Even Icosahedral Galois Representations of Prime Conductor

Darrin Doud *

Department of Mathematics, Brigham Young University, Provo, UT 84602

Michael W. Moore

Department of Mathematics, Brigham Young University, Provo, UT 84602

Abstract

In this paper, we use a series of targeted Hunter searches to prove that the minimal prime conductor of an even icosahedral Galois representation is 1951. In addition, we give a complete list of all prime conductors less than 10,000 of even icosahedral Galois representations.

1 Introduction

Galois representations and their connections to modular forms have played a key role in modern number theory. Odd two-dimensional Galois representations and their connection to holomorphic modular forms were important in Wiles' proof of Fermat's Last Theorem. Even two-dimensional Galois representations are conjectured to correspond to Maass wave forms. Among the simplest examples of Galois representations are those which are ramified at only one prime. In the two-dimensional case, they have been studied by Serre [12] and Vignéras [14]. Serre studied odd irreducible Galois representations with prime conductor, and determined that, besides the dihedral ones, there were three major classes of such representations. Vignéras extended Serre's study to even Galois representations and classified them similarly. She gave several examples of dihedral and octahedral representations but was unable to find

* Corresponding Author

Email addresses: doud@math.byu.edu (Darrin Doud), mike@math.byu.edu (Michael W. Moore).

Article published in Journal of Number Theory **118** *(2006), pp. 62-70.*

any even icosahedral Galois representation of prime conductor. This is no surprise, as the discriminants of the number fields describing such representations are far larger than 2×10^7, and hence cannot be found even in modern tables of number fields [8]. In this paper, we describe the techniques that we used to find the even icosahedral representation of minimal prime conductor. An analogous result for odd icosahedral Galois representations (namely that the minimal prime conductor is 2083) can be found in [2]. We also give a table of all prime conductors less than 10,000 of even icosahedral representations.

2 Even Galois representations

For our purposes, a Galois representation is a continuous homomorphism $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$, where $G_{\mathbb{Q}}$ is the absolute Galois group of $\mathbb{Q}$, or $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Continuity in this case implies that the image of ρ is finite. Given a Galois representation ρ, we may construct a projective representation $\tilde{\rho} = \pi \circ \rho$, where $\pi : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{PGL}_2(\mathbb{C})$ is the natural projection map. Such a projective representation has as its image a finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$. Any such subgroup is well known to be isomorphic to a cyclic group, a dihedral group, A_4 (tetrahedral), S_4 (octahedral), or A_5 (icosahedral).

A theorem of Tate [12] shows that given any continuous homomorphism $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$, there is a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ such that $\tilde{\rho} = \pi \circ \rho$. In fact, this lift is not uniquely defined but can be chosen to have many different ramification properties. In particular, ρ can be chosen to be ramified only at those primes at which $\tilde{\rho}$ is ramified.

Complex conjugation is a well defined element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, which we will denote by τ. A Galois representation is called odd if $\det(\rho(\tau)) = -1$; it is called even if $\det(\rho(\tau)) = 1$.

Vignéras [14] classified even Galois representations of prime conductor. Her description involved the fixed field E of the kernel of $\tilde{\rho}$ and the ramification index e_p of p in $E/\mathbb{Q}$. She showed that the irreducible even Galois representations ρ with prime conductor p are either dihedral or correspond to totally real field extensions $E/\mathbb{Q}$ satisfying

1. $\mathrm{Gal}(E/\mathbb{Q}) \cong A_4$, $p \equiv 1 \pmod 3$, $E/\mathbb{Q}$ is the normal closure of a quartic field of discriminant p^2, and $e_p = 3$,

2a. $\mathrm{Gal}(E/\mathbb{Q}) \cong S_4$, $p \equiv 5 \pmod 8$, $E/\mathbb{Q}$ is the normal closure of a quartic field of discriminant p, and $e_p = 2$,

2b. $\mathrm{Gal}(E/\mathbb{Q}) \cong S_4$, $p \equiv 1 \pmod 8$, $E/\mathbb{Q}$ is the normal closure of a quartic field of discriminant p or p^3, and $e_p = 2$ or $e_p = 4$,

