Explicit computations with modular Galois representations

Bosman, J.G.

Chapter 4

Some polynomials for level one forms

The contents of this chapter will appear in the final version of the manuscript [28] that will eventually be published as a volume of the Annals of Mathematics Studies.

4.1 Introduction

In this chapter we explicitly compute mod ℓ Galois representations associated to modular forms. To be precise, we look at cases with $\ell \leq 23$ and the modular forms considered will be cusp forms of level 1 and weight up to 22. We present the result in terms of polynomials associated to the projectivised representations. As an application, we will improve a known result on Lehmer's non-vanishing conjecture for Ramanujan's tau function (see [47, p. 429]) .

To fix a notation, for any $k \in \mathbb{Z}$ satisfying $\dim S_k(\mathrm{SL}_2(\mathbb{Z})) = 1$ we will denote the unique normalised cusp form in $S_k(\mathrm{SL}_2(\mathbb{Z}))$ by Δ_k. We will denote the coefficients of the q-expansion of Δ_k by $\tau_k(n)$:

$$\Delta_k(z) = \sum_{n \geq 1} \tau_k(n) q^n \in S_k(\mathrm{SL}_2(\mathbb{Z})).$$

From $\dim S_k(\mathrm{SL}_2(\mathbb{Z})) = 1$ it follows that the numbers $\tau_k(n)$ are integers. For every Δ_k and every prime ℓ there is a continuous representation

$$\rho_{\Delta_k,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

such that for every prime $p \neq \ell$ we have that the characteristic polynomial of $\rho_{\Delta_k,\ell}(\mathrm{Frob}_p)$ is congruent to $X^2 - \tau_k(p)X + p^{k-1}$ mod ℓ. For a summary on the exceptional representations $\rho_{\Delta_k,\ell}$ and the corresponding congruences for $\tau_k(n)$, see [83].

4.1.1 Notational conventions

Throughout this chapter, for every field K we will fix an algebraic closure $\overline{K}$ and all algebraic extension fields of K will be regarded as subfields of $\overline{K}$. Furthermore, for each prime number p we will fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and hence an embedding $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

whose image we call D_p. We will use I_p to denote the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

For any field K, a linear representation $\rho : G \to \mathrm{GL}_n(K)$ defines a projective representation $\tilde{\rho} : G \to \mathrm{PGL}_n(K)$ via the canonical map $\mathrm{GL}_n(K) \to \mathrm{PGL}_n(K)$. We say that a projective representation $\tilde{\rho} : G \to \mathrm{PGL}_n(K)$ is *irreducible* if the induced action of G on $\mathbb{P}^{n-1}(K)$ fixes no proper subspace. So for $n = 2$ this means that every point of $\mathbb{P}^1(K)$ has its stabiliser subgroup not equal to G. Representations are assumed to be continuous.

4.1.2 Statement of results

Theorem 4.1. *For every pair (k,ℓ) occurring in Table 4.1 on page 87, let the polynomial $P_{k,\ell}$ be defined as in that same table. Then the splitting field of each $P_{k,\ell}$ is the fixed field of* $\mathrm{Ker}(\tilde{\rho}_{\Delta_k,\ell})$ *and has Galois group* $\mathrm{PGL}_2(\mathbb{F}_\ell)$. *Furthermore, if $\alpha \in \overline{\mathbb{Q}}$ is a root of $P_{k,\ell}$ then the subgroup of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *fixing α corresponds via $\tilde{\rho}_{\Delta_k,\ell}$ to a subgroup of* $\mathrm{PGL}_2(\mathbb{F}_\ell)$ *fixing a point of* $\mathbb{P}^1(\mathbb{F}_\ell)$.

For completeness we also included the pairs (k,ℓ) for which $\rho_{k,\ell}$ is isomorphic to the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the ℓ-torsion of an elliptic curve. These are the pairs in Table 4.1 with $\ell = k-1$, as there the representation is the ℓ-torsion of $J_0(\ell)$, which happens to be an elliptic curve for $\ell \in \{11,17,19\}$. A simple calculation with division polynomials [46, Chapter II] can be used to treat these cases. In the general case, one has to work in the more complicated Jacobian variety $J_1(\ell)$, which has dimension 12 for $\ell = 23$ for instance.

