2004-07-02

PSL(2,7)-Extensions with Certain Ramification at Two Primes

Glen E. Simpson
Brigham Young University - Provo

$\mathrm{PSL}_2(\mathbb{F}_7)$-extensions with certain ramification at two primes

by

Glen Simpson

A project submitted to the faculty of

Brigham Young University

in partial fulfillment of the requirements for the degree of

Master of Science

Advisor: Darrin Doud

Department of Mathematics

Brigham Young University

August 2004

$\mathrm{PSL}_2(\mathbb{F}_7)$-EXTENSIONS WITH CERTAIN RAMIFICATION AT TWO PRIMES

GLEN SIMPSON

Abstract. We conduct a parallel Hunter search in order to find a degree seven number field, K, ramified at primes q and p with discriminant $d(K) = q^6p^2$ where $q = 11$ and $3 \leq p \leq 103$. The number field we seek will satisfy certain criteria allowing for refinement of a conjecture of Ash, Doud, and Pollack. In the course of our search, we prove that the smallest p for which such an example occurs is $p = 31$ and that the next possible example occurs at $p = 103$.

1. Introduction

In [1] Ash, Doud, and Pollack present a conjecture relating certain Galois representations to arithmetic cohomology. In this paper, we will conduct a series of targeted Hunter searches in order to find examples of Galois representations fitting the conditions of their conjecture. These examples may allow the conjecture to be refined.

The specific examples that we seek will be three-dimensional Galois representations with image isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$. In order to be interesting, we want the representations to have *niveau* three [7], which for our purposes means that they should be mod q representations, with $q = 11$ and the ramification index at q equal to 7. In addition, in order that the representation have small level, we will require that it be ramified at only one additional prime p, with ramification index 2. Computational limitations restrict verification of the conjecture to representations with p small. One example with $p = 31$ is known [1], and a second example with $p = 103$ was discovered during the course of this search. This second example may be used for verification of the conjecture, but is too large to help refine the conjecture using current computational techniques.

The Galois representations we seek will be defined by degree seven polynomials. Using Hunter's Theorem, we are able to bound the coefficients of a candidate polynomial. In so doing, we refine the search to a finite (albeit large) search space. In addition, we know that any candidate polynomial must satisfy certain congruences modulo the primes q and p. These facts together with basic search methods and bounds found in [3] make the search feasible in a relatively short time period.

2. Hunter's Theorem and its Implications

2.1. **Needed Theorems, Formulas, and Functions.** Hunter's Theorem [3, Thm. 9.3.1] will force bounds upon the coefficients based on the degree, $n = 7$, of K over $\mathbb{Q}$ and the discriminant $d(K) = q^6p^2$. We will also use Newton's formulas and the elementary symmetric functions in determining the bounds.

Date: July 2, 2004.
2000 *Mathematics Subject Classification.* 11R21.

2.1.1. *Hunter's Theorem.* In Hunter's Theorem, we will use Hermite's constant, denoted by γ_n where n is the dimension. Some of its first values are known to be $\gamma_1 = 1,\ \gamma_2^2 = 4/3,\ \gamma_3^3 = 2,\ \gamma_4^4 = 4,\ \gamma_5^5 = 8,\ \gamma_6^6 = 64/3,\ \gamma_7^7 = 64,\ \gamma_8^8 = 256.$

Theorem 1. [3, p. 445] *Let K be a number field of degree n over $\mathbb{Q}$ and discriminant $d(K)$. There exists $\alpha \in \mathfrak{O}_K \setminus \mathbb{Z}$ that satisfies the following additional properties.*
(1) *If α_j denotes the conjugates of α in $\mathbb{C}$, then*

$$\sum_{1\le j\le n} |\alpha_j|^2 \le \frac{(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha))^2}{n} + \gamma_{n-1}\left(\frac{|d(K)|}{n}\right)^{1/(n-1)},$$

where γ_{n-1} is Hermite's constant in dimension $n-1$.
(2) $0 \le \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \le n/2$.

