

ON MODULAR MOD ℓ GALOIS REPRESENTATIONS WITH EXCEPTIONAL IMAGES.

IAN KIMING, HELENA A. VERRILL

ABSTRACT. We give a parametrization of the possible Serre invariants (N, k, ν) of modular mod ℓ Galois representations of the exceptional types A_4 , S_4 , A_5 , in terms of local data attached to the fields cut out by the associated projective representations. We show how this result combined with certain global considerations leads to an effective procedure that will determine for a given eigenform f and prime ℓ whether a mod ℓ representation attached to f is exceptional. We illustrate with numerical examples.

1. INTRODUCTION.

Suppose that f is a eigenform of weight ≥ 2 for some $\Gamma_1(M)$, and let ℓ be a prime number. If λ is a prime of $\overline{\mathbb{Q}}$ above ℓ then by a construction [12] of Deligne followed by reduction mod λ and semisimplification, there is attached to f a mod λ representation $\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_{\ell})$ of the absolute Galois group of \mathbb{Q} . If ρ is irreducible, the classification [16] of finite subgroups of $\mathrm{GL}_2(\overline{\mathbb{F}}_{\ell})$ implies that the image of the projectivisation

$$\mathrm{Proj}(\rho): G_{\mathbb{Q}} \rightarrow \mathrm{PGL}_2(\overline{\mathbb{F}}_{\ell})$$

of ρ is (i) dihedral, (ii) isomorphic to one of the groups A_4 , S_4 , A_5 , or (iii) isomorphic to $\mathrm{PGL}_2(\mathbb{F}_{\ell^n})$ or $\mathrm{PSL}_2(\mathbb{F}_{\ell^n})$ for some n . Thanks to work by Swinnerton-Dyer, Serre, Ribet and Momose, cf. [41], [42], [36], [31], [32], [28], one knows that the cases (i) and (ii) occur for only a finite number of primes ℓ . Also, if we are in case (i) or (ii) for our particular prime λ , then this implies the existence of certain exceptional mod λ congruences for the Fourier coefficients of f . The link to exceptional mod λ congruences is one the the main reasons for interest in determining for the given pair (f, λ) whether ρ has ‘small image’, i.e., whether we are in one of the cases (i) or (ii).

It is thus natural to ask whether we can devise a method that will determine by a finite amount of computation the image of ρ , or at least that of $\mathrm{Proj}(\rho)$. In principle the explicit version of Chebotarev’s theorem [25] provides us with such a method, but it seems impractical to use this since the bounds involved are generally astronomical. Of course, if one expects to be in case (iii), one can hope to quickly notice this by finding — via the Fourier coefficients of f — elements in the image of ρ whose presence imply that case (iii) prevails. This seems to work remarkably well, see for example [17]. On the other hand, since case (i) means that ρ is induced from a 1-dimensional character on G_M for some quadratic M/\mathbb{Q} , it is not hard to see how one can obtain through algebraic number theory combined with [40] a

method that will confirm or deny that case (i) prevails. These considerations may convince us that the cases (ii) — which we refer to as the exceptional cases — are especially problematic to confirm for a given (f, λ) . For example, in the works [41], [42], [36] that deal with classical forms f of level 1, it was precisely the case where $f = Q\Delta$ is the normalized cusp form of weight 16 and level 1, $\ell = 59$ and where $\text{Im Proj}(\rho)$ turns out to be of S_4 -type, that caused the most trouble. This example was finally settled by Haberland in [21] who worked hard with the Fourier coefficients of $Q\Delta$.

The contribution of the present article is the systematic development of the following simple idea: If ρ is of the exceptional type (ii), then $\text{Proj}(\rho)$ cuts out an extension K/\mathbb{Q} with Galois group isomorphic to one of the groups A_4, S_4, A_5 . Then K/\mathbb{Q} gives rise to a *complex* projective Galois representation π (by choosing an embedding $\text{Gal}(K/\mathbb{Q}) \hookrightarrow \text{PGL}_2(\mathbb{C})$) which — in an appropriate sense — may be assumed to yield $\text{Proj}(\rho)$ upon reducing mod λ , cf. the discussion in section 4 below. Then, if we lift π to a linear representation $r: G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{C})$ and make this ℓ -adically integral, ρ is a twist of the mod λ reduction of r . Utilizing then the extensive information — as given in [4], [46], [23] — about the behavior of complex lifts upon twisting, we are able to determine purely in terms of local data attached to the extension K/\mathbb{Q} the (infinitely many) possible Serre invariants (N, k, ν) of representations ρ that cut out K/\mathbb{Q} projectively. Here, and in the following, by ‘Serre invariant’ (N, k, ν) we mean the quantities attached by Serre in [38] to an irreducible mod ℓ representation ρ , with the small modification in connection with the weight k as given in [19]. Combining this with results on Serre’s refined conjecture as given in [33], [14], [19], [8], we can predict the minimal types (N, k, ν) of eigenforms whose attached projective mod ℓ representations cut out a given K/\mathbb{Q} . This is what Theorem 1 below does: It gives a parametrization of these (infinitely many) minimal types (N, k, ν) purely in terms of local data attached to K/\mathbb{Q} .

One remark about the theorem: We discuss only minimal types (N, k, ν) where every prime divisor of N is a ramification point for the given K/\mathbb{Q} ; this is because, as one immediately checks, any other minimal type will then have the shape $(N \cdot m^2, k, \nu \cdot \phi^2)$ where ϕ is a character of conductor m whose prime divisors are all different from ℓ and unramified in K .

The information obtained from Theorem 1 is sufficient to actually prove exceptionality for some particular examples of modular mod ℓ representations. We give some of these immediately in section 3 below. For instance, we are able to quickly reprove Haberland’s result in connection with $Q\Delta$ and $\ell = 59$ without knowing a single Fourier coefficient of the form. Another and somewhat more complicated example concerns the unique normalized cusp form of weight 4 on $\Gamma_0(8)$ and $\ell = 11$. These examples have also been dealt with by Boylan [3] by different methods.

We also discuss an A_5 -type example occurring in Ribet’s paper [34]: Here we are able to immediately confirm — under an suitable modularity condition — a conjecture in that paper.

In section 4 we discuss the above lifting of exceptional projective mod λ representations to complex ones. After that, in the beginning of section 5 we describe first the structure of the proof of Theorem 1 in detail, and then proceed with the actual proof. Finally, in section 6 we show how Theorem 1 can be complemented by certain global considerations to yield an effective general procedure that will decide whether the exceptional case prevails for any explicitly given pair (f, λ) .

Notation. The Galois group of a separable closure of a field k will be denoted G_k .

The symbol ℓ denotes a fixed *odd* prime number, but p may be any prime. We fix a prime λ of $\overline{\mathbb{Q}}$ above ℓ . More generally, if p is any prime it will be convenient to assume that a prime of $\overline{\mathbb{Q}}$ over p has been fixed. Corresponding to this prime over p we have a decomposition subgroup and an inertia subgroup of $G_{\mathbb{Q}}$; the inertia subgroup will be denoted by I_p .

Generally, K/\mathbb{Q} will denote a not totally real extension with Galois group isomorphic to one of the groups A_4 , S_4 , A_5 ; in this situation, l and p will denote primes of K over ℓ and p respectively.

All Galois representations occurring are assumed to cut out a finite extension of the base field in question.

If ρ is a linear or projective representation of $G_{\mathbb{Q}}$, we shall denote by ρ_p the restriction of ρ to the decomposition group in $G_{\mathbb{Q}}$ corresponding to the fixed prime of $\overline{\mathbb{Q}}$ over p . We then view ρ_p as a representation of $G_{\mathbb{Q}_p}$. By the *projective kernel field* of ρ we mean the field fixed by the kernel of ρ if ρ is projective, or the kernel of the projectivisation of ρ if ρ is linear.