3a. $\mathrm{Gal}(E/\mathbb{Q}) \cong A_5$, $p \equiv 1 \pmod 5$, $E/\mathbb{Q}$ is the normal closure of a quintic field of discriminant p^4, and $e_p = 5$,

3b. $\mathrm{Gal}(E/\mathbb{Q}) \cong A_5$, $p \equiv 1 \pmod 3$, $E/\mathbb{Q}$ is the normal closure of a quintic field of discriminant p^2, and $e_p = 3$,

3c. $\mathrm{Gal}(E/\mathbb{Q}) \cong A_5$, $p \equiv 1 \pmod 4$, $E/\mathbb{Q}$ is the normal closure of a quintic field of discriminant p^2, and $e_p = 2$.

Note that determining a Galois extension E with the properties described here is equivalent to defining a projective representation $\tilde{\rho}$, so that finding even Galois representations of prime conductor is reduced to finding number fields with certain properties.

Vignéras indicated that there were no even representations of prime conductor of type 1 with $p < 106$; in fact, checking tables of quartic number fields [8] (which were not available to Vignéras) we find that the smallest p for which such a representation exists is $p = 163$.

Vignéras gave several examples of representations of type 2. Using a combination of class field theory and number field tables [8], we may determine that the minimal prime conductor of a representation of type 2a is 8069, and of a representation of type 2b is 2713.

Vignéras gave no examples of representations of type 3. She indicates that the tables of Buhler [3] contain no such representations. These tables, which contain representations of conductor up to 10,000, make no claim of completeness, so that the possibility remains that such representations exist. Modern tables of number fields [8], which give all totally real quintic number fields of discriminant at most 2×10^7 yield no examples of such a representation. This shows that any representation of type 3b or 3c must have $p > 4472$ (since $p^2 > 2 \times 10^7$), and that any representation of type 3a must have $p > 66$ (since $p^4 > 2 \times 10^7$).

Representations of type 3a with conductor much smaller than 10,000, but corresponding to number fields of discriminant much greater than 2×10^7 do exist. Because the discriminants of the fields are so large, the fields cannot be found in any standard tables of number fields. We will use a series of targeted Hunter searches to find all representations of type 3a with prime conductor less than 10,000. In addition, we will show that there are no representations of types 3b and 3c with conductor less than 10,000 and determine the minimal conductor of each of the three types of representation.

3 Targeted Hunter Searches

Given a discriminant D and a degree n, the goal of a Hunter search [6] is to find a polynomial defining a number field K of degree n and discriminant D or to determine that no such number field exists. Such a search is conducted by using Hunter's theorem and various relations between coefficients of polynomials to bound the coefficients of a polynomial defining a number field with the given degree and discriminant. Such a search generally yields a set of possible polynomials which is far too large to examine in a reasonable time (especially for large n or D). A refinement of the Hunter search [9,10] can be used if we are only interested in searching for K with a desired ramification type at a certain prime p. We use our knowledge of the ramification of the desired field K to determine congruence conditions on the defining polynomial of K. This allows us to drastically decrease the number of polynomials which need to be investigated. This "targeting" of a specific ramification structure is a powerful tool and can make otherwise impractical searches quite feasible. We describe both the traditional Hunter search and also the details behind a targeted search in this paper. These techniques are not original; they were described in [6], [9], and [10] in some detail, and our purpose in describing them here is to use them to find even icosahedral representations of prime conductor.

3.1 Hunter's Theorem

Hunter's theorem [5, Theorem 6.4.2] states:

Theorem 1 *Let K be a number field of degree n over $\mathbb{Q}$. There exists $\theta \in \mathfrak{O}_K \setminus \mathbb{Z}$ such that*

$$\sum_{i=1}^{n} |\theta_i|^2 \leq \frac{1}{n}\mathrm{Tr}(\theta)^2 + \gamma_{n-1}\left(\frac{|d(K)|}{n}\right)^{1/(n-1)}$$

where $d(K)$ is the discriminant of K, $\mathrm{Tr}(\theta)$ is the trace of θ, γ_{n-1} is Hermite's constant [7, p. 20] in dimension $n-1$, and $\theta_1, \ldots, \theta_n$ are the conjugates of θ. In addition, we may assume that $0 \leq \mathrm{Tr}(\theta) \leq n/2$.

