

$PGL_2(\mathbb{F}_\ell)$  NUMBER FIELDS  
WITH RATIONAL COMPANION FORMS

DAVID P. ROBERTS

ABSTRACT. We give a list of  $PGL_2(\mathbb{F}_\ell)$  number fields for  $\ell \geq 11$  which have rational companion forms. Our list has fifty-three fields and seems likely to be complete. Some of the fields on our list are very lightly ramified for their Galois group.

1. INTRODUCTION

One of the great recent advances in number theory is the proof by Khare and Wintenberger [KW09a, KW09b] of the Serre reciprocity conjecture [Ser87]. The Khare-Wintenberger reciprocity theorem says that certain two-dimensional Galois representations in prime characteristic  $\ell$  necessarily come from classical modular forms. Once certain normalizations are in place, a given representation  $\rho$  typically comes from just one form  $g$ . However if  $\rho$  is tamely or minimally wildly ramified at  $\ell$ , then it comes from two forms  $g$  and  $h$ , called companions.

The purpose of this paper is to give a systematic collection of fifty-three examples of this phenomenon of companion forms. Our collection illustrates all three types of companion forms, which we label 1T or *diagonalizable*, 2T or *supersingular*, and 2W or *peu ramifiée*. Important early theoretical developments on companion forms in these senses took place in letters among Deligne, Fontaine, and Serre in the 1970s. The theory for Type 1T was established by Gross in 1990 [Gro90]. Edixhoven gave the first complete proofs for cases 2T and 2W in 1992 [Edi92]. To be noted is that the term “companion form” is often used in the context of 1T only. We are using it more broadly, because the three cases are very similar from the viewpoint of this paper.

In Section 2, we present two of the fifty-three examples in some detail, both of diagonalizable type with  $\ell = 11$ . Each example starts from a degree twelve polynomial  $f(x) \in \mathbb{Q}[x]$  with Galois group  $PGL_2(\mathbb{F}_{11})$  and ends with a pair  $(g, h)$  of companion forms in  $\mathbb{Q}[[q]]$ . Our focus is not on the polynomials themselves, but rather on the degree twelve fields  $K = \mathbb{Q}[x]/f(x)$  they define.

In Section 3, we ask for all fields  $K$  belonging to triples  $(K, g, h)$  of the same general nature, including the very strong requirement that both  $g$  and  $h$  have coefficients in  $\mathbb{Q}$ . We restrict to  $\ell \geq 11$  to keep the final collection of manageable size. Pairwise comparing all known rational forms, we extract those pairs  $(g, h)$  which satisfy the companionship condition. We find in Theorem 3.1 fifty-three fields  $K$  which are part of triples in this way, and we conjecture that there are no more. The distribution of the number fields  $K$  with regard to  $\ell$  and the three

notions of companionship is as follows:

| $\ell$ :            | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 |
|---------------------|----|----|----|----|----|----|----|----|----|----|
| 1T=Diagonalizable:  | 6  | 5  | 2  | 2  | 1  | 2  | 1  |    | 1  |    |
| 2T = Supersingular: | 8  | 7  | 4  | 3  |    | 3  |    | 1  |    | 1  |
| 2W=Peu ramifiée:    | 5  |    | 1  |    |    |    |    |    |    |    |

While the forms themselves can easily be made very explicit, our computations in Section 3 do not produce defining polynomials  $f(x)$  for the fields  $K$ . Note that our requirement of rationality on  $g$  and  $h$  is imposed simply to get attractive examples: whether or not  $K$  belongs to a triple cannot be read off from  $K$ ; it can only be determined by computing the corresponding modular forms.

In Section 4, we study the fifty-three fields further, finding defining polynomials when possible. Some of these number fields  $K$  are very lightly ramified for their Galois group. We explain how incorporating our fields into a systematic tabulation of number fields based on Serre reciprocity seems possible. This systematic tabulation would involve totally dropping our rationality conditions. To a large extent, it would then consist of repeating our computations here in the resulting larger context. In particular, beating our best fields or establishing them as true minima seems within reach by modular methods.

Computations in this paper were done using a mix of *Magma* [BCP97], *Pari* [PAR13], and *Mathematica* [Res16]. Together with the closely related paper [Rob16b], this paper grew from a talk given by the author at *Automorphic Forms: theory and computation* at King’s College London, in September 2016. The author’s research was supported by grant #209472 from the Simons Foundation and grant DMS-1601350 from the National Science Foundation.

## 2. TWO $PGL_2(\mathbb{F}_{11})$ FIELDS WITH RATIONAL COMPANION FORMS

In this section we present two remarkably parallel examples, centering on triples  $(K_1, g_1, h_1)$  and  $(K_2, g_2, h_2)$ . We exhibit very concretely how Galois-theoretic invariants of the  $K_i$  are connected with modular invariants from the  $(g_i, h_i)$ . We keep background theory to an absolute minimum, with some of this theory being presented in the next two sections.

**2.1. Mathieu group sources.** Our two examples have the added interest that the number fields were first found “accidentally” in a context very far removed from elliptic curves and modular forms. Let

$$(2.1) \quad f_1(x) = x^{12} - 4x^{11} - 4x^{10} + 16x^9 + 24x^8 - 30x^7 - 78x^6 - 18x^5 + 72x^4 + 86x^3 + 52x^2 + 16x + 2,$$

$$(2.2) \quad f_2(x) = x^{12} - 6x^{10} - 6x^9 - 6x^8 + 126x^7 + 104x^6 - 468x^5 + 258x^4 + 456x^3 - 1062x^2 + 774x - 380.$$

The fact that both polynomials have Galois group  $PGL_2(\mathbb{F}_{11})$  can be rapidly confirmed by *Magma’s* `GaloisGroup`. Their exotic source in each case is related to one of the five sporadic simple groups  $M_n$  discovered by Mathieu in the mid-1800s. The first comes from the degenerate specialization at  $y = -47^2/2^63$  of Malle’s one-parameter family of  $M_{22}.2$  fields [Mal88, Theorem 2]. The second comes from the degenerate specialization at  $t = -17^3/2^7$  of a one-parameter family of  $M_{12}.2$

fields [Rob16a, Cover D2, Table 4.5]. These two sources actually give polynomials of degree 22 and 24 respectively, and we used *Magma*'s `GaloisSubgroup` to obtain degree twelve polynomials with the same splitting field. Finally we used *Pari*'s `polredabs` to reduce the size of coefficients.

Note that the action of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on the roots of a degree  $\ell + 1$  polynomial with Galois group  $PGL_2(\mathbb{F}_\ell)$  gives a surjective homomorphism  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow PGL_2(\mathbb{F}_\ell)$ . Shortly we will lift these projective representations to linear representations into  $GL_2(\mathbb{F}_\ell)$ . Throughout this paper, we are emphasizing number fields rather than the corresponding Galois representations emphasized in more theoretical papers.

**2.2. Frobenius partitions.** For a degree  $n$  number field  $K = \mathbb{Q}[x]/f(x)$  and a prime  $p$  not dividing its discriminant  $D$ , one has a factorization partition  $\lambda_p$ . The parts of  $\lambda_p$  are the degrees of the irreducible factors of  $f(x)$  in  $\mathbb{Q}_p[x]$ . If  $p$  does not divide the discriminant  $Dc^2$  of the defining polynomial  $f(x) \in \mathbb{Z}[x]$ , then  $\lambda_p$  is more easily computed as the degrees of the irreducible factors of  $f(x)$  in  $\mathbb{F}_p[x]$ .

The polynomial discriminants of  $f_1$  and  $f_2$  are quickly calculated as

$$D_1c_1^2 = -2^{14} \cdot 3^{30} \cdot 11^9, \quad D_2c_2^2 = -2^{12} \cdot 3^{14} \cdot 11^9 \cdot 17^2 \cdot 1907473^2 \cdot 2615189^2.$$

One can not immediately identify the  $D_i$  and  $c_i$  themselves by elementary methods. However from the construction of the stem fields  $K_i = \mathbb{Q}[x]/f_i(x)$  via specialization of understood covers, one knows at least that in each case only the primes 2, 3, and 11 can divide the field discriminant  $D_i$ . Table 2.1 gives in each case the factorization partition  $\lambda_p$  for the twenty-two good primes  $p$  less than a hundred. It also gives the parity  $d_p$  of the partition. Both polynomial discriminants are  $-11$  modulo squares, so the  $d_p$  agree in the two cases. More explicitly,  $p$  occurs on a row with  $d_p = +$  if and only if  $p$  is a square modulo 11, i.e. if and only if  $p \equiv 1, 3, 4, 5, 9 \pmod{11}$ .

|        | $\lambda_p$ | $d_p$ | density | Primes $p$ for $K_1$  | Primes $p$ for $K_2$ | $s_p$ |
|--------|-------------|-------|---------|-----------------------|----------------------|-------|
| inert  | 12          | −     | 1/6     | 13, 29, 79, 83        | 7, 13, 61, 73, 83    | 7, 8  |
| torus  | $4^3$       | −     | 1/12    | 7, 17                 | 29                   | 2     |
|        | $6^2$       | +     | 1/12    | 31, 47, 97            | 23, 59               | 3     |
|        | $3^4$       | +     | 1/12    | 37, 71                | 37, 47               | 1     |
|        | $2^6$       | +     | 1/24    |                       | 71                   | 0     |
| split  | $10^1 1^2$  | −     | 1/5     | 19, 41, 43, 61, 73    | 19, 41, 43, 79       | 6, 10 |
| torus  | $2^5 1^2$   | −     | 1/20    |                       | 17                   | 0     |
|        | $5^2 1^2$   | +     | 1/5     | 5, 23, 53, 59, 67, 89 | 53, 67, 89, 97       | 5, 9  |
| uni-   | $11^1 1$    | +     | 1/11    |                       | 5, 31                | 4     |
| potent | $1^{12}$    | +     | 1/1320  |                       |                      | 4     |

TABLE 2.1. Frobenius partitions  $\lambda_p$  correlating with modular quantities  $s_p = a_p^2/p^{k-1}$  in our two examples. Here  $a_p$  and  $k$  depend on choices, but  $s_p$  does not, as explained in §3.1.