The projectivisation of a given linear representation ρ will be denoted by $\text{Proj}(\rho)$.

We denote by U_p the group of units in \mathbb{Z}_p . If ϵ_p is a character of \mathbb{Q}_p , we denote by $c_p(\epsilon_p)$ the *exponent* of the conductor of ϵ_p .

We use (local) class field theory freely and without special notice. Thus for example, if ϵ_p is a character of $G_{\mathbb{Q}_p}$ we may view the restriction of ϵ_p to the inertia subgroup of $G_{\mathbb{Q}_p}$ as a character on U_p .

The symbol χ always denotes the mod ℓ cyclotomic character $\chi: G_{\mathbb{Q}} \longrightarrow \mathbb{F}_{\ell}^{\times}$.

2. STATEMENT OF RESULTS.

Let ℓ be an odd prime, and suppose that K/\mathbb{Q} is a non-real Galois extension with Galois group G isomorphic to one of the groups A_4 , S_4 , A_5 .

Suppose that p is a prime that ramifies in K and that $\phi_p: U_p \rightarrow \mathbb{C}^{\times}$ is a homomorphism.

In section 5.1 we will define a character

$$\epsilon_p = \epsilon(K_p/\mathbb{Q}_p): U_p \longrightarrow \overline{\mathbb{F}}_{\ell}^{\times}$$

depending only on the extension K_p/\mathbb{Q}_p , and also non-negative integers

$$n_p(\phi_p) = n_p(K_p/\mathbb{Q}_p, \phi_p) \quad \text{and} \quad \delta_p(\phi_p) = \delta_p(K_p/\mathbb{Q}_p, \phi_p)$$

that depend on K_p/\mathbb{Q}_p as well as on ϕ_p .

Also, in sections 5.3–5.5 we define a set

$$\mathfrak{W}_{\ell} = \mathfrak{W}(K_l/\mathbb{Q}_{\ell})$$

of natural numbers depending on the extension K_1/\mathbb{Q}_ℓ . The set \mathfrak{W}_ℓ also comes equipped with a partition $\mathfrak{W}_\ell = \mathfrak{W}_\ell^+ \cup \mathfrak{W}_\ell^-$ in case $\ell \neq 5$ and K_1/\mathbb{Q}_ℓ has degree divisible by 5.

In this situation and with these definitions our main result can be formulated as follows.

Theorem 1. *Retaining the above notation, let S denote the product of the finite primes different from ℓ that ramify in K .*

Suppose that N is a natural number whose prime divisors all divide S , that

$$\nu: (\mathbb{Z}/\mathbb{Z}N)^\times \longrightarrow \overline{\mathbb{F}}_\ell^\times$$

is a homomorphism, and that $k \in \{2, \dots, \ell - 1\}$.

(a) Suppose that (N, k, ν) is the triple of Serre invariants of a modular mod λ representation cutting out K/\mathbb{Q} projectively.

Then $k \in \mathfrak{W}_\ell$ and there exists a global character of order prime to ℓ

$$\phi: G_\mathbb{Q} \rightarrow \mathbb{C}^\times$$

unramified outside $S \cdot \infty$, such that

$$N = \prod_{p|S} p^{n_p(\phi|_{I_p}) - \delta_p(\phi|_{I_p})},$$

and such that

$$\nu(r) = \prod_{p|S} \epsilon_p(r)^{-1} \cdot (\phi_p(r)^{-2} \pmod{\lambda}), \quad \text{for } (r, N) = 1.$$

(b) Conversely, suppose that N and ν have the forms as in (a) for some global character ϕ of order prime to ℓ . Assume also that K/\mathbb{Q} is cut out projectively by some (2-dimensional) modular mod λ representation.

Then if either K_1/\mathbb{Q}_ℓ has degree not divisible by 5 or if $\ell = 5$, there exists for any $k \in \mathfrak{W}_\ell$ an eigenform of type (N, k, ν) and with K the projective kernel field of the attached mod λ representation.

If on the other hand, K_1/\mathbb{Q}_ℓ does have degree divisible by 5 and $\ell \neq 5$, there exists a $\mu \in \{+, -\}$ such that: For any $k \in \mathfrak{W}_\ell^\mu$ there exists an eigenform of type (N, k, ν) and with K the projective kernel field of the attached mod λ representation.

For an outline of the proof of the theorem see the beginning of section 5 below.

Remarks: (1) In the theorem, the numbers $n_p(\phi|_{I_p})$ actually depend only on (K_p/\mathbb{Q}_p) and the conductor of ϕ_p except possibly when K_p/\mathbb{Q}_p is cyclic.

(2) The small indeterminacy concerning the weight k in part (b) of the theorem stems from the fact that there are 2 inequivalent embeddings $A_5 \hookrightarrow \text{PGL}_2(\overline{\mathbb{F}}_\ell)$ if $\ell \neq 5$. It is true — in an appropriate sense — that swapping between these 2 embeddings will change the sign μ . The point is however that our proof of the theorem is by purely local means and that the *simultaneous* specification of all of the 3 quantities N , k and ν really requires some sort of global information in

this case. An example of this type of phenomenon can be found in [4], Chap. 6. We shall indicate in section 6 below how the question can be resolved by certain global information in any explicitly given case.

(3) By results of Langlands and Tunnell, cf. [26], [44], the modularity assumption in part (b) of the theorem, i.e., that K/\mathbb{Q} be cut out projectively by some modular mod λ representation, is always true if K/\mathbb{Q} is of type S_4 or A_4 . In case that K/\mathbb{Q} is of A_5 -type, the assumption is not an extremely strong one, as follows from recent progress on the Artin conjecture for odd icosahedral representations of $G_{\mathbb{Q}}$, cf. [6], [43].

One could define a non-real extension K/\mathbb{Q} of one of the types A_4 , S_4 , or A_5 to be modular if it is the projectivisation of the reduction mod λ of the 2-dimensional λ -adic representation attached by Deligne and Serre [13] to an eigenform of weight 1 for some $\Gamma_1(N)$. With this definition it would not be hard to show that K/\mathbb{Q} is modular if and only if K/\mathbb{Q} is cut out by *some* modular mod λ representation if and only if *any* mod λ representation cutting out K/\mathbb{Q} projectively is modular (for this one needs the results of [19], and in case that K/\mathbb{Q} is of A_5 -type and $\ell \neq 5$ where we have 2 inequivalent embeddings $A_5 \hookrightarrow \mathrm{PGL}_2(\overline{\mathbb{F}}_{\ell})$ as mentioned above, the argument requires a small special consideration involving the complex conjugation of modular forms).

(4) It would have been possible to include a discussion of non-optimal levels ([15] and [5]). Also, we could have discussed weights outside the interval $2 \leq k \leq \ell - 1$; the main purpose for restricting to this interval is to exclude the case where the weight of the mod ℓ representation is 1. This case would occur if the given extension K/\mathbb{Q} was unramified over ℓ which is a rather uninteresting situation in the context of the present paper. Of course, for a general modular mod ℓ representation the natural interval of weights to discuss is the full range $1 \leq k \leq \ell + 1$; however, for representations of the exceptional types studied in this paper, restricting to the interval $2 \leq k \leq \ell - 1$ causes only a small inconvenience in the very special case that $\ell = 3$ and K/\mathbb{Q}_{ℓ} is totally ramified dihedral of order 6, in which case the weight $k = 4$ may occur ‘naturally’. See the proof of part (b) of the Theorem for more details.

Finally, one should notice that the proof of the theorem obviously enables one to actually count the number of modular mod ℓ representations with a given triple of Serre invariants (N, k, ν) (of course under the appropriate modularity assumption in the A_5 -case and with the minor indeterminacy of part (b)).

These possible extensions of Theorem 1 have been discarded mainly in order to prevent overloading in the statement of the theorem.