If K is a primitive field, then the element $\theta \in K$ which is guaranteed to exist, by Hunter's theorem, is in fact a generator of K over $\mathbb{Q}$; i.e. $K = \mathbb{Q}(\theta)$. Then the minimal polynomial of θ is a defining polynomial for K.

In order to conduct a Hunter search for a primitive number field with a given discriminant D and degree $n = 5$, we first assume that such a number field exists. By Hunter's theorem there will then be a $\theta \in K$ with conjugates

$\theta = \theta_1, \ldots, \theta_5$, such that

$$\sum_{i=1}^{5} |\theta_i|^2 \leq \frac{1}{5}\mathrm{Tr}(\theta)^2 + \gamma_4 \left(\frac{|D|}{5}\right)^{1/4} = t_2$$

and $0 \leq \mathrm{Tr}(\theta) \leq 5/2$. We now write the minimal polynomial f of θ as

$$f(x) = x^5 - a_1 x^4 + a_2 x^3 - \cdots - a_5,$$

with $a_i \in \mathbb{Z}$ for $1 \leq i \leq 5$, and we see that $a_1 = \mathrm{Tr}(\theta)$, so $0 \leq a_1 \leq 5/2$. For future reference, we will define $a_0 = 1$.

For $k > 0$, we now define

$$S_k = \sum_{i=1}^{5} \theta_i^k \quad \text{and} \quad T_k = \sum_{i=1}^{5} |\theta_i|^k.$$

We note that the S_k are symmetric polynomials in the roots of f, and are thus integers. Now for $k > 1$, we see [6, pg. 453] that $|S_k| \leq T_k \leq T_2^{k/2} \leq t_2^{k/2}$. We will also use Newton's relations, which state that

$$ka_k = \sum_{j=1}^{k} (-1)^{j-1} a_{k-j} S_j.$$

In the case $k = 2$, solving Newton's relations for a_2 shows that

$$a_2 = \frac{(a_1 S_1 - a_0 S_2)}{2},$$

and since $-t_2 \leq S_2 \leq t_2$ and $S_1 = a_1$, we see that

$$\frac{a_1^2 - t_2}{2} \leq a_2 \leq \frac{a_1^2 + t_2}{2}.$$

We may improve this bound by using the fact that the field K for which we are searching must be totally real. In this case, [6, Prop. 9.3.7(2)] shows that $a_2 \leq (a_1^2 - 6)/2$. Hence, each possible value for a_1 gives a finite range of possibilities for a_2.

Similarly, solving Newton's relation with $k = 3$ for a_3, we obtain

$$a_3 = \frac{a_2 a_1 - a_1 S_2 + a_0 S_3}{3}.$$

Now, note that $|S_3| \leq T_3 \leq S_2^{3/2}$. In addition, we know that $S_2 = a_1^2 - 2a_2$. Putting these into the expression for a_3, we see that

$$\frac{-a_1^3 + 3a_1 a_2 - S_2^{3/2}}{3} \leq a_3 \leq \frac{-a_1^3 + 3a_1 a_2 + S_2^{3/2}}{3},$$

so that each possible pair of values for a_1 and a_2 gives a finite range of values for a_3.

