S_4 AND $\widetilde{S}_4$ EXTENSIONS OF $\mathbb{Q}$ RAMIFIED AT ONLY ONE PRIME.

Darrin Doud

University of Illinois
Department of Mathematics
Urbana, IL 61801

August 4, 1998

Abstract. For each prime p in a certain family of odd primes, we construct an S_4 extension of $\mathbb{Q}$ unramified outside p. We show that for all $p \equiv 3 \pmod 8$ in our family, this S_4 extension embeds in an $\widetilde{S}_4$ extension, which is also unramified outside p. Invoking Serre's conjecture (in a proven case) allows us to relate the splitting of primes in these extensions to certain modular forms of level 1.

1. Introduction

In this paper we will be interested in analyzing the structure of certain S_4 extensions which are ramified at only one prime. We give a conjecturally infinite family of primes, and for each such prime p we define an explicit polynomial which has an S_4 extension unramified outside p as its splitting field. We show that when $p \equiv 3 \pmod 8$, the given S_4 extension can be enlarged to an $\widetilde{S}_4$ extension which is unramified outside p (where $\widetilde{S}_4$ is the central extension of S_4 by ± 1 isomorphic to $\mathrm{GL}_2(\mathbb{F}_3)$). Finally, a proven case of Serre's conjecture allows us to produce a modular form of level 1 which encodes the splitting of the primes in this $\widetilde{S}_4$ extension.

2. S_4 extensions

Theorem 1. *Let p be an odd prime such that*

$$(-1)^{(p-1)/2}p = p^* = (256n^3 - k^2)/27,$$

1991 *Mathematics Subject Classification.* 11R21,11F11.

Typeset by $\mathcal{AMS}$-TeX

with k divisible by 27 if n is divisible by 3. Suppose that $p^* \neq 1+4n$. Then the splitting field of $f(x) = (x+n)^4 - p^*x$ is an S_4 extension of $\mathbb{Q}$ which is ramified only at p.

Remarks. Given the conditions on n and k, we see that k must be odd. Also, either n is exactly divisible by 3, or $n \equiv 1 \pmod 3$. Any p of this form must be congruent to either 3 or 5 mod 8, since $p^* \equiv -k^2/27 \equiv 5 \pmod 8$. There are conjecturally infinitely many such primes, even if we fix n or k. In fact, such primes are not rare: the ones below 1000 are 59, 107, 139, 229, 283, 307, 331, 419, 491, 499, 733, 883.

This list can be shown to be complete. Lemmas 1 and 2 show that 3 cannot be on the list, since if p were 3, we would have a quartic field with discriminant dividing -27, and such a field cannot exist[6]. For any other prime p to be on the list, we must have $p \equiv 3$ or $5 \pmod 8$, and the class number of $\mathbb{Q}(\sqrt{p^*})$ must be divisible by three. Other than the primes above, only eight primes less than 1000 satisfy these conditions. Seven of these (83, 211, 379, 547, 563, 643, and 971) can be eliminated by observing that a certain modular form of weight $1+(p^2-1)/8$ does not exist. The last (907) can be eliminated by showing the nonexistence of certain integral points on an elliptic curve, which we do not describe in this paper.

Fix $p^* = (256n^3 - k^2)/27$, as in the theorem, and define $f(x) = (x+n)^4 - p^*x$. We see easily that $(n,p) = (k,p) = 1$, so that f is irreducible (since $f(x-n)$ is Eisenstein). The discriminant of f is $k^2{p^*}^3$. Let K_4 be the field $\mathbb{Q}(\alpha)$ where α is a root of f. We define $t(k)$ to be the unique element in $\{-1,0,1\}$ such that $t(k) \equiv k \pmod 3$.

Lemma 1. *If $(n,3) = 1$, the elements*

$$\left\{1, \alpha, \alpha^2, \frac{1}{k}\left(\alpha^3 + \frac{13n - t(k)k}{3}\alpha^2 + \frac{67n^2 + (n+1)t(k)k}{9}\alpha - 3n^3\right)\right\}$$

are all algebraic integers.