3. EXAMPLES.

In this section we give a few simple examples of the use of Theorem 1 in connection with questions about the image of modular mod ℓ representations.

3.1. An interesting class of S_4 -type representations arises in connecting with non-real S_4 -extensions K/\mathbb{Q} where K/\mathbb{Q}_{ℓ} is dihedral of order 8. In that case, we must have $\ell \equiv 3 \pmod{4}$ as there are no dihedral extensions of \mathbb{Q}_{ℓ} of order 8 if $\ell \equiv 1 \pmod{4}$.

(4). Certainly, the extension K/\mathbb{Q} is cut out projectively by some modular mod λ representation: Embedding $\text{Gal}(K/\mathbb{Q}) \hookrightarrow \text{PGL}_2(\mathbb{C})$ and lifting this to a linear representation, which is possible by a theorem of Tate, cf. [37], results of Langlands and Tunnell, [26], [44], imply that K/\mathbb{Q} is cut out projectively by the complex representation attached to a modular form of weight 1. Making this representation λ -adically integral and reducing mod λ proves the claim.

Now, the definition of \mathfrak{W}_ℓ in this case is:

$$\mathfrak{W}_\ell := \left\{ \frac{\ell+5}{4}, \frac{3\ell+7}{4} \right\},$$

cf. section 5.3.4 below. Part (b) of Theorem 1 then informs us that there are exceptional modular mod λ representations with K/\mathbb{Q} the projective kernel field for any of the weights $k \in \mathfrak{W}_\ell$.

Let us now specialize even further to the case where K/\mathbb{Q} is unramified outside $2 \cdot \ell \cdot \infty$, and is either unramified or of S_4 -type locally above 2. So, if \mathfrak{p}_2 a prime of K over 2 we have either $K_{\mathfrak{p}_2} = \mathbb{Q}_2$, or else — see Weil [45] — $K_{\mathfrak{p}_2}$ is one the the following three extensions M_i/\mathbb{Q}_2 , $i = 2, 3, 4$:

$$M_i := \mathbb{Q}_2(\zeta, \omega, \sqrt{x_i}, \sqrt{\sigma x_i}, \sqrt{\sigma^2 x_i})$$

where ζ is a primitive 3'rd root of unity, $\omega^3 = 2$, σ is the automorphism of $\mathbb{Q}_2(\zeta, \omega)$ given by $\sigma\omega = \zeta\omega$, and $x_2 := (1 + \omega)(1 + \omega^2)(1 + \omega^3)$, $x_3 := (1 + \omega)(1 + \omega^3)$, $x_4 := (1 + \omega^2)$.

We have then the following immediate corollary to Theorem 1.

Corollary 1. *Suppose that $\ell \equiv 3 \pmod{4}$ and that K/\mathbb{Q} is a non-real S_4 -type extension which is unramified outside $2 \cdot \ell \cdot \infty$, and such that K_1/\mathbb{Q}_ℓ is the unique dihedral extension of order 8 of \mathbb{Q}_ℓ . Suppose further that K is either unramified or of S_4 -type locally above 2. Let \mathfrak{p}_2 a prime of K over 2.*

Let $\phi: \mathbb{Z}/\mathbb{Z}2^c \rightarrow \mathbb{C}^\times$ be a Dirichlet character of conductor 2^c , and define the non-negative integer n and the character $\epsilon: U_2 \rightarrow \overline{\mathbb{F}}_\ell^\times$ as follows:

$$\left\{ \begin{array}{lll} \epsilon = 1 & \text{and} & n = 2c & \text{if } K_{\mathfrak{p}_2} = \mathbb{Q}_2, \\ \epsilon(-1) = -1, \epsilon(5) = 1 & \text{and} & \left\{ \begin{array}{ll} n = 7 & \text{if } c \leq 3 \\ n = 2c & \text{if } c \geq 4 \end{array} \right\} & \text{if } K_{\mathfrak{p}_2} = M_2, \\ \epsilon = 1 & \text{and} & \left\{ \begin{array}{ll} n = 7 & \text{if } c \leq 3 \\ n = 2c & \text{if } c \geq 4 \end{array} \right\} & \text{if } K_{\mathfrak{p}_2} = M_3, \\ \epsilon = 1 & \text{and} & \left\{ \begin{array}{ll} n = 3 & \text{if } c \leq 1 \\ n = 2c & \text{if } c \geq 2 \end{array} \right\} & \text{if } K_{\mathfrak{p}_2} = M_4. \end{array} \right.$$

Then for each of the weights $k = \frac{\ell+5}{4}, \frac{3\ell+7}{4}$, there exists a mod λ eigenform whose attached mod λ representation cuts out the extension K/\mathbb{Q} projectively, and which has type $(2^n, k, \nu)$ with ν given by:

$$\nu(r) = \epsilon(r)^{-1} \cdot (\phi(r)^{-2} \pmod{\lambda}), \quad \text{for odd } r.$$

Proof. The result follows immediately from Theorem 1 once one reviews for this particular case the definitions, in section 5.1.3, 5.2, and 5.3.4 below, of the numbers $n_2(\phi|_{I_2})$ and $\delta_2(\phi|_{I_2})$, of the character $\epsilon = \epsilon_2: U_2 \rightarrow \overline{\mathbb{F}}_\ell^\times$, and of the set \mathcal{W}_ℓ . \square

3.1.1. Suppose additionally that K/\mathbb{Q} is unramified outside $\ell \cdot \infty$. In [18] such fields were studied using other methods than ours and under an additional condition on ℓ made to ensure the solvability of a certain embedding problem associated with lifting $G_\mathbb{Q} \twoheadrightarrow \text{Gal}(K/\mathbb{Q}) \hookrightarrow \text{PGL}_2(\mathbb{C})$ to a linear representation. By solving explicitly this embedding problem and studying the behavior of the solution locally at ℓ the author of that paper was able to find the connection to cusp forms of weight $\frac{\ell+5}{4}$. Here we proceed without any further assumptions than those already made on K and conclude from Theorem 1 that there are modular mod ℓ representations of level 1 and the above weights with K the associated projective kernel field. The classical example of this phenomenon concerns the unique cusp form $Q\Delta$ of level 1 and weight 16 in connection with $\ell = 59$. This case was first considered by Swinnerton–Dyer in [41] who found strong reasons to believe that the mod 59 representation attached to $Q\Delta$ is exceptional of type S_4 . This was then subsequently proved in [21] by Haberland who — having less powerful theorems at his disposal than we do — worked hard numerically with the Fourier expansion of $Q\Delta$. We can reprove the statement easily and without knowing any Fourier coefficients: One knows (cf. [21]) that there is a unique S_4 -extension of \mathbb{Q} unramified outside 59 and ∞ . In fact, the splitting field K of the polynomial

$$x^4 - x^3 - 7x^2 + 11x + 3$$

is seen to be such a field. It is non-real, and dihedral of order 8 over 59. Theorem 1 implies the existence of modular mod 59 representations of level 1 and weights $\frac{59+5}{4} = 16$, $\frac{3 \cdot 59 + 7}{4} = 46$ with K as projective kernel field. Since $Q\Delta$ is the unique cusp form of level 1 and weight 16, the claim follows.

