2008-06-12

Lifting Galois Representations in a Conjecture of Figueiredo

Wayne Bennett Rosengren
Brigham Young University - Provo

LIFTING GALOIS REPRESENTATIONS IN A CONJECTURE OF FIGUEIREDO

by

Wayne Bennett Rosengren

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 2008

BRIGHAM YOUNG UNIVERSITY

GRADUATE COMMITTEE APPROVAL

of a thesis submitted by

Wayne Bennett Rosengren

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	William Lang
Date	Jasbir Chahal

BRIGHAM YOUNG UNIVERSITY

As chair of the candidate's graduate committee, I have read the thesis of Wayne Bennett Rosengren 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

William Lang
Graduate Coordinator

Accepted for the College

Thomas Sederberg, Associate Dean
Physical and Mathematical Sciences

ABSTRACT

LIFTING GALOIS REPRESENTATIONS IN A CONJECTURE OF FIGUEIREDO

Wayne Bennett Rosengren

Department of Mathematics

Master of Science

In 1987, Jean-Pierre Serre gave a conjecture on the correspondence between degree 2 odd irreducible representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and modular forms. Letting M be an imaginary quadratic field, L.M. Figueiredo gave a related conjecture concerning degree 2 irreducible representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$ and their correspondence to homology classes. He experimentally confirmed his conjecture for three representations arising from $PSL_2(\mathbb{F}_3)$-polynomials, but only up to a sign because he did not lift them to $SL_2(\mathbb{F}_3)$ polynomials. In this paper we compute explicit lifts and give further evidence that his conjecture is accurate.

Table of Contents

1 Introduction

1.1 Galois Representations

Given a group, G, a representation of G is a continuous group homomorphism from G into a matrix group. Often we are interested in studying representations of groups that arise as Galois groups of extensions of number fields.

If $K \subset L$ is a Galois extension of number fields, $\mathfrak{P} \subset \mathcal{O}_L$ is a prime ideal, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, and f is the inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$ then there is a unique element, Frob$_{\mathfrak{P}}$ $\in$Gal(L/K) having the property that Frob$_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{P}$ for all $x \in L$. Here, $N(p)$ is the size of $\mathcal{O}_K/\mathfrak{p}$. This is called the Frobenius element of Gal(L/K) corresponding to the prime $\mathfrak{P}$.

Theorem 1.1. *If $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are different primes of L both having the property that $\mathfrak{p} = \mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{P}_j \cap \mathcal{O}_K$, then Frob$_{\mathfrak{P}_i}$ is conjugate to Frob$_{\mathfrak{P}_j}$.*

Proof. See [1, pg. 107]. □

Of course, if Gal(L/K) happens to be abelian, every conjugacy class consists of a single element. This allows us to unambiguously define Frob$_{\mathfrak{p}}$ as the unique element of Gal(L/K) that is the Frobenius element for every $\mathfrak{P}$ containing $\mathfrak{p}$. In the case that Gal(L/K) is not abelian Frob$_{\mathfrak{p}}$ is not well-defined as an element of Gal(L/K), but it is still well-defined as a conjugacy class.

The ambiguity in defining Frob$_{\mathfrak{p}}$ just discussed does not present a problem when considering Galois representations. A representation takes conjugate group elements to similar matrices. Matrix attributes such as the determinant and trace are similarity invariants. Thus, while Frob$_{\mathfrak{p}}$ is not a well-defined automorphism, $Tr(\rho(\text{Frob}_{\mathfrak{p}}))$ is well-defined. This will be important later on.

Complex conjugation is also a particularly important automorphism in many instances, which gives rise to the definitions of "evenness" and "oddness" of representations. Let $G_{\mathbb{Q}}$ =Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). Let τ denote complex conjugation.

Definition 1.2. If $\rho : G_{\mathbb{Q}} \to GL_2(F)$ where char $F \neq 2$ is a representation, then ρ is said to be an *odd* representation if $\det(\rho(\tau)) = -1$. A representation is *even* if $\det(\rho(\tau)) = 1$.

1.2 Extending Serre's Conjecture

Jean-Pierre Serre conjectured that to every odd irreducible representation of $G_{\mathbb{Q}} =$ Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) into $GL_2(\overline{\mathbb{F}}_p)$ there corresponds a modular form [6]. For even representations we don't get a correspondence with modular forms. It is desirable, though, to have some more general setting than modular forms in which to discuss a similar conjecture with even representations. L.M. Figueiredo used homology classes to address this issue.

Figueiredo started with even representations of $G_{\mathbb{Q}}$ and restricted them to the group $G_M =$ Gal($\overline{\mathbb{Q}}/M$), where M is an imaginary quadratic field. The relevance of this is that complex conjugation no longer fixes the base field and so is not an element of the Galois group G_M. Since complex conjugation is not a concern here Figueiredo could extend Serre's conjecture without regard to oddness or evenness.

We can now state Figueiredo's conjecture.

Conjecture 1.3. *Given the following definitions:*

1. *Let l be a prime integer, M be an imaginary quadratic field, and ρ :Gal($\overline{\mathbb{Q}}/M$) $\to$ $GL_2(\overline{\mathbb{F}}_l)$ be an irreducible representation.*

2. *Let Frob*$_{\mathfrak{P}}$ *be a Frobenius map in Gal*$(\overline{\mathbb{Q}}/M)$ *corresponding to* $\mathfrak{P} \subset \mathcal{O}_M$.

3. *Given an ideal* $\mathcal{I} \subset \mathcal{O}_M$, *let*

$$\Gamma_1(\mathcal{I}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O}_M) | c \in \mathcal{I}, d \equiv \epsilon \bmod \mathcal{I} \text{ for some } \epsilon \in \mathcal{O}_M^* \right\}.$$

4. *Let the level* $N(\rho)$ *be the part of the Artin conductor of* ρ *prime to* l *and* $\tilde{N}(\rho) = N(\rho) \prod_{\lambda | l} \lambda^2$ *where* λ *is a prime of* $\mathcal{O}_M$ *lying above* l.

5. *Let* $\det \rho = \epsilon(\rho)\chi^h$, *where* χ^h *is some power of the mod* l *cyclotomic character* χ *and* $\epsilon(\rho) : (\mathcal{O}_M/\tilde{N}(\rho)\mathcal{O}_M)^*/\mathcal{O}_M^* \to \overline{\mathbb{F}}_l^*$ *is a character.*

Then there is a homology class $v \in H_1^*(\Gamma_1(\tilde{N}(\rho)), \overline{\mathbb{F}}_l)_{\epsilon(\rho)}$ *such that* v *is a common eigenvector for the Hecke operators and, for all prime* $\mathfrak{P}$ *not dividing* $\tilde{N}(\rho)$, *Tr*$(\rho($*Frob*$_{\mathfrak{P}})) = a_{\mathfrak{P}}$ *where* $a_{\mathfrak{P}}$ *is the eigenvalue of* v *for the Hecke operator* $T_{\mathfrak{P}}$.*[3]*

1.3 Testing Figueiredo's Conjecture

A polynomial, $P \in \mathbb{Z}[x]$, with Galois group G isomorphic to a subgroup of $GL_2(F)$ for some F, yields a natural representation $\rho : G_{\mathbb{Q}} \to G \hookrightarrow GL_2(F)$. The first arrow in this representation takes $\sigma \to \sigma|_K$ where K is the splitting field of P. As there was already substantial evidence for Serre's Conjecture in the odd case Figueiredo looked for even representations.