We can apply Theorem 4.1 to verify the following result.

Corollary 4.1. *The non-vanishing of $\tau(n)$ holds for all*

$$n < 22798241520242687999 \approx 2 \cdot 10^{19}.$$

In [34], the non-vanishing of $\tau(n)$ was verified for all

$$n < 22689242781695999 \approx 2 \cdot 10^{16}.$$

To compute the polynomials, the author used a weakened version of algorithms described elsewhere in this book. After a suggestion of Couveignes, Complex approximations were used. We worked directly in $X_1(\ell)$ rather than $X_1(5\ell)_{\mathbb{Q}(\zeta_\ell)}$ and we guessed the rational coefficients of our polynomials using lattice reduction techniques [49, Proposition 1.39]. instead of computing the height first. Also reduction techniques were used to make the coefficients smaller [16]; after the initial computations some of the polynomials had coefficients of almost 2000 digits. The used algorithms do not give a proven output, so we have to concentrate on the verification. We will show how to verify the correctness of the polynomials in Section 4.3 after setting up some preliminaries about Galois representations in Section 4.2. In Section 4.4 we will point out how to use Theorem 4.1 in a calculation that verifies Corollary 4.1. All the calculations were performed using MAGMA (see [6]).

4.2 Galois representations

This section will be used to state some results on Galois representations that we will need in the proof of Theorem 4.1.

4.2.1 Liftings of projective representations

Let G be a topological group, let K be a topological field and let $\tilde{\rho} : G \to \mathrm{PGL}_n(K)$ be a projective representation. Let L be an extension field of K. By a *lifting* of $\tilde{\rho}$ over L we shall mean a representation $\rho : G \to \mathrm{GL}_n(L)$ that makes the following diagram commute:

$$\begin{array}{ccc} G & \xrightarrow{\tilde{\rho}} & \mathrm{PGL}_n(K) \\ {\scriptstyle\rho}\downarrow & & \downarrow \\ \mathrm{GL}_n(L) & \twoheadrightarrow & \mathrm{PGL}_n(L) \end{array}$$

where the maps on the bottom and the right are the canonical ones. If the field L is not specified then by a lifting of $\tilde{\rho}$ we shall mean a lifting over $\overline{K}$.

An important theorem of Tate arises in the context of liftings. For the proof we refer to [66, Section 6]. Note that in the reference representations over $\mathbb{C}$ are considered, but the proof works for representations over arbitrary algebraically closed fields.

Theorem 4.2 (Tate)**.** *Let K be a field and let $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_n(K)$ be a projective representation. For each prime number p, there exists a lifting $\rho'_p : D_p \to \mathrm{GL}_n(\overline{K})$ of $\tilde{\rho}|_{D_p}$. Assume that these liftings ρ'_p have been chosen so that all but finitely many of them are unramified. Then there is a unique lifting $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{K})$ such that for all primes p we have*

$$\rho|_{I_p} = \rho'_p|_{I_p}.$$

Lemma 4.1. *Let p be a prime number and let K be a field. Suppose that we are given a projective representation $\tilde{\rho}_p : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{PGL}_n(K)$ that is unramified. Then there exists a lifting $\rho_p : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_n(\overline{K})$ of $\tilde{\rho}_p$ that is unramified as well.*

Proof. Since $\tilde{\rho}$ is unramified, it factors through $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$ and is determined by the image of $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. By continuity, this image is an element of $\mathrm{PGL}_n(K)$ of finite order, say of order m. If we take any lift F of $\tilde{\rho}(\mathrm{Frob}_p)$ to $\mathrm{GL}_n(K)$ then we have $F^m = a$ for some $a \in K^\times$. So $F' := \alpha^{-1}F$, where $\alpha \in \overline{K}$ is any m-th root of a, has order m in $\mathrm{GL}_n(\overline{K})$. Hence the homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_n(\overline{K})$ obtained by the composition