Define $f(x) = x^7 - a_1x^6 + a_2x^5 - a_3x^4 + a_4x^3 - a_5x^2 + a_6x - a_7$ to be the minimal polynomial of α where α is an element given by Hunter's Theorem. Let t_2 to be the bound given by Hunter's Theorem so in our case

$$t_2 = \frac{a_1^2}{7} + \gamma_6\left(\frac{d(K)}{7}\right)^{1/6}.$$

2.1.2. *Symmetric Functions.* We will make use of the symmetric functions,

$$s_k = \sum_{1\le j\le n} (\alpha_j)^k \qquad (\text{for } k > 0)$$

in our deduction of the bounds.

In addition we will find it useful to define a related function

$$T_k = \sum_{1\le j\le n} |\alpha_j|^k \qquad (\text{for } k > 0).$$

With this notation, Hunter's Theorem asserts that $T_2 \le t_2$ which we will use later.

2.1.3. *Newton's Formulas.* The formulas

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

will be useful in relating the symmetric functions to the coefficients a_k.

2.2. **Deduction of Bounds.** First note that in Hunter's Theorem the α guaranteed to exist is an algebraic integer. Hence its minimal polynomial will have integer coefficients: $f(x) \in \mathbb{Z}[x]$. As another immediate result, the second property given in Hunter's Theorem implies that $0 \le a_1 \le 3.5$. Hence $a_1 \in \{0, 1, 2, 3\}$. From this we may deduce the bounds on the other coefficients as follows. Following [3, p. 451], we first note that in order to use Newton's formulas we must have bounds for the s_k found therein. By definition, $s_1 = a_1$ which implies $0 \le s_1 \le 3$. In addition,

$$|s_2| = |\sum_j \alpha_j^2| \le \sum_j |\alpha_j|^2 = T_2 \le t_2$$

so $-t_2 \le s_2 \le t_2$. As an implication of Lemma 9.3.6 [3, p. 452] we have the following result for the remaining symmetric functions:

$$|s_k| \le T_k \le T_2^{k/2} \le t_2^{k/2}.$$

Lower Bound	Coefficient	Upper Bound
0	a_1	3.5
$\frac{a_1^2 - t_2}{2}$	a_2	$\frac{a_1^2 + t_2}{2}$
$\frac{\sum_{j=1}^{2}(-1)^{j-1}a_{3-j}s_j - t_2^{3/2}}{3}$	a_3	$\frac{\sum_{j=1}^{2}(-1)^{j-1}a_{3-j}s_j + t_2^{3/2}}{3}$
$\frac{\sum_{j=1}^{3}(-1)^{j-1}a_{4-j}s_j - t_2^{2}}{4}$	a_4	$\frac{\sum_{j=1}^{3}(-1)^{j-1}a_{4-j}s_j + t_2^{2}}{4}$
$\frac{\sum_{j=1}^{4}(-1)^{j-1}a_{5-j}s_j - t_2^{5/2}}{5}$	a_5	$\frac{\sum_{j=1}^{4}(-1)^{j-1}a_{5-j}s_j + t_2^{5/2}}{5}$
$\frac{\sum_{j=1}^{5}(-1)^{j-1}a_{6-j}s_j - t_2^{3}}{6}$	a_6	$\frac{\sum_{j=1}^{5}(-1)^{j-1}a_{6-j}s_j + t_2^{3}}{6}$
$\frac{\sum_{j=1}^{6}(-1)^{j-1}a_{7-j}s_j - t_2^{7/2}}{7}$	a_7	$\frac{\sum_{j=1}^{6}(-1)^{j-1}a_{7-j}s_j + t_2^{7/2}}{7}$

TABLE 1. Hunter bounds on the a_k

Now consider a_2. By Newton's formulas, $2a_2 = \sum_{j=1}^{2}(-1)^{j-1}a_{2-j}s_j = a_1s_1 - a_0s_2 = a_1^2 - s_2$ which implies $s_2 = a_1^2 - 2a_2$. Combining this with the bound $|s_2| \leq t_2$ we obtain the bounds $-t_2 \leq a_1^2 - 2a_2 \leq t_2$ or equivalently

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

Hence as we cycle through each possible value of a_1, we find an associated range of values for a_2.

In choosing one of these admissible values for a_2, we see that s_2 may be calculated (in terms of a_1 and a_2) using the equality derived above from Newton's formulas: $s_2 = a_1^2 - 2a_2$. Hence s_2 will become a constant and it will appear in further bounds as such.