To find even representations ρ of $G_{\mathbb{Q}}$ he used the following construction. Let P be a monic irreducible polynomial with coefficients in $\mathbb{Z}$. Suppose that the Galois group of P is a subgroup of $PGL_2(\mathbb{F}_l)$. The existence of this extension yields a homomorphism $\tilde{\rho} : G_{\mathbb{Q}} \to PGL_2(\mathbb{F}_l)$, which we call a projective representation. In many cases, we can lift such a projective representation to an actual Galois representation $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_l)$. We will call such a representation ρ a Galois representation corresponding to the polynomial P.

Note that any Galois automorphism which maps to the identity in the projective representation $\tilde{\rho}$ will map to a scalar matrix under ρ. Hence, if the fixed field of $\tilde{\rho}$ (which is just the splitting field of P) is contained in the real numbers, then the representation ρ will be even.

Figueiredo looked for polynomials P having the following properties:

1. All roots of P are real, so that the corresponding representation is even.

2. The splitting field of P has small discriminant so that the corresponding representation is ramified for a small number of primes.

3. The Galois group of P is not too small so that the corresponding representation is irreducible. [3]

He found the three polynomials

$$F_1(x) = x^4 - 7x^2 - 3x + 1$$
$$F_2(x) = x^4 - x^3 - 24x^2 + x + 11$$
$$F_3(x) = x^4 - x^3 - 7x^2 + 2x + 9,$$

which have Galois group $A_4 \cong PSL_2(\mathbb{F}_3)$ over $\mathbb{Q}$. He picked these specifically because they each can lift to an $SL_2(\mathbb{F}_3)$-extension. That they can "lift" means that to each F_i there is a polynomial G_i such that the splitting field of G_i contains the splitting field of F_i and that $\mathrm{Gal}(G_i) = SL_2(\mathbb{F}_3)$. He did not explicitly find these G_i.

Each F_i corresponds to an A_4-extension of $\mathbb{Q}$. Figueiredo proved that each of the resulting A_4-extensions embeds in an $SL_2(\mathbb{F}_3)$-extension, yielding a Galois representation $\rho : G_{\mathbb{Q}} \to SL_2(\mathbb{F}_3)$. Letting $M = \mathbb{Q}(i)$, he restricted ρ to G_M, and for the resulting representation $\rho|_{G_M} : G_M \to SL_2(\mathbb{F}_3)$ he computed the level and the character. He then computed the corresponding cohomology class and found not one, but two Hecke eigenclasses that could correspond to $\rho|_{G_M}$. The only difference between the two was the sign of certain eigenvalues. This sign cannot be determined without computing the $SL_2(\mathbb{F}_3)$-extension in question.

In this thesis we explain why there are two distinct sets of eigenvalues for each of these polynomials. We do this by finding polynomials that give $SL_2(\mathbb{F}_3)$-extensions corresponding to the F_i. Specifically, we find two polynomials for each F_i. Then we give tables similar to those given by Figuereido and note that our tables of $\mathrm{Tr}(\rho(\mathrm{Frob}_{\mathfrak{P}}))$ for the various $\mathfrak{P}$ match exactly the tables of eigenvalues computed by Figueiredo [4]; not just up to a sign. This gives further evidence that his conjecture is accurate.

2 Lifting Figueiredo's Polynomials

L.M. Figueiredo considered the three polynomials,

$$F_1(x) = x^4 - 7x^2 - 3x + 1$$

$$F_2(x) = x^4 - x^3 - 24x^2 + x + 11$$

$$F_3(x) = x^4 - x^3 - 7x^2 + 2x + 9,$$

and showed that each F_n generates an A_4-extension, K_n of $\mathbb{Q}$. They also give extensions of $\mathbb{Q}(i)$. Those are obtained by taking the composite of $\mathbb{Q}(i)$ with K_n, which will in every case have degree 2 over K_n. These are of primary interest to us because Figueiredo's conjecture deals with representations of G_M, where M is an imaginary quadratic field, and not representations of $G_{\mathbb{Q}}$. They are however obtained by restricting representations, ρ of $G_{\mathbb{Q}}$. In our case we have $M = \mathbb{Q}(i)$ and we see that $G_{\mathbb{Q}(i)}/\ker(\rho|_{\mathbb{Q}(i)})$ is the Galois group of $K_n(i)/\mathbb{Q}(i)$, not $K_n/\mathbb{Q}$.

He also proved by considerations of the Witt invariant the existence of at least one field extension for each of these A_4-extensions whose Galois group over $\mathbb{Q}$ is $SL_2(\mathbb{F}_3)$.[3, pg.117]

We exhibit two such fields $L_{n,1}$ and $L_{n,2}$ corresponding to K_n, which are given explicitly as splitting fields of polynomials $G_{n,1}(x)$ and $G_{n,2}(x)$. One restriction on these fields is that their discriminant should be divisible only by 3 and those primes dividing the discriminant of K_n. We see that if α_n is a root of F_n, then the number field discriminants of $\mathbb{Q}(\alpha_1)$, $\mathbb{Q}(\alpha_2)$, and $\mathbb{Q}(\alpha_3)$ are $(3 \cdot 61)^2$, $(3^4 \cdot 79^2)$, and 163^2 respectively. This implies that K_1 is unramified at every prime except those containing 3 or 61, and similarly for K_2 and K_3.

After determining $L_{n,i}$ we compute Frobenius elements in $\mathrm{Gal}(L_{n,i}(i)/\mathbb{Q}(i))$ for each of the primes of $\mathbb{Q}(i)$ and then compute the traces of the images of $\mathrm{Frob}_{\mathfrak{p}}$ in $SL_2(\mathbb{F}_3)$. Then we compare those with the lists given by Figueiredo. We will show that each set of eigenvalues he computed corresponds to one of the two lifts to $SL_2(\mathbb{F}_3)$-extensions of each K_n and thus explain why there were two sets of eigenvalues per polynomial.

In order to determine $L_{n,i}$ we will make extensive use of the Fundamental Theorem of Galois Theory, which gives an inclusion reversing one-to-one correspondence between the subgroup lattice of $SL_2(\mathbb{F}_3)$ and the subfield lattice of $L_{n,i}$. So, in order to proceed further, we need to understand the group structure of $SL_2(\mathbb{F}_3)$.

2.1 The Group $SL_2(\mathbb{F}_3)$

The group $SL_2(\mathbb{F}_3)$ is by definition the group of two by two matrices with entries in $\mathbb{F}_3$ having determinant one. The group operation is matrix multiplication. Our goal is to completely determine the structure of this group. $SL_2(\mathbb{F}_3)$ is a subgroup of $GL_2(\mathbb{F}_3)$, which is the group of two-by-two matrices with entries in $\mathbb{F}_3$ having non-zero determinant.