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \xrightarrow{\sim} \hat{\mathbb{Z}} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z} \xrightarrow{1\mapsto F'} \mathrm{GL}_n(\overline{K})$$

lifts $\tilde{\rho}$ and is continuous as well as unramified. □

4.2.2 Serre invariants and Serre's conjecture

Let ℓ be a prime. A Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ has a *level* $N(\rho)$ and a *weight* $k(\rho)$. The definitions were introduced by Serre (see [70, Sections 1.2 & 2]). Later on, Edixhoven found an improved definition for the weight, which is the one we will use, see [27, Section 4]. The level $N(\rho)$ is defined as the prime-to-ℓ part of the Artin conductor of ρ and equals 1 if ρ is unramified outside ℓ. The weight is defined in terms of the local representation $\rho|_{D_\ell}$; its definition is rather lengthy so we will not write it out here. When we need results about the weight we will just state them. Let us for now mention that one can consider the weights of the twists $\rho \otimes \chi$ of a representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ by a character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{F}}_\ell^\times$. If one chooses χ so that $k(\rho \otimes \chi)$ is minimal, then we always have $1 \leq k(\rho \otimes \chi) \leq \ell + 1$ and we can in fact choose our χ to be a power of the mod ℓ cyclotomic character.

Serre conjectured [70, Conjecture 3.2.4] that if ρ is irreducible and odd, then ρ belongs to a modular form of level $N(\rho)$ and weight $k(\rho)$. Oddness here means that the image of a complex conjugation has determinant -1. A proof of this conjecture in the case $N(\rho) = 1$ has been published by Khare and Wintenberger:

Theorem 4.3 (Khare & Wintenberger, [38, Theorem 1.1])**.** *Let ℓ be a prime number and let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be an odd irreducible representation of level $N(\rho) = 1$. Then there exists a modular form f of level 1 and weight $k(\rho)$ which is a normalised eigenform and a prime $\lambda \mid \ell$ of K_f such that ρ and $\rho_{f,\lambda}$ become isomorphic after a suitable embedding of $\mathbb{F}_\lambda$ into $\overline{\mathbb{F}}_\ell$.*

4.2.3 Weights and discriminants

If a representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ is wildly ramified at ℓ it is possible to relate the weight to discriminants of certain number fields. In this subsection we will present a theorem of Moon and Taguchi on this matter and derive some results from it that are of use to us.

Theorem 4.4 (Moon & Taguchi, [55, Theorem 3])**.** *Consider a wildly ramified representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$. Let $\alpha \in \mathbb{Z}$ be such that $k(\rho \otimes \chi_\ell^{-\alpha})$ is minimal where $\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{F}_\ell^\times$ is the mod ℓ cyclotomic character. Put $\tilde{k} = k(\rho \otimes \chi_\ell^{-\alpha})$, put $d = \gcd(\alpha, \tilde{k}-1, \ell-1)$ and put $K = \overline{\mathbb{Q}}_\ell^{\mathrm{Ker}(\rho)}$. Define $m \in \mathbb{Z}$ by letting ℓ^m be the wild ramification degree of K over $\mathbb{Q}_\ell$. Then we have*

$$v_\ell(\mathscr{D}_{K/\mathbb{Q}_\ell}) = \begin{cases} 1 + \frac{\tilde{k}-1}{\ell-1} - \frac{\tilde{k}-1+d}{(\ell-1)\ell^m} & \text{if } 2 \leq \tilde{k} \leq \ell, \\ 2 + \frac{1}{(\ell-1)\ell} - \frac{2}{(\ell-1)\ell^m} & \text{if } \tilde{k} = \ell+1, \end{cases}$$

where $\mathscr{D}_{K/\mathbb{Q}_\ell}$ denotes the different of K over $\mathbb{Q}_\ell$ and v_ℓ is normalised by $v_\ell(\ell) = 1$.

We can simplify this formula to one which is useful in our case. In the proof of the following corollaries, v_ℓ denotes a valuation at a prime above ℓ normalised by $v_\ell(\ell) = 1$.