In the case of a_3, Newton's formulas imply that $3a_3 = a_2s_1 - a_1s_2 + a_0s_3$. Solving for s_3 and using the bound $|s_3| \leq t_2^{3/2}$ from above, we have $-t_2^{3/2} \leq 3a_3 - a_2s_1 + a_1s_2 \leq t_2^{3/2}$ or equivalently

$$\frac{a_2s_1 - a_1s_2 - t_2^{3/2}}{3} \leq a_3 \leq \frac{a_2s_1 - a_1s_2 + t_2^{3/2}}{3}.$$

Again, we may now calculate s_3 after making a choice for a_3. Using reasoning similar to that in the a_2 and a_3 cases, we compute the bounds for the remaining coefficients a_4, a_5, a_6, and a_7. We record them in Table 1 for future use.

Although each symmetric function may be calculated in terms of previously considered coefficients (as seen above following the a_2 case) we include the symmetric functions in the expressions of the bounds for better readability. It is worth noting that every bound given in the table may be expressed solely in terms of a power of t_2 and the preceding coefficients.

We now have basic bounds for the coefficients of a candidate polynomial, thus allowing for a finite search space.

2.3. **Search Time.** If we were to begin a search based on these bounds alone, it would take quite some time to test all of the possible polynomials against the criteria of the conjecture. Consider that the interval bounding the coefficient a_k ($2 \leq k \leq 7$) is centered at $\frac{1}{k}\sum_{j=1}^{k-1}(-1)^{j-1}a_{k-j}s_j$ and has radius $\frac{1}{k}t_2^{k/2}$. Hence with these bounds, we see that it would take more than 95,000 years to search just the $q = 11$ with $p = 3$ case. (In all

Possible Lower Bound	Possible Upper Bound
$\frac{1}{7}\left(\sum_{j=1}^{6}(-1)^{j-1}a_{7-j}s_j - t_2^{7/2}\right)$	$\frac{1}{7}\left(\sum_{j=1}^{6}(-1)^{j-1}a_{7-j}s_j + t_2^{7/2}\right)$
$-\frac{1}{7^{7/2}}(t_2)^{7/2}$	$\frac{1}{7^{7/2}}(t_2)^{7/2}$

TABLE 2. Dual bounds on a_7

cases, we use the generous assumption that a computer may search 20,000 polynomials per second.) If we wished to search the case $q = 11$ with $p = 31$ where an example is known to exist, we would need over 2.7 billion years. Overall, the search we are considering ($q = 11$ with $3 \leq p \leq 103$) would take approximately 2.18 trillion years. It is obvious that we must find better bounds or other ways of decreasing the number of polynomials necessary to check, for technology will probably not grow fast enough to allow us to ever check all of the polynomials.

3. Improvements in the Bounds

3.1. **Implications of Symmetry.** In the case where $a_1 = 0$, it is evident that certain polynomials will have roots differing by a factor of -1 and hence will generate identical number fields. For example, if α is a root of $f(x) = x^7 + a_2x^5 - a_3x^4 + a_4x^3 - a_5x^2 + a_6x - a_7$, then $-\alpha$ is a root of $g(x) = x^7 + a_2x^5 + a_3x^4 + a_4x^3 + a_5x^2 + a_6x + a_7$. As is easily seen, the second polynomial would not need to be considered. This leads us to eliminate any negative values for a_3 when $a_1 = 0$. Namely, a_3 has 0 as a lower bound. This is in the same spirit as forcing our lower bound for the coefficient a_1 to be 0 (i.e. to take on only nonnegative values). In addition, we may make the same conclusion for the lower bound for a_5 when $a_1 = a_3 = 0$. Although we could in a similar manner correctly deduce that $0 \leq a_7$ when $a_1 = a_3 = a_5 = 0$, it would actually reduce the efficiency of our program as the check that $a_5 = 0$ would have to be performed multiple times and would only rarely save processing time.

