text{Frob}_\ell))$. This is illustrated in Table 1. (This is justified by a theorem of Dedekind, described in Section 4.1.)

In this case, ρ is associated with Δ, where Δ is as defined in Section 2.1. Observe Table 2, where a_ℓ denotes the coefficient of q^ℓ in the q-expansion of Δ, reduced modulo 23.

2.3 Statement of the Generalized Conjecture

We now introduce a generalized version of Serre's conjecture, which we refer to more simply as the "generalized conjecture." This conjecture is due to Ash, Doud, and Pollack; see [1]. We begin with a few preliminary definitions.

ℓ	2	3	5	7	11	13	17	19	23	29	31	37
$\mathrm{Tr}(\rho(\mathrm{Frob}_\ell))$	-1	-1	0	0	0	-1	0	0	*	-1	-1	0
a_ℓ	-1	-1	0	0	0	-1	0	0	1	-1	-1	0

ℓ	41	43	47	53	59	61	67	71	73	79	83	89
$\mathrm{Tr}(\rho(\mathrm{Frob}_\ell))$	-1	0	-1	0	2	0	0	-1	-1	0	0	0
a_ℓ	-1	0	-1	0	2	0	0	-1	-1	0	0	0

Table 2: Association of ρ with Δ.

Definition 5. An n-dimensional Galois representation is a continuous homomorphism $\rho : G_{\mathbb{Q}} \to GL_n(\mathbb{F})$ from $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to the general linear group of invertible $n \times n$ matrices over a field $\mathbb{F}$ of characteristic p. If for all $g \in G_{\mathbb{Q}}$ we can write $\rho(g) = \rho_1(g) \oplus \rho_2(g)$ for representations ρ_1, ρ_2 of $G_{\mathbb{Q}}$, then ρ is said to be *reducible*.

As in the 2-dimensional case, the level N is an integer divisible only by ramified primes of ρ not equal to p, so that, once again, when ρ is ramified at a single prime, we have $N = 1$, forcing ϵ to be the trivial character.

The weight associated to a 3-dimensional Galois representation ρ will be a certain irreducible $GL_3(\mathbb{F}_p)$-module. These modules are denoted by $F(a, b, c)$, where a, b, c are p-restricted; that is,

$$0 \leq a - b \leq p - 1,$$

$$0 \leq b - c \leq p - 1,$$

$$0 \leq c \leq p - 2.$$

[1, p. 525] There are therefore $p^2(p-1)$ such modules. (The notation reflects the parametrization of irreducible $GL_3(\mathbb{F}_p)$-modules by p-restricted 3-tuples described in [5].)

In the following definition, the Hecke operator $T(\ell, k)$ is a linear transformation of a vector space to itself. Denote by $\mathcal{H}(N)$ a commutative $\bar{\mathbb{F}}_p$-algebra generated by the set $\{T(\ell, k) \mid \ell \nmid N\}$.

Definition 6. Let V be an $\mathcal{H}(pN)$-module and suppose that $v \in V$ is a simultaneous eigenvector for all $T(\ell, k)$ with $T(\ell, k)v = a(\ell, k)v$, where $a(\ell, k) \in \bar{\mathbb{F}}_p$ for all prime ℓ not dividing pN, and for $0 \leq k \leq 3$. Let $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_p)$ be a representation unramified outside pN and assume that

$$\sum_{k=0}^{3} (-1)^k \ell^{k(k-1)/2} a(\ell, k) X^k = \det(I - \rho(\mathrm{Frob}_\ell)X)$$

for all ℓ not dividing pN. Then we say that ρ is *attached* to v or that v corresponds to ρ. [1, p. 523]

A character of a group G is a homomorphism $\chi : G \to F^\times$, where $F^\times$ is the multiplicative group of a field F. Any character of the inertia group I_p (defined in Section 4.1) of order dividing $p-1$ is a power of a cyclotomic character ω (that is, $\omega(\mathrm{Frob}_\ell) = \ell$ for all prime $\ell \neq p$); in general, any character of I_p of order dividing $p^n - 1$ is a power of a fundamental character of niveau n (see [10, p. 267]). In our work, the image of I_p under a representation ρ is cyclic of order 8. Since the only irreducible representations of an abelian group are one-dimensional (see [6, p. 81]), we have that the restriction of a representation ρ ramified at p to I_p is similar to

$$\begin{bmatrix} \omega^a & & \\ & \omega^b & \\ & & \omega^c \end{bmatrix}.$$

The predicted weight for ρ is then the irreducible $GL_3(\mathbb{F}_p)$-module $V = F(a-2, b-1, c)$.

Vaguely stated, the generalized claim is that ρ is attached to an eigenclass in $H^3(\Gamma_0(N), V \otimes \epsilon)$. H^3 is the third cohomology group (the three-dimensional analog to modular forms; see [2]), and $\Gamma_0(N)$ is the subgroup of matrices in $SL_3(\mathbb{Z})$ whose first row is congruent to $(*, 0, 0)$ modulo N, as in [1].

Conjecture 2 (Generalized Conjecture). If $\rho : G_{\mathbb{Q}} \to GL_n(\mathbb{F}_p)$ is odd with level N and nebentype ϵ, then ρ is attached to a cohomology class in $H^*(\Gamma_0(N), V \otimes \epsilon)$ for some weight V. If $n = 3$ and ρ is not the sum of an odd 2-dimensional representation and a character, then * can be taken to be 3. [1, pp. 531-2]

Here ρ being odd means ρ "satisfies strict parity" (see Definition 2.10 in [1]). Note that Serre's conjecture is a special case of Conjecture 2. In addition, [1] gives specific predictions about which weights V yield eigenclasses attached to ρ. In the case above, where we can diagonalize the restriction of ρ to I_p in terms of powers of cyclotomic characters, we can take $V = F(a-2, b-1, c)$.