Corollary 4.2. *Let $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ be an irreducible projective representation that is wildly ramified at ℓ. Take a point in $\mathbb{P}^1(\mathbb{F}_\ell)$, let $H \subset \mathrm{PGL}_2(\mathbb{F}_\ell)$ be its stabiliser subgroup and let K be the number field defined as*

$$K = \overline{\mathbb{Q}}^{\tilde{\rho}^{-1}(H)}.$$

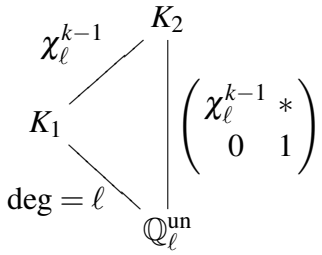
Then the ℓ-primary part of $\mathrm{Disc}(K/\mathbb{Q})$ is related to the minimal weight k of the liftings of $\tilde{\rho}$ by the following formula:

$$v_\ell(\mathrm{Disc}(K/\mathbb{Q})) = k + \ell - 2.$$

Proof. Let ρ be a lifting of $\tilde{\rho}$ of minimal weight. Since ρ is wildly ramified, after a suitable conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ we may assume

$$\rho|_{I_\ell} = \begin{pmatrix} \chi_\ell^{k-1} & * \\ 0 & 1 \end{pmatrix}, \tag{4.1}$$

where $\chi_\ell : I_\ell \to \mathbb{F}_\ell^\times$ denotes the mod ℓ cyclotomic character; this follows from the definition of weight. The canonical map $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell) \to \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ is injective on the subgroup $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$, so the subfields of $\overline{\mathbb{Q}}_\ell$ cut out by $\rho|_{I_\ell}$ and $\tilde{\rho}|_{I_\ell}$ are equal, call them K_2. Also, let $K_1 \subset K_2$ be the fixed field of the diagonal matrices in $\mathrm{Im}\,\rho|_{I_\ell}$. We see from (4.1) that in the notation of Theorem 4.4 we can put $\alpha = 0$, $m = 1$ and $d = \gcd(\ell - 1, k - 1)$. So we have the following diagram of field extensions:



The extension K_2/K_1 is tamely ramified of degree $(\ell-1)/d$ hence we have

$$v_\ell(\mathscr{D}_{K_2/K_1}) = \frac{(\ell-1)/d - 1}{(\ell-1)\ell/d} = \frac{\ell - 1 - d}{(\ell-1)\ell}.$$

Consulting Theorem 4.4 for the case $2 \le k \le \ell$ now yields

$$\begin{aligned} v_\ell(\mathscr{D}_{K_1/\mathbb{Q}_\ell^{\mathrm{un}}}) &= v_\ell(\mathscr{D}_{K_2/\mathbb{Q}_\ell^{\mathrm{un}}}) - v_\ell(\mathscr{D}_{K_2/K_1}) \\ &= 1 + \frac{k-1}{\ell-1} - \frac{k-1+d}{(\ell-1)\ell} - \frac{\ell-1-d}{(\ell-1)\ell} = \frac{k+\ell-2}{\ell} \end{aligned}$$

and also in the case $k = \ell + 1$ we get

$$v_\ell(\mathscr{D}_{K_1/\mathbb{Q}_\ell^{\mathrm{un}}}) = 2 + \frac{1}{(\ell-1)\ell} - \frac{2}{(\ell-1)\ell} - \frac{\ell-2}{(\ell-1)\ell} = \frac{k+\ell-2}{\ell}.$$

Let L be the number field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\tilde{\rho})}$. From the irreducibility of $\tilde{\rho}$ and the fact that $\mathrm{Im}\,\tilde{\rho}$ has an element of order ℓ it follows that the induced action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathbb{P}^1(\mathbb{F}_\ell)$ is transitive

and hence that L is the normal closure of K in $\overline{\mathbb{Q}}$. This in particular implies that $K/\mathbb{Q}$ is wildly ramified. Now from $[K:\mathbb{Q}] = \ell+1$ it follows that there are two primes in K above ℓ: one is unramified and the other has inertia degree 1 and ramification degree ℓ. From the considerations above it now follows that any ramification subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ at ℓ is isomorphic to a subgroup of $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right) \subset \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ of order $(\ell-1)\ell/d$ with $d \mid \ell-1$. Up to conjugacy, the only subgroup of index ℓ is the subgroup of diagonal matrices. Hence K_1 and $K_{\lambda_2}^{\mathrm{un}}$ are isomorphic field extensions of $\mathbb{Q}_\ell^{\mathrm{un}}$, from which