3.2. **A Special Case.** In another vein, a vital improvement on the bounds for the constant term a_7 surfaced towards the end of the program development. From [3, p. 447] we have $|a_n| \leq (\frac{t_2}{n})^{n/2}$. Since in our case $n = 7$, we have $-(\frac{t_2}{7})^{7/2} \leq a_7 \leq (\frac{t_2}{7})^{7/2}$. We find that this upper bound is usually better than that which we had derived before. This is apparent since we are now dividing the upper bound by $7^{7/2}$ instead of 7, creating an upper bound approximately 50 times smaller then that which we had before. Similarly, in many cases the lower bound thus obtained is better then that obtained via Hunter's Theorem and Newton's formulas. Hence it is worthwhile in our program to use the better of the two bounds derived. This gives the set of bounds found in Table 2.

As the second bounds depend only on t_2 which is in turn dependent upon only one coefficient, a_1, we may calculate this bound at an early stage (when a_1 alone is chosen). This requires little processing time, thus increasing the value of these second bounds.

3.3. **Effects of These Bounds.** We have improved the bounds moderately, allowing for an increase in speed on the order of about 100. Since we are still left with a total computing time of over 20 billion years, we note that other methods must be found allowing for a sufficient decrease in processing time so as to make the search feasible!

3.4. **A Minor Note.** In a similar targeted Hunter search in [4], the number fields sought were totally real. This allowed much better bounds which reduced the required processing time significantly. Although we do not have this luxury, we find other conclusions which will make this search feasible.

4. Applicable Congruence Relations Aiding the Search

4.1. **Congruence Modulo $q = 11$.** Using an idea in [5], we state a recent result of Doud and Moore and prove a specific case for our search.

4.1.1. *Theorems.*

Theorem 2. [4] *Let L/K be a finite extension of number fields such that $L = K(\alpha)$, with α a root of a monic irreducible polynomial $f(x) \in \mathfrak{O}_K[x]$. 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 $f \equiv \prod g_i^{e_i} \pmod{\mathfrak{p}}$ with $g_i \in \mathfrak{O}_K[x]$ and $\deg(g_i) = f_i$.*

We refer the reader to [4] for a proof of this more general result. We prove a specific case applicable to our search. This result is similar to [6, Thm. 5.1].

Theorem 3. *Let K be a degree seven number field totally ramified at a prime $q > 7$. Suppose that $K = \mathbb{Q}(\alpha)$ and $m_\alpha(x)$ is the minimal polynomial of $\alpha \in \mathfrak{O}_K$. Then $m_\alpha(x) \equiv (x + a)^7 \mod q$ where $a \in \{0, 1, ..., q - 1\}$.*

Proof. Let K be a degree seven number field totally ramified at q such that $K = \mathbb{Q}(\alpha)$. Let L be the Galois closure of K. Let

$$m_\alpha(x) = x^7 - a_1x^6 + a_2x^5 - a_3x^4 + a_4x^3 - a_5x^2 + a_6x - a_7$$

be the minimal polynomial of $\alpha \in \mathfrak{O}_K$ and let α_j for $j \in \{1, ..., 7\}$ be the conjugate roots of α. Let $\mathfrak{q}$ be the prime ideal in K above q and let $\mathfrak{q}_i$ for $i \in \{1, ..., l\}$ be the prime ideals in L above $\mathfrak{q}$.

First suppose that $\alpha \in \mathfrak{q}$. Then $\alpha \in \mathfrak{q}_i$ for all i. Let $\varphi \in \mathrm{Aut}(L)$. Then for every i we know that $\varphi(\mathfrak{q}_i) = \mathfrak{q}_j$ for some j. Hence $\varphi(\alpha) = \alpha_j$ for some j. Since φ permutes the roots of $m_\alpha(x)$, then for every i the ideal $\mathfrak{q}_i$ above $\mathfrak{q}$ will contain all the conjugates of α. This implies that

$$a_1 = \mathrm{Tr}(\alpha) = \sum_{j=1}^{7} \alpha_j \in \mathfrak{q}_i.$$

Since $\alpha \in \mathfrak{O}_K$ then $a_1 \in \mathbb{Z}$ also. Since $\mathbb{Z} \cap \mathfrak{q}_i = (q)$, then $a_1 \in (q)$. Similarly, every other coefficient a_k is in $\mathbb{Z}$ and since

$$a_k = \sum_{i_1 < i_2 < \ldots < i_k} \alpha_{i_1}\alpha_{i_2} \cdots \alpha_{i_k},$$

then each $a_k \in (q)$ by the same argument as above. Therefore, $m_\alpha(x) \equiv x^7 \pmod{q}$.