Theorem 2.1. *Given the definitions as above,*

1. $|GL_2(\mathbb{F}_3)| = 48$.

2. $|SL_2(\mathbb{F}_3)| = 24$.

Proof. To determine the order of $GL_2(\mathbb{F}_3)$ we note that a matrix, $M \in GL_2(\mathbb{F}_3)$, can have any non-zero first row, allowing 8 possibilities for the first row. Once the first row is determined the only restriction on the second row is that it may not be a scalar multiple of the first row. In particular, once the first row is determined there are 6 distinct choices for the second row and we conclude that $GL_2(\mathbb{F}_3)$ has 48 distinct elements.

Now $SL_2(\mathbb{F}_3)$ is the kernel of the homomorphism from $GL_2(\mathbb{F}_3)$ to $\{\pm 1\}$ given by the determinant function so the order of $SL_2(\mathbb{F}_3)$ must be 24. □

We make the following definitions:

$$A = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

These are both elements of $SL_2(\mathbb{F}_3)$.

Theorem 2.2. *The subgroup, $\langle A, B \rangle$, generated by A and B is all of $SL_2(\mathbb{F}_3)$.*

Proof. First, we see that

$$A^2 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

and that $A^3 = -I$, so that $A^4 = -A$, $A^5 = -A^2 = A^{-1}$, and $A^6 = I$. Thus, A generates a subgroup of order 6 and similarly, $B^2 = -I$, $B^3 = -B = B^{-1}$, and $B^4 = I$ so that B generates a subgroup of order 4. This implies that $\langle A, B\rangle$ has order at least $\operatorname{lcm}(6, 4) = 12$. So far we have accounted for eight elements of the group. Now,

$$BAB^{-1} = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \neq A$$

so in particular $AB \neq BA$. Since BAB^{-1} is conjugate to A it must also have order 6, but $BAB^{-1} \neq A^{-1}$ so the cyclic group it generates is different from the group generated by A. We have $(BAB^{-1})^2 = BA^2B^{-1} \neq \pm A^2$ where these elements each have order 3. Finally, $(BAB^{-1})^3 = BA^3B^{-1} = -BB^{-1} = -I$, so that the group $\langle BAB^{-1}\rangle = \{\pm I, \pm BAB^{-1}, \pm BA^2B^{-1}\}$.

Similarly, we find that

$$\begin{aligned} \langle A\rangle &= \{\pm I, \pm A, \pm A^2\} \\ \langle BAB^{-1}\rangle &= \{\pm I, \pm BAB^{-1}, \pm BA^2B^{-1}\} \\ \langle (AB)A(AB)^{-1}\rangle &= \{\pm I, \pm (AB)A(AB)^{-1}, \pm (AB)A^2(AB)^{-1}\} \\ \langle (A^2B)A(A^2B)^{-1}\rangle &= \{\pm I, \pm (A^2B)A(A^2B)^{-1}, \pm (A^2B)A^2(A^2B)^{-1}\} \end{aligned}$$

are subgroups of $SL_2(\mathbb{F}_3)$ with the property that the only elements in common between any two of them are $\pm I$. This accounts for 8 elements of order 6 and 8 elements of order 3, which proves that A and B generate $SL_2(\mathbb{F}_3)$. □

Continuing, we see that the elements listed as generators of the subgroups above are all of the conjugates of A. Thus, there are 2 conjugacy classes of elements of order 6, and similarly for elements of order 3. Since, $AB \neq BA$ the remaining 5 elements we have not listed are conjugates of B or $-B$ and have order 4. These must be given by $-B$, $\pm ABA^{-1}$, and $\pm A^2BA^{-2}$.

We now determine the list of subgroups of $SL_2(\mathbb{F}_3)$. We have the subgroups $\{I\}$ and $\{\pm I\}$ of orders 1 and 2, respectively. The only subgroups of order 3 must be given by elements of order 3 and so must be contained in one of the four cyclic subgroups of order 6. There are four subgroups of order 3. Generators for these groups are the conjugates of A^2. Since there is only one element of order 2, any subgroup of order 4 must be cyclic. There are three of these, generated by B, ABA^{-1}, and A^2BA^{-2}. The four cyclic subgroups of order 6 are given above.

There is a subgroup of order 8 by Sylow's Theorem. This must contain all of the elements of orders 1,2, and 4 because there are only 8 of them. Since $B(ABA^{-1}) \neq (ABA^{-1})B$, this group must not be abelian. It cannot be isomorphic to the dihedral group because the dihedral group has exactly two elements of order 4. Thus, this group must be isomorphic to the quaternion group Q_8, which is the only other non-abelian group of order 8.

Suppose $SL_2(\mathbb{F}_3)$ contained a subgroup of order 12; call it H. H would then have to be normal, being of index 2. By Cauchy's Theorem [2, pg.93] it would have to contain an element of order 2 (this is $-I$) and an element of order 3. Normality then implies that it contains all of the elements of order 3. Now, if there were an element of order 4 in H then normality implies that the quaternions are in H also. This cannot happen in a group of order 12. Similarly, H can have no element of order 6 because normality would force that all of the subgroups of order 6 be in H. As this accounts for 14 group elements this is a contradiction. Thus, there is no

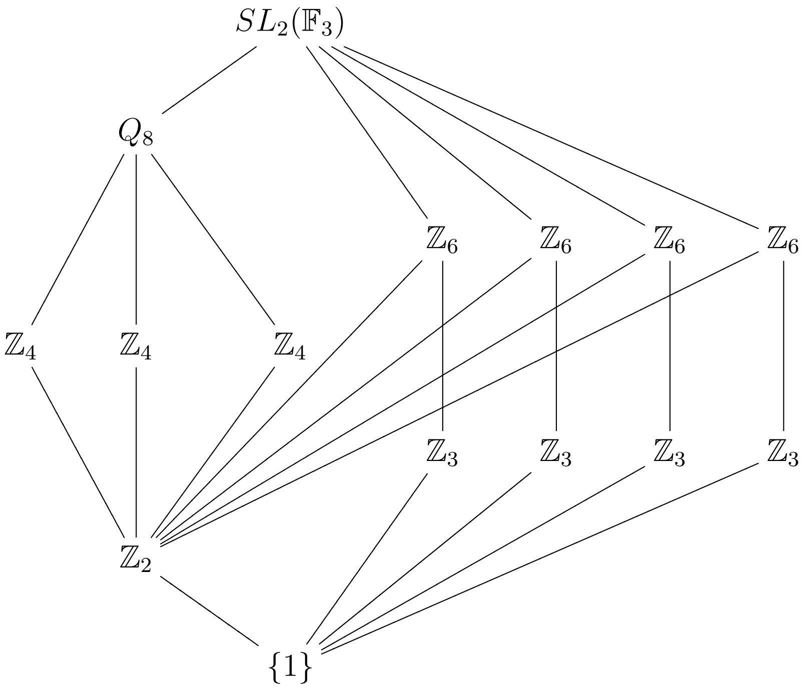

Figure 1: Subgroup lattice of $SL_2(\mathbb{F}_3)$

subgroup of order 12. The only other subgroup of $SL_2(\mathbb{F}_3)$ is $SL_2(\mathbb{F}_3)$ itself. This yields the subgroup lattice in Figure 1.