In general, a Frobenius partition  $\lambda_p$  reflects a more refined invariant, a conjugacy class  $\text{Fr}_p$  in the Galois group. For the group  $PGL_2(\mathbb{F}_{11}) \subset S_{12}$ , there are 13 conjugacy classes. They give rise to ten of the seventy-seven partitions of twelve, and these ten partitions are given in Table 2.1. For context, the column “density” gives the asymptotic frequency of each partition. Frobenius classes  $\text{Fr}_p$  and partitions

behave similarly for all  $PGL_2(\mathbb{F}_\ell)$ , and the words in the first column summarize a structure theory that applies for all  $\ell$ ; the split and non-split tori are often referred to as split and non-split Cartan subgroups.

**2.3. Ramification.** The discriminants of the two fields  $K_i$  can be calculated directly, say by *Pari's* `nfdisc`:

$$(2.3) \quad D_1 = -2^{14} \cdot 3^{10} \cdot 11^9, \quad D_2 = -2^{10} \cdot 3^{14} \cdot 11^9.$$

It is important for us to have a clear picture of the inertia groups  $I_p \subset PGL_2(\mathbb{F}_\ell)$  underlying the discriminants. This information is given automatically by the  $p$ -adic identifier at the website of [JR06]. Here, underlying the two exponents 10, ramification is tame of order  $|I_p| = 11$ . Underlying the two instances of  $11^9$ , ramification is tame of order  $|I_{11}| = 10$ . The completions of the two fields at 11 are actually isomorphic, both being  $\mathbb{Q}_{11}[\pi]/(\pi^{10} - 66) \times \mathbb{Q}_{11} \times \mathbb{Q}_{11}$ . This agreement is a little unexpected because  $\mathbb{Q}_{11}[\pi]/(\pi^{10} - 66)$  is one of ten different totally ramified decic 11-adic fields, all with cyclic Galois group  $C_{10}$ .

Since the exponents 14 are greater than or equal to the degree 12, ramification must be wild at 2 in  $K_1$  and at 3 in  $K_2$ . The database describes this ramification in terms of the slope-contents  $[4/3, 4/3]_3^2$  and  $[3/2]_2^2$  respectively, the numbers in square brackets being wild slopes as explained in [JR06]. At 2, the field  $K_1$  has decomposition group  $S_4$ , inertia group  $A_4$ , and wild inertia group  $V$ . Similarly, at 3 the field  $K_2$  has decomposition group the dihedral group  $D_6$ , inertia group  $S_3$ , and wild inertia group  $A_3$ .

It is often enlightening to work not with the discriminant  $D$  of a degree  $n$  field  $K$ , but rather with the root discriminant  $\delta = |D|^{1/n}$ . For example,  $\delta$  relates well to the root discriminant  $\Delta$  of a Galois closure  $L$ : one has  $\delta \leq \Delta$  with equality if and only if  $L/K$  is unramified. For our two cases, the renormalization to root discriminants works out to

$$(2.4) \quad \delta_1 \approx 33.87, \quad \delta_2 \approx 38.77.$$

The Galois root discriminants are best calculated one prime at a time. If  $p$  is tamely ramified with  $|I_p| = t$ , then its multiplicative contribution is  $p^{(t-1)/t}$ . If  $t$  is wildly ramified then the contribution can be directly computed from the slope content as explained in [JR06]. In our cases, one obtains

$$\Delta_1 = 2^{7/6} 3^{10/11} 11^{9/10} \approx 52.75, \quad \Delta_2 = 2^{10/11} 3^{7/6} 11^{9/10} \approx 58.55.$$

The root discriminants  $\delta_1$ ,  $\delta_2$ ,  $\Delta_1$ , and  $\Delta_2$  are all unusually small for the Galois group  $PGL_2(\mathbb{F}_{11})$ , as we discuss further at various points of Section 4.

**2.4. Lifts.** Serre reciprocity is naturally formulated at the linear level of  $GL_2$ , while we in this paper are working as much as possible at the computationally more accessible projective level of  $PGL_2$ . To make the connection to modular forms, we first have to lift from the projective level to the linear level.

Let  $SL_2^\pm(\mathbb{F}_{11})$  be the group of two-by-two matrices over  $\mathbb{F}_{11}$  with determinant  $\pm 1$ . Let  $C_5$  be the group of scalar matrices of odd order. Via the product decomposition  $GL_2(\mathbb{F}_{11}) = SL_2^\pm(\mathbb{F}_{11}) \times C_5$ , one can focus attention on  $SL_2^\pm(\mathbb{F}_{11})$ . This group has computational appeal because, unlike  $GL_2(\mathbb{F}_{11})$ , it is a subgroup of  $S_{24}$ .

For context, note that the polynomials  $f_1(x^2)$  and  $f_2(x^2)$  both have Galois group isomorphic to the full wreath product  $C_2 \wr PGL_2(\mathbb{F}_{11})$  of order  $2^{12} \cdot |PGL_2(\mathbb{F}_{11})|$ . At issue is whether the defining polynomials  $f_i$  can be adjusted so that replacing  $x$

by  $x^2$  yields the group  $SL_2^\pm(\mathbb{F}_{11})$ . For this to happen, a sign  $\epsilon_v \in \{-1, 1\}$  has to be 1 for all the ramified places  $\{\infty, 2, 3, 11\}$ . Remarkably indeed  $\epsilon_v = 1$  always, and so lifted fields  $\tilde{K}_i$  are known to exist.

Finding the better polynomial for the two  $\tilde{K}_i$  requires a computation with  $S$ -units with  $S = \{2, 3, 11\}$ , as discussed in [Coh00, Chpt 5]. In the first case, a polynomial for a lifted field  $\tilde{K}_1$  with Galois group  $SL_2^\pm(\mathbb{F}_{11})$  is

$$\begin{aligned} \tilde{f}_1(x) = & x^{24} - 20x^{22} + 208x^{20} - 1380x^{18} + 6432x^{16} - 21696x^{14} + 52824x^{12} \\ & - 90432x^{10} + 100128x^8 - 65728x^6 + 31808x^4 - 17152x^2 - 14256. \end{aligned}$$

As  $d$  runs over square-free integers, the fields defined by  $\tilde{f}_1(\sqrt{d}x)$  run over all lifts of  $K_1$ . The field  $\tilde{K}_1 = \mathbb{Q}[x]/\tilde{f}_1(x)$  we have chosen has discriminant  $\tilde{D}_1 = -2^{32}3^{20}11^{19}$ . Our choice is one of the two with smallest discriminant, the other one being given by  $f_1(\sqrt{-11}x)$ . A corresponding  $\tilde{f}_2(x) = \tilde{f}_{11}(21, -26, x)$ , giving a lifted field discriminant of  $\tilde{D}_2 = -2^{20}3^{30}11^{19}$ , is a specialization of the parametric family (4.11).

**2.5. Conductors.** To make the connection with modular forms, we need to study the ramification in the lifted fields  $\tilde{K}_i$ , and then translate to conductors. From the discriminants reported above,  $\tilde{K}_1/K_1$  is ramified at 2 and 11 while  $\tilde{K}_2/K_2$  is ramified at 3 and 11. At the wild prime 2 in the first case, an extra wild slope appears so that slope content is now  $[3/2, 4/3, 4/3]_3^2$ . At the wild prime 3 in the second case, the tame part of inertia gets larger, so that slope content becomes  $[3/2]_4^2$ .

The conductors of the Galois representations coming from the inclusion  $SL_2^\pm(\mathbb{F}_{11}) \subset GL_2(\mathbb{F}_{11})$  are again small:

$$(2.5) \quad N_1 = 24 = 2^3 \cdot 3, \quad N_2 = 54 = 2 \cdot 3^3.$$

The source of the exponents 1 is that  $I_p$  in both cases can be taken to be strictly upper-triangular matrices, and so the subspace  $\mathbb{F}_{11}^2$  fixed by  $I_p$  has codimension one. At the primes with exponent 3, the subspace fixed by  $I_p$  is just  $\{0\}$ . However the exponent is 3 rather than the codimension 2 because of wildness; 3 arises in both cases as the codimension 2 of inertial invariants times the highest slope 3/2.