At this point, it is convenient to bound a_5 before bounding a_4. By [6, Prop. 9.3.7(1)] we see that $|a_5| < S_2^{5/2}/5^{5/2}$, and note that this bound depends only on the values of a_1 and a_2. Finally, solving Newton's relation with $k = 4$ for a_4, we obtain

$$a_4 = \frac{a_1(a_3 + S_3) - a_2 S_2 - S_4}{4}.$$

Using the fact that $5|a_5|^{4/5} \leq S_4 \leq S_2^2$ [6, Prop. 9.3.7(3)], we obtain the inequalities

$$\frac{(a_3 + S_3)a_1 - a_2 S_2 - S_2^2}{4} \leq a_4 \leq \frac{(a_3 + S_3)a_1 - a_2 S_2 - 5|a_5|^{4/5}}{4}.$$

At this point, since each a_k is constrained to lie in a finite interval, we have constructed a finite set of polynomials, which contains a defining polynomial for K (under the assumption that K exists). We now need only check each polynomial, and find the ones defining a number field of the correct discriminant. If no such polynomial exists in the search space, then we are guaranteed that no totally real field with the desired degree and discriminant can exist.

Although our search space is finite, for even moderately large D these bounds give a search space which is far too large to search exhaustively. It is possible to get better bounds on the coefficients by more sophisticated methods [11], but we chose instead to reduce our search space by using ramification properties of the desired field K.

3.2 Targeted searches

Hunter's theorem gives us a finite (although very large) search space which is guaranteed to contain a polynomial defining the field for which we are searching (if such a field exists). Targeting is a technique to take advantage of the fact that we may know something about the ramification of the fields for which we are searching.

Theorem 2 *Let L/K be a finite extension of number fields such that $L = K(\alpha)$, with α a root of a monic irreducible polynomial $g(x) \in \mathfrak{O}_K[x]$. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$, and suppose that $\mathfrak{p}\mathfrak{O}_L = \prod \mathfrak{P}_i^{e_i}$ is a product of powers of distinct prime ideals in L, such that the inertial degree of $\mathfrak{P}_i$ is f_i. Then $g \equiv \prod g_i^{e_i} \pmod{\mathfrak{p}}$ with $g_i \in \mathfrak{O}_K[x]$ and $\deg(g_i) = f_i$.*

Remark: Note that there is no guarantee that the g_i are irreducible. In order to guarantee their irreducibility, we would need to know something about the index of $\mathfrak{O}_K[\alpha]$ in $\mathfrak{O}_L$.

PROOF. Denote by $K_\mathfrak{p}$ and $L_{\mathfrak{P}_i}$ the completions of K and L with respect to the indicated primes. We know [4] that

$$K_\mathfrak{p} \otimes_K L \cong \bigoplus_{\mathfrak{P}_i} L_{\mathfrak{P}_i},$$

which immediately implies that in $K_\mathfrak{p}$, we have $g = \prod h_i$, with each h_i monic of degree $e_i f_i$, and $L_{\mathfrak{P}_i} \cong K_\mathfrak{p}[x]/(h_i(x))$ [4, page 58]. We thus only need to show that each h_i is congruent modulo $\mathfrak{p}$ to some $g_i^{e_i}$.

Let M be a splitting field of h_i over $K_\mathfrak{p}$, let $\mathfrak{P}$ be the unique prime ideal of M, let I be the inertia group of $M/K_\mathfrak{p}$, and let β be any root of h_i in M. Let e and f be the ramification index and inertial degree of $M/K_\mathfrak{p}$, and let e_i and f_i be the ramification index and inertial degree of $K_\mathfrak{p}(\beta)/K_\mathfrak{p}$. Note that the values of e_i and f_i are the same as the e_i and f_i defined above, and that they are independent of the choice of β. Let I_β be the inertia group of $M/K_\mathfrak{p}(\beta)$. Then I_β has order $e' = e/e_i$, and is equal to $I \cap \mathrm{Gal}(M/K_\mathfrak{p}(\beta))$. If we consider the action of I on the roots of h_i, we see that the stabilizer of β is just I_β. Then the orbit-stabilizer relationship shows that the orbit of β under the action of I has order e_i. However, the image of β under any element of I is congruent to β modulo $\mathfrak{P}$. Hence each root β of h_i is congruent modulo $\mathfrak{P}$ to the e_i roots in its orbit. Let $\beta_1, \ldots, \beta_{f_i}$ be a set of representatives of the orbits. Define