$$v_\ell(\mathrm{Disc}(K/\mathbb{Q})) = v_\ell(\mathrm{Disc}(K_1/\mathbb{Q}_\ell^{\mathrm{un}})) = \ell \cdot v_\ell(\mathscr{D}_{K_1/\mathbb{Q}_\ell^{\mathrm{un}}}) = k+\ell-2.$$

follows. □

Corollary 4.3. *Let $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ be an irreducible projective representation and let ρ be a lifting of $\tilde{\rho}$ of minimal weight. Let K be the number field belonging to a point of $\mathbb{P}^1(\mathbb{F}_\ell)$, as in the notation of Corollary 4.2. If $k \geq 3$ is such that*

$$v_\ell(\mathrm{Disc}(K/\mathbb{Q})) = k+\ell-2$$

holds, then we have $k(\rho) = k$.

Proof. From $v_\ell(\mathrm{Disc}(K/\mathbb{Q})) = k+\ell-2 \geq \ell+1$ it follows that $\tilde{\rho}$ is wildly ramified at ℓ so we can apply Corollary 4.2. □

4.3 Proof of the theorem

To prove Theorem 4.1 we need to do several verifications. We will derive representations from the polynomials $P_{k,\ell}$ and verify that they satisfy the conditions of Theorem 4.3. Then we know there are modular forms attached to them that have the right level and weight and uniqueness follows then easily.

First we we will verify that the polynomials $P_{k,\ell}$ from Table 4.1 have the right Galois group. The algorithm described in [29, Algorithm 6.1] can be used perfectly to do this verification; proving $A_{\ell+1} \not\leq \mathrm{Gal}(P_{k,\ell})$ is the most time-consuming part of the calculation here. It turns out that in all cases we have

$$\mathrm{Gal}(P_{k,\ell}) \cong \mathrm{PGL}_2(\mathbb{F}_\ell). \tag{4.2}$$

That the action of $\mathrm{Gal}(P_{k,\ell})$ on the roots of $P_{k,\ell}$ is compatible with the action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ follows from the following well-known lemma:

Lemma 4.2. *Let ℓ be a prime and let G be a subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ of index $\ell+1$. Then G is the stabiliser subgroup of a point in $\mathbb{P}^1(\mathbb{F}_\ell)$. In particular any transitive permutation representation of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ of degree $\ell+1$ is isomorphic to the standard action on $\mathbb{P}^1(\mathbb{F}_\ell)$.*

Proof. This follows from [82, Proof of Theorem 6.25]. □

So now we have shown that the second assertion in Theorem 4.1 follows from the first one.

Next we will verify that we can obtain representations from this that have the right Serre invariants. Let us first note that the group $\mathrm{PGL}_2(\mathbb{F}_\ell)$ has no outer automorphisms. This implies that for every $P_{k,\ell}$, two isomorphisms as in (4.2) define isomorphic representations $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ via composition with the canonical map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(P_{k,\ell})$. In other words, every $P_{k,\ell}$ gives a projective representation $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ that is well-defined up to isomorphism.

Now, for each (k,ℓ) in Table 4.1, the polynomial $P_{k,\ell}$ is irreducible and hence defines a number field

$$K_{k,\ell} := \mathbb{Q}[x]/(P_{k,\ell}),$$

whose ring of integers we will denote by $\mathscr{O}_{k,\ell}$. It is possible to compute $\mathscr{O}_{k,\ell}$ using the algorithm from [11, Section 6] (see also [11, Theorems 1.1 & 1.4]), since we know what kind of ramification behaviour to expect. In all cases it turns out that we have

$$\mathrm{Disc}(K_{k,\ell}/\mathbb{Q}) = (-1)^{(\ell-1)/2}\ell^{k+\ell-2}.$$

We see that for each (k,ℓ) the representation $\tilde{\rho}_{k,\ell}$ is unramified outside ℓ. From Lemma 4.1 it follows that for each $p \neq \ell$, the representation $\tilde{\rho}_{k,\ell}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ has an unramified lifting. Above we saw that via $\tilde{\rho}_{k,\ell}$ the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of roots of $P_{k,\ell}$ is compatible with the action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$, hence we can apply Corollary 4.3 to show that the minimal weight of a lifting of $\tilde{\rho}_{k,\ell}$ equals k. Theorem 4.2 now shows that every $\tilde{\rho}_{k,\ell}$ has a lifting $\rho_{k,\ell}$ that has level 1 and weight k. From $\mathrm{Im}\,\tilde{\rho}_{k,\ell} = \mathrm{PGL}_2(\mathbb{F}_\ell)$ it follows that each $\rho_{k,\ell}$ is absolutely irreducible.