Proof. The only question in this lemma is whether the fourth element (which we will denote by β) is an algebraic integer. Since $(256n^3 - k^2)/27$ is an integer, $(k,3) = 1$, and in fact, $n \equiv 1 \pmod 3$. Thus, $13n - t(k)k \equiv 0 \pmod 3$. Using the fact that $n^3 \equiv 1 \mod 9$, we see that $k^2 \equiv 4 \pmod 9$, so that $k \equiv \pm 2 \pmod 9$ and $t(k)k \equiv -2 \pmod 9$. Hence,

$$\begin{aligned} n(67n^2 + (n+1)t(k)k) &\equiv 67n^3 + (n^2+n)t(k)k \pmod 9 \\ &\equiv 4 + 2t(k)k \pmod 9 \\ &\equiv 0 \pmod 9. \end{aligned}$$

Since n is invertible mod 9, $67n^2 + (n+1)t(k)k \equiv 0 \pmod 9$. This shows that at least $k\beta$ is an algebraic integer. We may easily compute the four conjugates of

β over $\mathbb{Q}$ (by replacing α by each of the four roots of f in turn); denoting these conjugates by $\beta=\beta_0,\beta_1,\beta_2,\beta_3$, the polynomial

$$\prod_{i=0}^{3}(x-\beta_i)$$

can be computed by using a computer algebra system (such as *Mathematica*) and the relations between symmetric polynomials in roots of f and coefficients of f. This polynomial is $x^4+a_3x^3+a_2x^2+a_1x+a_0$, where

$$\begin{aligned}
a_3 &= \frac{k+t(k)(16n^2+4n)}{9}\\
a_2 &= \frac{nk^2-t(k)(4n^2+n)k-(288n^4+48n^3+2n^2)}{3^3}\\
a_1 &= \frac{1}{3^9}\big(t(k)k^4-(30n+2)k^3+t(k)(229n^3-144n^2-30n-1)k^2\\
&\qquad +(8976n^4+1592n^3+81n^2)k-t(k)(10944n^5+1200n^4+148n^3)\big)\\
a_0 &= \frac{1}{3^8}\big(-t(k)n^3k^3+(-n^5-29n^4+2n^3)k^2\\
&\qquad -t(k)(192n^6+112n^5-28n^4+n^3)k-(9216n^7-1632n^6+112n^5-n^4)\big)
\end{aligned}$$

We now note that $k\beta$ has minimal polynomial $x^4+ka_3x^3+k^2a_2x^2+k^3a_1x+k^4a_0$, which has integer coefficients. Thus, the denominators of the a_i must divide k^4. However, $(k,3)=1$, so the a_i must all be integers. $\square$

Lemma 2. *If* $3|n$, *then the elements*

$$\left\{1,\alpha,\frac{1}{3}(\alpha^2-t(n/3)\alpha),\frac{3}{k}\left(\alpha^3+\frac{13n}{3}\alpha^2+\frac{67n^2}{9}\alpha-3n^3\right)\right\}$$

are all algebraic integers.

Proof. Let γ be the third element of this set, and δ be the fourth. Using *Mathematica*, as before, we find that the minimal polynomial of δ is

$$x^4+\frac{k}{3}x^3+\frac{32n^3+k^2}{27}x^2+\frac{176kn^3+k^3}{729}x+\frac{k^2n^3}{81},$$

which is easily seen to have integral coefficients (since $3|n$ and $27|k$).

The minimal polynomial of γ is

$$\begin{aligned}
x^4 &- \frac{4}{3}(n^2+t(n/3)n)x^3+\frac{2210n^4+1092t(n/3)n^3+162n^2-8k^2n-3t(n/3)k^2}{243}x^2\\
&+\frac{1}{19683}\Big(-13156n^6+32724t(n/3)n^5+18900n^4+(296k^2+3996t(n/3))n^3\\
&\qquad -162t(n/3)k^2n^2-108k^2n+(-k^4-27t(n/3)k^2)\Big)x\\
&+\frac{27n^8-148t(n/3)n^7+162n^6+108t(n/3)n^5+(t(n/3)k^2+27)n^4}{2187}.
\end{aligned}$$

We note that the coefficient of x^3 and the constant coefficient are trivially integers, since $3|n$ and $27|k$. The coefficient of x^2 is an integer, since $2210n^4+1092t\left(\frac{n}{3}\right)n^3 = 3^4\left(2210\left(\frac{n}{3}\right)^4+364t\left(\frac{n}{3}\right)\left(\frac{n}{3}\right)^3\right) = 3^4\left(\frac{n}{3}\right)(2210(n/3)-364t(n/3))$ is a multiple of 3^5. To show that the coefficient of x is an integer, we need only show that 3^9 divides $-13156n^6+18900n^4+3996t(n/3)n^3$. Letting $m=n/3$, this is equivalent to showing that $-13156m^3+2100m+148t(m)\equiv 0 \pmod{27}$. Note that m is relatively prime to 3. By checking each possible value of m mod 27, we see that this is true. $\square$