3 Galois representations with image isomorphic to $\widetilde{S}_4$

3.1 Structure of $\widetilde{S}_4$

The Galois representations in this paper have image isomorphic to $\widetilde{S}_4$, where $\widetilde{S}_4$ is a central extension of S_4 isomorphic to $GL_2(\mathbb{F}_3)$. In order to fully understand these Galois representations, we first need to understand the structure of $\widetilde{S}_4$. We use the isomorphism between $\widetilde{S}_4$ and $GL_2(\mathbb{F}_3)$ and rational canonical form to study this structure.

Using rational canonical form, we may prove

Theorem 1. *$GL_2(\mathbb{F}_3)$ has eight conjugacy classes.*

Proof. Table 3 gives the lists of invariant factors for each possible characteristic polynomial of elements in $GL_2(\mathbb{F}_3)$. (The other quadratics with coefficients in $\mathbb{F}_3$ have rational canonical form with determinant 0.) Each matrix represents a conjugacy class in $GL_2(\mathbb{F}_3)$. □

We will focus on the two conjugacy classes containing elements of order 8. The elements in one class have trace 1, while those in the other have trace -1. Note that an element of order 8 in $GL_2(\mathbb{F}_3)$ is conjugate to its cube: if $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in GL_2(\mathbb{F}_3)$, then

$$\mathrm{Tr}(A^3) = a^3 + 3abc + 3bcd + d^3,$$

which, when reduced modulo 3, becomes $a + d = \mathrm{Tr}(A)$ (note that all elements in $\mathbb{F}_3$ are cubes of themselves). Since there are only two conjugacy classes of elements of order 8 in $GL_2(\mathbb{F}_3)$, each having a different trace, A and A^3 must be conjugate.

Characteristic Polynomial	Invariant Factors	Rational Canonical Form	Order
x^2+x+1	$x+2, x+2$	$\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$	1
x^2+x+1	x^2+x+1	$\left[\begin{smallmatrix}0 & 2\\ 1 & 2\end{smallmatrix}\right]$	3
x^2+2x+1	$x+1, x+1$	$\left[\begin{smallmatrix}2 & 0\\ 0 & 2\end{smallmatrix}\right]$	2
x^2+2x+1	x^2+2x+1	$\left[\begin{smallmatrix}0 & 2\\ 1 & 1\end{smallmatrix}\right]$	6
x^2+2	x^2+2	$\left[\begin{smallmatrix}1 & 0\\ 0 & 2\end{smallmatrix}\right]$	2
x^2+1	x^2+1	$\left[\begin{smallmatrix}0 & 2\\ 1 & 0\end{smallmatrix}\right]$	4
x^2+x+2	x^2+x+2	$\left[\begin{smallmatrix}0 & 1\\ 1 & 2\end{smallmatrix}\right]$	8
x^2+2x+2	x^2+2x+2	$\left[\begin{smallmatrix}0 & 1\\ 1 & 1\end{smallmatrix}\right]$	8

Table 3: Rational Canonical Forms in $GL_2(\mathbb{F}_3)$

Note, however, that A^5 and A^7 are not conjugate to A, which can be checked by a similar argument.

3.2 Choosing ρ

In this section we define the Galois representation ρ that we will study, and we give a brief description of what we will do in the rest of the thesis.

Let K_{48} be the splitting field of

$$f(x) = x^8 - 3137(13204809x^6 + 17449903959258x^4 - 19634266857241x^2 + 2521744).$$

Using the software program Magma [3], we find $\mathrm{Gal}(K_{48}/\mathbb{Q}) \cong \widetilde{S}_4$. Also, K_{48} is ramified only at $p = 3137$, with ramification index 8. Let π be the projection of $G_{\mathbb{Q}}$ onto $\mathrm{Gal}(K_{48}/\mathbb{Q}) \cong \widetilde{S}_4$ and let i be an injective map from $\widetilde{S}_4$ to $GL_2(\mathbb{F}_p)$. Define θ to be the composition $i \circ \pi$.

Often we will speak of $\theta(s)$ where $s \in \mathrm{Gal}(K_{48}/\mathbb{Q})$. In this case we will actually mean $\theta(s')$ where $s' \in G_{\mathbb{Q}}$ is any element such that $\pi(s') = s$. For the structures that we study, such as inertia groups and Frobenius elements, this makes sense because they are preserved by the map π.

In our example, θ is even, since all roots of f are real (so that complex conjugation is the identity map, which is sent to the identity matrix). Hence Serre's conjecture does not apply to θ. There are two possible nonconjugate injections i; we choose i so that the restriction of θ to the inertia group $I_p \subset G_{\mathbb{Q}}$ is similar to a representation of the form

$$\begin{bmatrix} \omega^{\frac{p-1}{8}} & & \\ & & \\ & & \omega^{\frac{3(p-1)}{8}} \end{bmatrix},$$

as in [1]. We apply the generalized conjecture to θ by twisting and adding characters to θ: define $\rho = (\theta \otimes \omega^{-\frac{p-1}{8}}) \oplus \omega = (\theta \otimes \omega^{-392}) \oplus \omega$. Then ρ is 3-dimensional and odd, with

$$\rho|_{I_p} \sim \begin{bmatrix} \omega^{\frac{(p-1)}{4}} & & \\ & \omega & \\ & & \omega^0 \end{bmatrix} = \begin{bmatrix} \omega^{784} & & \\ & \omega & \\ & & \omega^0 \end{bmatrix}.$$

The predicted weight is thus $F(\frac{p-1}{4} - 2, 1 - 1, 0) = F(782, 0, 0)$.

Let σ be a generator of an inertia group at p in $\mathrm{Gal}(K_{48}/\mathbb{Q})$. We will compute $\mathrm{Tr}(\theta(\sigma))$ and determine whether $\sigma \in \mathrm{Frob}_3$, both using similar complex approximation techniques. Combining the results, we will obtain $\mathrm{Tr}(\theta(\mathrm{Frob}_3)) \equiv 3040 \bmod 3137$. Substituting this value into relation (3) (Section 6.1) will yield $\mathrm{Tr}(\rho(\mathrm{Frob}_3)) \equiv 60 \bmod 3137$, which is the computed eigenvalue referred to in [1, p. 545].

