2006-07-07

Proven Cases of a Generalization of Serre's Conjecture

Jonathan H. Blackhurst
Brigham Young University - Provo

PROVEN CASES OF A GENERALIZATION OF SERRE'S CONJECTURE

by

Jonathan Blackhurst

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 2006

BRIGHAM YOUNG UNIVERSITY

GRADUATE COMMITTEE APPROVAL

of a thesis submitted by

Jonathan Blackhurst

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	Jasbir Chahal

BRIGHAM YOUNG UNIVERSITY

As chair of the candidate's graduate committee, I have read the thesis of Jonathan Blackhurst 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

Date	Gregory R. Conner Graduate Coordinator

Accepted for the College

Date	Tom Sederberg, Associate Dean College of Physical and Mathematical Sciences

ABSTRACT

PROVEN CASES OF A GENERALIZATION OF SERRE'S CONJECTURE

Jonathan Blackhurst

Department of Mathematics

Master of Science

In the 1970's Serre conjectured a correspondence between modular forms and two-dimensional Galois representations. Ash, Doud, and Pollack have extended this conjecture to a correspondence between Hecke eigenclasses in arithmetic cohomology and n-dimensional Galois representations. We present some of the first examples of proven cases of this generalized conjecture.

Table of Contents

List of Tables

1 Introduction

Serre's conjecture has played an important role in number theory in recent years. Specifically, it was fundamental in establishing Fermat's Last Theorem. In the 1980's, the German mathematician Gerhard Frey claimed that a counterexample to Fermat's Last Theorem would give rise to an elliptic curve that was not modular. The Taniyama-Shimura conjecture, however, says that all elliptic curves are modular, so if Frey were correct, then the Taniyama-Shimura conjecture would imply Fermat's Last Theorem. Some months later, the American mathematician Ken Ribet was able to establish Frey's claim by proving part of a weak form of Serre's conjecture (Serre's epsilon conjecture). In the 1990's Princeton's Andrew Wiles proved a special case of the Taniyama-Shimura conjecture (the semistable case), and that was enough to establish Fermat's Last Theorem. Wiles's proof relied on proven cases of Serre's conjecture, so Serre's conjecture was key at two distinct instances in the historical development of the proof of Fermat's Last Theorem.

This paper will present examples of proven cases of a generalization of Serre's conjecture. We will begin in Section 2 by explaining Serre's conjecture, which outlines a correspondence between two-dimensional Galois representations and modular forms. To explain Serre's conjecture, we will need to define both Galois representations and modular forms. We will then describe the conjectured correspondence.

In Section 3 we will explain a generalization of this conjecture due to Ash, Doud, and Pollack. Where Serre's conjecture is a correspondence between two-dimensional Galois representations and modular forms, the ADP conjecture is a correspondence between n-dimensional Galois representations and Hecke eigenclasses in arithmetic cohomology. We will first describe the correspondence, then show how it includes

Serre's conjecture in the two-dimensional case.

In the following sections, we will find examples of proven cases of the ADP conjecture. We will build and prove these examples in four stages. First, we will find degree-4 and degree-5 polynomials which define the fixed field of the kernel of certain two-dimensional projective representations (and thus determine the representations). Second, we will lift these projective representations to non-projective representations using a theorem of Tate. Third, we will turn these two-dimensional non-projective representations into three-dimensional representations by an operation called taking the symmetric square. Finally, we can, in many cases, apply a theorem of Ash and Tiep to these three-dimensional representations to give us proven examples of the ADP conjecture.

2 Serre's Conjecture

Serre's conjecture gives a correspondence between analytic objects called modular forms and algebraic objects called Galois representations. We will first describe these two objects, then explain the conjectured correspondence, and finally illustrate the conjecture with an example.

We should note that Chandrasekhar Khare has given a proof of Serre's conjecture. A preprint of the proof of a special case (the only case we need for this paper–the level one case) can be found on the internet [7].

2.1 Galois Representations

In this section we will first define Galois representations and discuss two related characters ω and ψ. We will then describe the level of a representation and the weight of the associated modular form predicted by Serre.

Definition 2.1. A Galois representation is a continuous homomorphism ρ from $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{GL}_n(k)$ for some algebraically closed field k. Here $G_{\mathbb{Q}}$ is given the profinite topology (subgroups of finite index and their cosets form a basis of open sets) and $\mathrm{GL}_n(k)$ inherits the product topology from k.

For our purposes, k will be the algebraic closure of a finite field $\bar{\mathbb{F}}_p$ (for p fixed) with the discrete topology. In addition, Serre's conjecture applies only when $n = 2$ and ρ is odd and irreducible. An odd Galois representation is one which takes complex conjugation to a nonscalar matrix (one which is not a scalar multiple of the identity).

The Characters ω and ψ In what follows, restricting he domain of the representation will allow us to describe a Galois representation as a diagonal matrix where the non-zero entries are powers of certain characters from inertia at p to $\bar{\mathbb{F}}_p$. These characters are the cyclotomic character ω and the niveau two characters ψ and ψ'. The cyclotomic character has order $p-1$. The niveau two characters have order p^2-1 and satisfy the relations $\psi^p = \psi'$ and $\psi'^p = \psi$. In addition, the niveau two characters are related to the cyclotomic character in that $\psi^{p+1} = \psi'^{p+1} = \omega$. These characters and their properties are described more explicitly in [10].

2.1.1 Level

For the representations we will consider, the level will always be 1. For the general case, Serre gives a formula for the level in [12], which we repeat here for convenience.

Given a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(V)$, where V is a two-dimensional vector space over $\bar{\mathbb{F}}_p$, for every prime $\ell \neq p$ we choose an extension to $\bar{\mathbb{Q}}$ of the ℓ-adic valuation of $\mathbb{Q}$ and let

$$G_0 \supset G_1 \ldots \supset G_i \supset \ldots$$

be the chain of ramification groups of G corresponding to that valuation. We let V_i be the subspace of V fixed by G_i and define

$$n(\ell, \rho) = \sum_{i=0}^{\infty} \frac{1}{[G_0 : G_i]} \dim V/V_i.$$

The level N of ρ is then defined to be

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

Since the representations we are concerned with are ramified only at p, we have that $n(\ell, \rho) = 1$ for all ℓ in the product and hence that $N = 1$.

2.1.2 Weight

The predicted weight of a modular form associated to a two-dimensional Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ is related to a conjugacy class of elements in $G_{\mathbb{Q}}$ called the Frobenius at p. The Frobenius at p is the inverse limit in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ of Frobenius elements in finite extensions. Let $\rho|_{I_p}$ be ρ's restriction to inertia at p. If $\rho|_{I_p}$ has order prime to p then its image is cyclic hence similar to a diagonal matrix

$$\rho|_{I_p} \sim \begin{pmatrix} \chi & \\ & \chi' \end{pmatrix}$$

where χ, χ' are powers of the niveau two characters ψ and ψ'.

If $\sigma \in I_p$ then $\mathrm{Fr}_p \, \sigma \, {\mathrm{Fr}_p}^{-1} = \sigma^p$[8, page 167]. Since conjugating a matrix leaves its eigenvalues unchanged, and since the eigenvalues of a diagonal matrix are its diagonal entries, conjugating a diagonal matrix just permutes its entries on the diagonal. Then $\rho(\mathrm{Fr}_p)\rho(\sigma)\rho(\mathrm{Fr}_p)^{-1} = \rho(\mathrm{Fr}_p \, \sigma \, \mathrm{Fr}_p^{-1}) = \rho(\sigma)^p$ so $\{\chi, \chi'\} = \{\chi^p, \chi'^p\}$ and there are two cases: either $\chi = \chi^p$ or $\chi = \chi'^p$.

In the $\chi = \chi^p$ case we have $\chi = \psi^c = \psi^{cp}$ so that $\psi^{c(p-1)} = 1$. Since ψ has order $p^2 - 1$, $c | p + 1$ so $c = a(p + 1)$ for some a. Since $\psi^{p+1} = \omega$ we have that $\chi = \psi^c = \psi^{a(p+1)} = \omega^a$, and, similarly, $\chi' = \omega^b$ for some b. Restricting to inertia, we now have

$$\rho|_{I_p} \sim \begin{pmatrix} \omega^a & \\ & \omega^b \end{pmatrix}.$$

By conjugating $\rho|_{I_p}$ if necessary, we can swap ω^a and ω^b to ensure that $a > b$. Then the predicted weight k of the modular form is $1 + a + pb$.

In the $\chi = \chi'^p$ case we have that $\chi = \psi^a = \psi'^{bp}$. Since $\psi = \psi'^p$ this gives that $\psi'^{ap} = \psi'^{bp}$ so that $a = b$. Then

$$\rho|_{I_p} \sim \begin{pmatrix} \psi^a & \\ & \psi'^a \end{pmatrix}$$

where ψ is the niveau two character. Since ψ has order p^2-1 we can ensure that $1 \leq a < p^2-1$ and can write a in the form $a = \alpha + p\beta$ where $\alpha > \beta$. The predicted weight of the modular form is $k = 1 + \alpha + p\beta$.

2.2 Modular Forms

In this section, we define and discuss modular forms. We then describe a set of linear operators on the vector space of modular forms called Hecke operators. Finally, we discuss two special types of modular forms: cusp forms and eigenforms.

Definition A modular form is a complex analytic function defined on the upper half-plane that satisfies a kind of functional equation and growth condition. If $f(z)$ is a modular form, then for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the functional equation dictates that

$$f(\gamma z) = (cz+d)^k f(z) \quad \text{where} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad \gamma z = \frac{az+b}{cz+d}$$

for some fixed even integer k called the weight of the modular form. Letting $a = b = d = 1$ and $c = 0$, we see that $f(z+1) = f(z)$ so f has a Fourier series expansion. The growth condition guarantees that the first nonzero term in the series is nonnegative so that

$$f(z) = \sum_{n=0}^{\infty} c_n q^n, \quad q = e^{2\pi i z}.$$

Hecke Operators There is a family of commuting linear operators $\{T_\ell\}$ called Hecke operators that act on the space of modular forms. For the modular forms we are concerned with (level 1, trivial nebentype) the action of the Hecke operators is

$$T_\ell(f) = \sum_{n=0}^{\infty} c_{np} q^n + p^{k-1} \sum_{n=0}^{\infty} c_n q^{np}$$

where f is given as a Fourier series, as above, and k is its weight [9, page 199].

Cusp Forms and Eigenforms A cusp form is a modular form such that $c_0 = 0$. If f is a cusp form normalized so that $c_1 = 1$ and such that f is also an eigenform of T_ℓ (so that $T_\ell(f) = \lambda f$ for some λ), then by examining the q^1 coefficient in the definition of the action of T_ℓ we see that $\lambda = c_\ell$. A more detailed exposition of modular forms is given in [13].