2.2 Finding $SL_2(\mathbb{F}_3)$-Extensions Above K_n

Recall that K_n was defined to be the splitting field of $F_n(x)$ and that $L_{n,i}$, if it exists, was defined to be a field extension of K_n whose Galois group over $\mathbb{Q}$ is $SL_2(\mathbb{F}_3)$. First, we note that $L_{n,i}$ is a quadratic extension of K_n, and thus can be described as $K_n(\sqrt{\beta})$ where β is an algebraic integer in K_n. Now, the ring of integers of K_n is computationally somewhat difficult to deal with directly. However, using the Fundamental of Theorem of Galois Theory we can use Figure 1 to simplify the problem.

K_n corresponds to the subgroup $\{\pm I\}$, but the subgroups of order 3 correspond to degree 8 subfields of $L_{n,i}$ not contained in K_n. Thus, if we can determine these degree 8 fields then $L_{n,i}$ will be given as their composite with K_n. This composite field is also the splitting field of the degree 8 polynomial.

Now, let α_n be an arbitrary root of $F_n(x)$. Exactly one of the subgroups of order 6 corresponds to the field $\mathbb{Q}(\alpha_n)$. We begin searching for $G_{n,j}(x)$ by considering quadratic extensions of $\mathbb{Q}(\alpha_n)$. We know that some quadratic extension, $M_{n,j}$ of $\mathbb{Q}(\alpha_n)$ is contained in $L_{n,j}$, if $L_{n,j}$ exists. (This corresponds to an order 3 subgroup in Figure 1.) Also, $M_{n,j}$, should be unramified at every prime for which the corresponding A_4-extension, K_n, is unramified. To continue we need a supplementary lemma about ramification in quadratic field extensions.

Theorem 2.3. *Let K be a number fields and let $L = K(\sqrt{u})$ be a quadratic extension with $u \in \mathcal{O}_K$, and let $\mathfrak{p}$ be prime in $\mathcal{O}_K$. If $2u \notin \mathfrak{p}$, then $\mathfrak{p}$ is unramified in L.*

Proof. See [1, pg.114]. □

Thus, as any quadratic extension is given by adjoining the square root of a field element $\beta \in \mathbb{Q}(\alpha_n)$, we may suppose that β is an algebraic integer not contained in any prime ideal except possibly those above (3) or primes that ramify in K_n.

There are infinitely many β giving isomorphic field extensions of K_n. This is because, given $\gamma \in \mathcal{O}_{K_n}$, the element β and $\beta\gamma^2$ generate the same extension. If we require that our β not have a square factor in $\mathcal{O}_{K_n}$ (excluding units), then we can reduce our infinite list of possibilities for β modulo squares. Thus, we may restrict our search for β to a finite list of algebraic integers which are units or generators of specific prime ideals.

2.3 Number Field Computations

We use GP/PARI to carry out computations in these number fields [8]. The command `bnfinit` takes as its argument a polynomial, in our case F_n, and initializes the number field it generates, R_n. Then we use the command `nf.zk` to produce an integral basis of $\mathcal{O}_{R_n}$. We use the command `bnfunit` to find the units of this ring, and the command `idealprimedec` to find the factorization of (3) into prime ideals of $\mathcal{O}_{R_n}$. After factoring (3), we use the command `idealisprincipal` on each of the ideals above 3. If one of these ideals is principal this command returns a generator for it. In two of the three cases we deal with in this paper it happens that the ideals above (3) are not principal, so we are left to work with only the units.

After finding the units and the generators of primes above (3) we consider the list of all possible square-free products of such objects. Call these $x_1, x_2, \ldots x_k$. We are interested in computing the degree 8 minimal polynomial of $\sqrt{x_i}$ for each i. Note that it is necessarily of degree 8 because x_i is of degree 4. We could use the `algdep` command with an argument of $\sqrt{x_i}$ and 8, which searches for a dependence relation on powers of $\sqrt{x_i}$ up to the eighth power. The drawback of this is that the `algdep` command becomes less accurate as one allows higher powers in the dependence relation. As a result the given dependence relation may not actually be the minimal polynomial of $\sqrt{x_i}$.

To circumvent this issue consider the minimal polynomial of x_i, $p_i(x)$. Then the minimal polynomial of $\sqrt{x_i}$ is $p_i(x^2)$. Thus, we may use the `algdep` command with an argument of x_i and 4 without losing any information. This is much more accurate.

Having thus obtained minimal polynomials for the x_i we initialize number fields corresponding to them (using `bnfinit`). Then we use the command `nf.disc` to take the number field discriminant of these polynomials. This should be divisible only by 3 or those primes dividing the discriminant of R_n. If it satisfies that condition then we use the command `polgalois` to find the Galois group of the polynomial. If it is $SL_2(\mathbb{F}_3)$ we use the command `nfisincl` to verify that R_n is contained in the splitting field of the minimal polynomial for $\sqrt{x_i}$. This finishes the outline of the first technique for finding lifts of F_n.

2.4 Finding $SL_2(\mathbb{F}_3)$-Extensions Above K_n cont.

Having fixed α_n as a root of $F_n(x)$ and using the process above we find algebraic integers of $\mathbb{Q}(\alpha_n)$ that will yield the desired field extensions. For α_1 we see that $-\alpha_1^2 + 3\alpha_1 - 1$ and $-8\alpha_1^3 + 52\alpha_1 - 33$ are generators of the unique prime ideal above 3. For α_2 and α_3 we see that $\frac{-\alpha_2^3+4\alpha_2^2+7\alpha_2+3}{5}$ and $-\alpha_3 - 2$ are units. Again, with reference to Section 2.3 we determine that

$$M_{1,1} = \mathbb{Q}\left(\alpha_1, \sqrt{-\alpha_1^2 + 3\alpha_1 - 1}\right) \qquad M_{1,2} = \mathbb{Q}\left(\alpha_1, \sqrt{-8\alpha_1^3 + 52\alpha_1 - 33}\right)$$

$$M_{2,1} = \mathbb{Q}\left(\alpha_2, \sqrt{\frac{-\alpha_2^3 + 4\alpha_2^2 + 7\alpha_2 + 3}{5}}\right)$$

$$M_{3,1} = \mathbb{Q}\left(\alpha_3, \sqrt{-\alpha_3 - 2}\right)$$

are quadratic extensions of $\mathbb{Q}(\alpha_n)$ whose splitting fields have the right Galois group and ramification over $\mathbb{Q}$. Now, $L_{i,j}$ is the Galois closure of $M_{i,j}$ for those $M_{i,j}$ given above. We see also that $L_{1,1}$ is the splitting field of the minimal polynomial over $\mathbb{Q}$

for $\sqrt{-\alpha_1^2 + 3\alpha_1 - 1}$, which is

$$G_{1,1}(x) = x^8 + 18x^6 + 63x^4 + 45x^2 + 9.$$

Similarly, we determine $L_{1,2}, L_{2,1}$ and $L_{3,1}$ as splitting fields of the following polynomials:

$$\begin{aligned}
G_{1,2}(x) &= x^8 - 60x^6 + 702x^4 - 396x^2 + 9 \\
G_{2,1}(x) &= x^8 - 29x^6 + 60x^4 - 17x^2 + 1 \\
G_{3,1}(x) &= x^8 + 9x^6 + 23x^4 + 14x^2 + 1.
\end{aligned}$$