$$p(x) = \prod_{j=1}^{f_i} (x - \beta_j).$$

Clearly the coefficients of $p(x)$ are fixed modulo $\mathfrak{P}$ by $\mathrm{Gal}(M/K_\mathfrak{p})$, so that the reduction $\bar{p}(x)$ modulo $\mathfrak{P}$ actually has coefficients in $\mathfrak{O}_{K_\mathfrak{p}}/\mathfrak{p}$. Hence, $\bar{p}(x)$ is actually the reduction modulo $\mathfrak{p}$ of a polynomial $g_i(x) \in \mathfrak{O}_K[x]$, and we see that $h_i(x) \equiv g_i(x)^{e_i} \pmod{p}$, as desired. $\square$

For each of the three types of even icosahedral Galois representation described by Vignéras, we need to search for a totally real quintic field K ramified only at one prime p, with a specific type of ramification at p. We do this by conducting a Hunter search for a polynomial f which defines K. Since we know the desired discriminant and signature of K, we know that a defining polynomial exists in a finite (but large) set of polynomials. In addition, because we know the desired ramification of p in K, we know how this defining polynomial must factor modulo p. We give details for each type of representation.

Type 3a: Here $p \equiv 1 \pmod{5}$ is ramified with $e = 5$. Hence, the desired polynomial is of the form $(x-a)^5 \pmod{p}$. In our program, as soon as we determine a_1, we know exactly what a is (since $a_1 \equiv 5a \pmod{p}$), and this determines the values of $a_2, \ldots, a_5$ modulo p. Rather than examining all values of $a_2, \ldots, a_5$ within our bounds, we only examine those satisfying the given congruence conditions. This results in examining approximately 1 of every p^4 polynomials in the search space, dramatically reducing the time required for the search.

Type 3b: Here $p \equiv 1 \pmod{3}$ and p is ramified with $e = 3$. There may be either one or two other primes above p (besides the ramified one), with inertial degrees either 2 or 1. In any case, we see easily that $f \equiv (x-a)^3(x^2+bx+c)$ $\pmod{p}$, where the quadratic factor may be either reducible or irreducible. As we proceed through our Hunter search, we determine a_1, a_2, and a_3. This allows us to solve for a (as a root of a cubic polynomial modulo p) and afterward determine b and c. Once a, b, and c are determined, the values of a_4 and a_5 are determined modulo p. Hence, we only need to examine about 1 of every p^2 polynomials in the search space.

Type 3c: Here $p \equiv 1 \pmod{4}$ and p splits in K as either P^2Q with P having inertial degree 2 or as P^2Q^2R with all primes having inertial degree 1. In the first case, f factors modulo p as $(x^2+ax+b)^2(x+c)$, and in the second case, f factors modulo p as $(x+d)^2(x+e)^2(x+c)$. In either case we may write $f \equiv (x^2+ax+b)^2(x+c) \pmod{p}$, where the quadratic factor may be reducible. As above, the first three coefficients of f determine a, b, and c modulo p, which determine a_4 and a_5 modulo p. Hence, we need only examine 1 of every p^2 polynomials in our search space.

4 Computational Results

We programmed the targeted Hunter searches described above in the GP/Pari [13] programming language. For each prime congruent to 1 modulo 5 and below 10,000 we searched for an A_5-extension corresponding to a representation of type 3a. The results of our search are summarized in table 1. We stress that for primes p less than 10,000 and not included in this table, no even icosahedral Galois representation of conductor p can exist. We found a total of six primes p for which there exists an even icosahedral Galois representation of conductor p. For each of these primes we list a defining polynomial for the quintic field K. We note that of these extensions, at least two were previously known [1, Section 5.1.3]; however, the extension with minimal conductor seems not to have been known. From the table, we see that the minimal prime conductor of an even icosahedral Galois representation is 1951.