2.3 The Correspondence

Serre's conjecture states that for every odd, irreducible, two-dimensional Galois representation ρ of weight k there exists a cusp form $f(z)$ of weight k such that if

$$\sum_{n=1}^{\infty} c_n q^n, \quad q = e^{2\pi i z}$$

is the Fourier series expansion of f, then

$$c_\ell \equiv \mathrm{Tr}(\rho(\mathrm{Fr}_\ell)) \pmod{\ell}$$

for almost all primes ℓ. (Note this imposes the restriction that the c_n are integers or the congruence mod ℓ would not make sense.) Since the trace of a matrix is a similarity invariant, $\mathrm{Tr}(\rho(\tau))$ is the same for every $\tau \in \mathrm{Fr}_\ell$ and there is no ambiguity in defining $\mathrm{Tr}(\rho(\mathrm{Fr}_\ell))$.

2.4 Example

Let K be the splitting field of $f(x) = x^3 - x + 1$. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$. Since $G_\mathbb{Q}$ is the inverse limit of the Galois groups of the finite normal extensions of $\mathbb{Q}$, there is a natural projection $\pi : G_\mathbb{Q} \to \mathrm{Gal}(K/\mathbb{Q})$. There also exists a homomorphism $\sigma : S_3 \to \mathrm{GL}_2(\bar{\mathbb{F}}_{23})$ determined by

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

Identifying $\mathrm{Gal}(K/\mathbb{Q})$ with S_3, the composition $\rho = \sigma \circ \pi$ becomes a Galois representation.

Since 23 is the only prime that ramifies from $\mathbb{Q}$ to K, the inertia group of 23 in $\mathrm{Gal}(K/\mathbb{Q})$ has order 2, which is prime to 23, so the image of ρ restricted to inertia at 23 is similar to a diagonal matrix of order 2. Thus one of the diagonal entries is -1. Since $(-1)^{23} = -1$ we are in the $\chi = \chi^p$ case. In this case, we have that

$$\rho|_{I_p} \sim \begin{pmatrix} \omega^a & \\ & \omega^b \end{pmatrix}$$

which must have order 2. Noting that ω has order 22 and $a > b$ gives that $a = 11$ and $b = 0$ so that the weight of the Galois representation is $k = 1 + a + pb = 12$.

The corresponding weight-12 modular form is

$$\Delta = q \prod_{m=1}^{\infty} (1 - q^n)^{24} = \sum_{n=0}^{\infty} c_n q^n, \quad q = e^{2\pi i z}.$$

For all primes $\ell \neq 23$, $\pi(\mathrm{Fr}_\ell)$ reflects how f splits mod ℓ: if f splits completely $\pi(\mathrm{Fr}_\ell)$ is the identity; if f splits into a linear term and an irreducible quadratic, $\pi(\mathrm{Fr}_\ell)$ is the conjugacy class of 2-cycles; and if f is irreducible $\pi(\mathrm{Fr}_\ell)$ is the 3-cycles. From the way we specified σ above we see that $\mathrm{Tr}(\rho(\mathrm{Fr}_\ell))$ is then 2, 0, or -1, respectively. Expanding Δ and comparing its ℓth coefficient mod 23 with the factorization of f mod ℓ shows that

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41
$\mathrm{Tr}(\rho(\mathrm{Fr}_\ell))$	-1	-1	0	0	0	-1	0	0	*	-1	-1	0	-1
c_ℓ	-1	-1	0	0	0	-1	0	0	1	-1	-1	0	-1

ℓ	43	47	53	59	61	67	71	73	79	83	89	97
$\mathrm{Tr}(\rho(\mathrm{Fr}_\ell))$	0	-1	0	2	0	0	-1	-1	0	0	0	0
c_ℓ	0	-1	0	2	0	0	-1	-1	0	0	0	0

thus demonstrating the correspondence for primes less than 100.

3 The Conjecture of Ash, Doud, and Pollack

Ash, Doud and Pollack [1] have generalized Serre's Conjecture to a correspondence between n-dimensional Galois representations and Hecke eigenclasses of arithmetic cohomology. In this paper, we will concern ourselves only with the $n = 3$ case. We will begin by describing the weight and level of three-dimensional Galois representations. Next, we will explain the correspondence conjectured by Ash, Doud, and Pollack. Finally, we will show how the ADP Conjecture reduces to Serre's Conjecture in the two-dimensional case.

3.1 Level and Weight

Level The level for the ADP Conjecture is defined to be the same as the level in Serre's Conjecture as explained in section 2.1.1. As mentioned before, every representation we consider in this paper will be of level 1, or, in other words, ramified only at p.

Weight The weight of a Hecke eigenclass associated to a three-dimensional Galois representation is an irreducible $\mathrm{GL}_3(\bar{\mathbb{F}}_p)$ module. By a theorem of Doty and Walker [5], such modules are parameterized by p-restricted triples.

Definition 3.1. A p-restricted triple is a triple of integers (a, b, c) such that $0 \leq a - b \leq p - 1$, $0 \leq b - c \leq p - 1$, and $0 \leq c \leq p - 2$.

Definition 3.2. We denote by $F(a, b, c)$ the irreducible $\mathrm{GL}_3(\bar{\mathbb{F}}_p)$ module parameterized by the p-restricted triple (a, b, c).

Thus, unlike the two-dimensional case, three-dimensional Galois representations are described by a triple (a, b, c) instead of a single number. For three-dimensional

representations we are concerned with in this paper (the niveau 1 and 2 cases), we use the definition of weight as given in [6]. We repeat the definition here for convenience

Definition 3.3. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_3(\bar{\mathbb{F}}_p)$ be an odd, irreducible Galois representation. If

$$\rho|_{I_p} \sim \begin{pmatrix} \phi_1 & & \\ & \phi_2 & \\ & & \phi_3 \end{pmatrix}$$

then,

1. if $\phi_i = \omega^{a_i}$, we set $a_i = \alpha_i$;

2. if $\phi_i = \psi^m$, and $\phi_j = \psi'^m$ (with $i < j$), we write $m = a + bp$, with $0 \leq a - b \leq p - 1$, and take $a_i = a$, $a_j = b$.

The weight V of a Hecke eigenclass attached to ρ is then $V = F(a_1 - 2, a_2 - 1, a_3)$.

Remark 3.4. Note that by conjugating $\rho|_{I_p}$, we can permute the diagonal entries and thus get 6 possible weights for every representation ρ.

3.2 The Correspondence

To explain the correspondence, we first need to discuss Hecke operators, then define what it means for a three-dimensional Galois representation to be attached to an eigenvector, and, finally, prove a lemma about families of commuting linear operators.

Hecke operators Our description of Hecke operators comes from [1, page 253]. Let $\Gamma_0(N)$ be the subgroup of matrices in $\mathrm{SL}_n(\mathbb{Z})$ 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.

Let $\mathcal{H}(N)$ denote 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. 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, $0 \leq k \leq n$, 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 3.5. Let V be an $\mathcal{H}(pN)$-module and let $v \in V$ be a simultaneous eigenvector of all Hecke operators so that $T_{\ell,k}(v) = a_{\ell,k} \cdot v$ for ℓ prime and $0 \leq k \leq 3$. We say that a Galois representation ρ is attached to v if

$$\sum_{k=0}^{3} (-1)^k \ell^{\frac{k(k-1)}{2}} a_{\ell,k} x^k = \det(I - \rho(\mathrm{Fr}_\ell)x)$$

for all but finitely many primes ℓ.

Remark 3.6. Note that ρ being attached to v means that the eigenvalues of v determine the coefficients of the characteristic polynomials of $\rho(\mathrm{Fr}_\ell)$.

Remark 3.7. This definition would not be useful if simultaneous eigenvectors did not exist. That such vectors do exist is the content of the next lemma.

Lemma 3.8. *Let $\{T_2, T_3, T_5, \dots\}$ be a family of commuting linear operators over a finite-dimensional vector space V. Then there exists $v \in V$ such that v is a simultaneous eigenvector of the T_ℓ.*

Proof. Let λ_2 be an eigenvalue of T_2 and let E_2 be its corresponding eigenspace. Then for all p, T_ℓ takes E_2 to E_2. To see this, let $x \in E_2$ so that $T_2(x) = \lambda_2 x$. Then $T_2(T_\ell(x)) = T_\ell(T_2(x)) = T_\ell(\lambda_2 x) = \lambda_2 T_\ell(x)$ so $T_\ell(x) \in E_2$. Now let λ_3 be an eigenvalue of $T_3 : E_2 \to E_2$ and E_3 be the corresponding eigenspace. Inductively define λ_ℓ and E_ℓ in the same manner for all p, and let $v \in \bigcap E_\ell$ such that $v \neq 0$. (We can do this since E_ℓ has dimension at least one for all ℓ so that $\bigcap E_\ell$ has dimension at least 1.) Then v is a simultaneous eigenvector of the T_ℓ. □

With this background we can now state the Ash, Doud, Pollack conjecture:

Conjecture 3.9. *Given any odd three-dimensional representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_3(\bar{\mathbb{F}}_p)$ of weight V and level N, ρ is attached to a Hecke eigenclass in $H^3(\Gamma_0(N), V)$.*

3.3 ADP and Serre

The ADP Conjecture gives a correspondence between Galois representations and Hecke eigenclasses; whereas, Serre's Conjecture gives a correspondence between Galois representations and modular forms. To show that ADP implies Serre, there must be a relationship between Hecke eigenclasses and modular forms. Ash and Stevens have established this connection [2].

Theorem 3.10. *Modular forms of weight k level 1 correspond one-to-one with eigenclasses in $H^1(\mathrm{SL}_2(\mathbb{Z}), F(k-2, 0))$*

In the two-dimensional case, the equation that defines the ADP correspondence between Galois representations and Hecke eigenclasses is

$$\sum_{k=0}^{2}(-1)^k \ell^{\frac{k(k-1)}{2}} a_{\ell,k} x^k = \det(I - \rho(\mathrm{Fr}_\ell)x).$$

Now the definition of weight in the ADP Conjecture is enough to ensure that the x^2 term on both sides is the same. Furthermore, the constant coefficient on each side of the equation is 1. Thus the only thing we need to check is that the x coefficients on both sides are the same. The x coefficient on the right side is $-\operatorname{Tr}(\rho(\mathrm{Fr}_\ell))$; whereas, the x coefficient on the left side is $-a_{\ell,1}$. Now $T_{\ell,1} = T_\ell$ in the two-dimensional case, so, as noted in section 2.2, $a_{\ell,1} = c_\ell$. Thus $\operatorname{Tr}(\rho(\mathrm{Fr}_\ell)) = c_\ell$ and we see that ADP reduces to Serre's Conjecture in the two-dimensional case.