3.1.2. A somewhat more complicated example occurs in connection with the mod 11 representation ρ attached to the unique cusp form $\eta(2z)^4 \cdot \eta(4z)^4$ of weight 4 on $\Gamma_0(8)$ where $\eta(z)$ is the Dedekind eta function:

$$\eta(z) = e^{2\pi iz/24} \prod_{n=1}^{\infty} (1 - e^{2\pi inz}).$$

Numerical experiments performed by the second author suggested strongly that ρ is exceptional of S_4 -type; verifying this was one of the initial starting points of the present article. If we wish to verify this via Theorem 1 we must begin by looking for a candidate K/\mathbb{Q} for the corresponding projective kernel field. Thus, K/\mathbb{Q} should be a non-real S_4 -extension unramified outside $2 \cdot 11 \cdot \infty$. By class field theory one finds that the unique S_3 -subextension L/\mathbb{Q} contained in K/\mathbb{Q} would have to be the splitting field of

$$x^3 - x^2 - x - 1,$$

which is in fact an S_3 -extension of \mathbb{Q} unramified outside $2 \cdot 11 \cdot \infty$. Now we have to look for an embedding of this L/\mathbb{Q} in an S_4 -extension K/\mathbb{Q} of the desired type. It turns out that there is more than one such K/\mathbb{Q} but we shall focus on the one

that is relevant for our example. We seek to find the candidate K/\mathbb{Q} by utilizing the method of [2]:

Consider the elliptic curve $-22y^2 = x^3 - x^2 - x - 1$ which has minimal Weierstrass model

$$E: y^2 = x^3 + x^2 - 645x + 14771 .$$

The curve E has good reduction outside $2 \cdot 11$, and has the rational point

$$P = (-26, 121) \in E(\mathbb{Q}) \setminus 2 \cdot E(\mathbb{Q}) .$$

According to [2], the field generated over \mathbb{Q} by the x -coordinates of points $Q \in E(\overline{\mathbb{Q}})$ with $2 \cdot Q = P$ is a (non-real) S_4 -extension K/\mathbb{Q} unramified outside $2 \cdot 11 \cdot \infty$. Using the 2-division polynomial for E we find that this K is the splitting field of the polynomial

$$x^4 + 104x^3 + 1394x^2 - 185248x + 1893125 .$$

Applying to this polynomial the function `polred` in PARI, cf. [29], we find that K can also be given as the splitting field of

$$x^4 - 2x^3 - 4x^2 + 16x - 13 .$$

One can then verify directly that K/\mathbb{Q} is indeed a non-real S_4 -extension unramified outside $2 \cdot 11 \cdot \infty$, that the local extension over 11 is the unique D_4 -extension of \mathbb{Q}_{11} , and finally that the local extension over 2 is the S_4 -extension that was denoted M_4 in [23] and in 3.1 above. Thus, Corollary 1 applies and gives the existence of an exceptional S_4 -type modular mod 11 representation of level 8, weight 4 and trivial nebentypus, which must then be our representation ρ .

Similarly, one can show that the mod 19 representation attached to the unique cusp form $\eta(2z)^{12}$ of weight 6 on $\Gamma_0(4)$ is exceptional of S_4 -type with projective kernel field the splitting field of

$$x^4 - x^3 - 2x^2 - 6x - 2 .$$

3.2. An interesting A_5 -type example occurs in Ribet's paper [34], p. 284: There are exactly 2 newforms of weight 2 on $\Gamma_0(23)$; call them f_1, f_2 . The example concerns the mod 3 representations ρ_i attached to f_i . Arguments given *loc. cit.*, suggested that each of the representations ρ_i is of A_5 -type, and in fact with projective kernel field the A_5 -extension of \mathbb{Q} given as the splitting field K of the polynomial

$$(*) \quad x^5 + 3x^3 + 6x^2 + 9 .$$

It was further stated *loc. cit.*, that computations performed by Mestre were consistent with this claim. We shall show here how Theorem 1 immediately implies this statement under the assumption of modularity of a 2-dimensional complex representation associated with K .

The polynomial $(*)$ occurs as the second entry of the table in [1], and if we choose an embedding $A_5 \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$ we obtain a complex, odd A_5 -type representation ρ of conductor $3^3 \cdot 23^2$. It should be fairly clear that a rigorous verification of the above statement about the ρ_i must involve either a proof of the Artin conjecture of this complex ρ or else the application of some form of explicit Chebotarev. The

authors have not considered how to practically implement the second option. Concerning the first, let us remark that the results of the papers [6] and [43] do not suffice to prove the Artin conjecture for ρ (in K , a Frobenius over 2 has order 5, and 3 is totally ramified of degree 6). Furthermore, an attempt at a direct computational verification of Artin's conjecture for this ρ utilizing methods similar to those employed in [24], can be estimated to lead to an intractably large computation. Thus, we shall be content with giving a relative statement: Assuming the weight 1 modularity for this particular ρ , the ρ_i are both of A_5 -type with projective kernel field the above K . This is readily done: Denoting by \mathfrak{p}_{23} and \mathfrak{p}_3 primes of K over 23 and 3 respectively, one finds that $K_{\mathfrak{p}_{23}}/\mathbb{Q}_{23}$ is the unique dihedral extension of degree 6 of \mathbb{Q}_{23} , and that $K_{\mathfrak{p}_3}/\mathbb{Q}_3$ is totally ramified dihedral of degree 6. One checks that the latter extension is *peu ramifié*: An easy calculation shows that *peu* and *très ramifié* implies the contribution 3^4 and 3^6 respectively to the discriminant of a quintic subfield of K (cf. also Table 3.1 of [4]); as this discriminant is in fact $3^4 \cdot 23^2$ ([1], Table 1), $K_{\mathfrak{p}_3}/\mathbb{Q}_3$ is *peu ramifié*.

The recipes in section 5 then give: $n_{23}(1) = 1$, $\epsilon_{23} = 1$, and $\mathfrak{W}_3 = \{2\}$. Under the above weight 1 modularity assumption Theorem 1 thus implies the existence of a modular mod 3 representation ρ of level 23, weight 2 and trivial character that cuts out this K/\mathbb{Q} projectively. On the other hand, choosing the other embedding $A_5 \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$, we obtain similarly another modular mod 3 representation which is not equivalent to ρ but has the same level, weight and character. As $S_2(\Gamma_0(23))$ has dimension 2, the desired conclusions about the ρ_i follow.

4. LIFTING EXCEPTIONAL MOD ℓ REPRESENTATIONS TO COMPLEX REPRESENTATIONS.

In this section we prove some simple statements about lifting mod ℓ representations to complex ones. Everything in this section is probably fairly standard knowledge but we have included it for lack of appropriate references.

Though we need only the case $n = 2$, we start by discussing the more general case of n -dimensional representations as this causes no extra work.

Given an irreducible Galois representation $\pi: G_{\mathbb{Q}} \rightarrow \mathrm{PGL}_n(\mathbb{C})$ with finite image, by the reduction mod λ of π we mean the representation $\mathrm{Proj}(\bar{\pi}): G_{\mathbb{Q}} \rightarrow \mathrm{PGL}_n(\overline{\mathbb{F}}_{\ell})$ constructed as follows:

Let $r: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(\mathbb{C})$ be a lift of π , i.e., a representation which has projectivisation equal to π . By a theorem of Tate (cf. [37]) such a lift r does exist. We may consider r as a representation $r: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}})$. Denote by $\overline{\mathbb{Z}}$ the ring of integers of $\overline{\mathbb{Q}}$. Since every finitely generated ideal of $\overline{\mathbb{Z}}$ is principal, we can conjugate r to a representation $G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(\overline{\mathbb{Z}})$ which by abuse of notation we still denote by r . Now let \bar{r} be the mod λ reduction of r , and consider the projectivisation $\mathrm{Proj}(\bar{r}): G_{\mathbb{Q}} \rightarrow \mathrm{PGL}_n(\overline{\mathbb{F}}_{\ell})$ of \bar{r} . One easily checks that $\mathrm{Proj}(\bar{r})$ is independent up to equivalence of the various choices made. We refer then to $\mathrm{Proj}(\bar{r})$ as the mod λ reduction of π . For clarity, the four representations π , r , \bar{r} , and $\mathrm{Proj}(\bar{r})$ are shown

in the following diagram:

$$\begin{array}{ccccc}
 & & G_{\mathbb{Q}} & & \\
 & \swarrow r & & \searrow \pi & \\
 & \text{GL}_n(\overline{\mathbb{Z}}) & & & \text{PGL}_n(\overline{\mathbb{Z}}) \\
 & \downarrow & \nearrow \bar{r} & \text{Proj}(\bar{r}) & \downarrow \\
 & \text{GL}_n(\overline{\mathbb{F}}_{\ell}) & \longrightarrow & & \text{PGL}_n(\overline{\mathbb{F}}_{\ell})
 \end{array}$$

Reversing the roles of π and $\text{Proj}(\bar{r})$, if $\Pi: G_{\mathbb{Q}} \rightarrow \text{PGL}_n(\overline{\mathbb{F}}_{\ell})$ is given and assumed to be irreducible, we may ask for a representation $\pi: G_{\mathbb{Q}} \rightarrow \text{PGL}_n(\mathbb{C})$ whose mod λ reduction is the given Π . If such a π exists we may and will then refer to it as a *complex lift* of Π .