Suppose on the other hand that $\alpha \notin \mathfrak{q}$. Since our number field is totally ramified at q, then $\mathfrak{O}_K/\mathfrak{q} = \mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$. Hence there exists an element $a \in \mathbb{Z}$ such that $\beta = \alpha + a \in \mathfrak{q}$. Let

$$m_\beta(x) = x^7 - b_1x^6 + b_2x^5 - b_3x^4 + b_4x^3 - b_5x^2 + b_6x - b_7 \in K[x]$$

be the minimal polynomial of β so that $m_\beta(\alpha + a) = m_\beta(\beta) = 0$. Since $\beta \in \mathfrak{q}$, we have shown before that for every i, $b_i \equiv 0 \pmod{q}$. To find the minimal polynomial of α, let $h(x) = m_\beta(x + a)$. It is clear that α is a root of $h(x)$. Furthermore $h(x)$ is degree 7,

hence $h(x)$ is the minimal polynomial of α: $h(x) = m_\alpha(x)$. Since each $b_i \equiv 0 \pmod{q}$, we have $m_\alpha(x) \equiv (x+a)^7 \mod q$. This proves the result.

□

4.1.2. *Deductions.* As a result of Theorem 3, we know that the following congruence relation must hold for a candidate polynomial in our particular circumstances:

$$f(x) \equiv (x+a)^7 \mod 11.$$

Expanding the expression via the Binomial Theorem and equating coefficients, we have a system of seven congruences modulo 11 in one unknown, a:

$$\begin{aligned} -a_1 &\equiv 7a \\ a_2 &\equiv 21a^2 \\ -a_3 &\equiv 35a^3 \\ a_4 &\equiv 35a^4 \\ -a_5 &\equiv 21a^5 \\ a_6 &\equiv 7a^6 \\ -a_7 &\equiv a^7 \end{aligned}$$

Once we assign a_1 a value (recall that $0 \leq a_1 \leq 3$ where $a_1 \in \mathbb{Z}$) we know that $a \equiv \frac{-a_1}{7} \pmod{11}$. Hence the other coefficients may be determined modulo 11 at the outset, restricting the search space on the order of 11 at each successive stage of coefficient choice.

This leads to an overall savings in processing time on the order of about 11^6, reducing our projected time to about 21,000 years.

4.2. **Congruence Modulo p.** As another improvement in our search, we note that polynomials of the form we are searching must factor in a certain way modulo the prime p in order to generate the number field we are seeking. This factorization is derived from Theorem 2 above (i.e. the factorization of the prime p in K). In our search, we will have

$$f(x) \equiv \left(x^3 + bx^2 + cx + d\right)\left(x^2 + ex + f\right)^2 \pmod{p}.$$

Note that this is satisfied by the known example $h(x) = x^7 - 11x^5 - 22x^4 + 33x^2 + 33x + 11$ described in [1]. PARI/GP [8] reports that in the prime ideal decomposition of 31 in the number field generated by this polynomial, $h(x)$ factors as a product of a linear function, a quadratic function, and a quadratic function squared.

When we simplify the general relation and equate coefficients, we obtain a system of seven congruences modulo p in five unknowns:

$$\begin{aligned} -a_1 &\equiv 2e + b \\ a_2 &\equiv c + e^2 + 2f + 2be \\ -a_3 &\equiv 2ce + 2fe + d + 2bf + be^2 \\ a_4 &\equiv 2cf + ce^2 + f^2 + 2de + 2bef \\ -a_5 &\equiv 2cfe + de^2 + 2df + bf^2 \\ a_6 &\equiv cf^2 + 2def \\ -a_7 &\equiv df^2 \end{aligned}$$