4 Constructing Projective Representations

In this section we will build two-dimensional projective representations—representations $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\bar{\mathbb{F}}_p)$. We build these representations by finding number fields K whose Galois group is isomorphic to a subgroup of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$. We get a projective representation by composing the projection of $G_{\mathbb{Q}}$ onto $\mathrm{Gal}(K/\mathbb{Q})$ with the isomorphism from $\mathrm{Gal}(K/\mathbb{Q})$ to the subgroup of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$. In section 5, we will lift these representations to nonprojective representations $\rho : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\bar{\mathbb{F}}_p)$. Finally, in section 6, we will turn these two-dimensional representations into three-dimensional ones by taking their symmetric square. It is from these three-dimensional representations that we will find proven examples of the ADP conjecture.

We build projective representations first for two reasons. First, it is easier to detect odd representations since scalar matrices in $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ are the identity. This means that any complex number field K we find will give us an odd representation. Second, the finite subgroup structure of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ is much simpler than $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$. In fact, it consists of only five types of groups: cyclic, dihedral, A_4, S_4, and A_5. Klein proved that these are the only finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ and since none of these groups have order divisible by p for $p > 5$ these are the only subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ for $p > 5$.

In this and the next paragraph, we will give a sketch of Klein's reasoning. First $\mathrm{PGL}_2(\mathbb{C})$ is isomorphic to the automorphisms of the Riemann Sphere $\mathrm{Aut}(\hat{\mathbb{C}})$. The reason is that automorphisms of $\hat{\mathbb{C}}$ are meromorphic functions on $\hat{\mathbb{C}}$, and such meromorphic functions are, in turn, rational functions. A rational function gives an n-to-1 mapping of $\hat{\mathbb{C}}$ to itself where n is the larger of the degrees of the numerator and the denominator of the function. Since automorphisms are 1-to-1 mappings,

$n = 1$, and the automorphisms of $\hat{\mathbb{C}}$ are fractional linear transformations. Fractional linear transformations, in turn, can be thought of as 2-by-2 matrices where function composition becomes matrix multiplication. Under this identification, all and only the scalar matrices act as the identity on $\hat{\mathbb{C}}$, so $\mathrm{Aut}(\hat{\mathbb{C}})$ is isomorphic to $\mathrm{GL}_2(\mathbb{C})$ mod scalar matrices, or, in other words, $\mathrm{Aut}(\hat{\mathbb{C}}) \cong \mathrm{PGL}_2(\mathbb{C})$.

We have reduced the question of finding the finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ to finding the finite subgroups of $\mathrm{Aut}(\hat{\mathbb{C}})$ which is easier since $\hat{\mathbb{C}}$ is a sphere, so we need to classify the finite automorphism groups of a sphere. Clearly such groups include all cyclic and dihedral groups, but are there any more? It turns out the only other ones are the rotation groups of the platonic solids: A_4 for the tetrahedron, S_4 for the cube and octahedron, and A_5 for the icosahedron and dodecahedron.

We have shown that finding projective representations is equivalent to finding cyclic, dihedral, A_4-, S_4-, and A_5-extensions of $\mathbb{Q}$. Because we want the symmetric square (which will be explained in section 6) to be irreducible, we will only want to find A_4-, S_4-, and A_5-extensions. Furthermore, to apply a result of Ash and Tiep, these extensions will need to be ramified at only one prime. Finally, since we want these projective representations to be odd, the extensions must be complex. We will represent these extensions with degree-4 and degree-5 polynomials.

In summary, then, we build projective two-dimensional representations in this section by finding degree-4 and degree-5 polynomials that define complex A_4-, S_4-, and A_5-extensions of $\mathbb{Q}$ ramified at only one prime. Except for Table 7 (where all roots of each polynomial are real), the tables in this section contain only polynomials with complex roots.

4.1 Nonexistence of A_4 Type

Serre's 1977 paper [9] implies the following theorem:

Theorem 4.1. *If $p > 5$ is prime, there are no complex A_4 extensions of $\mathbb{Q}$ ramified only at p.*

Proof. Suppose that K were such an extension ramified at p. Since the Klein-4 group is a normal subgroup of A_4 and the quotient of A_4 by this subgroup is $\mathbb{Z}/3\mathbb{Z}$, K contains a $\mathbb{Z}_3$ extension K_3 of $\mathbb{Q}$. Because $\mathbb{Z}_3$ is Abelian, K_3 is contained in a cyclotomic extension of $\mathbb{Q}$ by the Kronecker-Weber theorem. K_3 is ramified only at p, since K is, so K_3 is the subfield of $\mathbb{Q}(\zeta_p)$ corresponding to the index 3 subgroup of $\mathbb{Z}_p^\times$. This makes sense only if $3|(p-1) = \left|\mathbb{Z}_p^\times\right|$.

Since 3 is prime, p must be completely ramified in K_3. Because $p > 5$, p is tamely ramified in K, so the inertia groups I_p of the primes above p in K are cyclic of order divisible by 3. Since the largest cyclic subgroups of A_4 have order 3, $|I_p| = 3$.

Now K gives rise to a two-dimensional projective resolution $\tilde{\rho}$. By the lemma on page 248 of [9], the conductor of $\tilde{\rho}$ is exactly p. By Theorem 5 on page 228 of the same paper, we can then lift $\tilde{\rho}$ to a representation ρ which satisfies the hypotheses of Theorem 7 (page 245) and therefore must be of type S_4 or A_5, contradicting that it is of type A_4. Thus K does not exist. □

4.2 Type S_4

We can use the fundamental theorem of Galois theory to determine how a prime p can ramify in an S_4-extension ramified only at p.

Lemma 4.2. *An S_4-extension ramified only at p has ramification index 2 or 4.*

Proof. Since S_4 has A_4 as its unique index-2 subgroup, an S_4-extension K of $\mathbb{Q}$ has a unique subfield K_2 that is a quadratic extension of $\mathbb{Q}$. If S_4 is ramified only at $p > 3$, then K_2 is also, so $K_2 = \mathbb{Q}(\sqrt{p^*})$ where $p^* = \pm p$ with the sign chosen so that $p^* \equiv 1 \pmod 4$. Since p is ramified in K_2, its ramification index in K is divisible by 2. Since $p > 3$, it is tamely ramified in K so the inertia groups of the primes above p are cyclic. The even cyclic subgroups of S_4 have orders 2 and 4, so the ramification index of p in K is 2 or 4. □

We can use class field theory to give us a lemma that will help us speed up our search for S_4-extensions ramified at only one prime.

Lemma 4.3. *With the notation above, if p is the only prime ramified in K, then 3 divides the class number of K_2 and determines an S_3 extension K_6 of $\mathbb{Q}$. Furthermore, 4 must divide the ray class number of K_6 mod p.*

Proof. Since the Klein-4 group is the only normal subgroup of S_4 of index 6, and since the quotient of S_4 by this group is S_3, K has a unique subfield K_6 that is an S_3 extension of $\mathbb{Q}$. Since S_3 has a subgroup of index 2, K_6 contains a quadratic extension of $\mathbb{Q}$ and since this subfield is also a subfield of K, it must be K_2. Since the ramification index of p in K is not divisible by 6, primes above p cannot ramify from K_2 to K_6. Since no other primes can ramify, either, K_6 must be contained in the Hilbert class field of K_2 and thus 3 must divide the class number of K_2. Since only p can ramify in going from K_6 to K and $[K : K_6] = 4$ the ray class group of K_6 for p must be divisible by 4. □

For the following tables $[a, b, c, d]$ represents the polynomial $x^4+ax^3+bx^2+cx+d$.

p	Polynomial	4729	$[0, 3, -1, 4]$
229	$[0, 0, -1, 1]$	5261	$[-1, 4, -3, 7]$
257	$[0, 1, -1, 1]$	5333	$[-1, 1, -1, 3]$
761	$[-1, 1, 2, 1]$	5477	$[-1, -3, 3, 5]$
1129	$[-1, 0, -1, 2]$	5521	$[-2, 3, -1, 3]$
1229	$[-1, 3, -1, 3]$	5741	$[-1, 4, 2, 1]$
1489	$[-1, 4, -1, 2]$	5821	$[-2, 2, 1, 2]$
2089	$[-1, 0, 1, 3]$	6637	$[-1, 0, 4, 3]$
2213	$[0, -2, -1, 3]$	6997	$[0, 2, -5, 3]$
2677	$[-1, 0, -2, 3]$	7537	$[0, 5, -1, 4]$
2917	$[0, 4, -1, 2]$	7537	$[-1, 5, -4, 5]$
3221	$[0, 2, -3, 2]$	7573	$[0, 4, -5, 2]$
3229	$[-1, 2, -4, 3]$	7673	$[-1, -2, 1, 4]$
3877	$[0, 2, -1, 3]$	8069	$[0, -2, -1, 4]$
3889	$[-2, 1, 1, 2]$	8069	$[-1, 1, 5, 3]$
4001	$[-1, 3, -4, 3]$	8581	$[-1, 3, 1, 3]$
4481	$[-1, -2, 1, 5]$	8597	$[-1, 2, 1, 5]$
4493	$[-1, 4, -4, 3]$	9133	$[-1, 1, 1, 3]$
4649	$[0, 3, -3, 2]$	9281	$[0, 1, -8, 9]$

Table 1: S_4, $e = 2$, $p \equiv 1 \pmod 4$

p	Polynomial	p	Polynomial	p	Polynomial
283	$[0,0,-1,-1]$	3967	$[-1,-2,5,1]$	6691	$[-1,4,-2,-1]$
331	$[-1,1,1,-1]$	4027	$[0,-2,-1,-2]$	6763	$[0,-2,-5,-3]$
491	$[-1,-1,3,-1]$	4027	$[-1,0,2,-3]$	6791	$[-1,-1,-4,-1]$
563	$[-1,1,-1,-1]$	4423	$[-1,-3,4,1]$	6863	$[-1,-4,-3,-2]$
643	$[-1,0,-2,1]$	4663	$[-1,2,-5,2]$	6883	$[-1,-5,-1,3]$
751	$[-2,1,-1,-1]$	4703	$[0,-3,-3,1]$	6883	$[-1,-2,-2,5]$
1399	$[-1,0,1,-2]$	4799	$[-1,-4,5,3]$	6883	$[-2,-2,1,4]$
1423	$[-1,1,-2,-1]$	4999	$[-2,-1,-1,2]$	6967	$[-1,0,1,-5]$
1823	$[-1,0,3,-2]$	5231	$[-1,-1,2,-3]$	7331	$[-1,0,-6,7]$
1879	$[-1,-2,-3,1]$	5323	$[-2,0,-1,-2]$	7351	$[-2,3,6,-4]$
1931	$[0,0,-3,1]$	5431	$[-1,-2,-1,-2]$	7699	$[-1,0,-4,3]$
2243	$[-1,-1,-3,-1]$	5591	$[-1,-2,7,-9]$	7703	$[0,-1,-1,-3]$
2687	$[0,-3,-3,-2]$	5867	$[-2,2,3,-1]$	8123	$[-1,0,-4,-1]$
2767	$[-1,0,-3,2]$	5987	$[-2,4,1,-1]$	8287	$[-2,-1,-1,5]$
2843	$[-1,2,2,-1]$	6043	$[-1,3,-5,1]$	8707	$[-1,-3,-1,3]$
3119	$[-1,-2,-3,-4]$	6079	$[0,-3,-5,-1]$	8867	$[-2,-2,-3,5]$
3163	$[-1,-2,-2,1]$	6091	$[0,2,-3,-1]$	9059	$[0,2,-7,-1]$
3271	$[0,3,-1,-1]$	6199	$[-1,1,-2,-4]$	9127	$[-1,-5,6,4]$
3407	$[-1,-2,1,-3]$	6343	$[0,1,-8,1]$	9187	$[-2,-2,-3,-2]$
3559	$[-2,3,-1,-2]$	6571	$[-1,-2,4,1]$	9463	$[-1,0,3,-4]$
3571	$[-1,-5,5,3]$	6571	$[0,-2,-3,2]$	9491	$[-1,-3,-3,1]$
3919	$[0,1,-3,-1]$	6571	$[0,4,-5,1]$	9887	$[-2,3,-1,-3]$