**2.6. Corresponding newforms.** We will use a standard notation for modular forms, in which  $S_k(N)$  denotes the space of cusp forms of weight  $k$  on the group  $\Gamma_0(N)$ . Via expansion at the cusp  $\infty$ , a modular form can be viewed simply as an element of the power series ring  $\mathbb{C}[[q]]$ . Of particular importance for us are the new subspaces  $S_k^{\text{new}}(N)$ , which has a canonical basis  $P_k(N)$  of forms  $q + \dots$  which are eigenforms for both the Atkin-Lehner operators  $w_{p^e}$ , with  $p^e \parallel N$ , and the Hecke operators  $T_n$ , for  $n \nmid N$ . The word newform always refers to an element of a  $P_k(N)$ . Standard references include [Kob93], [Ste07]. Our use of modular forms in this paper is mostly limited to extracting particular newforms from the collection of newforms with rational coefficients drawn up in [Rob16b]. Section 2 of this reference is a brief synopsis of modular forms, adapted to our current needs.

The Serre reciprocity theorem in our cases says that  $K_i$  comes from a newform in  $P_k(N_i)$ , where  $k \in \{2, 4, 6, 8, 10, 12\}$ . Because of the nature of tameness at 11, Gross's theory of companion forms of Type 1T says that it comes from two forms, in weights adding to 12.

In the first case, the sets  $P_k(24)$  respectively have size 1, 1, 3, 3, 5, and 5. Looking through the eighteen forms, only two match out through  $p < 100$ , these being

$$(2.6) \quad \begin{aligned} g_1 &= q + 3q^3 + 14q^5 - 24q^7 + 9q^9 - 28q^{11} + \cdots \in P_4(24), \\ h_1 &= q + 27q^3 - 530q^5 + 120q^7 + 729q^9 - 7196q^{11} + \cdots \in P_8(24). \end{aligned}$$

Here and always for  $PGL_2(\mathbb{F}_{11})$  fields, a field  $K$  and a newform  $\sum a_n q^n \in P_k(N)$  correspond if and only if the partition  $\lambda_p$  and the normalized square  $s_p = a_p^2/p^{k-1} \in \mathbb{F}_{11}$  match for all  $p \nmid 11N$  via the  $\lambda_p$  and  $s_p$  columns of Table 2.1. As an example, whenever  $\lambda_p = 12$ , one must have  $s_p \in \{7, 8\}$ . Similarly, if  $s_p = 4$ , one must have  $\lambda_p \in \{11^1 1, 1^{12}\}$ . As a completely explicit instance of the correspondence being discussed, consider  $K_1$  and  $(g_1, h_1)$  at  $p = 5$ . One has  $\lambda_5 = 5^2 1^2$  because the irreducible factorization of  $f_1(x)$  in  $\mathbb{F}_5[x]$  is

$$(x^5 + 4x + 2)(x^5 + 3x^3 + 3x^2 + 3x + 2)(x + 2)(x + 4).$$

Indeed the normalized squares  $14^2/5^3$  and  $530^2/5^7$  both reduce to 5 in  $\mathbb{F}_{11}$ , in conformity with Table 2.1.

The second case is similar. The sets  $P_k(54)$  have sizes 2, 4, 6, 8, 10, and 12. Looking through these forms, four match  $K_2$  through  $p < 100$ , two of which are

$$(2.7) \quad \begin{aligned} g_2 &= q - q^2 + q^4 + 3q^5 - q^7 + \cdots \in P_2(54), \\ h_2 &= q + 16q^2 + 256q^4 - 435q^5 - 2527q^7 + \cdots \in P_{10}(54). \end{aligned}$$

The other two which match are twists  $g_2^X$  and  $h_2^X$  of the first two, differing only in that coefficients  $a_n$  with  $n \equiv 2(3)$  are negated. This twisting is not seen in the matching criterion.

A subtlety of the general situation is nicely illustrated by looking at weights more closely in our pair of examples. The field  $L = \mathbb{Q}_{11}[x]/(x^{10} - 66)$  is a splitting field for both polynomials  $f_1$  and  $f_2$ . Let  $G_i$  be the Galois group of  $f_i$  with respect to this splitting field, so that both  $G_i$  contain the cyclic group  $C = \text{Gal}(L/\mathbb{Q}_{11})$  of order ten. Note that  $C$  has four automorphisms  $i_j$ , where  $i_j(\sigma) = \sigma^j$ , and  $j$  can be 1, 3, 7 or 9. The normalizer of  $C$  in  $G_i$  is  $D_i$ , a dihedral group of order 20. This means that of the  $|PGL_2(\mathbb{F}_{11})| = 12 \cdot 11 \cdot 10$  isomorphisms from  $G_1$  to  $G_2$ , twenty take  $C$  to  $C$ . Ten of these are some  $i_j$  and ten are  $i_{j'}$ , with  $j + j' = 10$ . A Galois-theoretic computation shows that  $\{j, j'\} = \{3, 7\}$ , not the other possibility,  $\{1, 9\}$ . This is why the two weight sets  $\{4, 8\}$  and  $\{2, 10\}$  are different. Refining this computation further, one can see purely Galois-theoretically that the weights for  $f_1$  and  $f_2$  are  $\{4, 8\}$  and  $\{2, 10\}$  respectively.

### 3. FIFTY-THREE $PGL_2(\mathbb{F}_\ell)$ FIELDS WITH RATIONAL COMPANION FORMS

In this section, we prove the existence of fifty-three  $PGL_2(\mathbb{F}_\ell)$  fields  $K$  with associated rational companion forms  $g$  and  $h$ . In contrast to the previous section, here we start with  $(g, h)$  and obtain only the abstract existence of  $K$ , not an explicit defining polynomial  $f(x)$ . The examples of the previous section provide helpful illustrations, but to a large extent this section can be read independently.

**3.1. Triples  $(K, g, h)$ .** In the introduction, we explained that we are seeking fields  $K$  belonging to triples  $(K, g, h)$  similar to the triples  $(K_i, g_i, h_i)$  of the previous section. In this subsection, we define precisely the type of triples we seek.

Throughout, a prime  $\ell$  is present, typically not incorporated into the notation. We exclude the prime  $\ell = 2$  because it behaves slightly differently. When we pursue classification starting in §3.3, we will take  $\ell \geq 11$ . The fields  $K$  we allow

are those that can be presented in the form  $\mathbb{Q}[x]/f(x)$  with  $f(x) \in \mathbb{Q}[x]$  a degree  $\ell + 1$  polynomial with Galois group  $PGL_2(\mathbb{F}_\ell)$ . Note that our focus on the abstract stem field  $K$  of  $f(x)$  rather than the splitting field  $K^{\text{gal}} \subset \mathbb{C}$  of  $f(x)$  is a question of language, as the abstract non-Galois extension  $K$  and the embedded Galois extension  $K^{\text{gal}}$  each determine the other.

Beyond the prime  $\ell$ , three more invariants associated to a triple  $(K, g, h)$  are positive integers  $N$ ,  $k$ , and  $k'$ . The integer  $N$ , called the level or the conductor, is required to not be a multiple of  $\ell$ . The integers  $k$  and  $k'$ , called the weights, are even. Without loss of any fields  $K$ , by the results of [Edi92, §7], we require also that  $k$  and  $k'$  are in the range  $[2, \ell + 1]$ . The remaining entries of the triples are newforms with the common level  $N$ , trivial character, rational coefficients, and the indicated weights:

$$g = \sum a_n q^n \in S_k^{\text{new}}(N), \quad h = \sum b_n q^n \in S_{k'}^{\text{new}}(N).$$

Here basic notation for newforms has been recalled in a formalistic way at the beginning of §2.6, with references also given there.

A triple  $(K, g, h)$  has yet more invariants. In particular, for primes  $p$  not dividing  $N$ , the field  $K$  yields a factorization partition  $\lambda_p$ , the form  $g$  determines a normalized square  $s_p = a_p^2/p^{k-1} \in \mathbb{F}_\ell$ , and the form  $h$  likewise determines a normalized square  $s'_p = b_p^2/p^{k'-1} \in \mathbb{F}_\ell$ . These numeric invariants are required to correspond as follows. First,  $s_p = s'_p$ . Second, let  $o_p$  be the least common multiple of the parts of  $\lambda_p$ . Let  $O_p$  be the common order of the elements

$$\begin{pmatrix} 0 & -1 \\ p^{k-1} & a_p \end{pmatrix} \text{ and } \begin{pmatrix} 0 & -1 \\ p^{k'-1} & b_p \end{pmatrix}$$

in the group  $PGL_2(\mathbb{F}_\ell)$ . Then it is required that either  $o_p = O_p$  or  $(o_p, O_p) = (1, \ell)$ . Table 2.1 illustrates this correspondence for  $\ell = 11$ .