Lemma 3. *K_4 has discriminant ${p^*}^3$.*

Proof. Lemmas 1 and 2 show that the discriminant of K_4 divides ${p^*}^3$ (since $\mathbb{Z}[\alpha]$ has index at least k in the ring of integers). Using that $(n,p)=1$, a simple application of Dedekind's Criterion ([2], pp. 299-300) shows that the order $\mathbb{Z}[\alpha]$ is p-maximal, and thus the discriminant of K_4 is ${p^*}^3$. $\square$

Lemma 4. *If $p^*\neq 1+4n$, then the Galois group of f is S_4.*

Proof. We note that the resolvent cubic of $f(x-n)$ is $x^3-4np^*x-{p^*}^2$. This is reducible exactly when it has a rational root. It is easy to see that $\pm1, \pm{p^*}^2$, are not roots. Now, p^* is a root exactly when $p^*=1+4n$, and $-p^*$ is a root exactly when $p^*=-1+4n$. Since $p^*\equiv 1 \pmod 4$, the second case can never happen, and we have excluded the first in our hypothesis. Then, since the resolvent cubic defines a field contained in the splitting field of f, we see that the Galois group has cardinality divisible by 3. In fact, since the discriminant of the resolvent cubic is $-k^2{p^*}^3$, it has Galois group S_3, so the Galois group of f must have S_3 as a quotient. Thus, the Galois group of f is S_4. $\square$

This completes the proof of Theorem 1, since by Lemma 4, the splitting field of f is an S_4 extension of $\mathbb{Q}$, and by Lemma 3 it is unramified outside p.

We note that Theorem 1 does not give all S_4 extensions unramified outside p. In particular it misses all those whose quartic subfield has discriminant p^*. This is not a great loss, since such quartic fields have small discriminant, and are easy to find in tables of number fields. Theorem 1 also misses some S_4 extensions whose quartic subfield has discriminant ${p^*}^3$, even for $p\equiv 3$ or $5 \pmod 8$.

Remark. If we relax the condition on n and k somewhat, and allow $p^*=1+4n$, then we have that $1+4n=(256n^3-k^2)/27$. Solving this for k, we find that $k^2=(4n-3)(8n+3)^2$. Thus, $4n-3=m^2$, so $4n+1=m^2+4=p^*$, and we see that $p^*=m^2+4$.

In this case, the splitting field of f has no cubic subfield, and is hence either D_4, the Klein four group, or cyclic of order 4. The first two possibilities are eliminated because in both cases the splitting field would contain more than one quadratic subfield, and hence would be ramified outside p. In fact, for any prime $p=m^2+4$, if we let $n=(p-1)/4$, then $f(x)=(x+n)^4-p^*x$ defines a cyclic quartic field ramified only at p.

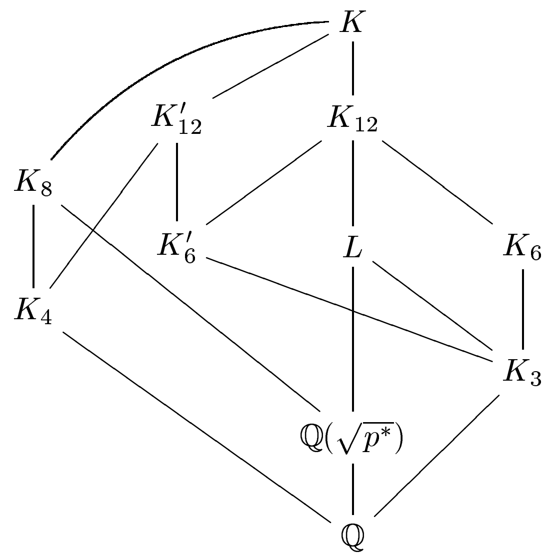

Diagram 1

3. The splitting of p

We now proceed to determine exactly how p splits in K, the splitting field of f. We have seen that K is a degree 24 extension of $\mathbb{Q}$, with Galois group isomorphic to S_4. Diagram 1 gives an inclusion diagram for the subfields of K (the degree of a field over $\mathbb{Q}$ is indicated by its subscript, and L is Galois over $\mathbb{Q}$ with Galois group S_3). This diagram shows only one representative of each conjugacy class of subfields of K, and K_6, K_{12}, and K'_{12} are fixed fields of a four cycle, a double transposition, and a transposition, respectively.