We solve for b in the first congruence and substitute it into the others. We successively solve for and substitute c and d, obtaining the following system:

$$\begin{aligned}
b &\equiv -(a_1 + 2e) \\
c &\equiv -(-a_2 + e^2 + 2f + 2(-a_1 - 2e)e) \\
d &\equiv -(a_3 + 2ea_2 + 4e^3 - 6fe + 3e^2a_1 - 2fa_1) \\
0 &\equiv -a_4 + 2fa_2 - 3f^2 + 6fea_1 - 3e^2a_2 - 5e^4 - 4e^3a_1 - 2ea_3 + 12fe^2 \\
0 &\equiv a_5 - 2fea_2 + 4fe^3 + 6f^2e - e^2a_3 - 2e^3a_2 - 4e^5 - 3e^4a_1 - 2fa_3 + 3f^2a_1 \\
a_6 &\equiv cf^2 + 2def \\
a_7 &\equiv -df^2
\end{aligned}$$

Finding simultaneous solutions for the fourth and fifth congruences, we may then calculate the final two coefficients modulo p. This may be done as soon as the first 5 coefficients are determined, providing a savings in processing time discussed momentarily.

4.3. **Chinese Remainder Theorem.** Since we have found that any possibilities for a_6 and a_7 must simultaneously satisfy congruences modulo q and modulo p, we apply the Chinese Remainder Theorem, finding the value these coefficients must take on modulo qp. Hence, at the point in the program where the first five coefficients for a candidate polynomial have been chosen, we may determine a_6 and a_7 modulo qp.

This speeds up the processing time by a factor of p^2, a more significant factor as p increases. On average, the total processing time is increased on an order of 3000 per prime p, leading us to conclude that the search will take around 7 years. Although the search may be lengthy, we know that it is now possible in a relatively short time using current technology.

5. The Program

In Appendix A, we record the final version of the program with the improved bounds and congruence relations implemented. The program was written and run using the PARI/GP package [8]. Executed on BYU's Maryloux supercomputer [2] with 2.4GHz Pentium Xeon processors via parallel programming methods, the program required less than two weeks (a total combined processing time of one year). Hence the better bounds and congruences we applied improved the search far more than expected.

6. Conclusions

In the course of our Hunter search, we have proved that for primes $q = 11$ and $3 \leq p \leq 103$ the smallest prime p at which a degree seven extension fitting the criteria of the conjecture exists is $p = 31$. We also discovered that the next p for which such an example occurs is $p = 103$. The known example has been shown to support a refinement of the conjecture. The example we found has been checked and yields the related cohomology suggested in the original conjecture. However it is too large to verify the refined conjecture at this time. It is merely awaiting technology improvements so that it may be calculated and the connections verified as corroboration to a refinement of the conjecture.

Number fields satisfying the given conditions tend to come in nonisomorphic pairs since any $\mathrm{PSL}_2(\mathbb{F}_7)$-extension has two non conjugate subgroups isomorphic to S_4. In both cases ($p = 31$ and $p = 103$) polynomials defining these number fields were found as expected.

For $q = 11$ with $p = 31$ the following polynomials generate nonisomorphic number fields with Galois group $\mathrm{P}SL_2(\mathbb{F}_7)$.
$f_1(x) = x^7 + 11x^5 - 176x^3 - 1045x^2 + 3355x - 583$
$f_2(x) = x^7 - 11x^5 - 33x^4 - 55x^3 - 66x^2 - 44x - 11$
The second polynomial generates a number field isomorphic to that generated by the known example $h(x) = x^7 - 11 * x^5 - 22 * x^4 + 33 * x^2 + 33 * x + 11$.

For $q = 11$ with $p = 103$, we found the following polynomials generating nonisomorphic fields as expected.
$f_3(x) = x^7 - 11x^5 - 55x^3 - 264x^2 - 44x + 176$
$f_4(x) = x^7 - 11x^5 - 22x^4 - 132x^3 + 363x^2 + 330x + 1199$
In both cases, many other polynomials were found generating isomorphic number fields to those of the given polynomials.

For future research, we could easily extend this search to number fields ramified similarly at $q = 23$ and $3 \leq p \leq 17$, and number fields ramified at $q = 37$ and $3 \leq p \leq 5$. In so doing, we may find other calculable examples having the appropriate Galois group, ramification, and discriminant.