We need some results about group cohomology to continue. To find possible Galois groups for quadratic extensions of K_n we need to know all possible choices for H in the exact sequence:

$$0 \longrightarrow \mathbb{Z}_2 \longrightarrow H \longrightarrow A_4 \longrightarrow 0$$

Definition 2.4. A group extension (of G by A) is a short exact sequence

$$0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 0$$

of groups in which A is an abelian group, on which G acts.

Theorem 2.5. *The equivalence classes of extensions of G by A with a given action of G on A are in one-to-one correspondence with the cohomology group $H^2(G; A)$.*

Proof. See [9, pg.183]. □

It is well known that $H^2(A_n, \mathbb{Z}_2) = \mathbb{Z}_2$ for $n \geq 4$ [7, pg.97-98]. These results will allow us to find $L_{2,2}$ and $L_{3,2}$ without the need for a generating element. (Though we will give defining polynomials for these extensions later.)

$$\begin{tikzcd}
 & L_{n,1}(\sqrt{-3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K_n\left(\sqrt{-3}\right) \arrow[dr, dash] \arrow[dd, dash] & L_{n,1} = K_n\left(\sqrt{\beta}\right) \arrow[d, dash] & K_n\left(\sqrt{-3\beta}\right) \arrow[dl, dash] \\
 & K_n \arrow[dd, dash] & \\
\mathbb{Q}\left(\sqrt{-3}\right) \arrow[dr, dash] & & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Figure 2: A Klein-4 Extension of K_n

Now, to find the other two extensions, $L_{2,2}$ and $L_{3,2}$, we consider Figure 2. Let β be any element of $L_{n,1}$ that generates $L_{n,1}$ as a simple extension of K_n. Let p be any rational prime unramified in K_n, in particular $p \neq 3$. By construction, p is unramified in $L_{n,1}$. Also p does not ramify in $\mathbb{Q}(\sqrt{-3})$ and so does not ramify in the composite field $K_n(\sqrt{-3})$. This implies that p does not ramify in $L_{n,1}(\sqrt{-3})$ being the composite of $L_{n,1}$ and $K_n(\sqrt{-3})$. Thus, p cannot ramify in $K_n(\sqrt{-3\beta})$ implying that this field is unramified at every prime except 3 and those primes ramifying in K_n, indicating that it could be $L_{n,2}$.

Theorem 2.6. *The field $K_n(\sqrt{-3\beta})$ is Galois over $\mathbb{Q}$.*

Proof. It is clear that $K_n(\sqrt{-3})$ and $K_n(\sqrt{\beta})$ are both Galois over $\mathbb{Q}$. This implies that $K_n(\sqrt{-3}, \sqrt{\beta})$ is also Galois over $\mathbb{Q}$ necessarily yielding the Klein-4 extension of Figure 2. Suppose that $K_n(\sqrt{-3\beta})$ were not Galois, then there would be some automorphism of $\mathrm{Gal}\big(K_n(\sqrt{-3}, \sqrt{\beta})/\mathbb{Q}\big)$ that sends $K_n(\sqrt{-3\beta})$ to a fourth subfield of $K_n(\sqrt{-3}, \sqrt{\beta})$ of index 2 containing K_n, which is absurd. Thus, $K_n(\sqrt{-3\beta})$ is Galois over $\mathbb{Q}$. □

Theorem 2.7. *The Galois group of $K_n(\sqrt{-3\beta})$ is isomorphic to $SL_2(\mathbb{F}_3)$.*

Proof. To begin with we notice that if a degree 2 extension of K_n is Galois over $\mathbb{Q}$ then there are only two possibilities for its Galois group, because it must have A_4 as a quotient. These groups are $A_4 \times \mathbb{Z}_2$ and $SL_2(\mathbb{F}_3)$ (see [7, pg.97-98] and Theorem 2.5).

If $K_n\left(\sqrt{-3\beta}\right)$ had Galois group $A_4 \times \mathbb{Z}_2$ over $\mathbb{Q}$ then it would have a quadratic subfield corresponding to the subgroup $A_4 \times \{0\}$ of $A_4 \times \mathbb{Z}_2$. The only quadratic extension of $\mathbb{Q}$ contained in $L_{n,1}(\sqrt{-3})$ is $\mathbb{Q}(\sqrt{-3})$ which is not contained in $K_n\left(\sqrt{-3\beta}\right)$. Thus, the Galois group is $SL_2(\mathbb{F}_3)$. □

Note that this argument guarantees the existence of two $SL_2(\mathbb{F}_3)$-lifts of an A_4-extension whenever there is one such lift. Thus, the fact that Figueiredo found two eigenclasses instead of one was to be expected. This immediately yields

$$L_{2,2} = K_2\left(\sqrt{-3\left(\frac{-\alpha_2^3 + 4\alpha_2^2 + 7\alpha_2 + 3}{5}\right)}\right)$$

$$L_{3,2} = K_3\left(\sqrt{-3\left(-\alpha_3 - 2\right)}\right).$$

These are the splitting fields of the following polynomials in $\mathbb{Q}[x]$:

$$G_{2,2}(x) = x^8 + 87x^6 + 540x^4 + 459x^2 + 81$$

$$G_{3,2}(x) = x^8 - 27x^6 + 207x^4 - 378x^2 + 81.$$

3 Finishing Testing Figueiredo's Conjecture

We now have two polynomials defining distinct field extensions of K_n for each n. In order to test Figueiredo's conjecture we need to compute the order of

$$\mathrm{Frob}_{\mathfrak{p}} = \left(\frac{L_{n,j}(i)/\mathbb{Q}(i)}{\mathfrak{p}} \right)$$

where $\mathfrak{p}$ is a prime of $\mathbb{Q}(i)$ unramified in $L_{n,j}$ and the expression on the right is the corresponding Artin symbol.

Let $\mathfrak{q}$ be a prime of $L_{n,j}(i)$ dividing $\mathfrak{p} \subset \mathcal{O}_{\mathbb{Q}(i)}$. The order of $\mathrm{Frob}_{\mathfrak{p}}$ is the inertial degree of $\mathfrak{q}$ over $\mathfrak{p}$. Since $L_{n,j}(i)/\mathbb{Q}(i)$ is Galois we need not specify a specific $\mathfrak{q}$ above $\mathfrak{p}$ since the inertial degree for each will be the same. In order to determine this inertial degree we would factor $G_{n,i}(x)$mod $\mathfrak{p}$ for each $\mathfrak{p}$. The factorization of $G_{n,i}(x)$ tells us the cycle structure of $\mathrm{Frob}_{\mathfrak{p}}$ considered as an element of S_8. In particular, this would tell us the order of $\mathrm{Frob}_{\mathfrak{p}}$. See [5, pg.128].