4 Frobenius Elements

4.1 Definition

Let $\mathfrak{p}$ be a prime in a number ring $\mathfrak{O}_K = \mathbb{A} \cap K$, where $\mathbb{A}$ is the ring of algebraic integers in $\bar{\mathbb{Q}}$ and K is a finite extension of $\mathbb{Q}$. Let L be a finite normal extension of K, and let $\mathfrak{P}$ be a prime in $\mathfrak{O}_L = \mathbb{A} \cap L$ lying over $\mathfrak{p}$. Let $G = \mathrm{Gal}(L/K)$.

Definition 7. The decomposition and inertia groups of $\mathfrak{P}$ over $\mathfrak{p}$ are, respectively,

$$D = D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}\},$$

$$E = E(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \text{ for all } \alpha \in \mathfrak{O}_L\}.$$

When $p \in \mathbb{Z}$, we use I_p to denote the inertia group. Clearly $E \subseteq D$; we will show $E \trianglelefteq D$ later. The decomposition group has fixed field of degree ef below L, where e, f are the ramification index and inertial degree, respectively, of $\mathfrak{p}$ in L. The inertia group has fixed field of degree e below L. [9, pp. 98-100]

Suppose now that $\mathfrak{p}$ is unramified in L. Then for each $\mathfrak{P}_i$ lying above $\mathfrak{p}$, the corresponding inertia group $E(\mathfrak{P}_i|\mathfrak{p})$ is trivial. This gives an isomorphism from the decomposition group $D(\mathfrak{P}_i|\mathfrak{p})$ to the Galois group $\bar{G}$ of $\mathfrak{O}_L/\mathfrak{P}_i$ over $\mathfrak{O}_K/\mathfrak{p}$. To see this, let $\sigma \in D$, and define $\bar{\sigma} : \mathfrak{O}_L/\mathfrak{P}_i \to \mathfrak{O}_L/\mathfrak{P}_i$ by

$$\bar{\sigma}(\alpha + \mathfrak{P}_i) = \sigma(\alpha) + \mathfrak{P}_i$$

for $\alpha \in \mathfrak{O}_L$. Using the fact that $\sigma \in D$, one may show that $\bar{\sigma}$ is a well-defined homomorphism fixing $\mathfrak{O}_K/\mathfrak{p}$. Because the kernel of a field homomorphism is either trivial or the entire image, and $\bar{\sigma}(1) = 1$, we must have that $\bar{\sigma}$ is 1-1. Also, $\bar{\sigma}$ is onto by virtue of the fact that σ is an automorphism. Hence $\bar{\sigma} \in \bar{G} =$

$\mathrm{Gal}((\mathfrak{O}_L/\mathfrak{P}_i)/(\mathfrak{O}_K/\mathfrak{p}))$. The kernel of the map $\sigma \mapsto \bar{\sigma}$ is E since if $\alpha+\mathfrak{P} = \sigma(\alpha)+\mathfrak{P}$, we have $\sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}$; i.e., $\sigma \in E$. (This implies $E \trianglelefteq D$.) Also, by [9, p. 101], $|D/E|$ is the inertial degree f, which by definition is equal to $|\bar{G}|$. Hence $D/E \cong \bar{G}$. In the case where $\mathfrak{p}$ is unramified in L, we have that E is trivial; therefore, $D \cong \bar{G}$.

Definition 8. Let the Galois group $\bar{G}$ of the finite field extension $(\mathfrak{O}_L/\mathfrak{P}_i)/(\mathfrak{O}_K/\mathfrak{p})$ be generated by the mapping ϕ which sends every $x \in \mathfrak{O}_L/\mathfrak{P}_i$ to $x^{\|\mathfrak{p}\|}$, where $\|\mathfrak{p}\|$ is the index of $\mathfrak{p}$ in $\mathfrak{O}_K$, i.e., $|\mathfrak{O}_K/\mathfrak{p}|$. Define the *Frobenius* $\mathrm{Frob}_{\mathfrak{P}_i}$ to be the unique $\sigma \in D(\mathfrak{P}_i|\mathfrak{p})$ such that $\bar{\sigma} = \phi$, where $\bar{\sigma}$ is defined as above.

The Frobenius satisfies

$$\mathrm{Frob}_{\mathfrak{P}_i}(\alpha) \equiv \alpha^{\|\mathfrak{p}\|} \pmod{\mathfrak{P}_i}$$

for all $\alpha \in \mathfrak{O}_L$. Since $\mathfrak{p}$ is unramified in $\mathfrak{O}_L$, $\mathrm{Frob}_{\mathfrak{P}_i}$ is the only element in G with this property. Also,

$$\mathrm{Frob}_{\sigma\mathfrak{P}_i} = \sigma \mathrm{Frob}_{\mathfrak{P}_i} \sigma^{-1} \tag{1}$$

for each $\sigma \in G$. Since all primes lying over $\mathfrak{p}$ are of the form $\sigma\mathfrak{P}_i$ for some $\sigma \in G$, Frobenius elements of primes lying above $\mathfrak{p}$ are conjugate, so that the conjugacy class of such elements is uniquely determined by $\mathfrak{p}$ [9, pp. 108-9]. This class is therefore denoted $\mathrm{Frob}_{\mathfrak{p}}$. Because the trace function is an invariant over a similarity class of matrices, the trace of the image of a Frobenius class under a Galois representation is well-defined.

Suppose now $L = K[\alpha]$, where $\alpha \in \mathfrak{O}_L = \mathbb{A} \cap L$, and let p be the prime in $\mathbb{Z}$ lying under $\mathfrak{p}$. Let g be the minimal polynomial of α over K. We can write, for appropriate integers e_i and r,

$$\bar{g} = \prod_{i=1}^{r} \bar{g}_i^{e_i},$$

where the g_i are polynomials over $\mathfrak{O}_K$ and the bar represents reduction mod $\mathfrak{p}$. We wish to establish a relation between the cycle structure of $\mathrm{Frob}_{\mathfrak{p}}$, considered as a permutation of the roots of g, and the factorization of g. This will prove useful in determining the Frobenius. We first state two lemmas from [9]:

Lemma 1. Assume $p \nmid |\mathfrak{O}_L/\mathfrak{O}_K[\alpha]|$. The prime decomposition of $\mathfrak{p}\mathfrak{O}_L$ is given by

$$\mathfrak{p}\mathfrak{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i},$$

where $\mathfrak{q}_i$ is the ideal $(\mathfrak{p}, g_i(\alpha))$ in $\mathfrak{O}_L$ generated by $\mathfrak{p}$ and $g_i(\alpha)$. Furthermore, the inertial degree of $\mathfrak{q}_i$ over $\mathfrak{p}$ is equal to the degree of g_i for each i.