Let $\sqrt{\alpha}$ be one of the square roots of α. Then $\sqrt{\alpha}$ is a root of $f(x^2) = (x^2 + n)^4 - p^* x^2$. This polynomial factors over $\mathbb{Q}(\sqrt{p^*})$ as

$$f(x^2) = ((x^2+n)^2 - \sqrt{p^*}x)((x^2+n)^2 + \sqrt{p^*}x).$$

We now know that $\mathbb{Q}(\sqrt{\alpha})$ is of degree at most 8 over $\mathbb{Q}$, and contains α and $\sqrt{p^*} = \pm(\alpha+n)^2/\sqrt{\alpha}$. Thus, $\mathbb{Q}(\sqrt{\alpha}) = K_8$. Since the discriminant of $f(x^2)$ is $2^8 n^4 k^2 {p^*}^6$, and the discriminant of K_8 is divisible by at least ${p^*}^6$, we may find the factorization of p in K_8 by factoring $f(x^2) \pmod{p}$. To calculate this factorization, we use the fact that n is a quadratic residue mod p (since $n^3 \equiv k^2/256 \pmod{p}$). We find that for $p \equiv 3 \pmod 8$, $f(x^2)$ factors as $(x^2+n)^4$, but for $p \equiv 5 \pmod 8$, $f(x^2)$ factors as $(x-m)^4(x+m)^4$, where m is a square root of $-n$ mod p. In terms of primes, this says that the unique prime above p in K_4 is inert in K_8 when $p \equiv 3 \pmod 8$, but it splits when $p \equiv 5 \pmod 8$. We note that p must ramify in $\mathbb{Q}(\sqrt{p^*})$, and it must split into three primes in L. Thus, the number g of primes lying over p in K is divisible by 3, and each has ramification index e divisible by 4. If $p \equiv 5$

(mod 8), we have that g is even, so that $g = 6$ and $e = 4$, and the inertial degree $f = 1$. On the other hand, if $p \equiv 3 \pmod 8$, we have that $g = 3$, $e = 4$, and $f = 2$. This information, together with the fact that the inertia group is cyclic tells us that up to conjugation the inertia field of K at p is K_6 and the decomposition field is K_3 (resp. K_6) if $p \equiv 3 \pmod 8$ (resp. $p \equiv 5 \pmod 8$).

4. $\widetilde{S}_4$ EXTENSIONS

We will now investigate the problem of extending our family of S_4 extensions to $\widetilde{S}_4$ extensions. Recall [8, p. 97] that $\widetilde{S}_4$ is the unique central extension of S_4 in which each transposition lifts to an element of order 2, and each double transposition lifts to an element of order 4. We first show that if $p \equiv 5 \pmod 8$, there is no $\widetilde{S}_4$ extension of $\mathbb{Q}$ containing K. For such a prime the maximal real subfield of K is K_{12} (since f has no real roots, the maximal real subfield cannot contain K_4), so that complex conjugation in K would correspond to a double transposition. Then if K were contained in some $\widetilde{S}_4$ extension, complex conjugation in this extension would be a lift of a double transposition, and have order 4, which is impossible.

In the case $p \equiv 3 \pmod 8$, $\mathbb{Q}(\sqrt{p^*})$ is imaginary quadratic, so the following theorem of Bayer and Frey applies:

Theorem 2. *[1] If K is a Galois extension of $\mathbb{Q}$ with Galois group S_4, with K_4 one of its quartic subfields, and the quadratic subfield of K is imaginary, then K can be extended to an $\widetilde{S}_4$ extension if and only if the local invariant $e_{K,p}$ is trivial in the Brauer group of $\mathbb{Q}_p$ for each odd prime p which ramifies in K. The invariants $e_{K,p}$ may be calculated from the table below:*

Factorization of $p\mathfrak{O}_{K_4}$	$e_{K,p}$
$\mathfrak{p}_1^4$	$(-1)^{(p^2-1)/8}(-1)^{(p-1)/2}$
$\mathfrak{p}_1^3\mathfrak{p}_1'$	1
$\mathfrak{p}_1^2\mathfrak{p}_1'\mathfrak{p}_1''$	1
$\mathfrak{p}_1^2\mathfrak{p}_2'$	-1
$\mathfrak{p}_1^2{\mathfrak{p}_1'}^2$	$(-1)^{(p-1)/2} \cdot (d,p)_p$
$\mathfrak{p}_2^2$	$(-1)^{(p+1)/2}$