This sequence of searches took approximately 5 processor-weeks to complete on a dual processor Xeon 1.7 GHz machine. Without the improvement of

Conductor	Defining Polynomial for $E/\mathbb{Q}$
1951	$x^5 - x^4 - 780x^3 - 1795x^2 + 3106x + 344$
2141	$x^5 - x^4 - 856x^3 + 4025x^2 + 28501x - 40877$
3701	$x^5 - x^4 - 1480x^3 - 18209x^2 + 2191x + 9683$
3821	$x^5 - x^4 - 1528x^3 - 1987x^2 + 16629x - 12281$
8501	$x^5 - x^4 - 3400x^3 - 41825x^2 + 671511x - 966731$
9461	$x^5 - x^4 - 3784x^3 + 2649x^2 + 2960082x - 2781864$

Table 1
Defining polynomials for all even icosahedral Galois representations of prime conductor less than $10,000$.

targeting, the computational time required would have made such a calculation unrealistic even if we had used a much faster machine.

We also conducted a sequence of searches for representations of type 3b and 3c, using the targeting techniques described above. We found that the smallest prime p for which there is a representation of type 3b is $p = 10{,}267$ with a defining polynomial for $E/\mathbb{Q}$ equal to $x^5 - 25x^3 - 7x^2 + 116x - 45$, and the smallest prime p for which there is a representation of type 3c is $p = 13{,}613$ with a defining polynomial for $E/\mathbb{Q}$ equal to $x^5 - 23x^3 + 55x^2 - 33x - 1$. Each of these sequences of searches took about two to three hours. This time is dramatically shorter than the searches for type 3a representations, primarily because of the smaller size of the discriminants of the fields involved.

As a check that the program indeed searches all polynomials in the search space, we note that for every prime p congruent to 1 modulo 5 there is a $\mathbb{Z}/5\mathbb{Z}$-extension of $\mathbb{Q}$ ramified only at p and having discriminant p^4, namely the degree 5 subfield of the pth cyclotomic field. By Hunter's theorem, our search space should contain a polynomial defining this field. In fact for every such prime p within our search range, we did find a defining polynomial for this field.

A second check is that for every prime congruent to 1 modulo 4 such that the class number of $\mathbb{Q}(\sqrt{p})$ is divisible by 5 there is a dihedral extension of degree 10 ramified only at p. Since this dihedral extension will be defined by a quintic polynomial satisfying the same ramification and discriminant conditions as the quintic polynomial for a type 3c representation, it should also be found by our program. In fact, for every such prime within our search range we did find a defining polynomial for this dihedral extension.

References

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

[2] Jacques Basmaji and Ian Kiming, *A table of A_5-fields*, On Artin's conjecture for odd 2-dimensional representations, Lecture Notes in Math., vol. 1585, Springer, Berlin, 1994, pp. 37–46, 122–141.

[3] Joe Buhler, *Icosahedral Galois representations*, Lecture Notes In Mathematics, vol. 654, Springer-Verlag, Berlin, 1978.

[4] J. W. S. Cassels, *Global fields*, Algebraic Number Theory (J.W.S. Cassels and A. Fröhlich, eds.), Academic Press, 1967, pp. 42–84.

[5] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, New York-Berlin, 1993.

[6] ______, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York-Berlin, 1999.

[7] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, third ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999.

[8] Number field tables available by ftp at `megrez.math.u-bordeaux.fr`.

[9] John W. Jones and David P. Roberts, *Timing analysis of targeted Hunter searches*, Algorithmic number theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 412–423.

[10] John W. Jones and David P. Roberts, *Septic fields with discriminant* $\pm 2^a 3^b$, Math. Comp. **72** (2003), no. 244, 1975–1985.

[11] Michael Pohst, *On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields*, J. Number Theory **14** (1982), 99–117.

[12] J.-P. Serre, *Modular forms of weight one and Galois representations*, Algebraic number fields: L-functions and Galois properties (A. Fröhlich, ed.), Academic Press, London, 1977, pp. 193–268.

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

[14] M.-F. Vignéras, *Représentations galoisiennes paires*, Glasgow Math. J. **27** (1985), 223–237.