Proof. See [9, Thm. 27]. □

Lemma 2. Let M be the Galois closure of L/K, and let $G = \mathrm{Gal}(M/K)$. Let H be the subgroup of G fixing L, and denote by ϕ the Frobenius of a prime $\mathfrak{P} \subset \mathfrak{O}_M = \mathbb{A} \cap M$ lying over $\mathfrak{p}$. Suppose that the set of left cosets of H in G is partitioned into the sets

$$\{\sigma_1 H, \phi\sigma_1 H, ..., \phi^{m_1-1}\sigma_1 H\}, ..., \{\sigma_r H, \phi\sigma_r H, ..., \phi^{m_r-1}\sigma_r H\},$$

where each $\sigma_i \in G, m_i \in \mathbb{Z}^+$, and $\phi^{m_i}\sigma_i H = \sigma_i H$. Then the splitting of $\mathfrak{p}$ in L is given by

$$\mathfrak{p}\mathfrak{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i,$$

where for each i, $\mathfrak{q}_i = \sigma_i(\mathfrak{P}) \cap \mathfrak{O}_L$. Also, for each i, the inertial degree of $\mathfrak{q}_i$ over $\mathfrak{p}$ is m_i.

Proof. See [9, Thm. 33]. □

Theorem 2 (Dedekind). *Given a monic irreducible degree n polynomial $g(x) \in \mathbb{Z}[x]$ with splitting field K, the cycle structure of $Frob_p$ in the symmetric group S_n of permutations of the n roots of $g(x)$ for a prime p not dividing the discriminant of $g(x)$ is given by the factorization of $g(x)$ mod p. In other words, if*

$$g(x) = \prod_{i=1}^{k} g_i(x) \ (mod\ p),$$

then $Frob_p = \prod_{i=1}^{k}$ (d_i-cycles), where, for each i, d_i is the degree of $g_i(x)$.

Proof. Let p be a prime not dividing the discriminant of $g(x)$ and let α be a root of $g(x)$. By Lemma 1, we have that in $\mathbb{Q}(\alpha)$,

$$p\mathfrak{O}_{\mathbb{Q}(\alpha)} = \prod_{i=1}^{r} \mathfrak{q}_i,$$

where $\mathfrak{q}_i = (p, g_i(\alpha)) \subset \mathfrak{O}_{\mathbb{Q}(\alpha)} = \mathbb{A} \cap \mathbb{Q}(\alpha)$ and the inertial degree of $\mathfrak{q}_i$ over p is d_i. (Note that the ramification index for each i is 1 since p does not divide the discriminant of g.) On the other hand, the sizes m_i of the orbits of Frob_p as it acts on the cosets of $H = \mathrm{Gal}(K/\mathbb{Q}(\alpha))$ are d_i, by Lemma 2; therefore, the sizes of the orbits are the degrees of the g_i. Also, there is a natural bijection between the cosets of H and the roots of $g(x)$ which preserves the action of the Galois group: since H fixes α, we have that given $a \in G$, elements of aH send α to $a(\alpha)$, which is a root of $g(x)$. Hence we see that the m_i determine the cycle structure of the Frobenius, considered as a permutation of the roots of $g(x)$. Because the degrees of the irreducible factors of $g(x)$ reduced mod p are equal to the inertial degrees of the primes in the prime decomposition of p in $\mathbb{Q}(\alpha)$, which are equal to the lengths of the cycles in the cycle structure of the Frobenius, the result follows. □

4.2 Complex Approximations

Let q be a prime in $\mathbb{Q}$. For each prime in K_{48} with inertial degree 8 and ramification index 1 over q, there is a Frobenius element of order 8, which must be in one of the two conjugacy classes of elements of order 8 in $\widetilde{S}_4 \cong GL_2(\mathbb{F}_3)$. Let $\mathfrak{q}_{48}$ be a prime having decomposition group $H = \langle\sigma\rangle$, where σ is an element of order 8 in $\widetilde{S}_4$. (The decomposition group is necessarily cyclic; see [9, p. 101].) We may choose $\mathfrak{q}_{48}$ so that either σ or σ^7 is $\mathrm{Frob}_{\mathfrak{q}_{48}}$. We wish to determine whether σ is a Frobenius element for $\mathfrak{q}_{48}$.

As we saw in Section 3.1, if σ is a Frobenius element with order 8, then σ^3 is in the same Frobenius conjugacy class. Also, σ^5 is not conjugate to σ, so the two conjugacy classes may be distinguished by which of them contains σ and σ^3; the other contains σ^5 and σ^7.

Let f be as defined in Section 3.2, and denote its eight roots by $\alpha_1, ..., \alpha_8$. It suffices to show that the relation

$$\sigma(\alpha) \equiv \alpha^q \pmod{\mathfrak{q}_{48}} \tag{2}$$

does not hold for some $\alpha \in \mathfrak{O}_L$; we may then conclude that σ is not a Frobenius element for q. Let α be a root of f and $\beta = \sigma(\alpha) - \alpha^q$. Then if $\beta \notin \mathfrak{q}_{48}$, the relation (2) does not hold. Computations showing $\beta \notin \mathfrak{q}_{48}$ are not easily carried out in K_{48}; we therefore consider the norm N of β over the fixed field K_6 of H, given by

$$N = N_{K_6}^{K_{48}}(\beta) = \prod_{i=0}^{7} \sigma^i(\beta).$$

If $\beta \in \mathfrak{q}_{48}$, then we would have $N \in \mathfrak{q}_6$ (where $\mathfrak{q}_6 = \mathfrak{q}_{48} \cap K_6$). We therefore aim to show $N \notin \mathfrak{q}_6$, which would imply $\beta \notin \mathfrak{q}_{48}$. To do this, we investigate the minimal polynomial $g(x)$ of N over $\mathbb{Q}$; this enables us to perform calculations in