We require that  $g$  and  $h$  are related via cyclotomic twisting as follows. For either  $t = 1$  or  $t = 2$ , we require that  $k + k' = \ell - 1 + 2t$  and

$$(3.8) \quad n^t a_n \equiv n^k b_n \pmod{\ell}$$

for all  $n$ . Symmetry between  $g$  and  $h$  is present, because this last condition could be equivalently rewritten as  $n^{k'} a_n \equiv n^t b_n \pmod{\ell}$ . If  $k = k'$ , either congruence says that  $a_n \equiv \chi(n) b_n$ , with  $\chi(\cdot) = (\cdot/\ell)$  the quadratic character on  $\mathbb{F}_\ell$ . As our last requirement on triples, we partially normalize by demanding  $k \leq k'$ .

Given a triple  $(K, g, h)$ , one can sometimes trivially make a new one in three ways. First, one can replace  $g$  and/or  $h$  by a different form with the same reduction to  $\mathbb{F}_\ell[[q]]$  in the somewhat rare case that such a form exists. Second, one may be able to twist  $g$  and/or  $h$  by a quadratic character, keeping the level the same, as discussed with examples after (2.7). Finally if  $k = k'$  one can simply switch  $g$  and  $h$ . Note that in this final case,  $g$  and  $h$  are not trivially obtained from one another because twisting either  $g$  or  $h$  by the quadratic character  $\chi$  above increases the level from  $N$  to  $\ell^2 N$ . None of these operations change  $K$ , which is why Theorem 3.1 below counts  $K$  extendable to triples, rather than triples themselves.

**3.2. Conditions on  $K$  and companion forms.** This subsection discusses which  $PGL_2(\mathbb{F}_\ell)$  number fields  $K$  have a chance of being in a triple  $(K, g, h)$ . Our discussion defines the three types of companion forms, and in the process motivates

some of the definitions made in the previous subsection. The next four paragraphs do not use rationality.

Let  $K$  be any  $PGL_2(\mathbb{F}_\ell)$  field which is not totally real. Then, by Serre reciprocity,  $K$  comes from a newform  $g$ , perhaps with irrational coefficients, in some space  $S_k^{\text{new}}(N, \chi)$ . Here the Dirichlet character can be non-trivial in general, and the weight satisfies  $\chi(-1) = (-1)^k$  and is therefore allowed to be odd. Matching is between  $\lambda_p$  as before and now  $s_p = a_p^2 / (p^{k-1} \chi(p))$ . One can always take  $k$  in the interval  $[2, \ell + 1]$ , which accounts for our making this restriction on  $k$  in the previous section.

Let  $D$  be the discriminant of  $K$ , and write  $c = \text{ord}_\ell(D)$ . The largest  $c$  can be is  $2\ell - 1$ . Suppose  $c > \ell$ , so that  $c$  has the form  $\ell - 2 + k$  for  $k \in [3, \ell + 1]$ . Then  $g$  necessarily has weight  $k$ . The condition (3.8) makes sense for irrational forms reduced to characteristic  $\ell$  as well, and there is no companion form  $h$ . Examples with an explicit polynomial  $f(x)$  for  $K$  and  $g$  rational are given for  $N = 1$  and  $\ell \geq 11$  in [Bos11b], and for  $N \in \{2, 3, 4, 6, 8\}$  and  $\ell \leq 7$  in [Rob16b, §6.3].

Still allowing irrational forms and general character, consider the complementary case  $c \leq \ell$ , except that we temporarily exclude  $c = 0$ . For these more lightly ramified fields, there is always a companion form  $h$  with weight  $k'$  satisfying  $k + k' = \ell - 1 + 2t$  with  $t \in \{1, 2\}$  as for (3.8). The three cases are as follows:

|       | Case              | Size of $\ell$ -inertia | $\text{ord}_\ell(D)$ | Consequence for $(k, k')$   |
|-------|-------------------|-------------------------|----------------------|-----------------------------|
| (3.9) | 1T=diagonalizable | $(\ell - 1)/d$          | $\ell - 1 - d$       | $k + k' = \ell + 1$         |
|       | 2T=supersingular  | $(\ell + 1)/d$          | $\ell + 1 - d$       | $k + k' = \ell + 3$         |
|       | 2W=peu ramifiée   | $\ell(\ell - 1)$        | $\ell$               | $(k, k') = (2, \ell + 1)$ . |

The case  $c = 0$  would be similar, except that the two weights should be  $(k, k') = (1, \ell)$ , with the form of weight 1 usually living only in characteristic  $\ell$  [CV92]. Summarizing, a fundamental reason to be interested in companion forms from a number-theoretic viewpoint is that existence of a companion form translates into light ramification at  $\ell$ .

An important distinction between the cases deserves to be mentioned. If from  $g$  one sees that  $s_\ell$  is zero in  $\mathbb{F}_\ell$ , then one is automatically in Case 2T; one knows without looking that there is then a companion form  $h$  in weight  $\ell + 3 - k$ . However if  $s_\ell \neq 0$ , then one really needs to look for a companion form in weight  $\ell + 1 - k$  to identify ramification. One is in Case 1T only if there is a such a companion form. Otherwise,  $c = \ell - 2 + k$  as above, and ramification is wild. If  $k = 2$ , one is in the case 2W and there is necessarily a companion form, but now in weight  $\ell + 1$  rather than  $\ell - 1$ . If  $k > 2$ , one is in the generic case and there is no companion form.

Now we return to our requirement that both  $g$  and  $h$  have rational coefficients. Then the Nebentypus  $\chi$  is trivial, forcing the discriminant  $D$  to be  $(-1)^{(\ell-1)/2\ell}$  times a square. Moreover the field  $K$  has a lift to a field  $\tilde{K}$  with Galois group embedding in  $GL_2(\mathbb{F}_\ell)$ . For any  $\ell$  we expect infinitely many  $K$  to satisfy these two natural conditions. They all fit into a  $(K, g, h)$ , as long as we allow irrational  $(g, h)$ . Besides implying these two conditions, rationality of coefficients on the modular side does not translate into anything natural on the Galois side. Rather it just corresponds to restricting to a presumably much smaller subset of this collection of fields  $K$ .



**3.3. Finding and confirming triples  $(K, g, h)$ .** To obtain triples  $(K, g, h)$  with  $g$  and  $h$  rational, we use the collection of rational newforms without complex multiplication built up in [Rob16b]. For  $t \in 1, 2$  and each  $(\ell, N, k, k')$  within the range

| $\ell$ | $k = 2$          | 4                      | 6                    | 8                      | 10               | 12 | 14 | 16 | 18 | 20 | 22 |
|--------|------------------|------------------------|----------------------|------------------------|------------------|----|----|----|----|----|----|
| 11     | <b>54</b><br>182 | <b>24</b><br>42<br>120 | 78<br>78             | <b>24</b><br>42<br>120 | <b>54</b><br>182 |    |    |    |    |    |    |
| 13     |                  | 22                     | 7<br>70<br>84<br>210 | 7<br>70<br>84<br>210   | 22               |    |    |    |    |    |    |
| 17     |                  |                        | 24                   | 42                     | 42               | 24 |    |    |    |    |    |
| 19     |                  | 10                     |                      | 24                     |                  | 24 |    | 10 |    |    |    |
| 23     |                  |                        |                      |                        | 30               |    | 30 |    |    |    |    |
| 29     |                  |                        |                      |                        |                  | 6  | 8  | 8  | 6  |    |    |
| 31     |                  |                        |                      |                        |                  |    | 12 |    | 12 |    |    |
| 37     |                  |                        |                      |                        |                  |    |    |    |    | 3  |    |
| 41     |                  |                        |                      |                        |                  |    |    |    |    |    | 3  |

TABLE 3.2. Guide to the twenty triples  $(K, g, h)$  of type 1T. The conductor  $N$  associated to each  $K$  appears twice, once as the level of  $g$  and once as the level of  $h$ . The boldface **24**'s and **54**'s represent the triples of Section 2.

of the collection, we look at all potentially congruent rational pairs  $g \in S_k^{\text{new}}(N)$  and  $h \in S_{k'}^{\text{new}}(N)$ . Motivated by the definitional congruences (3.8), we consider  $\delta = \sum_n c_n q^n \in \mathbb{F}_\ell[[q]]$  with  $c_n = n^t a_n - b_n n^k$ . Let  $\theta = q^{\frac{d}{dq}}$  be Ramanujan's theta operator. As described in [Gro90, (4.5)], this operator increases weights of reduced modular forms in  $\mathbb{F}_\ell[[q]]$  by  $\ell + 1$ . The difference  $\delta = \theta^2 f - \theta^{k+2} g$  in question is then the reduction of a modular form in  $M_\kappa(N)$ , where  $\kappa = k' + (k + t)(\ell + 1)$ . Let  $\sigma_1(N) = \prod_{p^e \parallel N} (p^e + p^{e-1})$  be the index of  $\Gamma_0(N)$ . Then by [Ste07, Thm 9.18],  $\delta$  is determined by its Fourier coefficients  $c_n$  for  $n$  at most the Sturm bound  $S = \kappa \sigma_1(N) / 12$ . We compute these  $c_n$  until either one of them is nonzero or  $S$  is reached. In the latter case, we have confirmed that indeed  $(g, h)$  is a companion pair. Sometimes the common  $s_p = a_p^2 / p^{k-1} = b_p^2 / p^{k'-1}$  inspected for  $p \nmid \ell N$  do not suffice to ensure the surjectivity of the projective representation. In these few cases, we identify the relevant number field, so as to unconditionally confirm lack of surjectivity. Numerics associated to the fifty-three pairs remaining are in Tables 3.2 and 3.3. Each field  $K$  gives rise to a minimal conductor  $N$  appearing twice in the  $\ell$ -row, once in the  $k$  column and once in the  $k'$  column. The parenthesized entries  $(N)$  on Table 3.3 indicate two of the  $(g, h)$  discarded because of nonsurjectivity of the Galois representation into  $PGL_2(\mathbb{F}_\ell)$ .