Proposition 1. *Let $\Pi: G_{\mathbb{Q}} \rightarrow \text{PGL}_2(\overline{\mathbb{F}}_{\ell})$ be an irreducible representation such that $\text{Im } \Pi$ embeds in $\text{PGL}_2(\mathbb{C})$. Then Π has a complex lift.*

We start the proof of the proposition by an observation that is best isolated as a small lemma:

Lemma 1. *Let $\Pi: G_{\mathbb{Q}} \rightarrow \text{PGL}_n(\overline{\mathbb{F}}_{\ell})$ be an irreducible representation such that the finite group $\text{Im } \Pi$ embeds in $\text{PGL}_n(\mathbb{C})$, and is ℓ -solvable. Then Π has a complex lift.*

Proof. Let us first notice that we have

$$H^2(G_{\mathbb{Q}}, \overline{\mathbb{F}}_{\ell}^{\times}) = 0,$$

where the action of $G_{\mathbb{Q}}$ on $\overline{\mathbb{F}}_{\ell}^{\times}$ is trivial. This is because we have

$$\overline{\mathbb{F}}_{\ell}^{\times} \cong \prod_{p \neq \ell} \mathbb{Q}_p / \mathbb{Z}_p,$$

and because we know that

$$H^2(G_{\mathbb{Q}}, \mathbb{Q}_p / \mathbb{Z}_p) = 0,$$

cf. [37], §6.5. Consequently, Π has some lift $\rho: G_{\mathbb{Q}} \rightarrow \text{GL}_2(\overline{\mathbb{F}}_{\ell})$. Now, since $\text{Im } \Pi$ is ℓ -solvable then so is the image of ρ . So we may apply the theorem of Fong–Swan, cf. for example Théorème 3, p. III-19 of [35], to infer that ρ is in fact in the above sense the mod λ reduction of a complex representation r . The projectivisation of any such r is then a complex lift of Π . \square

Proof of Proposition 1: By the lemma we may assume that $G := \text{Im } \Pi$ is not ℓ -solvable. As G embeds into $\text{PGL}_2(\mathbb{C})$ this implies $G \cong A_5$ and $\ell \in \{3, 5\}$. For these cases we finish the proof by explicitly displaying a lift:

We first choose m large enough so that Π can be realized over \mathbb{F}_{ℓ^m} , and so that \mathbb{F}_{ℓ^m} contains a primitive 5'th root of unity if $\ell \neq 5$, i.e., if $\ell = 3$. Now recall the well-known fact that there is at most one conjugacy class of subgroups isomorphic to G in $\text{PGL}_2(\mathbb{F}_{\ell^m})$; this follows from the discussions in [16], §§258–259.

Consequently, any representation $G_{\mathbb{Q}} \rightarrow \mathrm{PGL}_2(\mathbb{F}_{\ell^m})$ with the same kernel field as Π will — up to equivalence — have the shape $\alpha \circ \Pi$ where α is some automorphism of $G = \mathrm{Im} \Pi \leq \mathrm{PGL}_2(\mathbb{F}_{\ell^m})$. If $\ell = 5$ then α must in fact be conjugation by some element of $\mathrm{PGL}_2(\mathbb{F}_{\ell^m})$, since $G \cong A_5 \cong \mathrm{PSL}_2(\mathbb{F}_5)$ has automorphism group $\mathrm{PGL}_2(\mathbb{F}_5)$ acting via conjugation ([39]). On the other hand, if $\ell = 3$ there are precisely 2 inequivalent embeddings $G \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_{\ell^m})$, as $\mathrm{PGL}_2(\mathbb{F}_{\ell^m})$ will not in this case contain a subgroup isomorphic to $\mathrm{PGL}_2(\mathbb{F}_5)$ (and as $\mathrm{PSL}_2(\mathbb{F}_5)$ has index 2 in $\mathrm{PGL}_2(\mathbb{F}_5)$).

In each of the cases we are considering, we now display an explicit complex lift of a given embedding $G \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_{\ell^m})$. In terms of the presentation $G \cong A_5 = \langle x, y \mid x^2 = y^5 = (xy)^3 = 1 \rangle$, the following assignments define an embedding $G \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_{\ell^m})$:

$$(\sharp) \quad x \mapsto \begin{pmatrix} -c & \omega \\ \omega & c \end{pmatrix}, \quad y \mapsto \begin{pmatrix} \varepsilon^2 & -\omega \\ 0 & \varepsilon^{-2} \end{pmatrix},$$

where $\omega := \varepsilon + \varepsilon^{-1}$, $c := \varepsilon^2 - \varepsilon^{-2}$, and where ε is a primitive 5'th root of unity if $\ell = 3$, but $\varepsilon = 1$ if $\ell = 5$. For $\ell = 3$ the substitution $\varepsilon \mapsto \varepsilon^2$ brings one embedding to the other inequivalent one. Viewing the matrices in (\sharp) as elements of $\mathrm{GL}_2(\mathbb{C})$ by interpreting ε as a primitive complex 5'th root of unity, we have explicit complex lifts in all cases. \square

Remark: The authors do not know to what extent Proposition 1 generalizes to higher-dimensional situations. The argument given for $n = 2$ in case $\mathrm{Im} \Pi$ is not ℓ -solvable is admittedly awkward, relying as it does on the classification of subgroups of $\mathrm{PGL}_2(\mathbb{F}_{\ell^m})$. But we have not been able to find a more conceptual approach in this case.

5. PROOF OF THEOREM 1.

In this section we prove Theorem 1. So, let K/\mathbb{Q} , G and S be as in the statement of the Theorem. Definitions of the quantities $n_p(K_p/\mathbb{Q}_p, \phi_p)$ and $\epsilon(K_p/\mathbb{Q}_p)$ will be given in section 5.1 below, and the definition of the set $\mathfrak{W}_\ell(K_1/\mathbb{Q}_\ell)$ is stated in section 5.3.

We start with the proof of part (a). Let

$$\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

be an irreducible modular mod λ representation with Serre invariants (N, k, ν) where $2 \leq k \leq \ell - 1$, every prime divisor of N divides S , and such that the extension cut out by the projectivisation

$$\mathrm{Proj}(\rho): G_{\mathbb{Q}} \rightarrow \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$$

of ρ is the given field K .

Let $\pi: G_{\mathbb{Q}} \rightarrow \mathrm{PGL}_2(\mathbb{C})$ denote a complex lift of $\mathrm{Proj}(\rho)$ in the sense of section 4 (which exists according to Proposition 1).