K_6. In determining Galois conjugates of N, consider the following alternate form of writing N:

$$N = \prod_{\phi \in H} \phi(\beta).$$

Given $\psi \in \widetilde{S}_4$, we have

$$\psi(N) = \prod_{\phi \in H} \psi\phi(\beta) = \prod_{\phi' \in \psi H} \phi'(\beta).$$

Therefore, any conjugate of N is a product of automorphisms evaluated at β, the product taken over a coset of H. This is equivalent to saying that $\psi(N) = \psi'(N)$ if and only if $\psi H = \psi' H$. Hence, each of the six conjugates of N may be expressed in terms of representatives of the six cosets of H—namely, the identity permutation, τ, τ^2, $\sigma\tau$, $\sigma^2\tau$, and $\tau\sigma\tau$, where if we take $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$, then $\tau = (1\ 3\ 8)(4\ 5\ 7)$ and σ generate $\widetilde{S}_4$. (The cosets can be found using the computer program Magma.) Then

$$g(x) = \prod_{\psi} (x - \psi(N)),$$

where ψ runs through the aforementioned coset representatives of H.

Because β is an algebraic integer, $g(x)$ is monic with integer coefficients. The roots of f, however, are given as complex number approximations, and therefore so are β, N, and the coefficients of $g(x)$. To recognize what the integer coefficients are, we calculate the approximations to far more digits than we expect the coefficients of $g(x)$ to have. For example, if the coefficient of $g(x)$ with greatest magnitude has 20 digits and we approximate the coefficients of $g(x)$ to 50 digits, it is easy for one to recognize what the corresponding integer coefficients for $g(x)$ are. (If we work with fewer digits than the coefficients have, the computer program GP/PARI [12] gives a truncation error when we try to round to the nearest integer) We then

create a simple procedure `checkint`, which determines whether a real number is within a predetermined range of an integer, returning an error message if not. The procedure is applied to the coefficients of our approximation to $g(x)$ to "recognize" the actual integer coefficients of $g(x)$. If there is no error message, we may conclude that we have the proper integers for the coefficients of $g(x)$, so that we may round each coefficient of the approximation of $g(x)$ to the nearest integer to finally obtain $g(x)$. (See Appendix)

To work with the number field defined by $g(x)$, we use the command `nfinit` in GP/PARI, which requires an irreducible polynomial in $\mathbb{Z}[x]$. We can therefore first check that $g(x)$ is irreducible. Now $K_6 = \mathbb{Q}(N)$ because $N \in K_6$ (so that $\mathbb{Q}(N) \subseteq K_6$) and the only subfield of degree 6 of K_6 is itself. Also, $\mathrm{Frob}_{\mathfrak{q}_{48}}$ is conjugate to $\mathrm{Frob}_{\mathfrak{q}_{48}}^3$ (see Section 3.1). Hence there is $\psi \in \widetilde{S}_4$ such that $\psi \mathrm{Frob}_{\mathfrak{q}_{48}} \psi^{-1} = \mathrm{Frob}_{\mathfrak{q}_{48}}^3$. From the property (1) noted in Section 4.1 above, we have $\psi(\mathfrak{q}_{48}) = \mathfrak{q}'_{48}$ for some prime $\mathfrak{q}'_{48}$, and $\mathrm{Frob}_{\mathfrak{q}'_{48}} = \mathrm{Frob}_{\mathfrak{q}_{48}}^3$. Since $\mathrm{Frob}_{\mathfrak{q}_{48}}$ and $\mathrm{Frob}_{\mathfrak{q}_{48}}^3$ are the only elements of the conjugacy class that are contained in H, there can be only two primes $\mathfrak{q}_6, \mathfrak{q}'_6$ with inertial degree 1 over q in K_6, $\mathfrak{q}_6$ lying under $\mathfrak{q}_{48}$, $\mathfrak{q}'_6$ lying under $\mathfrak{q}'_{48}$. The problem of determining whether $N \in \mathfrak{q}_6$ is resolved using a simple command in GP/PARI, namely, `nfeltval(F, x, P)`, which determines the largest power of a given prime P in which the element x appears in the prime ideal decomposition of P in the number field F. If `nfeltval` returns a 0 for both of the primes $\mathfrak{q}_6$ and $\mathfrak{q}'_6$, we can conclude that N is not an element of either prime, so that σ must not be a Frobenius element for q, implying that the Frobenius element for q must be in the other conjugacy class. If `nfeltval` returns a nonzero value for one of the primes, we run the program again for σ^7, which is in the other conjugacy class. If in both situations `nfeltval` returns a nonzero value for one of the primes, we cannot make a conclusion regarding

which of σ, σ^7 is in the Frobenius class. In the cases we checked, this last possibility never occurred, so that we were able to prove which class contains the Frobenius by proving which one does not contain the Frobenius.

5 Calculating Cyclotomic Characters

We now consider the 8-cycle σ as the generator of the inertia group $E(\mathfrak{p}_{48}|p)$ for a prime $\mathfrak{p}_{48}$ in K_{48} lying over a ramified prime p. (Note that $E(\mathfrak{p}_{48}|p)$ is the image of an inertia group $I_p \subset G_{\mathbb{Q}}$ at p.) We wish to calculate $\mathrm{Tr}(\theta(\sigma))$, where θ is as defined in Section 3.2. Combining this with the result of the immediately preceding discussion, we can obtain $\mathrm{Tr}(\theta(\mathrm{Frob}_q))$.