Computationally it is easier to consider a prime, $p \in \mathbb{Z}$, and a prime ideal, $\mathcal{Q} \subset \mathcal{O}_{L_{n,j}}$, dividing p and determine the inertial degree of $\mathcal{Q}$ over p. This is because it is harder to program a computer to factor polynomials over primes of an arbitrary number field than to factor polynomials over rational primes. There are several jumps to be made, however, to get from an inertial degree in $L_{n,j}/\mathbb{Q}$ to an inertial degree in $L_{n,j}(i)/\mathbb{Q}(i)$.

3.1 Computing Inertial Degrees

Denote by $f(\mathcal{Q}|p)$ the inertial degree of $\mathcal{Q}$ over p for any primes $\mathcal{Q}$ and p of specified number fields. Given notation as in Figure 3, we are concerned with computing $f(\mathfrak{q}|\mathfrak{p})$ from $f(\mathcal{Q}|p)$. There are a few separate cases to deal with.

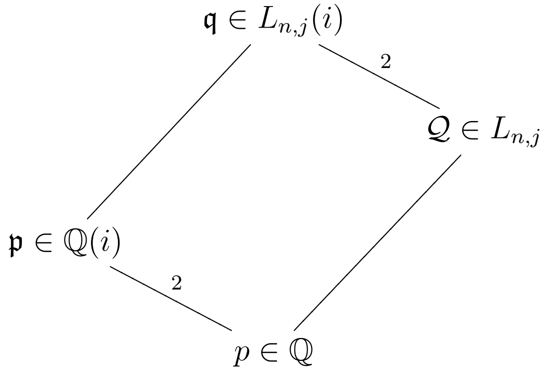
$\mathfrak{q} \in L_{n,j}(i)$
2
$\mathcal{Q} \in L_{n,j}$
$\mathfrak{p} \in \mathbb{Q}(i)$
2
$p \in \mathbb{Q}$

Figure 3: Lifting of Primes

First, consider the case $p = 2$, then p ramifies in $\mathbb{Q}(i)$, but not in $L_{n,j}$. We have $(1 + i)^2 = (2)$ and so $\mathcal{Q}$ must ramify in $L_{n,j}(i)$. Thus, it must be the case that $f(\mathfrak{q}|\mathfrak{p}) = f(\mathcal{Q}|p)$.

Second, consider the case $p \equiv 1 \bmod 4$, so that p splits in $\mathbb{Z}(i)$ and has inertial degree 1. To determine $f(\mathfrak{q}|\mathcal{Q})$ we notice that a defining polynomial for this extension is $p(x) = x^2 + 1$. If this polynomial factors mod $\mathcal{Q}$ then the inertial degree is 1, but we already know that $p(x)$ factors mod p and that $\mathcal{Q}$ divides p. Thus, $f(\mathfrak{q}|\mathcal{Q}) = f(\mathfrak{p}|p) = 1$. This implies $f(\mathfrak{q}|\mathfrak{p}) = f(\mathcal{Q}|p)$.

Third, consider the case $p \equiv 3 \bmod 4$. Then p is inert in $\mathbb{Z}(i)$ and $f(\mathfrak{p}|p) = 2$. We need to determine how $p(x) = x^2 + 1$ factors mod $\mathcal{Q}$. The field $\mathcal{O}_{L_{n,j}}/(\mathcal{Q})$ is isomorphic to $\mathbb{F}_{p^{f(\mathcal{Q}|p)}}$ in which -1 has a square root if and only if $f(\mathcal{Q}|p)$ is even. In this case $f(\mathfrak{q}|\mathcal{Q}) = 1$ and $f(\mathfrak{q}|\mathfrak{p}) = \frac{1}{2}f(\mathcal{Q}|p)$. Otherwise, $f(\mathfrak{q}|\mathcal{Q}) = 2$ and $f(\mathfrak{q}|\mathfrak{p}) = f(\mathcal{Q}|p)$.

We summarize these results in the following theorem.

Theorem 3.1. *With p, $\mathcal{Q}$, $\mathfrak{p}$, and $\mathfrak{q}$ as in Figure 3 we have the following relations* *between $f(\mathfrak{q}|\mathfrak{p})$ and $f(\mathcal{Q}|p)$:*

1. *If $p = 2$ or $p \equiv 1 \bmod 4$, then $f(\mathfrak{q}|\mathfrak{p}) = f(\mathcal{Q}|p)$.*

2. *If $p \equiv 3 \bmod 4$, then*

$$f(\mathfrak{q}|\mathfrak{p}) = \begin{cases} \frac{1}{2} f(\mathcal{Q}|p), & f(\mathcal{Q}|p) \text{ is even} \\ f(\mathcal{Q}|p), & f(\mathcal{Q}|p) \text{ is odd.} \end{cases}$$

Proof. QED. □

3.2 Computing $Tr(\rho(\mathbf{Frob}_p))$

Now, let ρ be the isomorphism taking $\mathrm{Gal}(L_{n,j}(i)/\mathbb{Q}(i))$ to $SL_2(\mathbb{F}_3)$. Let $Tr(\cdot)$ denote the trace of a matrix. It is easy to compute the traces of the various elements of $SL_2(\mathbb{F}_3)$ and sort them by order. Let A and B be the generators of $SL_2(\mathbb{F}_3)$ given above. First we see that $Tr(A) = Tr(A^{-1}) = Tr(-I) = 1$. Also, $Tr(B) = Tr(B^{-1}) = 0$ and $Tr(I) = Tr(A^2) = Tr(-A) = -1$. As we have given a representative of each conjugacy class and as the trace is a similarity invariant we can summarize these results as follows:

$$Tr(C) = \begin{cases} -1, & C \text{ has order } 1, 3 \\ 1, & C \text{ has order } 2, 6 \\ 0, & C \text{ has order } 4. \end{cases}$$

It is thus straightforward to compute $Tr(\rho(\mathrm{Frob}_{\mathfrak{p}}))$ for a given $\mathfrak{p}$.

We give examples of computing $Tr(\rho(\mathrm{Frob}_p))$ for a few primes, then we give the program used to compute it for as many primes as we wish.

First, consider $G_{1,1}(x) = x^8 + 18x^6 + 63x^4 + 45x^2 + 9$ and take $p = 5$ so that $\mathfrak{p} = 2 \pm i$. Since $p \equiv 1 \bmod 4$ we see that $f(\mathfrak{q}|\mathfrak{p}) = f(\mathcal{Q}|p)$, which is determined by factoring $G_{1,1}(x) \bmod p$. This is

$$x^8 + 18x^6 + 63x^4 + 45x^2 + 9 \equiv (x+2)(x-2)(x^3+x+1)(x^3+x-1) \mod 5$$

and implies that the order of $\mathrm{Frob}_{2\pm i} = o(\mathrm{Frob}_{2\pm i}) = 3$. This in turn gives that $Tr(\rho(\mathrm{Frob}_{2\pm i})) = -1$.