Table 2: S_4, $e=2$, $p \equiv 3 \pmod 4$

p	Polynomial	p	Polynomial
229	$[-1, 29, -43, 17]$	5333	$[-1, 667, 4333, 104056]$
229	$[-1, 29, -43, 246]$	5477	$[-1, 685, -1027, 8622]$
773	$[-1, 92, -504, 1864]$	5477	$[-1, 685, -1027, 36007]$
1373	$[-1, 172, -944, 1432]$	6053	$[0, 0, -6053, 90795]$
1901	$[-1, 238, 594, 8755]$	6133	$[0, 0, -6133, 128793]$
2213	$[-1, 277, -415, 6250]$	6637	$[0, 0, -6637, 79644]$
2213	$[-1, 277, -415, 26167]$	6637	$[-1, 830, -11200, 166625]$
2557	$[0, 0, -2557, 17899]$	6997	$[0, 0, -6997, 69970]$
2917	$[0, 0, -2917, 29170]$	6997	$[-1, 875, 5685, 356929]$
2917	$[-1, 365, -547, 22094]$	7573	$[0, 0, -7573, 75730]$
3221	$[0, 0, -3221, 22547]$	7573	$[-1, 947, -24139, 138296]$
3221	$[-1, 403, -3825, 20169]$	8069	$[0, 0, -8069, 104897]$
3229	$[0, 0, -3229, 22603]$	8069	$[0, 0, -8069, 266277]$
3229	$[-1, 404, -5449, 101045]$	8069	$[-1, 1009, 6556, 86332]$
3877	$[0, 0, -3877, 38770]$	8069	$[-1, 1009, -9582, 570472]$
3877	$[-1, 485, -727, 47781]$	8581	$[0, 0, -8581, 102972]$
4493	$[0, 0, -4493, 44930]$	8581	$[-1, 1073, -1609, 1164435]$
4493	$[-1, 562, -7582, 25747]$	8837	$[-1, 1105, -1657, 288963]$
4597	$[-1, 575, -862, 99464]$	9133	$[0, 0, -9133, 91330]$
4933	$[-1, 617, -925, 184737]$	9133	$[-1, 1142, -33678, 994177]$
5261	$[-1, 658, 1644, 93280]$	9293	$[0, 0, -9293, 139395]$
5261	$[-1, 658, 17427, 151151]$	9413	$[0, 0, -9413, 94130]$
5333	$[-1, 667, -16999, 173385]$	9749	$[0, 0, -9749, 126737]$

Table 3: S_4, $e = 4$, $p \equiv 5 \pmod 8$

p	Polynomial	p	Polynomial
59	$[-1,-7,11,3]$	1427	$[-1,-178,981,-2291]$
107	$[-1,-13,20,-28]$	1579	$[-1,-197,-1283,-2387]$
139	$[-1,-17,26,120]$	1619	$[-1,-202,-3744,-22432]$
283	$[-1,-35,53,-21]$	1931	$[0,0,-1931,-5793]$
283	$[-1,-35,53,262]$	1931	$[-1,-241,2293,-7988]$
307	$[-1,-38,211,-301]$	2243	$[0,0,-2243,11215]$
331	$[-1,-41,62,-128]$	2243	$[-1,-280,-5187,92147]$
331	$[-1,-41,393,-459]$	2699	$[-1,-337,-2193,59009]$
419	$[-1,-52,288,-437]$	2803	$[0,0,-2803,14015]$
491	$[-1,-61,92,608]$	2819	$[-1,-352,-3700,-1883]$
491	$[-1,-61,-399,-865]$	3011	$[0,0,-3011,-9033]$
499	$[-1,-62,-156,-115]$	3163	$[-1,-395,593,35349]$
883	$[-1,-110,-276,5536]$	3163	$[-1,-395,3756,-12096]$
907	$[-1,-113,-737,-1031]$	3259	$[-1,-407,7129,-47090]$
1187	$[-1,-148,816,-2425]$	3299	$[0,0,-3299,6598]$
1259	$[-1,-157,-1023,-959]$	3299	$[-1,-412,-1031,27075]$
1291	$[-1,-161,1533,-3404]$	3331	$[-1,-416,-4372,87712]$

Table 4: S_4, $e=4$, $p\equiv 3 \pmod 8$

p	Polynomial	p	Polynomial
3371	$[0, 0, -3371, 20226]$	5563	$[-1, -695, 1043, -2499]$
3547	$[-1, -443, 665, 55602]$	5827	$[-1, -728, -7648, 17959]$
3571	$[-1, -446, -1116, 70597]$	5851	$[-1, -731, -4754, 62464]$
3571	$[-1, -446, -4687, -15107]$	5867	$[-1, -733, -16501, -133543]$
4027	$[0, 0, -4027, -24162]$	5867	$[-1, -733, -4767, -80740]$
4027	$[0, 0, -4027, 20135]$	5987	$[-1, -748, 28064, 219765]$
4027	$[-1, -503, 755, 62623]$	5987	$[-1, -748, -25819, -223273]$
4027	$[-1, -503, 755, 70677]$	6067	$[-1, -758, 10238, -27183]$
4027	$[-1, -503, -11326, -118592]$	6091	$[-1, -761, 7233, 18963]$
4363	$[-1, -545, 5181, 1585]$	6091	$[0, 0, -6091, 12182]$
4483	$[0, 0, -4483, -31381]$	6211	$[0, 0, -6211, 12422]$
4523	$[-1, -565, 14417, -95036]$	6323	$[0, 0, -6323, -75876]$
4691	$[0, 0, -4691, 9382]$	6427	$[-1, -803, -5222, 147344]$
4987	$[-1, -623, 10909, 290746]$	6571	$[0, 0, -6571, -45997]$
5011	$[0, 0, -5011, 40088]$	6571	$[-1, -821, 7803, -26361]$
5099	$[-1, -637, -4143, -8983]$	6571	$[-1, -821, 20945, -85500]$
5443	$[-1, -680, -7144, -40376]$	6571	$[-1, -821, -11910, -59216]$

Table 4: S_4, $e = 4$, $p \equiv 3 \pmod 8$ (*Cont.*)

p	Polynomial	p	Polynomial
6763	$[0, 0, -6763, 54104]$	8747	$[-1, -1093, -7107, -109440]$
6763	$[-1, -845, 8031, -157319]$	8779	$[-1, -1097, -7133, 400439]$
6779	$[-1, -847, 21608, -167436]$	8867	$[-1, -1108, -29372, -195455]$
6971	$[-1, -871, -5664, -850108]$	8867	$[-1, -1108, 6096, -505800]$
7459	$[-1, -932, 5128, -18968]$	9011	$[0, 0, -9011, 72088]$
7499	$[-1, -937, -6093, 124583]$	9043	$[0, 0, -27129, -63301]$
7547	$[0, 0, -7547, -22641]$	9059	$[-27177, 344242]$
7699	$[0, 0, -7699, -46194]$	9059	$[-1, -1132, 24346, -156657]$
7699	$[-1, -962, 12992, -331869]$	9067	$[0, 0, -9067, -136005]$
8059	$[0, 0, -8059, 24177]$	9091	$[-1, -1136, -30114, -401531]$
8123	$[0, 0, -8123, 48738]$	9187	$[-1, -1148, -30432, 1113529]$
8123	$[-1, -1015, 17769, -84879]$	9187	$[-1, -1148, 43064, -135903]$
8387	$[-1, -1048, -11008, 403264]$	9491	$[0, 0, -9491, -28473]$
8467	$[-1, -1058, 14288, -51695]$	9491	$[-1, -1186, -69403, -893155]$
8627	$[0, 0, -8627, -258810]$	9851	$[0, 0, -9851, 59106]$
8707	$[-1, -1088, 5986, -920051]$	9859	$[0, 0, -9859, -59154]$
8707	$[-1, -1088, -37549, 194445]$	9907	$[0, 0, -9907, -128791]$

Table 4: S_4, $e = 4$, $p \equiv 3 \pmod 8$ (*Cont.*)

4.3 Type A_5

Since A_5 is not solvable, we could not build up to an A_5-extension from smaller extensions like we did for the S_4-extensions. Instead we used targeted Hunter searches to find the degree-5 polynomials that defined the extensions we were looking for.

4.3.1 Hunter Searches

Hunter searches are based on a theorem that states that every number field has an integer that satisfies certain properties, properties which depend on the degree of the number field. For a degree-5 extensions K of $\mathbb{Q}$ the theorem asserts there exists $\alpha \in \mathcal{O}_K - \mathbb{Z}$ such that $0 \leq \mathrm{Tr}(\alpha) \leq 2$ and such that

$$\sum_{i=1}^{5} |\alpha_i|^2 \leq \frac{(\mathrm{Tr}(\alpha))^2}{5} + \sqrt[4]{\frac{4D}{5}}$$

where the α_i are the conjugates in $\mathbb{C}$ of α and D is the discriminant of K [4, page 445]. We will call the expression on the right-hand side of the inequality t_2. In our case, the Galois closure of K is an A_5-extension of $\mathbb{Q}$ and ramified only at p, so D is a square divisible only by p. Thus D is a power of p^2, and in fact we will later show that D must be either p^2 or p^4.

Now if $f(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5$ is a defining polynomial for K, then we already have bounds on a_1 since it equals $\mathrm{Tr}(\alpha)$. Further, since we know D, for each possible value of a_1 we can calculate t_2 and thus get bounds for a_5 by the arithmetic-geometric mean inequality:

$$|a_5| = \prod_{i=1}^{5} |\alpha_i| = \left(\sqrt[5]{|\alpha_1|^2 \cdots |\alpha_5|^2}\right)^{\frac{5}{2}} \leq \left(\frac{|\alpha_1|^2 + \cdots + |\alpha_5|^2}{5}\right)^{\frac{5}{2}} \leq \left(\frac{t_2}{5}\right)^{\frac{5}{2}}.$$

We can also get bounds for a_2, a_3, and a_4 using Newton's formulas and an inequality derived from properties of L^p norms.