Let $f(x)$ be as before. Then a root α of $f(x)$ is a *uniformizer* of $\mathfrak{p}_{48}$; that is, $\alpha \in \mathfrak{p}_{48}$, $\alpha \notin \mathfrak{p}_{48}^2$. This is a result of $N_{\mathbb{Q}}^{K_{48}}(\alpha)$ being divisible by p but not by p^2. This ensures that (α) is divisible by a prime with norm p but not by a prime with norm p^2. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$ and a prime $\mathfrak{p}_8$ in $\mathbb{Q}(\alpha)$ lying over p has ramification index 8 in $\mathbb{Q}(\alpha)$, there can be no more ramification above that prime in K_{48}. Therefore, if $\alpha \in \mathfrak{p}_8$ but $\alpha \notin \mathfrak{p}_8^2$, we may conclude that $\alpha \in \mathfrak{p}_{48}$ and $\alpha \notin \mathfrak{p}_{48}^2$; i.e., that α is a uniformizer of $\mathfrak{p}_{48}$. Then

$$\omega^{\frac{p-1}{8}}(\sigma) \equiv \frac{\sigma(\alpha)}{\alpha} \pmod{\mathfrak{p}_8},$$

where ω is the cyclotomic character [10, p. 263]. We thus have

$$\mathrm{Tr}(\theta(\sigma)) = \omega^{\frac{p-1}{8}}(\sigma) + \omega^{\frac{3(p-1)}{8}}(\sigma) \equiv \frac{\sigma(\alpha)}{\alpha} + \left(\frac{\sigma(\alpha)}{\alpha}\right)^3 \pmod{\mathfrak{p}_8}.$$

Note that $\omega^{\frac{p-1}{8}}(\sigma)$ has order 8 in $\mathbb{F}_p^\times$. It is thus a primitive 8^{th} root of unity. Now, if ζ is a primitive 8^{th} root of unity, then ζ and ζ^3 are both roots of one of $x^2 + \bar{\eta}x - 1$ and $x^2 - \bar{\eta}x - 1$, where $\bar{\eta}$ is the mod p reduction of some $\eta \in \mathbb{Z}$ with

$\eta^2 \equiv -2 \bmod p$. To see this, let ζ be a root of $x^2 + \bar{\eta}x - 1$. Then

$$\begin{aligned}(\zeta^2)((\zeta^3)^2 + (\zeta^3)\bar{\eta} - 1) &= (\zeta^2)(-\zeta^2 + \zeta^3\bar{\eta} - 1) \\ &= -\zeta^4 - \zeta\bar{\eta} - \zeta^2 \\ &= 1 - \zeta\bar{\eta} - \zeta^2 \\ &= -(\zeta^2 + \zeta\bar{\eta} - 1) = 0,\end{aligned}$$

which implies $(\zeta^3)^2 + (\zeta^3)\bar{\eta} - 1 = 0$. Similarly, if ζ is a root of $x^2 - \bar{\eta}x - 1$, so is ζ^3. This implies $\mathrm{Tr}(\theta(\sigma)) = \pm\bar{\eta}$. We thus wish to determine whether

$$\beta = \frac{\sigma(\alpha)}{\alpha} + \left(\frac{\sigma(\alpha)}{\alpha}\right)^3 - \eta$$

has positive valuation at $\mathfrak{p}_{48}$. Note that where $\bar{\eta}$ exists modulo p, it can be represented by an integer, because all calculations are made mod p (For example, mod 3137, $\eta \equiv 97$ or 3040). Hence we know $\beta \in K_{48}$.

To see if the valuation of β at $\mathfrak{p}_{48}$ is positive, we use a method similar to that described for determining whether σ was a Frobenius element: we take the norm N of β over K_6 and find the minimal polynomial $g(x)$ corresponding to N. In this case, however, α is not contained in all primes in K_{48} lying above 2 and 397. Therefore, the principal ideals $(\sigma(\alpha))$ and (α) will not necessarily have the same prime factorization in K_{48}, meaning $\frac{\sigma(\alpha)}{\alpha}$, and hence β, is not necessarily an algebraic integer. So $g(x)$ cannot be expected to have integer coefficients, which is prerequisite to perform calculations in K_6. Unfortunately, there is no obvious choice of α that would cause β to be an algebraic integer. To eliminate this problem, observe that for any nonzero k and any positive integer i, because N is a root of $g(x)$, we have that k^iN is a root of $g(\frac{x}{k^i})$, hence also of $k^{6i}g(\frac{x}{k^i})$ (we multiply by k^{6i} because the degree of $g(x)$ is 6). We thus choose k divisible only by 2 and 397, and i large

enough that $h(x) = k^{6i} g(\frac{x}{k^i}) \in \mathbb{Z}[x]$. With $h(x)$, we can perform calculations in K_6, and because $\mathfrak{p}_{48}$ does not lie above either 2 or 397, $k^i\beta \in \mathfrak{p}_{48}$ if and only if β has positive valuation at $\mathfrak{p}_{48}$. Once again, using `nfeltval` we determine whether $N \in \mathfrak{p}_6$ (where $\mathfrak{p}_6 = \mathfrak{p}_{48} \cap K_6$), and this tells us whether $\beta \in \mathfrak{p}_{48}$.

6 Conclusion

6.1 Computational Results

Recall that in Section 3.2, we established $\rho = (\theta \otimes \omega^{-392}) \oplus \omega$. Taking the trace evaluated at the Frobenius element over q, we have

$$\mathrm{Tr}(\rho(\mathrm{Frob}_q)) \equiv q^{-392}(\mathrm{Tr}(\theta(\mathrm{Frob}_q))) + q \pmod{3137}, \tag{3}$$

since $\omega(\mathrm{Frob}_q) = q$ (ω being a cyclotomic character). As we have shown, if q has inertial degree 8,

$$\mathrm{Tr}(\theta(\mathrm{Frob}_q)) = \pm\bar{\eta}.$$

In [1, Sect. 8], Ash, Doud, and Pollack examined a cohomology class in the weight predicted by the generalized conjecture (specifically, $H^3(\Gamma_0(N), F(782, 0, 0))$), finding a unique one-dimensional Hecke eigenclass to which ρ should be attached. They computed the eigenvalue for $T(2, 1)$ and were able to show that it matched $\mathrm{Tr}(\rho(\mathrm{Frob}_2))$, since Frob_2 has order 3. The Frobenius Frob_3 at 3 has order 8, however, so they were unable to compute $\mathrm{Tr}(\rho(\mathrm{Frob}_3))$, although they did compute the two possible values for it. They also computed that $T(3, 1)$ has an eigenvalue equal to 60 (in $\mathbb{F}_{3137}$), and noted that this matched one of the two possible traces.