7. Acknowledgements

I am grateful to Darrin Doud for serving as my mentor in this research. I thank the Brigham Young University Mathematics Department for its support also. As always I am grateful for the constant support and insights of my wife.

Appendix A

```
Official Program Run

{testprimep()=
  for(a1=0,3,
    write(output,"a1=",a1);
    t2=a1^2/n+gamma6*(dK/n)^(1/(n-1));
    t2tothethreehalves=t2^(3/2);
    t2squared=t2^2;
    t2tothefivehalves=t2^(5/2);
    t2cubed=t2^3;
    t2tothesevenhalves=t2^(7/2);
    maxa7=floor(t2tothesevenhalves/(7^(7/2))+epsilon);
    possiblemina7=ceil(-t2tothesevenhalves/(7^(7/2))-epsilon);
    a=lift(Mod(a1,q)/(-7));
    a2congruentmodqto=(21*a^2)%q;
    a3congruentmodqto=(-35*a^3)%q;
    a4congruentmodqto=(35*a^4)%q;
    a5congruentmodqto=(-21*a^5)%q;
    a6congruentmodqto=(7*a^6)%q;
    a7congruentmodqto=(-a^7)%q;
    s1=a1;
    mina2=ceil((a1^2-t2)/2-epsilon);
```

```
    maxa2=floor((a1^2+t2)/2+epsilon);
    minb2=floor(mina2/q-epsilon);
    maxb2=ceil(maxa2/q+epsilon);
    while((minb2*q+a2congruentmodqto)<mina2,minb2=minb2+1);
    while((maxb2*q+a2congruentmodqto)>maxa2,maxb2=maxb2-1);
    for(b2=minb2,maxb2,
      a2=b2*q+a2congruentmodqto;
      write(output,"  a2=",a2,[mina2,maxa2]);
      s2=a1*s1-2*a2;
      middle3=a2*s1-a1*s2;
      mina3=ceil((middle3-t2tothethreehalves)/3-epsilon);
      if(a1==0,mina3=0);
      maxa3=floor((middle3+t2tothethreehalves)/3+epsilon);
      minb3=floor(mina3/q-epsilon);
      maxb3=ceil(maxa3/q+epsilon);
      while((minb3*q+a3congruentmodqto)<mina3,minb3=minb3+1);
      while((maxb3*q+a3congruentmodqto)>maxa3,maxb3=maxb3-1);
      for(b3=minb3,maxb3,
        a3=b3*q+a3congruentmodqto;
        write(output,"    a3=",a3,[mina3,maxa3]);
        s3=-a2*s1+a1*s2+3*a3;
        middle4=a1*a3-a2*s2+a1*s3;
        mina4=ceil((middle4-t2squared)/4-epsilon);
        maxa4=floor((middle4+t2squared)/4);
        minb4=floor(mina4/q-epsilon);
        maxb4=ceil(maxa4/q+epsilon);
        while((minb4*q+a4congruentmodqto)<mina4,minb4=minb4+1);
        while((maxb4*q+a4congruentmodqto)>maxa4,maxb4=maxb4-1);
        for(b4=minb4,maxb4,
          a4=b4*q+a4congruentmodqto;
          s4=a3*s1-a2*s2+a1*s3-4*a4;
          middle5=a4*s1-a3*s2+a2*s3-a1*s4;
          mina5=ceil((middle5-t2tothefivehalves)/5-epsilon);
          if(a1==0,if(a3==0,mina5=0));
          maxa5=floor((middle5+t2tothefivehalves)/5);
          minb5=floor(mina5/q-epsilon);
          maxb5=ceil(maxa5/q+epsilon);
          while((minb5*q+a5congruentmodqto)<mina5,minb5=minb5+1);
          while((maxb5*q+a5congruentmodqto)>maxa5,maxb5=maxb5-1);
          efpossibilities=vector(p,e,polrootsmod(-a4+2*x*a2-3*x^2+
6*x*e*a1-3*e^2*a2-5*e^4-4*e^3*a1-2*e*a3+12*x*e^2,p));
          for(b5=minb5,maxb5,
            a5=b5*q+a5congruentmodqto;
            for(e=1,p,
              for(k=1,length(efpossibilities[e]),
                f=lift(efpossibilities[e][k]);
                if((a5-2*f*e*a2+4*f*e^3+6*f^2*e-e^2*a3-2*e^3*a2-
4*e^5-3*e^4*a1-2*f*a3+3*f^2*a1)%p==0,
                  c=(a2+3*e^2-2*f+2*e*a1)%p;
```

```
                  d=(-a3-2*e*a2-4*e^3+6*f*e-3*e^2*a1+2*f*a1)%p;