Applying this to our extensions, in which p is the only ramified prime, ramifies totally in the quartic extension, and is congruent to 3 mod 8, we see that an $\widetilde{S}_4$ extension does exist. Finally, Serre [8, Corollary 2.1.8] shows that the existence of any $\widetilde{S}_4$ extension of $\mathbb{Q}$ containing K guarantees the existence of one which is unramified outside p, and this extension is unique. Thus, for any $p \equiv 3 \pmod 8$ of the specified form, we have an example of an $\widetilde{S}_4$ extension unramified outside p.

Table I

Conjugacy Class	1	2	3	4	5	6	7	8
Order	1	2	2	3	4	6	8	8
Size	1	1	12	8	6	8	6	6
χ_0	1	1	1	1	1	1	1	1
χ_1	1	1	-1	1	1	1	-1	-1
χ_2	2	2	0	-1	2	-1	0	0
χ_3	2	-2	0	-1	0	1	$\sqrt{-2}$	$-\sqrt{-2}$
χ_4	2	-2	0	-1	0	1	$-\sqrt{-2}$	$\sqrt{-2}$
χ_5	3	3	1	0	-1	0	-1	-1
χ_6	3	3	-1	0	-1	0	1	1
χ_7	4	-4	0	1	0	-1	0	0

We see easily that this new extension (which we will denote by $\widetilde{K}$) must be ramified at p over K, since if it is unramified the inertia group must be cyclic of order 4. Letting $\tilde{s}$ generate the inertia group, we note that the restriction s of $\tilde{s}$ to K must also have order 4 (and would thus be four cycle). However, then s^2 would be a double transposition, and would lift to $\tilde{s}^2$, which would then have to have order 4, giving us a contradiction.

5. Galois Representations

Let p be a prime congruent to $3 \pmod 8$, of the form indicated above, and let $\widetilde{K}$ be the corresponding $\widetilde{S}_4$ extension. Examining the character table of $\widetilde{S}_4$ (Table I) shows that there are two two-dimensional irreducible faithful complex representations of $\widetilde{S}_4$, which are actually defined over $\mathbb{Z}(\sqrt{-2})$. Choosing one and composing the projection $G_{\mathbb{Q}} \to \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ with it, we get a two-dimensional irreducible complex Galois representation $\rho_0 : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}(\sqrt{-2}))$. We may reduce this representation mod $\mathfrak{p}$ for one of the primes $\mathfrak{p}$ of $\mathbb{Q}(\sqrt{-2})$ lying over p. Since p splits in $\mathbb{Q}(\sqrt{-2})$, this gives rise to a representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$, with the fixed field of the kernel of ρ equal to $\widetilde{K}$. This representation is unramified outside p, by construction; hence its Artin conductor is a power of p. Since we know the ramification groups at p in $\widetilde{K}$, we may compute the Artin conductor; it is p^2. We note that the central element of $\widetilde{S}_4$ has fixed field K; this central element cannot be complex conjugation, since K is not real. Hence complex conjugation maps to a non-scalar matrix, so the representation ρ is odd.

Given a two-dimensional odd irreducible representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$, we have the following conjecture:

Conjecture. *(Serre) There is a cusp form f of some integer weight k greater than 1, some level N and some character ϵ, which is a simultaneous eigenform for the Hecke operators, such that if f has Fourier expansion at infinity $\sum a_n q^n$, and ℓ is an unramified prime for ρ which does not divide Np,*

$$\mathrm{Tr}(\rho(\mathrm{Fr}_\ell)) = \widetilde{a}_\ell \quad \textit{and} \quad \det \rho(\mathrm{Fr}_\ell) = \widetilde{\epsilon(\ell)\ell^{k-1}},$$

where the map $x \mapsto \widetilde{x}$ from the algebraic integers to $\overline{\mathbb{F}}_p$ denotes reduction modulo some place lying above p.

In fact, in [9], Serre gives a recipe which predicts the exact weight, level, and character of the eigenform which corresponds to f. So far, little progress has been made on the main part of Serre's conjecture, but the following, (often known as the "epsilon-conjecture") has been proven (for $p > 3$):

Theorem 3. *Given ρ as above, if there is an eigenform f which corresponds to ρ, then there is an eigenform which corresponds to ρ and has the weight, level and character predicted in* [9].