To apply Theorem 4.3 we should still verify that $\rho_{k,\ell}$ is odd. Let (k,ℓ) be given and suppose $\rho_{k,\ell}$ is even. Then a complex conjugation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is sent to a matrix $M \in \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ of determinant 1 and of order 2. Because ℓ is odd, this means $M = \pm 1$ so the image of M in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is the identity. It follows now that $K_{k,\ell}$ is totally real. One could arrive at a contradiction by approximating the roots of $P_{k,\ell}$ to a high precision, but to get a proof one should use only symbolic calculations. The fields $K_{k,\ell}$ with $\ell \equiv 3 \bmod 4$ have negative discriminant hence cannot be totally real. Now suppose that a polynomial $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ has only real roots. Then $a_{n-1}^2 - 2a_{n-2}$, being the sum of the squares of the roots, is non-negative and for a similar reason $a_1^2 - 2a_0a_2$ is non-negative as well. One can verify immediately that each of the polynomials $P_{k,\ell}$ with $\ell \equiv 1 \bmod 4$ fails at least one of these two criteria, hence none of the fields $K_{k,\ell}$ is totally real. This proves the oddness of the representations $\rho_{k,\ell}$. Of course, this can also be checked with more general methods, like considering the trace pairing on $K_{k,\ell}$ or invoking Sturm's theorem [32, Theorem 5.4].

So now that we have verified all the conditions of Theorem 4.3 we remark as a final step that all spaces of modular forms $S_k(\mathrm{SL}_2(\mathbb{Z}))$ involved here are 1-dimensional. So the modularity of each $\rho_{k,\ell}$ implies immediately the isomorphism $\rho_{k,\ell} \cong \rho_{\Delta_k,\ell}$, hence also $\tilde{\rho}_{k,\ell} \cong \tilde{\rho}_{\Delta_k,\ell}$, which completes the proof of Theorem 4.1.

4.4 Proof of the corollary

If τ vanishes somewhere, then the smallest positive integer n for which $\tau(n)$ is zero is a prime (see [47, Theorem 2]). Using results on the exceptional representations for $\tau(p)$, Serre pointed out [68, Section 3.3] that if p is a prime number with $\tau(p) = 0$ then p can be written as

$$p = hM - 1$$

with

$$M = 2^{14}3^7 5^3 691 = 3094972416000,$$
$$\left(\frac{h+1}{23}\right) = 1 \quad \text{and} \quad h \equiv 0, 30 \text{ or } 48 \bmod 49.$$

In fact p is of this form if and only if $\tau(p) \equiv 0 \bmod 23 \cdot 49 \cdot M$ holds. Knowing this, we will do a computer search on these primes p and verify whether $\tau(p) \equiv 0 \bmod \ell$ for $\ell \in \{11, 13, 17, 19\}$. To do that we will use the following lemma.

Lemma 4.3. *Let K be a field of characteristic not equal to 2. Then the following conditions on $M \in \mathrm{GL}_2(K)$ are equivalent:*

(1) $\mathrm{tr}\, M = 0$.

(2) For the action of M on $\mathbb{P}^1(K)$, there are 0 or 2 orbits of length 1 and all other orbits have length 2.

(3) The action of M on $\mathbb{P}^1(K)$ has an orbit of length 2.

Proof. We begin with verifying (1)$\Rightarrow$(2). Suppose $\mathrm{tr}\, M = 0$. Matrices of trace 0 in $\mathrm{GL}_2(K)$ have distinct eigenvalues in $\overline{K}$ because of $\mathrm{char}(K) \neq 2$. It follows that two such matrices are conjugate if and only if their characteristic polynomials coincide. Hence M and $M' := \left(\begin{smallmatrix} 0 & 1 \\ -\det M & 0 \end{smallmatrix}\right)$ are conjugate so without loss of generality we assume $M = M'$. Since M^2 is a scalar matrix, all the orbits of M on $\mathbb{P}^1(K)$ have length 1 or 2. If there are at least 3 orbits of length 1 then K^2 itself is an eigenspace of M hence M is scalar, which is not the case. If there is exactly one orbit of length 1 then M has a non-scalar Jordan block in its Jordan decomposition, which contradicts the fact that the eigenvalues are distinct.