                  a6congruentmodqpto=
lift(chinese(Mod(a6congruentmodqto,q),Mod(c*f^2+2*d*e*f,p)));
                  a7congruentmodqpto=
lift(chinese(Mod(a7congruentmodqto,q),Mod(-d*f^2,p)));
                  s5=-a4*s1+a3*s2-a2*s3+a1*s4+5*a5;
                  middle6=a5*a1-a4*s2+a3*s3-a2*s4+a1*s5;
                  mina6=ceil((middle6-t2cubed)/6-epsilon);
                  maxa6=floor((middle6+t2cubed)/6);
                  minb6=floor(mina6/ptimesq-epsilon);
                  maxb6=ceil(maxa6/ptimesq+epsilon);
                  for(b6=minb6,maxb6,
                    a6=b6*ptimesq+a6congruentmodqpto;
                    s6=a5*s1-a4*s2+a3*s3-a2*s4+a1*s5-6*a6;
                    middle7=a6*a1-a5*s2+a4*s3-a3*s4+a2*s5-a1*s6;
                    mina7=ceil((middle7-t2tothesevenhalves)/7-
epsilon);
                    if(a1==0,if(a3==0,if(a5==0,mina7=1)));
                    if(possiblemina7>mina7,mina7=possiblemina7);
                    minb7=floor(mina7/ptimesq-epsilon);
                    maxb7=ceil(maxa7/ptimesq+epsilon);
                    for(b7=minb7,maxb7,
                      a7=b7*ptimesq+a7congruentmodqpto;
                      if(a7==0,,
                        f=x^7-a1*x^6+a2*x^5-a3*x^4+a4*x^3-a5*x^2+
a6*x-a7;
                        if(issquare(poldisc(f)),
                          write(output,"found a square", factor(f));
                          if(polisirreducible(f),
                            if(polsturm(f)==3,
                              numberfielddiscriminant=
factor(nfdisc(f));
                              write(output,polgalois(f),
numberfielddiscriminant,f);
                              write(polys,polgalois(f),
numberfielddiscriminant,f); ) ) ) ) ) ) ) ) ) ) ) ) ) ) }
{q=11;n=7;gamma6=(64/3)^(1/6);epsilon=.00001;
  forprime(p=5,84,
    if(p!=q,
      dK=q^6*p^2;
      ptimesq=q*p;
      write(output,"Testing Prime p=",p);
      write(output,"Testing Prime q=",q);
      write(polys,"Testing Prime p=",p);
      write(polys,"Testing Prime q=",q);
      testprimep()
) ) }
```

References

1. Avner Ash, Darrin Doud, and David Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. **112** (2002), no. 3, 521–579.
2. Brigham Young University Supercomputing, Provo, UT 84601, *maryloux.et.byu.edu*, 2004, see `http://marylou.byu.edu/mx/maryloux.htm/`.
3. Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York-Berlin, 1999.
4. Darrin Doud and Michael W. Moore, *Even icosahedral Galois representations of prime conductor*, (2004), preprint.
5. John Jones and David Roberts, *Tables of number fields with prescribed ramification*, Online, 2001, available at `http://math.la.asu.edu/~jj/numberfields/`.
6. Michael W. Moore, *Even representations of prime conductor*, (2004), Brigham Young University Master's Project.
7. Jean-Pierre Serre, *Sur les représentations modulaires de degré 2 de Gal($\bar{\mathbb{Q}}/\mathbb{Q}$)*, Duke Math. J. **54** (1987), no. 1, 179–230.
8. The PARI Group, Bordeaux, *PARI/GP, Version 2.1.5*, 2002, available from `http://pari.math.u-bordeaux.fr/`.

Brigham Young University, Department of Mathematics, 292 TMCB, Provo, UT 84602
E-mail address: `simpsge@math.byu.edu`