As a second example using $G_{1,1}(x)$ take $p = 11$ so that $\mathfrak{p} = 11$ also. We need to compute $f(\mathcal{Q}|p)$ by factoring $G_{1,1}(x) \bmod 11$. This is

$$x^8 + 18x^6 + 63x^4 + 45x^2 + 9 \equiv (x^4 - 3x^2 - 3)(x^4 - x^2 - 3) \mod 11$$

so that $f(\mathcal{Q}|p) = 4$. By the above considerations we see that $|\mathrm{Frob}_{11}| = f(\mathfrak{q}|11) = \frac{1}{2}f(\mathcal{Q}|11) = 2$. This in turn implies that $Tr(\rho(\mathrm{Frob}_{11})) = 1$. Both of these examples appear in Table 1 underneath $G_{1,1}(x)$.

For time's sake we again use GP/PARI to carry out the computations for as many other primes as we want. The program for $G_{1,2}$ is given below. The others are identical, with the exception of the definition of f on the first line and pol$n$ in place of pol1.

```
{
    f=x^8-60*x^6+702*x^4-396*x^2+9;write(pol1,f)
    ;nf=bnfinit(f);tr=[-1,1,-1,0,5,1];
    for(p=4,1000,b=1;n=sqrt(p);m=round(n);
         if(n==m,
             if(isprime(m)&&(Mod(m,4)==3),
                b=1;R=idealfactor(nf,m);y=matsize(R)[1];
                for(z=1,y,b=lcm(b,R[z,1][4]));
                 if(Mod(b,2)==0, write(pol1,m," "
                    ,b/2," ",tr[b/2]),
                        write(pol1,m," ",b," ",tr[b])
                   )
               )
            );
         if(isprime(p)&&(Mod(p,4)==1),
             for(k=1,round(sqrt(p)),
             if(issquare(p-k^2),q=k+round(sqrt(p-k^2))*I
            )
        );
        b=1;R=idealfactor(nf,p);y=matsize(R)[1];
        for(z=1,y,b=lcm(b,R[z,1][4]));
        write(pol1,q," ",b," ",tr[b])
        )
    )
}
```

These traces are given in the tables in Appendix A for each of the $G_{n,i}$ for unramified primes of norm less than 678. We find that each distinct set of eigenvalues of Hecke operators computed by Figueiredo [4] matches exactly our list of traces, giving evidence that his conjecture is accurate.

Appendix A: Tables of Traces of Frobenius

	$G_{1,1}(x)$		$G_{1,2}(x)$	
Prime	$o(\text{Frob}_{\mathfrak{p}})$	$Tr(\rho(\text{Frob}_{\mathfrak{p}}))$	$o(\text{Frob}_{\mathfrak{p}})$	$Tr(\rho(\text{Frob}_{\mathfrak{p}}))$
$1{\pm}i$	3	-1	6	1
$2{\pm}i$	3	-1	6	1
$3{\pm}2i$	6	1	6	1
$4{\pm}i$	3	-1	6	1
$5{\pm}2i$	6	1	3	-1
$6{\pm}i$	4	0	4	0
$5{\pm}4i$	4	0	4	0
7	3	-1	3	-1
$7{\pm}2i$	4	0	4	0
$8{\pm}3i$	3	-1	3	-1
$8{\pm}5i$	4	0	4	0
$9{\pm}4i$	3	-1	3	-1
$10 \pm i$	3	-1	6	1
$10{\pm}3i$	6	1	6	1
$8{\pm}7i$	4	0	4	0
11	2	1	2	1
$11{\pm}4i$	3	-1	6	1
$10{\pm}7i$	4	0	4	0
$11{\pm}6i$	6	1	6	1
$13{\pm}2i$	6	1	3	-1
$10{\pm}9i$	3	-1	3	-1
$12{\pm}7i$	6	1	6	1
$14{\pm}i$	3	-1	6	1
$15{\pm}2i$	3	-1	3	-1
$13{\pm}8i$	2	1	1	-1
$15{\pm}4i$	4	0	4	0
$16{\pm}i$	6	1	3	-1
$13{\pm}10i$	6	1	6	1
$14{\pm}9i$	3	-1	4	0
$16{\pm}5i$	4	0	4	0

Table 1

	$G_{1,1}(x)$		$G_{1,2}(x)$	
Prime	$o(\text{Frob}_{\mathfrak{p}})$	$Tr(\rho(\text{Frob}_{\mathfrak{p}}))$	$o(\text{Frob}_{\mathfrak{p}})$	$Tr(\rho(\text{Frob}_{\mathfrak{p}}))$
$17\pm2i$	6	1	3	-1
$13\pm12i$	4	0	4	0
$14\pm11i$	6	1	3	-1
$16\pm9i$	6	1	6	1
$18\pm5i$	6	1	6	1
$17\pm8i$	6	1	3	-1
19	3	-1	3	-1
$18\pm7i$	3	-1	3	-1
$17\pm10i$	4	0	4	0
$19\pm6i$	3	-1	3	-1
$20\pm i$	3	-1	6	1
$20\pm3i$	6	1	6	1
$15\pm14i$	6	1	6	1
$17\pm12i$	3	-1	3	-1
$20\pm7i$	3	-1	6	1
$21\pm4i$	6	1	6	1
$19\pm10i$	2	1	1	-1
$22\pm5i$	3	-1	6	1
$20\pm11i$	1	-1	2	1
23	2	1	2	1
$21\pm10i$	4	0	4	0
$19\pm14i$	4	0	4	0
$20\pm13i$	2	1	1	-1
$24\pm i$	4	0	4	0
$23\pm8i$	6	1	3	-1
$24\pm5i$	4	0	4	0
$18\pm17i$	4	0	4	0
$19\pm16i$	6	1	3	-1
$25\pm4i$	6	1	3	-1
$22\pm13i$	3	-1	6	1
$25\pm6i$	3	-1	3	-1
$23\pm12i$	6	1	6	1
$26\pm i$	6	1	3	-1

Table 1 cont.