As an example, the largest Sturm bound encountered in a Type 1 pair occurs for  $(\ell, k, k', N) = (13, 6, 8, 210)$ . Here the forms are the unique newforms in their one-dimensional Atkin-Lehner eigenspaces,  $g \in S_6^{\text{new}}(210)^{-++}$  and  $h \in S_8^{\text{new}}(210)^{+--}$ . One has  $\kappa = 92$ ,  $\sigma_1(210) = 576$ , and so the Sturm bound is

| $\ell$ | $k = 2$   | 4   | 6        | 8  | 10       | 12        | 14       | 16  | 18       | 20 | 22 | 24 |
|--------|-----------|-----|----------|----|----------|-----------|----------|-----|----------|----|----|----|
| 11     | 14        |     |          |    |          | 14        |          |     |          |    |    |    |
|        | <i>15</i> |     |          |    |          | <i>15</i> |          |     |          |    |    |    |
|        | 20        |     | 10       | 10 |          | 20        |          |     |          |    |    |    |
|        | <i>24</i> |     | 42       | 42 |          | <i>24</i> |          |     |          |    |    |    |
|        | 30        | (8) | 70       | 70 | (8)      | 30        |          |     |          |    |    |    |
|        | <i>42</i> |     | 78       | 78 |          | <i>42</i> |          |     |          |    |    |    |
|        | <i>84</i> |     | 96       | 96 |          | <i>84</i> |          |     |          |    |    |    |
| 13     |           |     |          |    |          |           |          |     |          |    |    |    |
|        |           |     | <b>5</b> |    | <b>5</b> |           |          |     |          |    |    |    |
|        |           |     | 24       |    | 24       |           |          |     |          |    |    |    |
|        |           |     | 38       | 30 | 38       |           |          |     |          |    |    |    |
|        |           |     | 50       | 30 | 50       |           |          |     |          |    |    |    |
| 17     |           |     |          |    |          |           |          |     |          |    |    |    |
|        |           |     |          |    |          |           |          |     |          |    |    |    |
|        |           |     |          |    |          |           |          |     |          |    |    |    |
|        |           |     |          |    |          |           |          |     |          |    |    |    |
| 17     | 30        |     | 30       | 50 | 42       | 50        | 30       |     | 30       |    |    |    |
| 19     |           |     |          |    |          |           |          |     |          |    |    |    |
|        |           |     |          |    |          |           |          |     |          |    |    |    |
| 19     |           | 30  | (4)      |    | <b>3</b> | <b>3</b>  |          | (4) | 30       |    |    |    |
| 23     |           |     |          |    |          |           |          |     |          |    |    |    |
|        |           |     |          |    |          |           |          |     |          |    |    |    |
| 29     |           |     |          | 30 | 12       |           | <b>2</b> |     | <b>2</b> |    | 12 | 30 |
| 31     |           |     |          |    |          |           |          |     |          |    |    |    |
|        |           |     |          |    |          |           |          |     |          |    |    |    |
| 37     |           |     |          |    |          | 6         |          |     |          |    |    |    |
| 41     |           |     |          |    |          |           |          |     |          |    |    |    |
|        |           |     |          |    |          |           |          |     |          |    |    |    |
| 43     |           |     |          |    | 6        |           |          |     |          |    |    |    |

TABLE 3.3. Guide to the twenty-seven triples of type 2T and the six triples of type 2W, the latter italicized. The general format follows that of Table 3.2, so that entries are conductors  $N$ . To the right of the chart, there should also be 6's at locations  $(\ell, k) = (37, 28)$  and  $(43, 36)$ . The boldface **5**'s, **3**'s, and **2**'s are pursued in §4.4. Also in parentheses are two degenerate triples discussed in §4.5.2.

$S = 4416$ . A *Magma* computation using built-in commands in a straightforward way took 24 minutes to confirm that  $\delta \in \mathbb{F}_{13}[[q]]$  is indeed zero.

Summarizing, our computations prove the following theorem.

**Theorem 3.1.** *There are at least fifty-three number fields  $K$  belonging to triples  $(K, g, h)$  satisfying the following conditions:  $K$  has degree  $\ell + 1$  and associated Galois group  $PGL_2(\mathbb{F}_\ell)$  for a prime  $\ell \geq 11$ ;  $g$  and  $h$  are rational newforms which are companion forms modulo  $\ell$  and have projective modulo  $\ell$  representations corresponding to  $K$ .*

In the sequel, we will sometimes simply speak of the fifty-three triples  $(K, g, h)$ , always chosen with  $g$  and  $h$  having minimal level  $N$ , even though in a few cases there are the ambiguities in  $g$  or  $h$  mentioned at the end of §3.1. The last type of ambiguity mentioned there arises in the three cases where  $k = k'$  and so that one can interchange  $g$  and  $h$ . For example, the two forms of level 30 at position

$(\ell, k) = (13, 8)$  in Table 3.3 are

$$\begin{aligned} g &= q + 8q^2 - 27q^3 + 64q^4 + 125q^5 - 216q^6 + 512q^7 + \dots, \\ h &= q - 8q^2 - 27q^3 + 64q^4 - 125q^5 + 216q^6 - 1084q^7 + \dots. \end{aligned}$$

As explained in §3.1, when reduced to  $\mathbb{F}_{13}[[q]]$ , these forms become twists of one another by the quadratic character  $(\cdot/13)$ . However there is no such direct relation between  $g$  and  $h$  as forms in  $\mathbb{C}[[q]]$ , with  $(a_p, b_p) = (512, -1084)$  being illustrative of  $(a_p, b_p)$  for all  $p \geq 7$ .

**3.4. Conjectural completeness.** We believe that the list of fifty-three number fields in Theorem 3.1 is complete. In this subsection, we give our reasons; in brief, the fifty-three number fields arise towards the the beginning of our search. We have computed much further and found no more.

In general, for the weights  $k \leq k'$  associated to the pair  $(g, h)$ , one has  $k' \geq (\ell + 1)/2$ . Conjecture 1.1 of [Rob16b] says that there are no non-CM newforms with rational coefficients and weight  $k' \geq 52$ . This would imply that there are indeed no fields for  $\ell \geq 101$ . Conjecture 1.1 of [Rob16b] says moreover that all such newforms of weight  $k' \geq 18$  are known, as indeed their minimal levels  $N$  are always  $\leq 30$ . This would imply our list of three fields for  $\ell \geq 37$  is complete. It is moreover argued in [Rob16b] that all or very close to all such newforms in weights 10, 12, 14, 16 are known too. This makes our list twenty-one fields for  $\ell \geq 17$  likely to be complete too.

The evidence in [Rob16b] suggests that for  $k \in \{6, 8\}$ , there are likely a few non-CM rational newforms with minimal level beyond the cutoffs  $C_6 = 1000$  and  $C_8 = 700$  used there. However it seems unlikely to us that these unknown newforms are part of a companion pair, especially given that the largest level  $N$  appearing on Tables 3.2 and 3.3 is 294. It is for this reason that we believe that our lists of thirteen and nineteen fields for  $\ell = 13$  and  $\ell = 11$  respectively are complete as well.

**3.5. Explicit formulas.** In [Rob16b], we explained how to get completely explicit formulas for newforms in the cases  $N \in \{2, 3, 4, 6, 8\}$ . The entries for these  $N$  in Tables 3.2 and 3.3 correspond to the following companion forms

$$\begin{aligned} N = 2 : & \quad \Delta_{14}^+ \overset{29}{\sim} \Delta_{18}^-, \\ N = 3 : & \quad \Delta_{10}^- \overset{19}{\sim} \Delta_{12}^+, \quad \Delta_{20}^- \overset{41}{\sim} \Delta_{22}^{+a}, \\ N = 4 : & \quad (\Delta_6^- \overset{19}{\sim} \Delta_{16}^-), \\ N = 6 : & \quad \Delta_{12}^{--} \overset{29}{\sim} \Delta_{18}^{++}, \quad \Delta_{12}^{--} \overset{37}{\sim} \Delta_{28}^{+-}, \quad \Delta_{10}^{+-} \overset{43}{\sim} \Delta_{36}^{-+}, \\ N = 8 : & \quad (\Delta_4^+ \overset{11}{\sim} \Delta_{10}^-), \quad \Delta_{14}^+ \overset{29}{\sim} \Delta_{16}^{-b}. \end{aligned}$$

Here  $\Delta_k^\epsilon$  denotes the unique newform of weight  $k$  on  $\Gamma_0(N)$  with Atkin-Lehner eigenvalue string  $\epsilon$ . The unusual cases  $(k, N) = (3, 22)$  and  $(8, 16)$  are highlighted in [Rob16b], as in these cases a two-dimensional Atkin-Lehner space has two rational newforms. The above display identifies which newform is involved in the compansion forms, with completely explicit formulas for  $\Delta_{22}^{+a}$  and  $\Delta_{16}^{-b}$  given in §5.3 and §5.6 of [Rob16b] respectively.