The implication (2)$\Rightarrow$(3) is trivial so that leaves proving (3)$\Rightarrow$(1). Suppose that M has an orbit of length 2 in $\mathbb{P}^1(K)$. After a suitable conjugation, we may assume that this orbit is $\{[\binom{1}{0}], [\binom{0}{1}]\}$. But this means that $M \sim \left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right)$ for certain $a, b \in K$ hence $\mathrm{tr}\, M = 0$. □

Combining this lemma with Theorem 4.1 one sees that for $\ell \in \{11, 13, 17, 19\}$ and $p \neq \ell$ we have $\tau(p) \equiv 0 \bmod \ell$ if and only if the prime p decomposes in the number field $\mathbb{Q}[x]/(P_{12,\ell})$ as a product of primes of degree 1 and 2, with degree 2 occurring at least once. For $p \nmid \mathrm{Disc}(P_{12,\ell})$, which is a property that all primes p satisfying Serre's criteria possess, we can verify this condition by checking whether $P_{12,\ell}$ has an irreducible factor of degree 2 over $\mathbb{F}_p$. This can be easily checked by verifying

$$\bar{x}^{p^2} = \bar{x} \quad \text{and} \quad \bar{x}^p \neq \bar{x} \quad \text{in} \quad \mathbb{F}_p[x]/(\overline{P}_{12,\ell}).$$

Having done a computer search, it turns out that the first few primes satisfying Serre's criteria as well as $\tau(p) \equiv 0 \bmod 11 \cdot 13 \cdot 17 \cdot 19$ are

$$2279824152024268799 9,\ 6070719995093606399 9,\ 9343375396490649599 9.$$

Remark. The unpublished paper [34] in which Bruce Jordan and Blair Kelly obtained the previous bound for the verification of Lehmer's conjecture seems to be unfindable. Kevin Buzzard asked me the question what method they could have used. If we weaken the above search to using only the prime $\ell = 11$ we obtain the same bound as Jordan and Kelly did. So our speculation is that they searched for primes p satisfying Serre's criteria as well as $\tau(p) \equiv 0 \bmod 11$. This congruence can be verified using an elliptic curve computation, as was already remarked in Subsection 4.1.2.

4.5 The table of polynomials

In this section we present the table of polynomials that is referred to throughout this chapter.

Table 4.1: Polynomials belonging to projective modular representations

(k,ℓ)	$P_{k,\ell}$
$(12,11)$	$x^{12}-4x^{11}+55x^9-165x^8+264x^7-341x^6+330x^5$ $-165x^4-55x^3+99x^2-41x-111$
$(12,13)$	$x^{14}+7x^{13}+26x^{12}+78x^{11}+169x^{10}+52x^9-702x^8-1248x^7$ $+494x^6+2561x^5+312x^4-2223x^3+169x^2+506x-215$
$(12,17)$	$x^{18}-9x^{17}+51x^{16}-170x^{15}+374x^{14}-578x^{13}+493x^{12}$ $-901x^{11}+578x^{10}-51x^9+986x^8+1105x^7+476x^6+510x^5$ $+119x^4+68x^3+306x^2+273x+76$
$(12,19)$,	$x^{20}-7x^{19}+76x^{17}-38x^{16}-380x^{15}+114x^{14}+1121x^{13}-798x^{12}$ $-1425x^{11}+6517x^{10}+152x^9-19266x^8-11096x^7+16340x^6$ $+37240x^5+30020x^4-17841x^3-47443x^2-31323x-8055$
$(16,17)$	$x^{18}-2x^{17}-17x^{15}+204x^{14}-1904x^{13}+3655x^{12}+5950x^{11}$ $-3672x^{10}-38794x^9+19465x^8+95982x^7-280041x^6-206074x^5$ $+455804x^4+946288x^3-1315239x^2+606768x-378241$
$(16,19)$	$x^{20}+x^{19}+57x^{18}+38x^{17}+950x^{16}+4389x^{15}+20444x^{14}$ $+84018x^{13}+130359x^{12}-4902x^{11}-93252x^{10}+75848x^9$ $-1041219x^8-1219781x^7+3225611x^6+1074203x^5$ $-3129300x^4-2826364x^3+2406692x^2+6555150x-5271039$