For a discussion of this theorem, see [3] and [7].

The level predicted by Serre is just the prime to p part of the Artin conductor, which in this case is a power of p, so the desired level is 1. The predicted character is a character of $\mathbb{Z}/N\mathbb{Z}$, where N is the predicted level. Clearly, it is the trivial character.

In order to calculate the weight predicted by Serre, we need to distinguish between the two Galois representations corresponding to the two irreducible faithful two dimensional mod p representations of S_4. Let I be the inertia group (in $G_{\mathbb{Q}}$) of a place above p, and choose a generator x of its tame quotient I_t. We have two surjective fundamental characters $\Psi, \Psi' : I_t \to \mathbb{F}_{p^2}^*$, and we choose a square root of -2 in $\mathbb{F}_p$ by $\sqrt{-2} = \Psi^{(p^2-1)/8}(x) + \Psi'^{(p^2-1)/8}(x)$. We then choose the representation ρ such that $\rho(x) = \sqrt{-2}$. (The other representation will take x to $-\sqrt{-2}$.) Our choice of ρ guarantees that $\rho|_{I_t}$ decomposes as the direct sum of $\Psi^{(p^2-1)/8}$ and $\Psi'^{(p^2-1)/8}$. Now

$$\frac{p^2-1}{8} = \frac{3p-1}{8} + p\frac{p-3}{8} = b + pa,$$

with $a = (p-3)/8$ and $b = (3p-1)/8$. Serre's prediction for the weight is $1+pa+b = 1 + (p^2-1)/8$. If we had chosen the other representation (with $\rho(x) = -\sqrt{-2}$), a similar calculation would have predicted a weight of $1 + 5(p^2-1)/8$.

Let ρ_0 be a lift of ρ to $\mathrm{GL}_2(\mathbb{Z}(\sqrt{-2}))$, and let $\mathfrak{p}$ be a prime above p in $\mathbb{Q}(\sqrt{-2})$ such that the reduction of ρ_0 mod $\mathfrak{p}$ is ρ. Then ρ_0 is an odd, absolutely irreducible, complex two dimensional representation with image isomorphic to $\widetilde{S}_4$. By the theorem of Langlands-Tunnell[11], ρ_0 satisfies the conditions of the theorem of Weil-Langlands[10]. Hence, there is a weight 1 eigenform $f = \sum a_n q^n$ (of level equal to the Artin conductor of ρ_0 and character equal to the determinant of ρ_0), such that for $\ell \neq p$, $a_\ell = \mathrm{Tr}(\rho_0(\mathrm{Fr}_\ell))$.

If we multiply f by the Eisenstein series E_{p-1} of weight $p-1$ (which is congruent to 1 mod p), we obtain a modular form fE_{p-1} of weight p. This form might not be an eigenform for all the Hecke operators, but we do have that $fE_{p-1}|_{T_\ell} \equiv a_\ell f E_{p-1} \pmod{\mathfrak{p}}$ for all Hecke operators T_ℓ with $\ell \neq p$. A lemma of Deligne-Serre [4, 6.11] then gives the existence of a cuspidal eigenform $g = \sum b_n q^n$ (possibly defined over a larger field) which has eigenvalues $b_\ell \equiv a_\ell \pmod{\mathfrak{p}'}$ for some prime $\mathfrak{p}'$ lying over $\mathfrak{p}$, and for $\ell \neq p$. If $\bar{b}_n$ is the reduction of b_n mod $\mathfrak{p}'$, we see that $\bar{b}_\ell = \mathrm{Tr}(\rho(\mathrm{Fr}_\ell))$ for $\ell \neq p$.

We have now proven the existence of a characteristic p eigenform of weight p corresponding to ρ. By the epsilon conjecture, there is thus an eigenform of the weight, level, and character predicted by Serre, which corresponds to ρ.