One could also write down explicit formulas for other  $N$ . For example, define  $\Theta_t = \sum_{x,y \in \mathbb{Z}^2} q^{t(x^2+xy+y^2)}$ . Returning to our very first example with  $N = 24$ , the unique newform of weight two is  $\Delta_2^{-+} = 18^{-1}(\Theta_4 - \Theta_1)(\Theta_2 - 4\Theta_8)$ . Like all the

other generators of cuspidal ideals considered in [Rob16b], it is also an eta-product,  $\eta_2\eta_4\eta_6\eta_{12}$ . The companion forms from (2.6) have the explicit formulas

$$\begin{aligned} g_1 &= \Delta_4^{--} = 3^{-1}(\Theta_2^2 + 2\Theta_4^2)\Delta_2^{-+}, \\ h_1 &= \Delta_8^{+-} = 9^{-1}(\Theta_2^2 - 2\Theta_4^2)(7\Theta_2^4 - 44\Theta_2^2\Theta_4^2 + 28\Theta_4^4)\Delta_2^{-+}. \end{aligned}$$

The formulas constructible from [Rob16b] for the nine companion pairs displayed above are of a similar nature. The main congruence (3.8) can be seen explicitly, by expanding the power series. For example, for both  $g_1$  and  $h_1$ , the first five primes having Fourier coefficient congruent to zero modulo 11 are 103, 149, 179, 197, and 257.

#### 4. LIGHTLY RAMIFIED NUMBER FIELDS

This section first obtains polynomials for some of the fifty-three number fields from the last section. It next analyzes ramification in these number fields, finding that some root discriminants are particularly small. Finally it discusses the natural problem of obtaining complete lists of number fields with Galois group a finite subquotient of  $GL_2(\mathbb{F}_\ell)$  and small root discriminant.

**4.1. Polynomials from elliptic curves.** For eleven of our triples  $(K, g, h)$ , the modular weight of the form  $g$  is 2. As  $g$  has rational coefficients, there is a corresponding elliptic curve  $E_g$ , easily found on the LMFDB [LMF16]. A degree  $\ell + 1$  polynomial can then be obtained for  $K$  by looking at the  $\ell + 1$  different subgroups of  $E_g(\mathbb{C})$  of size  $\ell$ . *Magma's* `AtkinModularPolynomial` does this immediately.

For example, only one of eleven triples has  $\ell \neq 11$ , and its residual prime is  $\ell = 17$ . There are eight elliptic curves with the required conductor 30, all isogenous and hence all yielding the correct  $K$ . One of the  $j$ -invariants is  $71^3/(2^4 3^3 5)$ . Specializing the Atkin modular polynomial to this  $j$ -invariant and applying `polredabs` yields

$$\begin{aligned} (4.10) \quad & x^{18} - 2x^{17} - 714x^{15} + 3060x^{14} - 7854x^{13} + 258468x^{12} - 1062840x^{11} \\ & - 2425764x^{10} - 6360720x^9 + 224396532x^8 - 694308084x^7 \\ & - 1149382920x^6 + 8831732832x^5 - 3417673200x^4 - 68962605552x^3 \\ & + 206896699224x^2 - 267387716040x + 143842600848, \end{aligned}$$

with discriminant  $2^{16}3^{16}5^{16}17^{17}$ . The large coefficients are a reflection of the relatively large root discriminant  $\delta \approx 298.6$ . In general, to capture lifts to  $GL_2(\mathbb{F}_\ell)$  one has to work with polynomials of degree  $2^j(\ell + 1)$  where  $j = \text{ord}_2(\ell - 1)$ . The case of  $\ell \equiv 3 \pmod{4}$  is easiest, as  $j = 1$  and one can work with  $SL_2^\pm(\mathbb{F}_\ell)$  as a substitute for  $GL_2(\mathbb{F}_\ell)$ . The case  $\ell = 17$  is at the opposite extreme, and one would have to use a degree 288 polynomial to lift (4.10).

The other ten triples all have  $\ell = 11$  and so can be treated uniformly, even at the lifted level of degree 24 fields  $\tilde{K}$  with Galois group  $SL_2^\pm(\mathbb{F}_{11})$ . Here it does not suffice to work with  $j$ -invariants, as quadratic twisting is seen in the lift. Accordingly we work with actual elliptic curves  $y^2 = x^3 + ax + b$ . Starting with the Atkin modular polynomial with  $\ell = 11$ , lifting to degree 24 polynomials for individual  $j$ , and interpolating, we obtain the following polynomial with just seven terms:

$$\begin{aligned} (4.11) \quad \tilde{f}_{11}(a, b, x) &= d^{10}x^{24} - 15840d^5x^{12} - 337920ad^3x^8 \\ &\quad - 2280960bd^2x^6 + 811008a^2dx^4 + 663552abx^2 - 2816. \end{aligned}$$

Here we have abbreviated using the discriminant  $d = -4a^3 - 27b^2$ . Correctness of the seven-term polynomial is algebraically confirmed by comparing with a full 11-division polynomial of degree 120 and factoring a resolvent. The polynomial applies to our ten cases through the following chart:

| $N$ | 1T  |        | 2T    |      |       | 2W   |     |        |       |      |
|-----|-----|--------|-------|------|-------|------|-----|--------|-------|------|
|     | 54  | 182    | 14    | 20   | 30    | 15   | 24  | 42     | 84    | 96   |
| $a$ | 21  | 13861  | -675  | -108 | 1917  | -27  | 54  | -5211  | -108  | -189 |
| $b$ | -26 | 426358 | 13662 | 297  | 99198 | 8694 | 189 | 319734 | -1755 | -540 |

We remark that we have found analogs in  $\mathbb{Q}(a, b)[x]$  of the seven-term (4.11) for  $\ell = 7, 19,$  and  $23$ ; these analogs are even polynomials of degree  $2\ell + 2$  and Galois groups  $SL_2^\pm(\mathbb{F}_\ell)$  having 6, 15, and 18 terms respectively.

**4.2. Polynomials from higher weight modular forms.** For forty-two of our  $(K, g, h)$ , the smaller weight  $k$  is at least four. Our discussion so far has included a polynomial for only one of these fields  $K$ , namely our very first example  $K_1$ , with defining polynomial  $f_1(x)$  from (2.1).

It is however theoretically possible to take a modular form as a starting point and compute an associated mod  $\ell$  Galois representation. Explicit examples in the literature currently start from either forms with rational coefficients in level  $N = 1$  [Bos11c, Mas13] or forms with irrational coefficients in weight  $k = 2$  [Bos07, Bos11a].

Our collection of examples provides a testing ground for these methods in the setting of  $N > 1$  and  $k > 2$ . Most of our examples seem to be currently beyond computational reach, in part because one has to compute lifted polynomials on the way to projective polynomials. However Mascot has found polynomials in three of the forty-one cases left open by this paper, with many details given in [Mas16]. His most complicated case is the  $PGL_2(\mathbb{F}_{41})$  field on Table 3.2, where he finds a polynomial of degree  $2^3(41+1) = 336$  on the way to the final projective polynomial  $x^{42} - 2x^{41} + 8x^{40} + \dots$ .

**4.3. Ramification in modular fields.** One does not actually need polynomials to determine ramification in our fields  $K$ , as Serre reciprocity is refined enough to calculate it on the modular side.

For a prime  $p \neq \ell$  exactly dividing a minimal conductor  $N$ , ramification is tame of order  $\ell$ . It contributes  $p^{(\ell-1)/(\ell+1)}$  to the root discriminant and  $p^{(\ell-1)/\ell}$  towards the Galois root discriminant. If  $p^2$  exactly divides the minimal conductor  $N$ , then ramification is tame of order  $e = 3, 4,$  or  $6$ , so that  $e$  divides exactly one of  $\ell - 1$  or  $\ell + 1$ . If  $p = 2$  the only possibility is  $e = 3$  and if  $p = 3$  the only possibility is  $e = 4$ , as otherwise ramification would be wild. The contribution to the root discriminant is  $p^{(e-1)(\ell-1)/(e(\ell+1))}$  if  $e$  divides  $\ell - 1$  and  $p^{(e-1)/e}$  if  $e$  divides  $\ell + 1$ . The computation to the Galois root discriminant is always  $p^{(e-1)/e}$ . If  $\text{ord}_p(N) \geq 3$ , ramification is wild and the procedure is more complicated, as with the two examples given in Section 2.