Newton's Formulas Newton's formulas give relations between the coefficients $a_1, \ldots, a_5$ of $f(x)$, which are the elementary symmetric functions of the roots of $f(x)$, and the sums of the powers of those roots. The formulas state that

$$s_k = ka_k + \sum_{j=1}^{k-1} (-1)^j a_{k-j} s_j$$

where s_j is the sum of the j^{th} powers of the roots of $f(x)$. We can iteratively use these equations to express s_j as a function of $a_1, \ldots, a_i$ for $1 \leq i < j$. Then ka_k becomes s_k plus a polynomial in $a_1, \ldots, a_{k-1}$, so if we have chosen $a_1, \ldots, a_{k-1}$ and can bound s_k, we can get a range of possible values for a_k. To bound s_k we use the triangle inequality and the fact that, for $p \geq 1$, the L^p norm is less than or equal to the L^1 norm so that

$$|s_k| = \left| \sum_{i=1}^{5} \alpha_i^k \right| \leq \sum_{i=1}^{5} |\alpha_i|^k = \sum_{i=1}^{5} \left(|\alpha_i|^2 \right)^{\frac{k}{2}} \leq \left(\sum_{i=1}^{5} |\alpha_i|^2 \right)^{\frac{k}{2}} \leq t_2^{\frac{k}{2}}.$$

This inequality for s_k then determines upper and lower bounds for a_k, and for each value of a_k within these bounds we can then iterate this process to get the possible values of a_{k+1}. In this way we generate all possible combinations of coefficients of $f(x)$ and can then check one-by-one the polynomials thus generated to see if they define an A_5-extension ramified only at p.

To check each polynomial as quickly and efficiently as possible we determine, successively, whether its discriminant is a square, whether it is irreducible, and whether the number field it defines has Galois group A_5 and ramified only at p.

4.3.2 Targeting

We have just described a general Hunter search. We actually performed a targeted Hunter search because we knew the ramification properties of the fields we were

looking for. A targeted Hunter search uses the ramification of a number field to decrease the number of polynomials in the search space.

Ramification Possibilities If a prime p ramifies in a degree-5 extension K_5 of $\mathbb{Q}$, then p may factor one of nine ways in K_5:

$$\mathfrak{p}^5,\ \mathfrak{p}_1^4\mathfrak{p}_2,\ \mathfrak{p}_1^3\mathfrak{p}_2^2,\ \mathfrak{p}_1^3\mathfrak{p}_2\mathfrak{p}_3,\ \mathfrak{p}_3^3\mathfrak{p}_2,\ \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3,\ \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4,\ \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3,\ \mathfrak{p}_1^2\mathfrak{p}_2$$

If the Galois closure of K_5 is an A_5-extension of $\mathbb{Q}$, then the discriminant of K_5 is a square, so the exponent of the p-part of the discriminant must be even. Since the exponent of the p-part of the discriminant is $\sum_{i=1}^{r}(e_i-1)f_i$ [11, page 58] where $(p)=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ and f_i is the inertial degree of $\mathfrak{p}_i$, p must factor in one of five ways: $\mathfrak{p}^5$, $\mathfrak{p}_1^3\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_1^3\mathfrak{p}_2$, $\mathfrak{p}_1^2\mathfrak{p}_2$, or $\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3$. This implies that if p is the only prime that ramifies in K_5, then the discriminant of K_5 is p^2 or p^4.

The p^2 Case When the discriminant of K_5 was p^2, we had that p factored as $\mathfrak{p}_1^3\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_1^3\mathfrak{p}_2$, $\mathfrak{p}_1^2\mathfrak{p}_2$, or $\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3$ and we could combine the first two factorizations into one case so that there were two targeted Hunter searches to perform. A defining polynomial $f(x)$ for K_5 factored mod p in the first case as $(x+a)^3(x^2+bx+c)$ and in the second case as $(x^2+ax+b)^2(x+c)$ (where the quadratic may not or may be irreducible in the first case but definitely is not in the second). Both of these polynomials are determined by the three coefficients a, b, and c, so once we have chosen a_1, a_2, and a_3, we have limited the possibilities for a_4 and a_5 mod p. To determine these possibilities, we expand $f(x)$ and equate its x^4, x^3, and x^2 coefficients with $-a_1$, a_2, and $-a_3$, respectively. Using the a_1 equation in the first (respectively second) case, we could express b (respectively c) as a function of a_1 and a then use this expression in the a_2 equation to express c (respectively b) as a

polynomial in a_1, a_2, and a. Substituting these expressions for b and c into the a_3 equation then gave us a degree-3 polynomial satisfied by a whose coefficients were functions of a_1, a_2, and a_3. Factoring this polynomial mod p gave us up to three possible values of a. For each of these values of a we could determine b and c and thus a_4 and a_5 mod p. This reduced the number of polynomials we had to check by a factor of about p^2.

The p^4 Case When the discriminant of K_5 was p^4, p factored as $\mathfrak{p}^5$, so $f(x)$ factored as $(x+a)^5$ mod p. Once we had chosen a_1, a was determined so we knew the other four coefficients of $f(x)$ mod p. This decreased the search space by about a factor of p^4 over a general Hunter search, but the search still went much slower than the p^2 searches. This is because the discriminant of K_5 was larger, so t_2 and the bounds it determined on the coefficients of $f(x)$ were much bigger. We used the fact that we could loop through the possible values of a_5 before determining a_3 and a_4 together with a theorem in Cohen [4, page 458] to get better bounds on a_3 and a_4 based on the value of a_5. This sped up the search by more than a factor of 3. For degree-5 polynomials the theorem of Cohen describes the following process: For $1 \leq m \leq 4$, let z_m be the smallest positive solution of

$$(5-m)x^5 - \frac{t_2}{\sqrt[5]{|a_5|^2}}x^{5-m} + m = 0$$

and for $k = 3, 4$ let

$$t_k = |a_5|^{\frac{k}{5}} \max_{1 \leq m \leq 4} \left(m z_m^{k(m-5)/2} + (5-m) z_m^{km/2} \right)$$

Substitute t_k for $t_2^{\frac{k}{2}}$ as a bound for $|s_k|$ in the equation derived from Newton's formulas to bound a_k.

We checked the primes up to 10,000 but were unable to find any complex extensions with this kind of ramification. The reason is, there aren't any.

Before we prove that there aren't any, we prove a lemma about ramification in A_5-extensions of $\mathbb{Q}$.

Lemma 4.4. *Let K be an A_5-extension of $\mathbb{Q}$ with K_5 a subfield of K that is a degree-5 extension of $\mathbb{Q}$. If p is completely ramified in K_5 (has ramification index 5), then $p \equiv 1$ or $4 \pmod 5$.*

Proof. Let $\mathfrak{p}$ be the prime above p in K_5, let $\alpha \in \mathfrak{p} - \mathfrak{p}^2$, and let $f(x)$ be the minimal monic polynomial of $\beta = 5\alpha - \mathrm{Tr}(\alpha)$. Note that we have ensured that the x^4 coefficient of $f(x)$ is zero. Since α is in the only prime above p in K_5, it is in every prime $\mathfrak{P}$ above p in K, and its conjugates are also. Thus $\mathrm{Tr}(\alpha)$ is in every prime $\mathfrak{P}$, hence in $\mathfrak{P} \cap \mathbb{Q} = (p)$. This implies that $\mathrm{Tr}(\alpha) \in (p) = \mathfrak{p}^5$ in K_5 and thus that $\beta \in \mathfrak{p} - \mathfrak{p}^2$. Now the norm of β, $\mathrm{N}(\beta)$, is p since $\mathrm{N}(\beta) = \mathrm{N}((\beta)) = \mathrm{N}(\mathfrak{p}\prod_{i=1}^{r}\mathfrak{q}_i) = \mathrm{N}(\mathfrak{p})\,\mathrm{N}(\prod_{i=1}^{r}\mathfrak{q}_i) = p \cdot \mathrm{N}(\prod_{i=1}^{r}\mathfrak{q}_i)$ where $\mathfrak{q}_i$ are primes of K_5 not lying above p, so $p \| \mathrm{N}(\beta)$. Since p is completely ramified in K_5, $f(x)$ factors mod p as $(x-r)^5$. Since the x^4 coefficient of $f(x)$ is zero, r must be zero, and $f(x) \equiv x^5 \pmod p$. Thus $f(x) = x^5 + p(ax^3 + bx^2 + cx + d)$ and $p \nmid d$. Then the polynomial discriminant D of $f(x)$ is something times p^5 plus $5^5 d^4 p^4$ and is a square since $f(x)$ defines an A_5-extension of $\mathbb{Q}$. Then $\frac{D}{p^4}$ is also a square, hence a square mod p, hence $5^5 d^4$ is a square mod p, which implies that 5 is a square mod p, so by quadratic reciprocity, $p \equiv 1, 4 \pmod 5$. □

With this lemma, we are now ready to prove that there are no examples of the p^4 case.

Theorem 4.5. *Let K be a complex A_5-extension of $\mathbb{Q}$ ramified only at a prime $p > 5$ and let K_5 be a subfield of K that is a degree-5 extension of $\mathbb{Q}$. Then p is not completely ramified in K_5.*

Proof. Assume, by way of contradiction, that p is completely ramified in K_5. By the lemma, we know that $p \equiv 1$ or $4 \pmod 5$. Since p is completely ramified in K_5, $5 | |I_p|$ where I_p is the inertia group of the primes above p in K. Since K is an A_5-extension and $p > 5$, p is tamely ramified in K, so I_p is cyclic of order 5. Then since p is the only prime ramified in K, the discriminant of K is p^4 by [11].

Now K gives rise to a two-dimensional projective resolution $\tilde{\rho}$. If $p \equiv 1 \pmod 5$, then by the lemma on page 248 of [9], the conductor of $\tilde{\rho}$ is exactly p, so by Theorem 8 of the same paper, K must have discriminant p^2, contradicting that its discriminant is p^4.