In our case, the unramified prime with inertial degree 8 in K_{48} was $q = 3$ and the ramified prime was $p = 3137$. Reduced modulo 3137, the two square roots of -2 are 97 and 3040. Our explicit computations show that $\mathrm{Tr}(\theta(\sigma)) \equiv 3040 \pmod{3137}$ and $\sigma \in \mathrm{Frob}_3$. Substituting 3040 for $\mathrm{Tr}(\theta(\mathrm{Frob}_3))$ into (3), we obtain $\mathrm{Tr}(\rho(\mathrm{Frob}_3)) \equiv 60 \pmod{3137}$. This matches the prediction of [1], giving more evidence for the generalized conjecture.

6.2 Future Work

Example 5.1 of [1] deals with the polynomial $x^4 - x^3 - 1017x^2 + 9665x + 60608$, whose splitting field K is ramified only at $p = 2713$. Considering the $\widetilde{S}_4$-extension containing $\mathrm{Gal}(K/\mathbb{Q})$, there is ambiguity in distinguishing between two possibilities for eigenvalues which would correspond to ρ at primes having Frobenius of order 8. (This problem has not been solved yet because no eigenvalues have been computed where there is any ambiguity.) The technique described in this paper can therefore be applied to such primes to resolve the problem.

In Example 5.2 of the same paper, as well as the successive paragraph, there are similar ambiguities in $\hat{A}_5$-extensions, only dealing in these cases with primes having Frobenius of order 5 or 10, since there are two conjugacy classes of elements of each of these orders. The ramified primes in the examples are $p = 3701$ and $p = 3821$, respectively. Using our method (with modification in the computer program to accommodate for the differing orders of Frobenius elements and the different Galois groups), we should once again be able to distinguish between the possibilities for eigenvalues corresponding to ρ in each case.

In all these examples, the eigenvalues of an eigenclass which should correspond to a Galois representation ρ have been calculated, but the authors of [1] were unable to unambiguously calculate $\mathrm{Tr}(\rho(\mathrm{Frob}_q))$ to compare with these eigenvalues. We propose to calculate these traces to strengthen the evidence given in [1] for the generalized conjecture.

Appendix: Computer Software

In the following program, `frob2` calculates whether `s` is a Frobenius for `p`. The procedure `order` rearranges the components of the vector `r` (which are the roots of `f`) to correspond with the coset representatives, expressed in terms of `u` and `t`. The program is executed in GP/PARI first with $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$ as `s`, then with $\sigma^7 = (1\ 8\ 7\ 6\ 5\ 4\ 3\ 2)$ as `s`. The outputs of the program are `0,8` for σ and `0,0` for σ^7, indicating that σ^7 is not a Frobenius for `p`, so that σ must be.

```
\p1000;

t=[3,2,8,5,7,6,4,1];
u=[2,3,4,5,6,7,8,1];

order(r,v)=[r[v[1]],r[v[2]],r[v[3]],r[v[4]],r[v[5]],r[v[6]],
r[v[7]],r[v[8]]];

checkint(c)=if(abs(c-round(c))>.0001,0,1);

{frob2(f,v,s,p)=r=polroots(f);r=order(r,v);
s2=[s[s[1]],s[s[2]],s[s[3]],s[s[4]],s[s[5]],s[s[6]],s[s[7]],s[s[8]]];
s3=[s[s[s[1]]],s[s[s[2]]],s[s[s[3]]],s[s[s[4]]],s[s[s[5]]],
s[s[s[6]]],s[s[s[7]]],s[s[s[8]]]];
s4=[s[s[s[s[1]]]],s[s[s[s[2]]]],s[s[s[s[3]]]],s[s[s[s[4]]]],
s[s[s[s[5]]]],s[s[s[s[6]]]],s[s[s[s[7]]]],s[s[s[s[8]]]]];
s5=[s[s[s[s[s[1]]]]],s[s[s[s[s[2]]]]],s[s[s[s[s[3]]]]],
s[s[s[s[s[4]]]]],s[s[s[s[s[5]]]]],s[s[s[s[s[6]]]]],
s[s[s[s[s[7]]]]],s[s[s[s[s[8]]]]]];
s6=[s[s[s[s[s[s[1]]]]]],s[s[s[s[s[s[2]]]]]],s[s[s[s[s[s[3]]]]]],
s[s[s[s[s[s[4]]]]]],s[s[s[s[s[s[5]]]]]],s[s[s[s[s[s[6]]]]]],
s[s[s[s[s[s[7]]]]]],s[s[s[s[s[s[8]]]]]]];
s7=[s[s[s[s[s[s[s[1]]]]]]],s[s[s[s[s[s[s[2]]]]]]],
s[s[s[s[s[s[s[3]]]]]]],s[s[s[s[s[s[s[4]]]]]]],
s[s[s[s[s[s[s[5]]]]]]],s[s[s[s[s[s[s[6]]]]]]],
s[s[s[s[s[s[s[7]]]]]]],s[s[s[s[s[s[s[8]]]]]]]];
ss=[s,s2,s3,s4,s5,s6,s7,[1,2,3,4,5,6,7,8]];
n=1;for(i=1,8,n=n*(r[ss[(i+1)%8+1][1]]-(r[ss[i%8+1][1]])^p));
n2=1;for(i=1,8,n2=n2*(r[t[ss[(i+1)%8+1][1]]]-
(r[t[ss[i%8+1][1]]])^p));
n3=1;for(i=1,8,n3=n3*(r[t[t[ss[(i+1)%8+1][1]]]]-
(r[t[t[ss[i%8+1][1]]]])^p));
n4=1;for(i=1,8,n4=n4*(r[u[t[ss[(i+1)%8+1][1]]]]-
(r[u[t[ss[i%8+1][1]]]])^p));
n5=1;for(i=1,8,n5=n5*(r[u[u[t[ss[(i+1)%8+1][1]]]]]-
```

```
(r[u[u[t[ss[i%8+1][1]]]]]^p));
n6=1;for(i=1,8,n6=n6*(r[t[u[t[ss[(i+1)%8+1][1]]]]]-
(r[t[u[t[ss[i%8+1][1]]]]]^p));
g=(x-n)*(x-n2)*(x-n3)*(x-n4)*(x-n5)*(x-n6);
for(i=0,5,if(checkint(polcoeff(g,i)),1,print(erra)));
g=round((x-n)*(x-n2)*(x-n3)*(x-n4)*(x-n5)*(x-n6));print(g);
d=poldisc(g);m=factor(d,0);addprimes(m[matsize(m)[1],1]);
nf=nfinit(g);pfact=idealprimedec(nf,p);
print(nfeltval(nf,x,pfact[1]));print(nfeltval(nf,x,pfact[2]));}


o=[2,3,4,5,6,7,8,1];oinv=[8,1,2,3,4,5,6,7];

f=x^8-41423485833*x^6+54740348720192346*x^4-
61592695131165017*x^2+7910710928
frob2(f,[6,5,1,2,3,4,8,7],o,3)
frob2(f,[6,5,1,2,3,4,8,7],oinv,3)
```