The contribution of  $\ell$  to the root discriminant depends on the type and weights. Taking (3.9) as a starting point, and writing  $-$  in type 1T and  $+$  in type 2T, put  $d = \gcd(k - 1, \ell \pm 1) = \gcd(k' - 1, \ell \pm 1)$  and  $e = (\ell \pm 1)/d$ . The size of the inertia group  $I_\ell$  is then  $e$ . The contributions of  $\ell$  are  $\ell^{(e-1)(\ell \pm 1)/(e(\ell+1))}$  to the root discriminant and  $\ell^{(e-1)/e}$  to the Galois root discriminant. As  $k$  and  $k'$  are even,  $d$  is always odd. In fact  $d = 1$  except for the cases  $(\ell, N) = (11, 78), (13, 22), (19, 10)$  on

Table 3.2, (13, 30), (17, 42), (29, 12) on Table 3.3, and the degenerate cases (11, 8) and (19, 4) on Table 3.3. Here the inertial group size reductions are respectively  $d = 5, 3, 3, 7, 9, 3, 3$ , and 5. For cases of type 2W, the contribution to the root discriminant is  $\ell^{\ell/(\ell+1)}$ , while the contribution to the Galois root discriminant is  $\ell^{1+(\ell-2)/(\ell(\ell-1))}$ .

**4.4. Four lightly ramified fields.** The root discriminant  $\delta$  and Galois root discriminant  $\Delta$  for four of our fields are in the middle block of Table 4.4. The last

| $\ell$ | Tame at $\ell$ from<br>companion forms |              |              | wild at $\ell$ from<br>Ramanujan's $\Delta_{12}$ |          |          |
|--------|--|--------------|--------------|--|----------|----------|
|        | $N$                                    | $\delta$     | $\Delta$     | $N$  | $\delta$ | $\Delta$ |
| 11     | 24                                     | 33.87        | 52.75        | 1  | 66.44    | 118.39   |
| 13     | 5                                      | 43.00        | <i>47.82</i> | 1  | 67.62    | 112.04   |
| 19     | 3                                      | <i>44.07</i> | <i>46.43</i> | 1  | 71.48    | 103.60   |
| 29     | 2                                      | <i>49.50</i> | <i>50.62</i> | 1  | 79.64    | 103.59   |

TABLE 4.4. Root discriminants  $\delta$  and Galois root discriminants  $\Delta$  for eight lightly ramified number fields with Galois group  $PGL_2(\mathbb{F}_\ell)$ . Italicized entries are candidates for smallest possible for their context.

three cases are uniformly behaved as they all have type 2T with  $N = p$  prime. Their root discriminants are given by  $p^{(\ell-1)/(\ell+1)}\ell^{\ell/(\ell+1)}$  while their Galois root discriminants are given by the slightly larger number  $p^{(\ell-1)/\ell}\ell^{\ell/(\ell+1)}$ . The rest of this subsection puts the four pairs  $(\delta, \Delta)$  into context.

**4.4.1. Comparison with the Serre-Odlyzko constant  $\Omega$ .** Analytic lower bounds on root discriminants of degree  $n$  fields increase as  $n \rightarrow \infty$  to an asymptotic limit of  $\Omega' = 4\pi e^\gamma$ , with  $\gamma \approx 0.5772$  being Euler's gamma constant. Under the generalized Riemann hypothesis, these bounds are increased so that the asymptotic limit becomes  $\Omega = 2\Omega' \approx 44.76$  [Odl90, (2.6)]. In [JR07] and then [JR14, §9,10], we put forward the principle that it is extremely unusual for a large degree Galois number field to have root discriminant less than  $\Omega$ . In the four cases of Table 4.4, the Galois root discriminants are quite close to  $\Omega$ .

**4.4.2. Comparison with fields from the Ramanujan newform.** An alternative approach to keeping root discriminants small is simply to insist that levels  $N$  be just 1. The smallest weight newform with  $N = 1$  is the famous Ramanujan form  $\Delta_{12} \in S_{12}(1)$ . Its projective mod  $\ell$  Galois representations are known to be surjective onto  $PGL_2(\mathbb{F}_\ell)$  except for  $\ell \in \{2, 3, 5, 7, 23, 691\}$  [SD75]. For surjective representations with  $\ell < 3500$ , Elkies and Atkin showed there is no companion form of type 1T [Gro90, §17]. The first two  $\ell$  for which there is a companion form of type 2T are known to be 2411 and 7758337633 [LR10]. When  $\ell > 7$  and no companion forms are present, the slope content at  $\ell$  is  $[(\ell + 10)/(\ell - 1)]_{(\ell-1)/w}$ ; here  $w = 10$  if  $\ell \equiv 1 \pmod{11}$  and otherwise  $w = 1$ . The resulting quantities, assuming  $w = 1$  in the case of  $\Delta$ , are

$$\delta = \ell^{(\ell+10)/(\ell+1)}, \quad \Delta = \ell^{(\ell^2+10\ell-12)/(\ell^2-\ell)}.$$

In the four examples of Table 4.4, the field from  $\Delta_{12}$  is substantially more ramified than the tame field.

4.4.3. *Comparison with other fields.* Schaeffer found a weight 1 modular form with level  $N = 3 \cdot 227$  and quadratic character  $\chi_{-227}$  living in characteristic 11 [Sch15, Table 4]. From this modular form, one knows that there is a  $PGL_2(\mathbb{F}_{11})$  field with root discriminant  $\delta = 3^{10/12}227^{5/12} \approx 23.94$  and Galois root discriminant  $\Delta = 3^{10/11}227^{1/2} \approx 40.90$ . These quantities are much smaller than the corresponding quantities on the  $\ell = 11$  line of Table 4.4. At present, one does not have a polynomial for this remarkable field.

More explicitly, from an elliptic curve with conductor 128 and  $j$ -invariant also 128, one gets a degree fourteen polynomial with Galois group  $PGL_2(\mathbb{F}_{13})$  and slope content  $[8/3, 8/3]_3$  at 2 and  $[13/12]_{12}$  at 13. This gives  $\delta = 2^{13/7}3^{13/14} \approx 39.21$  which undercuts 43.00 from Table 4.4. However the Galois root discriminant  $\Delta = 2^{13/6}13^{167/156} \approx 69.94$  is well above 47.82.

4.5. **The tabulation problem and group-drop.** A standard problem in the theory of number fields goes as follows: *Let  $G$  be a transitive permutation group of degree  $n$ ; let  $B$  be a positive real number; determine the complete list of degree  $n$  number fields  $K$  with associated Galois group  $G$  and root discriminant  $\leq B$ .* Often one thinks in terms of the ordered list of root discriminants,  $\delta_1(G) \leq \delta_2(G) \leq \delta_3(G) \leq \dots$ , with particular interest in finding  $\delta_1(G)$  for as many permutation groups as possible.

The database [JR14] contains solutions of this problem for many small  $G$  and large  $B$ . For solvable groups  $G$ , class field theory lets one obtain non-empty lists for quite large  $G$  in quite large degree  $n$ . However for almost simple non-solvable groups realized in their lowest degree, for example  $S_n$  itself or  $PGL_2(\mathbb{F}_\ell) \subseteq S_{\ell+1}$  for  $\ell \geq 7$ , the standard purely number-theoretic approach rapidly decays from easy to impossible as  $n$  increases from 5 to 10. The numbers  $\delta \approx 44.07$  and 49.50 from Table 4.4 are currently candidates for  $\delta_1(G)$  with  $G = PGL_2(\mathbb{F}_\ell) \subset S_{\ell+1}$ , with  $\ell = 19$  and 29 respectively. Similarly, the numbers  $\Delta \approx 47.82, 46.43,$  and 50.62 are candidates for  $G = PGL_2(\mathbb{F}_\ell) \subset S_{\ell^3-\ell}$  and  $\ell = 13, 19,$  and 29 respectively.

For larger permutation groups  $G \subseteq S_n$ , as studied especially in [KM01], one often starts with a parameterized family of fields  $K_t$  having Galois group in  $G$  for all  $t$  and equal to  $G$  for most  $t$ . One searches among these fields for the  $K_t$  with particularly small root discriminant. Often one encounters the phenomenon of *group-drop*: the  $K_t$  with the smallest root discriminant all have Galois group strictly smaller than  $G$ . When this phenomenon occurs with great strength, it is some heuristic indication that the smallest root discriminant of a  $G$ -field found is not too far above the actual minimum  $\delta_1(G)$  sought.

The phenomenon of group-drop has indeed occurred with great strength behind the scenes in §2.1, §3.3, and §4.1. We add some perspective now by discussing some numerics of the group-drops observed.

4.5.1. *Drops from Mathieu groups to  $PGL_2(\mathbb{F}_{11})$  in §2.1.* It seems that all the  $M_{22}.2$  fields and  $M_{12}.2$  fields obtain by generic specializations of the covers mentioned in §2.1 are much more heavily ramified than the exceptional  $PGL_2(\mathbb{F}_{11})$  specialization we are pursuing. While  $K_1$  has Galois root discriminant  $\Delta_1 \approx 52.75$ , the smallest GRD for an  $M_{22}.2$  field that we have found is  $\Delta_1^{\text{gen}} = 2^{139/48}3^{3/4}11^{2/3} \approx 83.91$ , coming from  $y = -5^2 139^2 / 2^7$  in the cover of [Mal88]. Similarly, while  $K_2$

has  $\Delta_2 \approx 58.55$ , the smallest GRD we have seen for an  $M_{12}.2$  specialization is  $\Delta_1^{\text{gen}} = 2^{2/3}3^{31/18}11^{11/12} \approx 94.84$ , coming from  $t = -5^3/2^2$  [Rob16a, Table 5.2].