Now, if $r: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{C})$ is any lift of π to a linear representation unramified outside $S\ell\infty$, and if $\bar{r}: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ is its mod λ reduction, the definition of the notion ‘complex lift’ implies that ρ is a twist of \bar{r} by some character $G_{\mathbb{Q}} \rightarrow \overline{\mathbb{F}}_\ell^\times$; we

may write this character as $\bar{\phi} \cdot \chi^i$ for some $i \in \mathbb{Z}$ and with $\bar{\phi}$ a character unramified at ℓ . In other words, if we make r integral in the sense of the previous section, we have the diagram:

$$\begin{array}{ccccc}
 & & G_{\mathbb{Q}} & & \\
 & \swarrow r & & \searrow \pi & \\
 \mathrm{GL}_2(\overline{\mathbb{Z}}) & & & & \mathrm{PGL}_2(\overline{\mathbb{Z}}) \\
 \downarrow & \searrow \bar{r} & \mathrm{Proj}(\rho) & \searrow & \downarrow \\
 \mathrm{GL}_2(\overline{\mathbb{F}}_{\ell}) & \longrightarrow & & \longrightarrow & \mathrm{PGL}_2(\overline{\mathbb{F}}_{\ell})
 \end{array}$$

where each of the 3 ‘triangles’ commute, and we have

$$\rho = \bar{r} \otimes \bar{\phi} \chi^i .$$

We may and will consider $\bar{\phi}$ as the mod λ reduction of a complex character $\phi: G_{\mathbb{Q}} \rightarrow \mathbb{C}^{\times}$ of order prime to ℓ , and view the restriction $\phi_p := \phi|_{I_p}$ for $p \mid S$ as a homomorphism $U_p \rightarrow \mathbb{C}^{\times}$.

In the following subsection we utilize the results of [23] to show the existence of a *particular* linear lift r as above which is unramified outside $S\ell \cdot \infty$ and has the property that each of the quantities

$$c_p(r \otimes \phi), \quad \text{for } p \mid S ,$$

and

$$\det(r)|_{U_p}, \quad \text{for } p \mid S ,$$

can (and will) be explicitly determined. The first of these quantities depends on the data K_p/\mathbb{Q}_p and ϕ_p , whereas the second depends only on K_p/\mathbb{Q}_p . Call the first of these quantities $n_p(\phi_p) = n_p(K_p/\mathbb{Q}_p, \phi_p)$, and let $\epsilon_p = \epsilon_p(K_p/\mathbb{Q}_p)$ denote the mod λ reduction of the second.

In section 5.2 we compute the number

$$\delta_p(\phi_p) = \delta_p(K_p/\mathbb{Q}_p, \phi_p) := n_p(\phi_p) - c_p(\bar{r} \otimes \bar{\phi})$$

for $p \mid S$, which depends only on the datum $(K_p/\mathbb{Q}_p, \phi_p)$. Then the conductor of $\rho = \bar{r} \otimes \bar{\phi} \chi^i$ is

$$\prod_{p \mid S} p^{n_p(\phi_p) - \delta_p(\phi_p)} ,$$

which by the assumption on ρ coincides with N . Further, for p dividing S , the restriction of the determinant of ρ to I_p is the character $\prod_{p \mid S} \epsilon_p \cdot (\phi_p^2 \bmod \lambda)$ which by definition coincides with $\nu|_{I_p}$ when ν is viewed, via global class field theory, as a character of $G_{\mathbb{Q}}$. As ν is unramified outside $S \cdot \infty$ we have — again by global class field theory — that ν is given by

$$x \mapsto \prod_{p \mid S} \epsilon_p(x)^{-1} \cdot (\phi_p(x)^{-2} \bmod \lambda), \quad \text{for } (x, N) = 1 ,$$

as a character on $(\mathbb{Z}/\mathbb{Z}N)^{\times}$.

In subsection 5.3 we study the local behavior of $\bar{r} \otimes \chi^i$ at ℓ and define the set $\mathfrak{W}_\ell = \mathfrak{W}(K_1/\mathbb{Q}_\ell)$ such that $k \in \mathfrak{W}_\ell$ may be inferred. This will then complete the proof of part (a) of Theorem 1.

5.1. Local lifts: Conductors and determinants. First we use a theorem of Tate, cf. [37], to reduce to a purely local question the problem of specifying a convenient lift r of π to a linear representation: Define the representation $\pi_p: G_{\mathbb{Q}_p} \rightarrow \mathrm{PGL}_2(\mathbb{C})$ as the restriction of π to $G_{\mathbb{Q}_p} \leq G_{\mathbb{Q}}$. Thus π_p factors as

$$\pi_p: G_{\mathbb{Q}_p} \rightarrow \mathrm{Gal}(K_p/\mathbb{Q}_p) \hookrightarrow \mathrm{PGL}_2(\mathbb{C}) .$$

Now, if we choose for each $p \mid S \cdot \ell$ a lift r_p of π_p to a linear representation, the above theorem of Tate states that there is a uniquely determined lift r of π which is unramified outside $S\ell \cdot \infty$ and satisfies:

$$(r)|_{I_p} \cong (r_p)|_{I_p} \quad \text{for } p \mid S\ell .$$

We shall now address the problem of specifying for each p a *particular* choice of r_p with the property that the quantities

$$c_p(r_p \otimes \phi_p) \quad \text{and} \quad \det(r_p)|_{U_p} ,$$

can be explicitly given for any character $\phi_p: U_p \rightarrow \mathbb{C}^\times$. Then

$$c_p(r \otimes \phi) = c_p(r_p \otimes \phi|_{I_p}) ,$$

and

$$\det(r)|_{U_p} = \det(r_p)|_{U_p}$$

are also explicitly known for any global character $\phi: G_{\mathbb{Q}} \rightarrow \mathbb{C}^\times$. This then completes the first step of the proof of Theorem 1 as described above.

The theory of local lifts r_p was initiated by Weil in [45], further developed by Buhler and Zink, cf. [4], [46], and complemented by the results in [23] where a full solution to the problem was given in all cases. Thus, we can simply quote from the latter article and briefly review the results given there. There are 3 subcases corresponding to whether the image of π_p is cyclic, dihedral, or isomorphic to A_4 or S_4 , respectively. Surprisingly, the most difficult of these subcases is the dihedral one. For the following review, let ϕ_p denote an arbitrary character $G_{\mathbb{Q}_p} \rightarrow \mathbb{C}^\times$.

5.1.1. Cyclic cases. This case is trivial: If $\mathrm{Im} \pi_p$ is cyclic then π_p is equivalent to

$$\pi_p \sim \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} : G_{\mathbb{Q}_p} \rightarrow \mathrm{PGL}_2(\mathbb{C}) ,$$

for some character $\alpha: G_{\mathbb{Q}_p} \rightarrow \mathbb{C}^\times$ which we may and will view as a character on \mathbb{Q}_p^\times . We can then choose $r_p \cong \alpha \oplus 1$ which gives

$$n_p(\phi_p) := c_p(r_p \otimes \phi_p) = c_p(\alpha|_{U_p} \cdot \phi_p) + c_p(\phi_p) ,$$

and

$$\epsilon_p := (\alpha|_{U_p} \pmod{\lambda}) .$$

5.1.2. *Dihedral cases.* Suppose that $\text{Im } \pi_p$ is a dihedral group. Then K_p/\mathbb{Q}_p contains a quadratic extension M/\mathbb{Q}_p such that K_p/M is cyclic and ramified. If the degree $[K_p : \mathbb{Q}_p]$ is greater than 4, the field M is uniquely determined. If $[K_p : \mathbb{Q}_p] = 4$ we let M be any quadratic subfield of K_p such that K_p/M is ramified. Let $\alpha: \mathbb{Q}_p^\times \rightarrow \mathbb{C}^\times$ be the quadratic character corresponding to M via local class field theory. Now, the restriction of π_p to G_M has the form

$$\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$$

for some character β on G_M which by local class field theory may and will be viewed as a character on M^\times . In Theorem 1 of [23] a special lift r_p of π_p is given, together with explicit formulas, depending on the data (M, β) , for $\det(r_p)|_{U_p}$ and for $c_p(r_p \otimes \phi_p)$. So, we let

$$\epsilon_p := (\det(r_p)|_{U_p} \pmod{\lambda})$$

and

$$n_p(\phi_p) := c_p(r_p \otimes \phi_p)$$

where r_p is the special lift given loc. cit.; we have then explicit formulas for these quantities, but as these are somewhat involved in the general case we shall not restate them in all detail but will be content to review their general shape and give a few special cases:

Let ω be a uniformizer of M , let $b \geq 1$ be the exponent of the conductor of β (i.e., β has conductor ω^b), and let t denote the break in the sequence of ramification groups of $\mathfrak{G} := \text{Gal}(M/\mathbb{Q}_p)$ in the lower numbering:

$$\mathfrak{G} = \mathfrak{G}_0 = \dots = \mathfrak{G}_t \neq \mathfrak{G}_{t+1} = 0.$$

Then $c_p(r_p \otimes \phi_p)$ is given via:

$$p^{n_p(\phi_p)} = p^{c_p(r_p \otimes \phi_p)} = D(M/\mathbb{Q}_p) \cdot N_{M/\mathbb{Q}_p}(\omega^{\max\{t+b, \gamma(\phi_p)\}}),$$

where $D(\cdot)$ and $N_{M/\mathbb{Q}_p}(\cdot)$ denote discriminant and norm respectively, and where

$$\gamma(\phi_p) \begin{cases} = c_p(\phi_p) & \text{if } M/\mathbb{Q}_p \text{ unramified} \\ \leq t & \text{if } M/\mathbb{Q}_p \text{ ramified and } c_p(\phi_p) \leq t \\ = 2 \cdot c_p(\phi_p) - 1 - t & \text{if } M/\mathbb{Q}_p \text{ ramified and } c_p(\phi_p) \geq t + 1 \end{cases}$$

(and where we corrected a small misprint in the statement of Theorem 1 of [23]). Thus, as is immediately seen, the number $n_p(\phi_p)$ depends only on K_p/\mathbb{Q}_p and on the conductor of ϕ_p (rather than on ϕ_p itself).

The character $\det(r_p)|_{U_p}$ has the general shape

$$\det(r_p)|_{U_p} = \alpha|_{U_p} \cdot \psi_1 \cdot \psi_2$$

where ψ_1, ψ_2 are the characters given loc. cit., which are both of 2-power order. The character ψ_1 is at most tamely ramified, whereas ψ_2 is wildly ramified if it is non-trivial, which may happen only if $p = 2$. The definitions of ψ_1 and ψ_2 are complicated in general and will not be restated, but we give a few special cases:

If the degree $m := [K_p : M]$ is odd then $\psi_1 = \psi_2 = 1$ so that ϵ_p is the trivial or quadratic character

$$\epsilon_p = (\alpha|_{U_p} \pmod{\lambda}).$$

If additionally we have $p \nmid m$ then one finds $n_p(1) = 2$.

On the other hand, if K_p/\mathbb{Q}_p is dihedral of order 8, but $p \neq 2$, then $p \equiv 3 \pmod{4}$ and K_p is unique. One has in this case that M is the unramified quadratic extension $\mathbb{Q}_p(\sqrt{-1})/\mathbb{Q}_p$ so that α is unramified. Further, $\psi_2 = 1$, but ψ_1 is the non-trivial quadratic character on $\{\pm 1\} \leq \mathbb{Q}_p^\times$. With the above notation one has $b = 1$ and $t = 0$ so that

$$n_p(\phi_p) = 2 \cdot \max\{1, c_p(\phi_p)\}.$$

5.1.3. *The ‘primitive’ cases for $p = 2$.* Finally, $\text{Im } \pi_p$ may be isomorphic to A_4 or S_4 in which case we must have $p = 2$. The study of these cases was initiated by Weil in [45]. In [4] Buhler computed the minimal possible conductor of a lift of π_2 and subsequently Zink determined in [46] all possible conductors of lifts of π_2 . In [23] these results were complemented by a discussion of the associated determinants. We can refer to Theorem 2 of [23] where a special lift r_2 of π_2 was given together with formulas for the restriction of its determinant to U_2 and for the conductor of $r_2 \otimes \phi_2$. We define then

$$n_2(\phi_2) := c_2(r_2 \otimes \phi_2)$$

and

$$\epsilon_2 := (\det(r_2)|_{U_2} \pmod{\lambda}),$$

where r_2 is a lift of π_2 as in Theorem 2 of [23]. Thus the formulas of that theorem give — depending on the extension $K_{\mathfrak{p}_2}/\mathbb{Q}_2$ (\mathfrak{p}_2 a prime of K over 2) — explicit formulas for the quantities $n_2(\phi_2)$ and ϵ_2 . The character ϵ_2 is at most quadratic, and the number $n_2(\phi_2)$ actually only depends on $c_2(\phi_2)$ in every case.

According to [45] there is exactly 1 extension of \mathbb{Q}_2 of A_4 -type; call it M_1 . Furthermore, there are exactly 3 extensions of S_4 -type; as already noted in section 3 above these are M_i/\mathbb{Q}_2 , $i = 2, 3, 4$, where:

$$M_i := \mathbb{Q}_2(\zeta, \omega, \sqrt{x_i}, \sqrt{\sigma x_i}, \sqrt{\sigma^2 x_i})$$

where ζ is a primitive 3’rd root of unity, $\omega^3 = 2$, σ is the automorphism of $\mathbb{Q}_2(\zeta, \omega)$ given by $\sigma\omega = \zeta\omega$, and $x_2 := (1 + \omega)(1 + \omega^2)(1 + \omega^3)$, $x_3 := (1 + \omega)(1 + \omega^3)$, $x_4 := (1 + \omega^2)$.

Theorem 2 of [23] then gives the above number $n_2(\phi_2)$ and the restriction of the above character ϵ_2 to U_2 as follows: Write $n_2 := n_2(\phi_2)$ and $c_2 := c_2(\phi_2)$ for

with α a ramified character of order not divisible by ℓ . We obtain

$$\delta_p(\phi_p) = 0$$

since — as α and ϕ_p have order prime to ℓ — the characters $\alpha\phi_p$ and $\bar{\alpha}\bar{\phi}_p$ are seen to have the same conductors, and similarly for ϕ_p and $\bar{\phi}_p$.

(2b) In the second case we have $r_p = \text{Ind}_{M/\mathbb{Q}_p}(\beta)$ where M/\mathbb{Q}_p is the unramified quadratic extension, and β is a ramified character on G_M that may be — and in fact has been — chosen to have order prime to ℓ . Then if σ denotes the non-trivial automorphism of M/\mathbb{Q}_p we have

$$\begin{aligned} (r_p \otimes \phi_p)|_{I_p} &\sim \begin{pmatrix} \beta \cdot (\phi_p)|_{G_M} & 0 \\ 0 & \beta^\sigma \cdot (\phi_p)|_{G_M} \end{pmatrix}, \\ (\bar{r}_p \otimes \bar{\phi}_p)|_{I_p} &\sim \begin{pmatrix} \bar{\beta} \cdot (\bar{\phi}_p)|_{G_M} & 0 \\ 0 & \bar{\beta}^\sigma \cdot (\bar{\phi}_p)|_{G_M} \end{pmatrix} \end{aligned}$$

and again we deduce

$$\delta_p(\phi_p) = 0 .$$

(3) Suppose finally that \bar{r}_p is reducible but not semisimple on I_p . Then $\text{Im } \pi_p = \text{Im Proj}(r_p)$ is either cyclic of order m divisible by ℓ , or is dihedral of order $2m$ with m divisible by ℓ . Since $\text{Im } \pi_p$ is isomorphic to a subgroup of one of the groups A_4 , S_4 , or A_5 , these cases can only occur if $\ell \in \{3, 5\}$ and $m = \ell$.