If $p \equiv 4 \pmod 5$, let ρ be the unique lifting of $\tilde{\rho}$ of Theorem 5 of [9]. Then

$$\rho|_{I_p} \sim \begin{pmatrix} \psi^a & \\ & \psi'^a \end{pmatrix}$$

where since ρ has order 5 and $|\psi| = |\psi'| = p^2 - 1$, a is a multiple of $\frac{p^2-1}{5}$ and thus even. Now since K is complex, if ϵ is complex conjugation $\det(\rho(\epsilon)) = -1$. This contradicts that $\det(\rho(\epsilon)) = \omega(\epsilon)^a = (-1)^a = 1$ (since a is even). Thus there are no complex A_5-extensions of $\mathbb{Q}$ ramified at only one prime $p > 5$ where the ramification index of p is 5. □

For the following tables $[a, b, c, d, e]$ represents the polynomial $x^5 + ax^4 + bx^3 + cx^2 + dx + e$.

p	Polynomial	p	Polynomial
653	$[0, 3, -6, 2, -1]$	6053	$[-1, 7, -3, 28, 19]$
1061	$[-1, -4, 15, 32, 16]$	6133	$[-1, -3, 20, 27, 72]$
1381	$[-2, 8, -18, -1, -36]$	6277	$[-2, 11, 1, 1, 95]$
1553	$[0, -1, -6, 16, -1]$	6421	$[-1, 7, 38, 73, 125]$
1733	$[-1, -3, -3, 16, -11]$	6521	$[-2, 9, -20, -4, -11]$
2029	$[-1, 9, -10, 1, 8]$	6529	$[-2, 4, -31, 64, -52]$
2053	$[0, -10, -1, 22, 15]$	7349	$[-2, -21, -15, 58, -200]$
2293	$[-2, -7, 11, 33, 10]$	7433	$[-1, 12, -3, 31, 15]$
2609	$[-2, -1, -15, 58, -24]$	7649	$[-1, 3, 0, -4, -64]$
2777	$[-1, -3, 12, 21, -1]$	7717	$[-1, -10, -56, -72, -64]$
2861	$[-1, -3, -12, -11, -8]$	7933	$[-2, 9, -29, 17, -106]$
3089	$[0, -10, -8, 1, -48]$	8101	$[-1, 8, 19, 39, 169]$
3329	$[-2, 14, -15, 44, -15]$	8161	$[0, 7, -14, 6, -9]$
3733	$[0, 10, -1, 21, 1]$	8269	$[-1, 9, -55, 14, 136]$
3733	$[-1, 7, -28, 53, -39]$	8353	$[-1, 3, 42, -11, -148]$
3929	$[-1, 3, 14, -17, 46]$	8737	$[-2, 15, 9, -11, -127]$
4073	$[-2, 21, -5, 77, 121]$	9281	$[-1, -13, 25, 108, -128]$
4789	$[0, 11, -4, 10, -43]$	9293	$[-1, -11, -2, 43, 44]$
5081	$[0, -10, -3, 46, -275]$	9677	$[0, 1, -4, 18, 65]$
5233	$[-2, 5, -23, 58, -32]$	9689	$[-2, -11, 46, -79, 66]$
5413	$[0, 10, -1, 24, 1]$	9721	$[-1, 11, 48, -53, -264]$
5749	$[-1, 15, 7, 50, 87]$	9721	$[0, 9, -38, -74, -31]$
5953	$[-1, 7, -10, 11, 116]$	9749	$[-2, -1, -6, -24, 115]$

Table 5: A_5, $e = 2$ $p \equiv 1 \pmod 4$

p	Polynomial
2083	$[-1, 5, 11, 4, -1]$
2707	$[-2, 2, -8, 21, -62]$
3203	$[-1, -1, -9, 20, -11]$
3547	$[0, -8, -2, 31, 74]$
4027	$[-1, 9, 38, 13, -23]$
4483	$[-2, 6, 4, 17, 70]$
5171	$[0, -2, -29, -49, -49]$
6163	$[-1, 2, 43, 21, -67]$
6199	$[-2, 18, -19, 72, -45]$
6827	$[-2, -7, -11, 110, -48]$
7523	$[-2, 23, -20, 144, -171]$
7547	$[0, -3, -39, -41, -125]$
8627	$[-1, -9, 30, 69, -80]$
8647	$[-1, 12, -28, 56, -160]$
9851	$[-2, 28, -31, 114, -67]$
9907	$[-1, 13, 10, 22, 131]$

Table 6: A_5, $e = 2$, $p \equiv 3 \pmod 4$

p	Polynomial
4253	$[-2, -10, 23, -6, -4]$
6131	$[-1, -12, -3, 19, 8]$
6359	$[-2, -25, 84, -61, -6]$
7019	$[-1, -29, 76, -56, 8]$
7649	$[-1, -21, 26, -1, -1]$
8081	$[-1, -16, 33, -1, -20]$
10267	$[0, -25, -7, 116, -45]$
10433	$[-2, -27, -20, 42, -11]$
14779	$[0, -27, -3, 83, -28]$
15733	$[0, -17, -23, -1, 5]$
16811	$[-2, -33, 13, 12, 1]$
19139	$[-1, -19, 32, 43, -69]$
20231	$[-1, -15, 0, 29, 4]$

p	Polynomial
21817	$[-1, -35, 12, 225, 189]$
22643	$[-2, -49, 106, 292, 32]$
22721	$[-2, -25, 48, 108, -135]$
23011	$[0, -30, -37, 160, 244]$
23789	$[-1, -49, 207, -274, 105]$
24121	$[-2, -40, 71, 276, -65]$
24419	$[-2, -45, 126, 140, -352]$
24763	$[-1, -21, -28, 17, 29]$
26171	$[0, -50, -104, 89, 176]$
26591	$[-2, -31, -24, 72, 27]$
26731	$[-1, -23, 9, 124, 77]$
28537	$[0, -18, -21, 8, 11]$
29527	$[-2, -22, 33, 110, -100]$

Table 7: A_5, $e = 3$

5 Lifting Projective Representations

In the previous section, we constructed a projective representation $\tilde{\rho}$ by finding the fixed field K of its kernel. In this section we lift $\tilde{\rho}$ to a non-projective representation ρ and describe $\rho|_{I_p}$. A Theorem of Tate tells us how to lift $\tilde{\rho}$.

Theorem 5.1. *If $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ is ramified only at p and if $\tilde{\rho}|_{D_p}$ (where D_p is the decomposition group of p) lifts to a representation ρ'_p then there exists a unique lifting ρ of $\tilde{\rho}$ ramified only at p and such that $\rho|_{I_p} = \rho'_p|_{I_p}$.*

Proof. This is theorem 5 of [9] □

We will see that $\rho|_{I_p}$ is determined by the ramification index and the conductor of $\tilde{\rho}$. Thus there are four cases to consider based on whether the ramification index e is 2 or 4 and whether the conductor is p or p^2.

Before we discuss each case individually, we prove a lemma about lifting the decomposition groups.

Lemma 5.2. *If $\tilde{\rho}(D_p)$ is cyclic, then $\tilde{\rho}|_{D_p}$ lifts with no change in e.*

Proof. Since $\tilde{\rho}(D_p)$ is cyclic of even order and is a subgroup of S_4 or A_5, $\tilde{\rho}(D_p)$ has order 2 or 4. If it has order 2 then the images of the inertia and decomposition groups are the same and both lift to the subgroup of $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$ generated by

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

so e is unchanged. If $\tilde{\rho}(D_p)$ has order 4, then the inertia group has order 2 or 4. The decomposition group can be lifted to

$$\left\langle \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \right\rangle < \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$

where i is a fourth root of one. The inertia group will then lift to

$$\left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \text{ or } \left\langle \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$$

depending on whether it has order 2 or 4. In either case, the order e will be unchanged. □

Now we discuss each of the four cases individually.

5.1 Case 1: $e = 2$ and conductor is p

Theorem 8 of Serre [9] tells us that in this case $p \equiv 3 \pmod 4$. Since the conductor is p, the decomposition group is cyclic and $\tilde{\rho}$ can be lifted without changing inertia. If we just wanted $\rho|_{I_p}$ to have order 2, we could have

$$\rho|_{I_p} \sim \begin{pmatrix} \omega^{\frac{p-1}{2}} & \\ & \omega^{\frac{p-1}{2}} \end{pmatrix}$$

for example. However, its projective image must be nontrivial which rules this possibility out. The only remaining possibility is

$$\rho|_{I_p} \sim \begin{pmatrix} \omega^{\frac{p-1}{2}} & \\ & 1 \end{pmatrix}.$$

5.2 Case 2: $e = 2$ and conductor is p^2

We first determine the decomposition group D of p.

Theorem 5.3. *If $e = 2$ and the conductor is p^2, the decomposition group D is the Klein four group V.*

Proof. The conductor is p^2, so the decomposition group is not cyclic. Since the only non-cyclic subgroup of S_4—and A_5—that has a normal cyclic subgroup of order 2 is V, this must be the decomposition group. □

To determine a lift of $\tilde{\rho}$ we must now lift V to a subgroup G of $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$. This lift must satisfy two properties: first, G must be metacyclic, meaning it is the extension of a cyclic group F by another cyclic group I, and such that the action of some generator of F on I by conjugation is the pth power map; second, G must have a representation in $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$ whose image in $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ is V.

Before we prove the following theorem, it will be helpful to note that since theorem 8 of Serre [9] cited in the previous case is an if and only if statement, p is not 3 (mod 4). Thus we can write $p \equiv 1 + 2^n \pmod{2)^{n+1}}$ where $n \geq 2$. This implies $p \equiv 1 \pmod{2)^n}$.

Theorem 5.4. *The group* $G = \langle a, b | a^{2^{n+1}} = b^2 = 1, bab^{-1} = a^{2^n+1} \rangle$ *satisfies the requirements for the decomposition group.*

Proof. First, note that G is the extension of $F = \langle b \rangle$ by $I = \langle a \rangle$, so G is metacyclic, and we must show that b acts by conjugation on $\langle a \rangle$ as the pth power map. Since the order of a is 2^{n+1} and $p \equiv 1 + 2^n \pmod{2)^{n+1}}$, conjugating a by b sends a to $a^{2^n+1} = a^p$. Thus b acts as desired on the elements of I and G satisfies the first property of the desired lift.

Second, we will show that G has a matrix representation in $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$ whose projective image is V. We can send

$$a \to \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{2^n+1} \end{pmatrix} \qquad b \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

in $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$ where ζ is a primitive 2^{n+1}st root of unity. Now a^2 is the scalar matrix with ζ^2 on the diagonals, so the image of $\langle a^2 \rangle$ in $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ is trivial. Note that the representatives a, b, and ab of the cosets of $\langle a^2 \rangle$ are not scalar matrices, so the kernel of the projection map is precisely $\langle a^2 \rangle$ and the image of G in $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ has

order 4. Since every non-trivial element in this image has order 2, the image is indeed V. $\square$

In this case we may choose the lift ρ so that

$$\rho|_{I_p} \sim \begin{pmatrix} \psi^{\frac{p^2-1}{2^{n+1}}} & \\ & \psi'^{\frac{p^2-1}{2^{n+1}}} \end{pmatrix}.$$

To find the weight of this representation we first write p as $p = m2^n + 1$ where m is odd. We can then write

$$\begin{aligned} \frac{p^2-1}{2^{n+1}} &= p\frac{p-(2^n+1)}{2^{n+1}} + \frac{p(2^n+1)}{2^{n+1}} \\ &= p\frac{m2^n+1-2^n-1}{2^{n+1}} + \frac{(m2^n+1)(2^n+1)}{2^{n+1}} \\ &= p\frac{m-1}{2} + m2^{n-1} + \frac{m+1}{2} \end{aligned}$$

so that in the definition of the weight of the representation (see section 2.1.2)

$$\beta = \frac{m-1}{2} \text{ and } \alpha = m2^{n-1} + \frac{m+1}{2}.$$

Note that we do have $\beta < \alpha$ since $(m-1)/2 < (m+1)/2$. The weight of this representation is then $1 + m + m^2 2^{n-1}$.