6. Splitting of Primes

For a prime ℓ, not equal to p, we can describe the splitting of ℓ in $\widetilde{K}$ by determining the Frobenius of ℓ (up to conjugacy). We note from the character table of $\widetilde{S}_4$, that the order of the Frobenius element is uniquely determined by its trace, and can be read directly off of the character table, except when the trace is 0, in which case the Frobenius has order 2 or 4. If the Frobenius is of order 2, and has trace 0, it cannot be the central element, so it must be a lift of a transposition in S_4, and its fixed field contains K_{12}, but not K, so its fixed field cannot contain $\mathbb{Q}(\sqrt{p^*})$. If the Frobenius is of order 4, then it is a lift of a double transposition in S_4, and its fixed field contains $\mathbb{Q}(\sqrt{p^*})$. In the first case, l cannot split completely in $\mathbb{Q}(\sqrt{p^*})$, while in the second case it must. Since the splitting of ℓ in $\mathbb{Q}(\sqrt{p^*})$ is completely determined by the Legendre symbol $\left(\frac{\ell}{p}\right)$, we see that if the trace of the Frobenius is 0, the Frobenius has order 2 if $\left(\frac{\ell}{p}\right) = -1$, and order 4 if $\left(\frac{\ell}{p}\right) = 1$. Thus, we can easily determine the conjugacy class of the Frobenius of ℓ from its trace, which is the ℓth coefficient of the Fourier series of the modular form corresponding to ρ.

7. Calculation of Eigenforms

Direct calculation of the eigenform of weight $1 + (p^2 - 1)/8$ is possible, but difficult, since the smallest prime in which we are interested is 59, which gives a weight 436 eigenform. However, Edixhoven has shown [5] that every system of eigenvalues of a characteristic p cusp form comes from the eigenvalues of a cusp form of weight at most $p+1$ via the θ operator. More precisely, if $f = \sum a_n q^n$ is a modular form $\pmod{p}$ of weight k, $\theta f = \sum n a_n q^n$ is a modular form $\pmod{p}$ of weight $k+p+1$, and we have:

Theorem 4. *(Edixhoven) Let f be a cusp form of type (N, k, ϵ). Then there is a cusp form g of type (N, k', ϵ) and an integer m such that $\theta^m g$ and f have the same Fourier expansion $\pmod p$, and $k' \leq p+1$.*

This shows that the modular form f which corresponds to our representation (and has weight $1 + (p^2 - 1)/8$) is obtained from a modular form g of weight $(p+5)/4$ by applying the $(p-3)/8$th power of θ.

We note that upon reduction, the modular form f has coefficients in $\mathbb{F}_p$ (in fact, its Fourier coefficients a_ℓ for $\ell \neq p$ a prime are in the set $\{0, \pm 1, \pm 2, \pm\sqrt{-2}\}$ of values of the trace of ρ), so that in fact g has coefficients in $\mathbb{F}_p$.

To calculate g explicitly, we begin with a basis for the space of modular forms of weight k and level 1: a suitable basis is the set $\{G_4^a G_6^b : 4a + 6b = k\}$, where G_4 and G_6 are the Eisenstein series of weights 4 and 6, respectively. These forms all have integer coefficients–we reduce them mod p for ease of calculation. It is a simple matter to compute the action of a Hecke operator on this space (in terms of the basis); we find the eigenvectors of the resulting matrix which correspond to eigenvalues in $\mathbb{F}_p$. The space spanned by these eigenvectors contains g, since g has eigenvalues in $\mathbb{F}_p$, and is stable under the action of all the Hecke operators. Thus, we may choose another Hecke operator, and repeat the process on this smaller space. We repeat this until the basis we are left with consists of simultaneous eigenvectors of the Hecke operators. One of these will be the Eisenstein series of weight k, the rest will be cusp forms. We apply the θ operator to the cusp forms the appropriate number of times, eliminate any of the resulting forms which have Fourier coefficients outside the allowable set (described above). This will reduce the choices for f considerably–if more than one form remains, we calculate the splitting for well chosen primes in order to distinguish which corresponds to our Galois representation. We give several examples.

For $p = 59$, there is a single cuspidal eigenform g of weight $(p+5)/4 = 16$. Then $\theta^7 g$ must be the eigenform we want. As a mod p eigenform, $g = 7(\overline{G}_4^4 - \overline{G}_4\overline{G}_6^2)$, where $\overline{G}_4$ and $\overline{G}_6$ are the mod p reductions of G_4 and G_6. If we calculate $\theta^7 g$, the coefficients in the Fourier expansion are as follows:

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
a_ℓ	36	1	58	58	23	0	0	58	0	58	0	0	1	0	0	58	0	23	23	0

For $p = 107$, there are two cuspidal eigenforms of weight $(p+5)/4 = 28$. As mod p eigenforms, they are

$$80\overline{G}_4^7 + 34\overline{G}_4^4\overline{G}_6^2 + 100\overline{G}_4\overline{G}_6^4,$$

and

$$51\overline{G}_4^7 + 92\overline{G}_4^4\overline{G}_6^2 + 71\overline{G}_4\overline{G}_6^4.$$

If we apply θ^{13} to both of them, we get the following coefficients:

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61
a_ℓ	0	1	76	0	106	1	76	1	1	0	0	106	1	31	0	106	0	106
b_ℓ	1	96	52	63	13	104	59	22	35	93	104	32	101	42	80	27	41	46

It is clear that the first of these is the form we want.