Continued on next page

Table 4.1 – continued from previous page

(k,ℓ)	$P_{k,\ell}$
$(16,23)$	$x^{24}+9x^{23}+46x^{22}+115x^{21}-138x^{20}-1886x^{19}+1058x^{18}$ $+59639x^{17}+255599x^{16}+308798x^{15}-1208328x^{14}$ $-6156732x^{13}-10740931x^{12}+2669403x^{11}+52203054x^{10}+106722024x^{9}$ $+60172945x^{8}-158103380x^{7}-397878081x^{6}-357303183x^{5}$ $+41851168x^{4}+438371490x^{3}+484510019x^{2}+252536071x+55431347$
$(18,17)$	$x^{18}-7x^{17}+17x^{16}+17x^{15}-935x^{14}+799x^{13}+9231x^{12}-41463x^{11}$ $+192780x^{10}+291686x^{9}-390014x^{8}+6132223x^{7}-3955645x^{6}+2916112x^{5}$ $+45030739x^{4}-94452714x^{3}+184016925x^{2}-141466230x+113422599$
$(18,19)$	$x^{20}+10x^{19}+57x^{18}+228x^{17}-361x^{16}-3420x^{15}+23446x^{14}+88749x^{13}$ $-333526x^{12}-1138233x^{11}+1629212x^{10}+13416014x^{9}+7667184x^{8}$ $-208954438x^{7}+95548948x^{6}+593881632x^{5}-1508120801x^{4}$ $-1823516526x^{3}+2205335301x^{2}+1251488657x-8632629109$
$(18,23)$	$x^{24}+23x^{22}-69x^{21}-345x^{20}-483x^{19}-6739x^{18}+18262x^{17}$ $+96715x^{16}-349853x^{15}+2196684x^{14}-7507476x^{13}+59547x^{12}$ $+57434887x^{11}-194471417x^{10}+545807411x^{9}+596464566x^{8}$ $-9923877597x^{7}+33911401963x^{6}-92316759105x^{5}+157585411007x^{4}$ $-171471034142x^{3}+237109280887x^{2}-93742087853x+97228856961$
$(20,19)$	$x^{20}-5x^{19}+76x^{18}-247x^{17}+1197x^{16}-8474x^{15}+15561x^{14}-112347x^{13}$ $+325793x^{12}-787322x^{11}+3851661x^{10}-5756183x^{9}+20865344x^{8}$ $-48001353x^{7}+45895165x^{6}-245996344x^{5}+8889264x^{4}$ $-588303992x^{3}-54940704x^{2}-538817408x+31141888$
$(20,23)$	$x^{24}-x^{23}-23x^{22}-184x^{21}-667x^{20}-5543x^{19}-22448x^{18}$ $+96508x^{17}+1855180x^{16}+13281488x^{15}+66851616x^{14}$ $+282546237x^{13}+1087723107x^{12}+3479009049x^{11}+8319918708x^{10}$ $+8576048755x^{9}-19169464149x^{8}-111605931055x^{7}-227855922888x^{6}$ $-193255204370x^{5}+176888550627x^{4}+1139040818642x^{3}$ $+1055509532423x^{2}+1500432519809x+314072259618$
$(22,23)$	$x^{24}-2x^{23}+115x^{22}+23x^{21}+1909x^{20}+22218x^{19}+9223x^{18}+121141x^{17}$ $+1837654x^{16}-800032x^{15}+9856374x^{14}+52362168x^{13}-32040725x^{12}$ $+279370098x^{11}+1464085056x^{10}+1129229689x^{9}+3299556862x^{8}$ $+14586202192x^{7}+29414918270x^{6}+45332850431x^{5}-6437110763x^{4}$ $-111429920358x^{3}-12449542097x^{2}+93960798341x-31890957224$