5.3 Case 3: $e = 4$ and conductor is p

Theorem 8 of Serre [9] tells us that in this case $p \equiv 5 \pmod 8$. Since the conductor is p, the decomposition group is cyclic and $\tilde{\rho}$ can be lifted without changing inertia. If we just wanted $\rho|_{I_p}$ to have order 4, we could have

$$\rho|_{I_p} \sim \begin{pmatrix} \omega^{\frac{p-1}{4}} & \\ & \omega^{\frac{p-1}{4}} \end{pmatrix} \text{ or } \begin{pmatrix} \omega^{3\frac{p-1}{4}} & \\ & \omega^{\frac{p-1}{4}} \end{pmatrix}$$

for example. However, its projective image must have order 4, which rules these two possibilities out. Another possibility is that

$$\rho|_{I_p} \sim \begin{pmatrix} \omega^{3\frac{p-1}{4}} & \\ & 1 \end{pmatrix}.$$

However, we can multiply this representation by a power of the cyclotomic character (twist it) to get a representation with a smaller weight. Specifically, if we twist it by ω^s where $s = (p-1)/4$, we have

$$\rho \otimes \omega^s|_{I_p} \sim \begin{pmatrix} 1 & \\ & \omega^{\frac{p-1}{4}} \end{pmatrix} \sim \begin{pmatrix} \omega^{\frac{p-1}{4}} & \\ & 1 \end{pmatrix}$$

and this final representation has smallest weight possible.

5.4 Case 4: $e = 4$ and conductor is p^2

Since the conductor is p^2, the decomposition group is not cyclic and thus must be D_8, the dihedral group of 8 elements, because this is the only subgroup of S_4 with a normal cyclic subgroup of order 4. Since the center of D_8 is non-trivial, we cannot lift $\tilde{\rho}$ without changing the inertia and decomposition groups. The lemma after theorem 8 of Serre [9] tells us that $p \equiv 3 \pmod 4$. If $p \equiv 7 \pmod 8$, then since $(p^2-1)/8$ is even, ρ would be an even representation. Thus we may assume $p \equiv 3 \pmod 8$. Note that $\langle a, b | a^8, b^2 = 1, bab = a^3 \rangle$ is metacyclic with $I = \langle a \rangle$ and $F = \langle b \rangle$ and b acts by conjugation on a as the pth power map (since $p \equiv 3 \pmod 8$). By consulting character tables, we also see that D_{16} has a two-dimensional representation whose projective image is D_8. In lifting $\tilde{\rho}$ the decomposition and inertia groups at p must increase by a factor of 2. Thus $\rho|_{I_p}$ has order 8 and

$$\rho|_{I_p} \sim \begin{pmatrix} \psi^{\frac{p^2-1}{8}} & \\ & \psi^{\frac{p^2-1}{8}} \end{pmatrix}.$$

Since $p \equiv 3 \pmod 8$, we can determine the values α and β used in the formula for the weight of the representation. We have that $\frac{p^2-1}{8} = \alpha + p\beta = \frac{3p-1}{8} + p\frac{p-3}{8}$, so $\alpha = \frac{3p-1}{8}$ and $\beta = \frac{p-3}{8}$.

6 Proven Cases of ADP

In this section, we find proven cases of the ADP conjecture in the three-dimensional case. We use two-dimensional Galois representations we constructed in section 4 to build these proven cases. By taking the symmetric square of these representations, we get three-dimensional representations. We can then use a result of Ash and Tiep to show that these three-dimensional representations correspond to Hecke eigenclasses in of a weight predicted by the ADP conjecture. Accordingly, in this section we first define the symmetric square, then state the result of Ash and Tiep, then find classes of proven cases of the ADP conjecture by using two-dimensional Galois representations we had already built.

6.1 Symmetric Squares

Let k be a field, V and W be two- and three-dimensional vector spaces over k, respectively. The symmetric square is a homomorphism from $\mathrm{GL}(V)$ to $\mathrm{GL}(W)$ where $\mathrm{GL}(U)$ is the group of linear transformations of the vector space U.

The subset M of $\mathrm{GL}_2(k)$ consisting of matrices of trace zero is a 3-dimensional vector space over k and $\mathrm{GL}_2(k)$ acts linearly on M by conjugation. We call this linear transformation of M the Ad^0 map so that Ad^0 is a homomorphism from $\mathrm{GL}_2(k)$ to $\mathrm{GL}(M)$. If A is in $\mathrm{GL}_2(k)$, we define the symmetric square of A to be $\det(A)Ad^0(A)$. Fixing

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

as a basis for M we can represent the symmetric square of a matrix in $\mathrm{GL}_2(k)$ as a

3×3 matrix according to the following formula: If

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

is a 2×2 invertible matrix then its symmetric square is

$$\mathrm{Sym}^2(A) = \begin{pmatrix} a_{11}a_{22} + a_{12}a_{21} & -a_{11}a_{21} & a_{12}a_{22} \\ -2a_{11}a_{21} & a_{11}^2 & -a_{12}^2 \\ 2_{21}a_{22} & -a_{21}^2 & a_{22}^2 \end{pmatrix}$$

Even though this representation of the symmetric square is dependent on our choice of basis for M, we are only concerned with the coefficients of its characteristic polynomial, which are independent of the choice of basis.

6.2 Result of Ash-Tiep

To find proven cases of the ADP conjecture from the symmetric squares of the two-dimensional representations we have already built, we need to prove that there is an eigenclass of an appropriate weight corresponding to those representations. This proof requires a result of Ash and Tiep.

Before stating this result, we define the variable h associated to a representation to be $k-2$ where k is the weight of the representation. We are now ready for the statement of the Ash-Tiep theorem [3, Theorem 2.2]:

Theorem 6.1. *Let θ be a Hecke eigenclass in $H^1(\mathrm{SL}_2(\mathbb{Z}), F(h,0))$ with $0 < h < \frac{p-1}{2}$ and eigenvalues c_ℓ. Then there exists a Hecke eigenclass in $H^3(\mathrm{SL}_3(\mathbb{Z}), V)$ with eigenvalues $a_{\ell,1} = c_\ell^2 - \ell^{h+1}$ and $a_{\ell,2} = \ell^h(c_\ell^2 - \ell^{h+1})$. Here $V = W(2h,h,0) = F(2h,h,0)$ since $0 < h < (p-1)/2$ see [3, page 393]*

For this paper, we will want to use a corollary relating the symmetric squares of our two-dimensional representations to appropriate eigenclasses.

Corollary 6.2. *Let $\rho \otimes \omega^s$ be a two-dimensional irreducible representation with weight k (as defined by Serre)such that $2 < k < (p+1)/3$. Then $\mathrm{Sym}^2(\rho \otimes \omega^s)$ corresponds to a Hecke eigenclass in $H^3(\mathrm{SL}_3(\mathbb{Z}), F(2h, h, 0)$.*

Proof. We know that $\rho \otimes \omega^s$ corresponds to an eigenclass θ with eigenvalues c_ℓ by Ash-Stevens, Theorem 3.10. We need to show that $\mathrm{Tr}(\mathrm{Sym}^2(\rho \otimes \omega^s(\mathrm{Fr}_\ell))) = c_\ell^2 - \ell^{h+1}$ and $T_2(\mathrm{Sym}^2(\rho \otimes \omega^s(\mathrm{Fr}_\ell))) = \ell^h(c_\ell^2 - \ell^{h+1})$. Now every matrix is similar to an upper triangular matrix, so if

$$A = \begin{pmatrix} a_1 & * \\ 0 & a_2 \end{pmatrix}$$

then the eigenvalues of A are a_1 and a_2 and computation shows that $\mathrm{Tr}(\mathrm{Sym}^2(A)) = \mathrm{Tr}(A)^2 - \det(A)$ and $T_2(\mathrm{Sym}^2(A)) = \det(A)(\mathrm{Tr}(A)^2 - \det(A))$. Noting that by Serre's conjecture $\mathrm{Tr}(\rho \otimes \omega^s(\mathrm{Fr}_\ell)) = c_\ell$ and that by the definition of weight $\det(\rho \otimes \omega^s(\mathrm{Fr}_\ell)) = \ell^{h+1}$ [12, page 182 eqn. (1.3.6)]we have proven the corollary. □

6.3 Proven Examples

We will go through the 4 cases of section 5 to find classes of proven examples of the ADP conjecture. Of the four cases, only case 2 will not yield examples that work.

Case 1: $e = 2$ and conductor is p In this case we had that

$$\rho|_{I_p} \sim \begin{pmatrix} \omega^{\frac{p-1}{2}} & \\ & 1 \end{pmatrix}$$

which has weight $k = (p+1)/2$ and twisting by a power of ω is not even necessary. Here $h = (p-3)/2$. By Ash-Tiep, $\mathrm{Sym}^2(\rho)$ corresponds to an eigenclass in $H^3(\mathrm{SL}_2(\mathbb{Z}), F(2h, h, 0))$. A conjugate of the symmetric square is

$$\mathrm{Sym}^2(\rho|_{I_p}) \sim \begin{pmatrix} \omega^{p-1} & & \\ & \omega^{\frac{p-1}{2}} & \\ & & 1 \end{pmatrix}$$

and the ADP conjecture predicts that this representation has weight $F(p-1-2, \frac{p-1}{2}-1, 0) = F(p-3, \frac{p-3}{2}, 0) = F(2h, h, 0)$. Hence, one of the predictions of ADP is proven for this representation. Table 2 thus gives 66 proven examples in this case and Table 6 gives 16 more.

Case 2: $e = 2$ and conductor is p^2 In this case we had that

$$\rho|_{I_p} \sim \begin{pmatrix} \psi^{\frac{p^2-1}{2^{n+1}}} & \\ & \psi'^{\frac{p^2-1}{2^{n+1}}} \end{pmatrix}.$$

If we twist by ω^s where $s = -\frac{p-1-2^n}{2^{n+1}}$ (this is an integer since $p \equiv 1+2^n \pmod{2)^{n+1}}$) we obtain that

$$\rho \otimes \omega^s|_{I_p} \sim \begin{pmatrix} \psi^{\frac{p+1}{2}} & \\ & \psi'^{\frac{p+1}{2}} \end{pmatrix}$$

which has weight $k = (p+3)/2$ which is just outside the desired range. Since this is the lowest weight we can get, examples of this case do not yield proven cases of the ADP conjecture.