If we set $p = 283$, compute the cuspidal eigenforms of weight 72, and compute θ^{35} of each such form, we immediately eliminate all but the two forms with the following Fourier coefficients:

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
a_ℓ	0	156	0	282	282	1	127	0	282	282	0	156	282	127	127
b_ℓ	127	0	127	1	282	282	127	127	282	1	156	127	282	0	0

As mod p eigenforms, these two forms correspond to θ^{35} of

$$212\overline{G}_4^{18} + 166\overline{G}_4^{15}\overline{G}_6^2 + 83\overline{G}_4^{12}\overline{G}_6^4 + 91\overline{G}_4^9\overline{G}_6^6 + 162\overline{G}_4^6\overline{G}_6^8 + 148\overline{G}_4^3\overline{G}_6^{10} + 270\overline{G}_6^{12},$$

and

$$-3\overline{G}_4^{18} + 11\overline{G}_4^{15}\overline{G}_6^2 + 189\overline{G}_4^{12}\overline{G}_6^4 + 37\overline{G}_4^9\overline{G}_6^6 + 245\overline{G}_4^6\overline{G}_6^8 + 87\overline{G}_4^3\overline{G}_6^{10}.$$

These two forms are associated to two non-isomorphic quartic fields of discriminant -283^3 which correspond to the two representations

$$-283 = \frac{256(-3)^3 - 27^2}{27} \quad \text{and} \quad -283 = \frac{256(4)^3 - 155^2}{27}.$$

To determine which form corresponds to which field, it will suffice to determine the splitting of one prime. If we let $\widetilde{K}$ be the $\widetilde{S}_4$ extensions corresponding to the first formula, then its quartic subfields are defined by the polynomial $f(x) = (x-3)^4 + 283x$. Now $\operatorname{disc}(f)$ is odd, and f is irreducible $\pmod 2$, so 2 is totally inert in the quartic subfield of $\widetilde{K}$. This implies that the order of the Frobenius at 2 is divisible by 4. However, $a_2 = 0$, and $\left(\frac{2}{283}\right) = -1$, so the first form above corresponds to a field with Frobenius at 2 of order 2. Hence, $\widetilde{K}$ corresponds to the second form, and the first form must correspond to the $\widetilde{S}_4$ extension derived from the polynomial $(x+4)^4 + 283x$.

References

1. P. Bayer and G. Frey, Galois representations of octahedral type and 2-coverings of elliptic curves, *Math. Z.* **207** (1991), 395-408.

2. H. Cohen, "A Course in Computational Algebraic Number Theory", Springer-Verlag, Berlin Heidelberg New York, 1993.
3. H. Darmon, Serre's Conjectures, *in* "Seminar on Fermat's Last Theorem", CMS Conf. Proc. 17, American Math. Soc., Providence, 1995, pp. 135-153.
4. P. Deligne and J.-P. Serre, Formes Modulaires de poids 1, *Ann. Sci. École Norm. Sup.* **7** (1974), 507-530.
5. B. Edixhoven, The weight in Serre's Conjectures on modular forms, *Invent. Math.* **109** (1992), 563-594.
6. A. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators, and zeros of zeta functions: A survey of recent results*, *Sem. Theorie des Nombres Bordeaux (2)* **2** (1990), 119-141.
7. K. Ribet, Report on mod ℓ representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *in* "Motives," Proc. Sympos. Pure Math., vol. 55, 1994, pp. 639-676.
8. J.-P. Serre, "Topics in Galois Theory (Lecture notes prepared by Henri Darmon)", Jones and Bartlett Publishers, Boston, 1992.
9. ______, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.* **54** (1987), 179-230.
10. ______, Modular forms of weight one and Galois representations, *in* "Algebraic Number Fields: L-functions and Galois properties," (Proc. Sympos. Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 193-268.
11. J. Tunnell, Artin's conjecture for representations of octahedral type, *Bull. Amer. Math. Soc. (N.S.)* **5** (1981), 173-175.