4.5.2. *Drops from  $PGL_2(\mathbb{F}_\ell)$  to solvable groups in §3.3.* In the process of searching for our fifty-three triples  $(K, g, h)$ , we encountered other triples  $(K, g, h)$  which satisfy all the required conditions, except that the image of the common projective representation is not all of  $PGL_2(\mathbb{F}_\ell)$ . Two such triples are reported via the (8)'s and (4)'s appearing in Figure 3.3. The Galois root discriminants, calculated by the general formulas presented in §4.3, are  $2^{7/6}11^{3/4} \approx 13.56$  and  $2^{2/3}19^{3/4} \approx 14.45$ . These numbers are so small that they contradict the unconditional lower bounds for fields of degree  $|PGL_2(\mathbb{F}_{11})|$  and  $|PGL_2(\mathbb{F}_{19})|$  respectively. In fact, the Galois group is  $S_4$  in each case, defining polynomials being respectively  $x^4 - 2x^3 - 4x^2 - 6x - 2$  and  $x^4 - x^3 - 2x^2 - 6x - 2$ .

4.5.3. *Drops from  $PGL_2(\mathbb{F}_{11})$  to solvable groups in §4.1.* As explained in §4.1, the field  $K_2$  from Section 2 arises also from specialization of the Atkin modular polynomial for  $\ell = 11$ . A computer search shows at least 394 values of  $j$  which keep ramification within  $\{2, 3, 11\}$ . The smallest seven GRDs are 20.70, 24.48, 24.77, 25.48, 29.34, 32.45, and 49.50. All of them come from degenerate specializations with solvable Galois group. The remaining 387 points all give Galois group  $PGL_2(\mathbb{F}_{11})$ , with the smallest GRD being  $\Delta_2 \approx 58.55$  from  $K_2$ .

4.6. **Modular approaches to the tabulation problem.** Let  $\lambda$  be a power of a prime  $\ell$ . Our concluding point is that modular methods can be brought to bear on the tabulation problem for  $G$  any subquotient of  $GL_2(\mathbb{F}_\lambda)$ , in any transitive permutation representation. Outside of  $\ell = 2$ , modular methods do not see totally real fields. However there are analytic lower bounds on the minimal root discriminants of totally real fields in degree  $n$ . As  $n \rightarrow \infty$ , these lower bounds tend unconditionally to  $4\pi e^{\gamma+1} \approx 60.84$  [Odl90, (2.5)]. When cutoffs are kept small enough, totally real fields are not present. In fact, under the generalized Riemann hypothesis, the above limit increases to  $8\pi e^{\gamma+\pi/2} \approx 215.33$  [Odl90, (2.6)]; so one does not expect to see totally real fields towards the beginning of tables at all.

In approaching this problem, it is natural to break into three cases:  $\ell$  is wildly ramified,  $\ell$  is tamely ramified, and  $\ell$  is unramified. In all cases, one needs to search among eigenforms without any rationality condition imposed, so that general characters and thus odd weights  $k$  are considered as well. As an example that stays mostly in the context of this paper, the unique newform in  $S_6^{\text{new}}(8)$  has an irrational companion form in  $S_{20}^{\text{new}}(8)$  for  $\ell = 23$ ; this yields a field with Galois group  $PGL_2(\mathbb{F}_{23})$  and the small Galois root discriminant  $\Delta = 2^{7/6}23^{23/24} \approx 45.30$ .

For a given cutoff  $B$ , it should be easiest to obtain complete lists in the wild-at- $\ell$  case, as the levels to be considered would be very small. Next easiest would be the tame-at- $\ell$  case, as modeled by our computations throughout this paper, including the previous paragraph; since ramification at  $\ell$  is lighter, the levels to be considered would no longer all be so small. By far the hardest, with our current theoretical knowledge, would be the unramified-at- $\ell$  case. This case requires computations either with weight 1 or weight  $\ell$  forms, both difficult for different reasons; also since there is no ramification at  $\ell$ , large levels would have to be inspected.



REFERENCES

- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478
- [Bos07] Johan Bosman, *A polynomial with Galois group  $SL_2(\mathbb{F}_{16})$* , LMS J. Comput. Math. **10** (2007), 1461–1570 (electronic). MR 2365691
- [Bos11a] ———, *Modular forms applied to the computational inverse galois problem*, arxiv:1109.6879, 13 pages, 2011.
- [Bos11b] ———, *Polynomials for projective representations of level one forms*, Computational aspects of modular forms and Galois representations, Ann. of Math. Stud., vol. 176, Princeton Univ. Press, Princeton, NJ, 2011, pp. 159–172. MR 2857091
- [Bos11c] ———, *Polynomials for projective representations of level one forms*, Computational aspects of modular forms and Galois representations, Ann. of Math. Stud., vol. 176, Princeton Univ. Press, Princeton, NJ, 2011, pp. 159–172. MR 2857091
- [Coh00] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR 2000k:11144
- [CV92] Robert F. Coleman and José Felipe Voloch, *Companion forms and Kodaira-Spencer theory*, Invent. Math. **110** (1992), no. 2, 263–281. MR 1185584
- [Edi92] Bas Edixhoven, *The weight in Serre’s conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594. MR 1176206
- [Gro90] Benedict H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod  $p$ )*, Duke Math. J. **61** (1990), no. 2, 445–517. MR 1074305
- [JR06] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97, website: <http://math.asu.edu/~jj/localfields>. MR 2194887
- [JR07] ———, *Galois number fields with small root discriminant*, J. Number Theory **122** (2007), no. 2, 379–407. MR 2292261 (2008e:11140)
- [JR14] ———, *A database of number fields*, LMS J. Comput. Math. **17** (2014), no. 1, 595–618, <http://math.asu.edu/~jj/numberfields>. MR 3356048
- [KM01] Jürgen Klüners and Gunter Malle, *A database for field extensions of the rationals*, LMS J. Comput. Math. **4** (2001), 182–196 (electronic). MR 2003i:11184
- [Kob93] Neal Koblitz, *Introduction to elliptic curves and modular forms*, second ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR 1216136
- [KW09a] Chandrashekhara Khare and Jean-Pierre Wintenberger, *Serre’s modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504. MR 2551763
- [KW09b] ———, *Serre’s modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586. MR 2551764
- [LMF16] The LMFDB Collaboration, *The L-functions and modular forms database*, <http://www.lmfdb.org>, 2016.
- [LR10] Nik Lygeros and Olivier Rozier, *A new solution to the equation  $\tau(p) \equiv 0 \pmod{p}$* , J. Integer Seq. **13** (2010), no. 7, Article 10.7.4, 11. MR 2669385
- [Mal88] Gunter Malle, *Polynomials with Galois groups  $\text{Aut}(M_{22})$ ,  $M_{22}$ , and  $\text{PSL}_3(\mathbb{F}_4) \cdot 2_2$  over  $\mathbb{Q}$* , Math. Comp. **51** (1988), no. 184, 761–768. MR 958642
- [Mas13] Nicolas Mascot, *Computing modular Galois representations*, Rend. Circ. Mat. Palermo (2) **62** (2013), no. 3, 451–476. MR 3118315
- [Mas16] ———, *Companion forms and explicit computation of  $PGL_2$  number fields with very little ramification*, Arxiv:1116.01464, 2016.
- [Odl90] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sémin. Théor. Nombres Bordeaux (2) **2** (1990), no. 1, 119–141. MR MR1061762 (91i:11154)
- [PAR13] The PARI Group, Bordeaux, *Pari/gp, version 2.6.2*, 2013.
- [Res16] Wolfram Research, *Mathematica 11.0*, 2016.
- [Rob16a] David P. Roberts, *Lightly ramified number fields with Galois group  $S.M_{12}.A$* , J. de Théorie des Nombres de Bordeaux **28** (2016), no. 2, 435–460. MR 3509719
- [Rob16b] ———, *Newforms with rational coefficients*, To appear in Ramanujan J., arxiv:1611.06967, 2016.
- [Sch15] George J. Schaeffer, *Hecke stability and weight 1 modular forms*, Math. Z. **281** (2015), no. 1-2, 159–191. MR 3384865

- [SD75] H. P. F. Swinnerton Dyer, *On  $l$ -adic representations and congruences for coefficients of modular forms. congruences for coefficients of modular forms*, Modular functions of one variable, III, Springer, Berlin, 1975, pp. 149. Lecture Notes in Math., Vol. 476. MR 0406932
- [Ser87] Jean-Pierre Serre, *Sur les représentations modulaires de degré 2 de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$* , Duke Math. J. **54** (1987), no. 1, 179–230. MR 885783
- [Ste07] William Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007, With an appendix by Paul E. Gunnells. MR 2289048

DIVISION OF SCIENCE AND MATHEMATICS, UNIVERSITY OF MINNESOTA-MORRIS, MORRIS, MN 56267

*E-mail address:* `roberts@morris.umn.edu`