	$G_{2,1}(x)$		$G_{2,2}(x)$	
Prime	$o(\mathrm{Frob}_{\mathfrak{p}})$	$Tr(\rho(\mathrm{Frob}_{\mathfrak{p}}))$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$Tr(\rho(\mathrm{Frob}_{\mathfrak{p}}))$
$1\pm i$	4	0	4	0
$2\pm i$	4	0	4	0
$3\pm 2i$	3	-1	3	-1
$4\pm i$	4	0	4	0
$5\pm 2i$	6	1	3	-1
$6\pm i$	6	1	6	1
$5\pm 4i$	3	-1	6	1
7	3	-1	3	-1
$7\pm 2i$	6	1	3	-1
$6\pm 5i$	3	-1	3	-1
$8\pm 3i$	3	-1	3	-1
$8\pm 5i$	2	1	1	-1
$9\pm 4i$	6	1	6	1
$10\pm i$	3	-1	6	1
$10\pm 3i$	6	1	6	1
$8\pm 7i$	6	1	3	-1
11	3	-1	3	-1
$11\pm 4i$	6	1	3	-1
$10\pm 7i$	4	0	4	0
$11\pm 6i$	6	1	6	1
$13\pm 2i$	6	1	3	-1
$10\pm 9i$	3	-1	3	-1
$12\pm 7i$	6	1	6	1
$14\pm i$	6	1	3	-1
$15\pm 2i$	6	1	6	1
$13\pm 8i$	3	-1	6	1
$15\pm 4i$	3	-1	3	-1
$16\pm i$	3	-1	6	1
$13\pm 10i$	3	-1	6	1
$14\pm 9i$	3	-1	3	-1
$16\pm 5i$	4	0	4	0

Table 2

	$G_{2,1}(x)$		$G_{2,2}(x)$	
Prime	$o(\mathrm{Frob}_{\mathfrak{p}})$	$Tr(\rho(\mathrm{Frob}_{\mathfrak{p}}))$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$Tr(\rho(\mathrm{Frob}_{\mathfrak{p}}))$
$17\pm2i$	4	0	4	0
$13\pm12i$	4	0	4	0
$14\pm11i$	6	1	3	-1
$16\pm9i$	6	1	6	1
$18\pm5i$	3	-1	3	-1
$17\pm8i$	4	0	4	0
19	3	-1	3	-1
$18\pm7i$	3	-1	3	-1
$17\pm10i$	3	-1	6	1
$19\pm6i$	3	-1	3	-1
$20\pm i$	4	0	4	0
$20\pm3i$	6	1	6	1
$15\pm14i$	6	1	6	1
$17\pm12i$	4	0	4	0
$20\pm7i$	6	1	3	-1
$21\pm4i$	3	-1	3	-1
$19\pm10i$	4	0	4	0
$22\pm5i$	6	1	3	-1
$20\pm11i$	6	1	3	-1
23	2	1	2	1
$21\pm10i$	4	0	4	0
$19\pm14i$	3	-1	6	1
$20\pm13i$	4	0	4	0
$24\pm i$	3	-1	3	-1
$23\pm8i$	3	-1	6	1
$24\pm5i$	3	-1	3	-1
$18\pm17i$	3	-1	3	-1
$19\pm16i$	3	-1	6	1
$25\pm4i$	6	1	3	-1
$22\pm13i$	3	-1	6	1
$25\pm6i$	4	0	4	0
$23\pm12i$	6	1	6	1
$26\pm i$	4	0	4	0

Table 2 cont.

	$G_{3,1}(x)$		$G_{3,2}(x)$	
Prime	$o(\mathrm{Frob}_{\mathfrak{p}})$	$Tr(\rho(\mathrm{Frob}_{\mathfrak{p}}))$	$o(\mathrm{Frob}_{\mathfrak{p}})$	$Tr(\rho(\mathrm{Frob}_{\mathfrak{p}}))$
$1 \pm i$	3	-1	6	1
$2 \pm i$	4	0	4	0
$3 \pm 2i$	4	0	4	0
$4 \pm i$	4	0	4	0
$5 \pm 2i$	6	1	3	-1
$6 \pm i$	4	0	4	0
$5 \pm 4i$	6	1	3	-1
7	3	-1	3	-1
$7 \pm 2i$	4	0	4	0
$6 \pm 5i$	4	0	4	0
$8 \pm 3i$	6	1	6	1
$8 \pm 5i$	3	-1	6	1
$9 \pm 4i$	3	-1	3	-1
$10 \pm i$	6	1	3	-1
$10 \pm 3i$	6	1	6	1
$8 \pm 7i$	6	1	3	-1
11	3	-1	3	-1
$11 \pm 4i$	6	1	3	-1
$10 \pm 7i$	3	-1	6	1
$11 \pm 6i$	4	0	4	0
$13 \pm 2i$	3	-1	6	1
$10 \pm 9i$	3	-1	3	-1
$12 \pm 7i$	4	0	4	0
$14 \pm i$	3	-1	6	1
$15 \pm 2i$	3	-1	3	-1
$13 \pm 8i$	3	-1	6	1
$15 \pm 4i$	2	1	2	1
$16 \pm i$	6	1	3	-1
$13 \pm 10i$	3	-1	6	1
$14 \pm 9i$	3	-1	3	-1
$16 \pm 5i$	3	-1	6	1

Table 3

	$G_{3,1}(x)$		$G_{3,2}(x)$	
Prime	$o(\text{Frob}_\mathfrak{p})$	$Tr(\rho(\text{Frob}_\mathfrak{p}))$	$o(\text{Frob}_\mathfrak{p})$	$Tr(\rho(\text{Frob}_\mathfrak{p}))$
$17\pm2i$	3	-1	6	1
$13\pm12i$	4	0	4	0
$14\pm11i$	3	-1	6	1
$16\pm9i$	3	-1	3	-1
$18\pm5i$	4	0	4	0
$17\pm8i$	4	0	4	0
19	3	-1	3	-1
$18\pm7i$	3	-1	3	-1
$17\pm10i$	3	-1	6	1
$19\pm6i$	6	1	6	1
$20\pm i$	6	1	3	-1
$20\pm3i$	3	-1	3	-1
$15\pm14i$	6	1	6	1
$17\pm12i$	3	-1	3	-1
$20\pm7i$	4	0	4	0
$21\pm4i$	3	-1	3	-1
$19\pm10i$	4	0	4	0
$22\pm5i$	6	1	3	-1
$20\pm11i$	6	1	3	-1
23	2	1	2	1
$21\pm10i$	3	-1	3	-1
$19\pm14i$	6	1	3	-1
$20\pm13i$	6	1	3	-1
$24\pm i$	3	-1	3	-1
$23\pm8i$	4	0	4	0
$24\pm5i$	6	1	6	1
$18\pm17i$	6	1	6	1
$19\pm16i$	6	1	3	-1
$25\pm4i$	6	1	3	-1
$22\pm13i$	2	1	1	-1
$25\pm6i$	3	-1	3	-1
$23\pm12i$	4	0	4	0
$26\pm i$	4	0	4	0

Table 3 cont.

References

[1] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[2] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[3] L. M. Figueiredo. Serre's conjecture for imaginary quadratic fields. *Compositio Math.*, 118(1):103–122, 1999.

[4] Luiz M. S. Figueiredo. *Serre's Conjecture Over Imaginary Quadratic Fields*. PhD thesis, University of Cambridge, 1995.

[5] Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

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

[7] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Damon [Henri Darmon], With a foreword by Darmon and the author.

[8] The PARI Group, Bordeaux. *PARI/GP, Version 2.3.3*, 2006. available from `http://pari.math.u-bordeaux.fr/`.

[9] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.