Case 3: $e = 4$ and conductor is p In this case we had that

$$\rho|_{I_p} \sim \begin{pmatrix} \omega^{\frac{p-1}{4}} & \\ & 1 \end{pmatrix}$$

which has weight $k = (p+3)/4$ and twisting by a power of ω is not even necessary. Here $h = (p-5)/4$. By Ash-Tiep, $\mathrm{Sym}^2(\rho)$ corresponds to an eigenclass in $H^3(\mathrm{SL}_2(\mathbb{Z}), F(2h, h, 0))$. A conjugate of the symmetric square is

$$\mathrm{Sym}^2(\rho|_{I_p}) \sim \begin{pmatrix} \omega^{\frac{p-1}{2}} & & \\ & \omega^{\frac{p-1}{4}} & \\ & & 1 \end{pmatrix}$$

and the ADP conjecture predicts that this representation has weight $F(\frac{p-1}{2}-2, \frac{p-1}{4}-1, 0) = F(\frac{p-5}{2}, \frac{p-5}{4}, 0) = F(2h, h, 0)$. Hence, one of the predictions of ADP is proven for this representation. Table 3 thus gives 46 proven examples of this case.

Case 4: $e = 4$, $M = p^2$ In this case we had that

$$\rho|_{I_p} \sim \begin{pmatrix} \psi^{\frac{p^2-1}{8}} & \\ & \psi'^{\frac{p^2-1}{8}} \end{pmatrix}.$$

We can twist by ω^s where $s = -\frac{p-3}{8}$ to get a representation with the proper weight. Since $\omega = \psi^{p+1} = \psi'^{p+1}$, we have that

$$\psi^{\frac{p^2-1}{8}}\omega^s = \psi^{p\frac{p-3}{8}+\frac{3p-1}{8}}\psi^{-(p+1)\frac{p-3}{8}} = \psi^{\frac{p+1}{4}} \text{ and } \psi'^{\frac{p^2-1}{8}}\omega^s = \psi'^{\frac{p+1}{4}}$$

so that

$$\rho \otimes \omega^s|_{I_p} \sim \begin{pmatrix} \psi^{\frac{p+1}{4}} & \\ & \psi'^{\frac{p+1}{4}} \end{pmatrix}$$

and the weight of this representation is $k = 1 + (p+1)/4 = (p+5)/4$. This gives $h = (p-3)/4$. By Ash-Tiep, $\mathrm{Sym}^2(\rho)$ corresponds to an eigenclass in $H^3(\mathrm{SL}_2(\mathbb{Z}), F(2h, h, 0))$. A conjugate of the symmetric square is

$$\mathrm{Sym}^2(\rho|_{I_p}) \sim \begin{pmatrix} \psi^{\frac{p+1}{2}} & & \\ & \omega^{\frac{p+1}{4}} & \\ & & \psi'^{\frac{p+1}{2}} \end{pmatrix}$$

and the ADP conjecture predicts that this representation has weight $F(\frac{p+1}{2}-2, \frac{p+1}{4}-1, 0) = F(\frac{p-3}{2}, \frac{p-3}{4}, 0) = F(2h, h, 0)$. Hence, one of the predictions of ADP is proven for this representation. Table 4 thus gives 102 proven examples of this case.

7 Conclusion

In conclusion, we found 230 proven cases of the ADP conjecture. Of these 214 were built from S_4-extensions and 16 were built from A_5-extensions.

8 Appendix

Here is the computer code used to find extensions. The *s4a* program looks for a degree-4 polynomial ramified only at p and such that $e = 2$. The *s4b* program does the same except with $e = 4$. The *a5a* program looks for degree-5 polynomials ramified only at p and such that $e = 2$. The *a5b* program does the same except with $e = 3$.

```
{s4a(p)=for(a1=0,2,t2=a1^2/4+(p/2)^(1/3);
for(a2=ceil((a1^2-t2)/2),floor((a1^2+t2)/2),
if(a1==0,b3=0,b3=ceil((-a1^3+3*a1*a2-t2^1.5)/3));
for(a3=b3,floor((-a1^3+3*a1*a2+t2^1.5)/3),
m=lift(factormod(4*x^3+3*a1*x^2+2*a2*x+a3,p)); n=matsize(m)[1];
for(k=1,n,h=m[k,1];if(poldegree(h)==1,
    a=-polcoeff(h,0);
    b=-a1-2*a;
    c=a2-a^2-2*a*b;
    b4=-t2^2/16;
    c4=a^2*c-p*floor((a^2*c-b4)/p);
    k4=floor(t2^2/(8*p));
for(d4=0,k4,
    a4=c4+d4*p;
    g=x^4-a1*x^3+a2*x^2-a3*x+a4;
    if(polisirreducible(g),
    if(polgalois(g)[1]==24,d=nfdisc(g);
    if(abs(d)==p,
```

```
    print([p,polredabs(g),polsturm(g)]))))))))))
}


{s4b(p)=i4=lift(Mod(4,p)^-1); for(a1=0,2,
    a=-a1*i4;
    t2=a1^2/4+p*.5^(1/3);
    b2=(a1^2-t2)/2;
    c2=6*a^2-p*floor((6*a^2-b2)/p);
    k2=floor(t2/p);
for(d2=0,k2,
    a2=c2+d2*p;
    b3=(-a1^3+3*a1*a2-t2^1.5)/3;
    if(a1==0,c3=lift(Mod(-4*a^3,p)),
         c3=-4*a^3-p*floor((-4*a^3-b3)/p));
    k3=floor(t2^1.5/(1.5*p));
    b4=-(t2/4)^2;
    c4=a^4-p*floor((a^4-b4)/p);
    k4=floor((2*(t2/4)^2)/p);
for(d4=0,k4,
    a4=c4+p*d4;
for(d3=0,k3,
    a3=c3+d3*p;
    g=x^4-a1*x^3+a2*x^2-a3*x+a4;
    if(polisirreducible(g),
    if(polgalois(g)[1]==24,d=nfdisc(g);
```

```
    if(abs(d)==p^3,
    print([p,polredabs(g),polsturm(g)])))))))))
}

{a5b(p)=for(a1=0,2,t2=a1^2/5+(4*p^2/5)^.25;
for(a2=ceil((a1^2-t2)/2),floor((a1^2+t2)/2),
if(a1==0,b3=0,b3=ceil((-a1^3+3*a1*a2-t2^1.5)/3));
for(a3=b3,floor((-a1^3+3*a1*a2+t2^1.5)/3),
m=lift(factormod(-5*x^3-6*a1*x^2-(2*a1^2+a2)*x-a1*a2+a3,p));
n=matsize(m)[1]; for(k=1,n,h=m[k,1];if(poldegree(h)==1,
    a=-polcoeff(h,0);
    c=-a1-2*a;
    b=(p+1)/2*(a2-a^2-2*a*c);
    b4=(4*a1*a3-4*a1^2*a2+2*a2^2+a1^4-t2^2)/4;
    c4=2*a*b*c+b^2-p*floor((2*a*b*c+b^2-b4)/p);
    k4=floor(t2^2/(2*p));
for(d4=0,k4,
    a4=c4+d4*p;
    b5=-(t2/5)^2.5;
    c5=-b^2*c-p*floor((-b^2*c-b5)/p);
    k5=floor((2*(t2/5)^2.5)/p);
for(d5=0,k5,
    a5=c5+p*d5;
    g=x^5-a1*x^4+a2*x^3-a3*x^2+a4*x-a5;
    D=poldisc(g);
```

```
    if(D\%p==0,
    if(issquare(D),
    if(polisirreducible(g),
    if(polgalois(g)[1]==60,d=nfdisc(g);
    if(d==p^2,
    print([p,polredabs(g),polsturm(g)])))))))))))))
}

{a5a(p)=for(a1=0,2,t2=a1^2/5+(4*p^2/5)^.25;
for(a2=ceil((a1^2-t2)/2),floor((a1^2+t2)/2),
if(a1==0,b3=0,b3=ceil((-a1^3+3*a1*a2-t2^1.5)/3));
for(a3=b3,floor((-a1^3+3*a1*a2+t2^1.5)/3),
m=lift(factormod(10*x^3+6*a1*x^2+3*a2*x+a3,p)); n=matsize(m)[1];
for(k=1,n,h=m[k,1];if(poldegree(h)==1,
    a=-polcoeff(h,0);
    b=-a1-3*a;
    c=a2-3*a^2-3*a*b;
    b4=(4*a1*a3-4*a1^2*a2+2*a2^2+a1^4-t2^2)/4;
    c4=3*a^2*c+a^3*b-p*floor((3*a^2*c+a^3*b-b4)/p);
    k4=floor(t2^2/(2*p));
for(d4=0,k4,
    a4=c4+d4*p;
    b5=-(t2/5)^2.5;
    c5=-a^3*c-p*floor((-a^3*c-b5)/p);
    k5=floor((2*(t2/5)^2.5)/p);
```

```
for(d5=0,k5,
    a5=c5+p*d5;
    g=x^5-a1*x^4+a2*x^3-a3*x^2+a4*x-a5;
    D=poldisc(g);
    if(issquare(D),
    if(polisirreducible(g),
    if(polgalois(g)[1]==60,d=nfdisc(g);
    if(d==p^2,
    print([p,polredabs(g),polsturm(g)])))))))))))
}
```

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. MR MR1896473 (2003g:11055)

[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. MR MR860675 (88h:11036)

[3] Avner Ash and Pham Huu Tiep, *Modular representations of* $\mathrm{GL}(3, \mathbf{F}_p)$*, symmetric squares, and mod-p cohomology of* $\mathrm{GL}(3, \mathbf{Z})$, J. Algebra **222** (1999), no. 2, 376–399. MR MR1727178 (2001d:11058)

[4] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts

in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR MR1728313 (2000k:11144)

[5] Stephen R. Doty and Grant Walker, *The composition factors of* $\mathbf{F}_p[x_1, x_2, x_3]$ *as a* $\mathrm{GL}(3, p)$*-module*, J. Algebra **147** (1992), no. 2, 411–441. MR MR1161301 (93h:20015)

[6] Darrin Doud, *Three-dimensional Galois representations with conjectural connections to arithmetic cohomology*, Number theory for the millennium, I (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 365–375. MR MR1956235 (2003k:11089)

[7] Chandrasekhar Khare, *On Serre's modularity conjecture for 2-dimensional mod p representations of* G_Q *unramified outside p*, preprint (2005), available at www.arxiv.org.

[8] Kenneth A. Ribet and William A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 143–232. MR MR1860042 (2002h:11047)

[9] J.-P. Serre, *Modular forms of weight one and Galois representations*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 193–268. MR MR0450201 (56 #8497)

[10] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR MR0387283 (52 #8126)

[11] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR MR554237 (82e:12016)

[12] ———, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230. MR MR885783 (88g:11022)

[13] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR MR1312368 (96b:11074)