In the next program, `frob4d` calculates whether `a` is the trace of the image of `u` under θ (where `u` is as in `frob2` and θ is as defined in Section 3.2). The identifiers `order`, `f`, `t` are as in `frob2`.

```
{frob4d(f,v,p,a)=r=polroots(f);r=order(r,v);n=1;
for(i=1,8,n=n*(r[(i+1)%8+1]/r[i%8+1]+(r[(i+1)%8+1]^3)/
(r[i%8+1])^3-a));
n2=1;for(i=1,8,n2=n2*(r[t[(i+1)%8+1]]/r[t[i%8+1]]
+(r[t[(i+1)%8+1]]^3)/(r[t[i%8+1]])^3-a));
n3=1;for(i=1,8,n3=n3*(r[t[t[(i+1)%8+1]]]/r[t[t[i%8+1]]]
+(r[t[t[(i+1)%8+1]]]^3)/(r[t[t[i%8+1]]])^3-a));
n4=1;for(i=1,8,n4=n4*(r[u[t[(i+1)%8+1]]]/r[u[t[i%8+1]]]
+(r[u[t[(i+1)%8+1]]]^3)/(r[u[t[i%8+1]]])^3-a));
n5=1;for(i=1,8,n5=n5*(r[u[u[t[(i+1)%8+1]]]]/r[u[u[t[i%8+1]]]]
+(r[u[u[t[(i+1)%8+1]]]]^3)/(r[u[u[t[i%8+1]]]])^3-a));
n6=1;for(i=1,8,n6=n6*(r[t[u[t[(i+1)%8+1]]]]/r[t[u[t[i%8+1]]]]
+(r[t[u[t[(i+1)%8+1]]]]^3)/(r[t[u[t[i%8+1]]]])^3-a));
g=(x-n)*(x-n2)*(x-n3)*(x-n4)*(x-n5)*(x-n6);condish=6;
for(i=0,5,while(condish>(5-i),if(checkint(polcoeff(g,i)),
condish=condish-1;print(condish,i),g=g*2^6*397^6;
print(condish,i))));
g=subst(g,x,x/(polcoeff(g,6)^(1/6)));print(g);
denom=denominator([bestappr(polcoeff(g,6),10^20),
bestappr(polcoeff(g,5),10^20),bestappr(polcoeff(g,4),10^20),
bestappr(polcoeff(g,3),10^20),bestappr(polcoeff(g,2),10^20),
bestappr(polcoeff(g,1),10^20),bestappr(polcoeff(g,0),10^20)]);
print(denom);
g=g*denom;
g=real(round(g));
```

```
g=g*(polcoeff(g,6)^5);
h=x^6+(polcoeff(g,5))*x^5+(polcoeff(g,4)*polcoeff(g,6))*x^4+
(polcoeff(g,3)*polcoeff(g,6)^2)*x^3
+(polcoeff(g,2)*polcoeff(g,6)^3)*x^2
+(polcoeff(g,1)*polcoeff(g,6)^4)*x
+polcoeff(g,0)*polcoeff(g,6)^5;
print(h);
d=poldisc(h);m=factor(d,0);addprimes(m[matsize(m)[1],1]);
nf=nfinit(h);pfact=idealprimedec(nf,p);
print(pfact);
for(i=1,matsize(pfact)[2],if(pfact[i][3]==1,if(pfact[i][4]==1,
print("f=1 prime #",i,": ",nfeltval(nf,x,pfact[i])))));}


f=x^8 - 41423485833*x^6 + 54740348720192346*x^4
- 61592695131165017*x^2 + 7910710928;
frob4d(f,[6,5,1,2,3,4,8,7],3137,3040)
```

References

[1] Avner Ash, Darrin Doud, and David Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. **112** (2002), no. 3, 521–579.

[2] Avner Ash and Glenn Stevens, *Modular forms in characteristic l and special values of their L-functions*, Duke Math. J. **53** (1986), no. 3, 849–868.

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The MAGMA algebra system, I: The user language*, J. Symb. Comp. **24** (1997), 235–265.

[4] Henri Darmon, *Serre's conjectures*, CMS Conf. Proc. **17** (1995), 135–153.

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

[6] Gordon James and Martin Liebeck, *Representations and characters of groups*, Cambridge Mathematical Textbooks, Cambridge University Press, 1993.

[7] Chandrasekhar Khare, *On Serre's modularity conjecture for 2-dimensional mod p representations of $gal(\bar{\mathfrak{q}}/\mathfrak{q})$ unramified outside p*, preprint (2005).

[8] Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, New Jersey, 1992.

[9] Daniel A. Marcus, *Number fields*, Springer-Verlag, New York-Berlin-Heidelberg, 1977.

[10] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[11] ———, *Sur les représentations modulaires de degré 2 de Gal($\bar{\mathbb{Q}}/\mathbb{Q}$)*, Duke Math. J. **54** (1987), no. 1, 179–230.

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