(3a) In the first case we have chosen r_p such that $\text{Im } r_p$ has the same order as $\text{Im } \pi_p$, i.e.,

$$r_p \sim \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$$

with α a character of order ℓ . Hence a priori

$$\dim(r_p \otimes \phi_p)^{I_p} = \begin{cases} 1 & \text{if } \phi_p \in \{1, \alpha^{-1}\} \\ 0 & \text{otherwise,} \end{cases}$$

where however the case $\phi_p = \alpha^{-1}$ actually does not occur because ϕ_p has order prime to ℓ whereas α has order ℓ .

On the other hand,

$$\bar{r}_p \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

with $* \neq 0$ and so

$$\dim(\bar{r}_p \otimes \bar{\phi}_p)^{I_p} = \begin{cases} 1 & \text{if } \bar{\phi}_p = 1 \\ 0 & \text{otherwise.} \end{cases}$$

We obtain

$$\delta_p(\phi_p) = 0 .$$

(3b) In the second case we have as in (2) above that $r_p = \text{Ind}_{M/\mathbb{Q}_p}(\beta)$ with M/\mathbb{Q}_p the unramified quadratic extension and β a ramified character on G_M . Hence,

$$(r_p \otimes \phi_p)|_{I_p} \sim \begin{pmatrix} \beta \cdot (\phi_p)|_{G_M} & 0 \\ 0 & \beta^\sigma \cdot (\phi_p)|_{G_M} \end{pmatrix}$$

with σ the non-trivial automorphism of M/\mathbb{Q}_p . Noticing that $(\phi_p)|_{G_M}$ is fixed under conjugation with σ whereas β is not ($\beta^{-1}\beta^\sigma$ is a character of order $m = \ell$), we obtain

$$\dim(r_p \otimes \phi_p)^{I_p} = 0 .$$

On the other hand, denoting by α the restriction to I_p of the quadratic character corresponding to M/\mathbb{Q}_p , we have

$$(\bar{r}_p \otimes \bar{\phi}_p)|_{I_p} \sim \begin{pmatrix} \bar{\alpha}\bar{\phi}_p & * \\ 0 & \bar{\phi}_p \end{pmatrix}$$

so that

$$\dim(\bar{r}_p \otimes \bar{\phi}_p)^{I_p} = \begin{cases} 1 & \text{if } \bar{\phi}_p = \bar{\alpha} \\ 0 & \text{otherwise.} \end{cases}$$

Consequently,

$$\delta_p(\phi_p) = \begin{cases} 1 & \text{if } \bar{\phi}_p = \bar{\alpha} \\ 0 & \text{otherwise.} \end{cases}$$

5.3. Local lifts: The weight. In this section we define in dependence on the extension K_ℓ/\mathbb{Q}_ℓ a set \mathfrak{W}_ℓ of natural numbers so that $k \in \mathfrak{W}_\ell$ may be deduced. Recall that K_ℓ/\mathbb{Q}_ℓ is the local extension cut out by the restriction to the decomposition group $G_{\mathbb{Q}_\ell} \leq G_{\mathbb{Q}}$ of $\text{Proj}(\rho)$ with ρ our given modular mod λ representation.

We start by quoting two theorems about the structure of the restriction ρ_ℓ of ρ to the decomposition group $G_{\mathbb{Q}_\ell} \leq G_{\mathbb{Q}}$. Let the corresponding mod λ cusp form be denoted by f . Thus f is a form of weight $k \in \{2, \dots, \ell - 1\}$. Denote by $a_n \in \overline{\mathbb{F}}_\ell$ the Fourier coefficients of f . The first theorem is due to Deligne; a proof can be found in [20]. The statement is that if $a_\ell \neq 0$ then ρ_ℓ is reducible and more precisely has the shape

$$\rho_\ell \sim \begin{pmatrix} u \cdot \chi^{k-1} & * \\ 0 & v \end{pmatrix}$$

where u and v are unramified characters. The second theorem — due to Fontaine with a proof to be found in [19] — states that if $a_\ell = 0$ then ρ_ℓ is irreducible and

$$(\rho_\ell)|_{I_\ell} \sim \begin{pmatrix} (\psi')^{k-1} & 0 \\ 0 & \psi^{k-1} \end{pmatrix}$$

where $\psi, \psi' : I_\ell \rightarrow \overline{\mathbb{F}}_\ell$ are the 2 fundamental characters of level 2. We have $\psi' = \psi^\ell$.

As usual, we refer to these two cases as the ordinary and the supersingular case respectively.

Now on the other hand we have defined above in section 5.1 a certain representation $r : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{C})$ such that in particular:

$$\rho_\ell \cong \bar{r}_\ell \otimes \chi^i \otimes (\text{unramified character}),$$

for some i , where \bar{r}_ℓ denotes the restriction of the mod λ reduction of r to the decomposition group $G_{\mathbb{Q}_\ell} \leq G_{\mathbb{Q}}$. We proceed now to compare these two descriptions of ρ in order to make statements about k .

The first observation is that if K_ℓ/\mathbb{Q}_ℓ were unramified, we would obviously be in the ordinary case whence the assumption $2 \leq k \leq \ell - 1$ would imply the contradiction $k = 1$. So we may start by defining

$$\mathfrak{W}_\ell := \emptyset \quad \text{if } K_\ell/\mathbb{Q}_\ell \text{ unramified.}$$

Secondly, as ℓ is odd the extension K_ℓ/\mathbb{Q}_ℓ is either cyclic or dihedral. We split up the discussion into 5 subcases.

5.3.1. *Tamely ramified cyclic case.* Suppose that K_l/\mathbb{Q}_ℓ is tamely ramified and cyclic of order $m \in \{2, 3, 4, 5\}$. Let $e \mid m$ be the ramification index of K_l/\mathbb{Q}_ℓ . Thus, $\ell \equiv 1 \pmod{e}$. The representation \bar{r}_ℓ has image of order m , and as $\ell \nmid m$ we have that \bar{r}_ℓ is semisimple and reducible. We are thus in the ordinary case, and so χ^{k-1} necessarily has order e . On the other hand, this order is $\frac{\ell-1}{(\ell-1, k-1)}$ so we see that

$$k-1 = a \cdot \frac{\ell-1}{e}$$

for some natural number a which must be less than e , as $k \leq \ell-1$.

So, if $e = 2, 3, 5$ we have $a = 1$, $a \in \{1, 2\}$ and $a \in \{1, 2, 3, 4\}$ respectively. If $e = 4$ we must have $a \in \{1, 3\}$ as $a = 2$ would imply $O(\chi^{k-1}) = 2$. So we may define

$$\mathfrak{W}_\ell = \mathfrak{W}_\ell(K_l/\mathbb{Q}_\ell) := \begin{cases} \left\{ \frac{\ell+1}{2} \right\} & \text{for } e = 2 \\ \left\{ \frac{\ell+2}{3}, \frac{2\ell+1}{3} \right\} & \text{for } e = 3 \\ \left\{ \frac{\ell+3}{4}, \frac{3\ell+1}{4} \right\} & \text{for } e = 4 \\ \left\{ \frac{\ell+4}{5}, \frac{2\ell+3}{5}, \frac{3\ell+2}{5}, \frac{4\ell+1}{5} \right\} & \text{for } e = 5. \end{cases}$$

5.3.2. *Wildly ramified cyclic case.* If K_l/\mathbb{Q}_ℓ is wildly ramified cyclic of order m , we have that \bar{r}_ℓ is twist-equivalent to

$$\begin{pmatrix} u & * \\ 0 & v \end{pmatrix}$$

with unramified characters u, v and $* \neq 0$. We deduce the contradiction $k = 1$ and may thus define $\mathfrak{W}_\ell := \emptyset$ in this case.

5.3.3. *Wildly ramified dihedral cases.* If K_l/\mathbb{Q}_ℓ is wildly ramified dihedral of order $2m$ then, as ℓ is odd, we must have $\ell \mid m$. As the Galois group of K_l/\mathbb{Q}_ℓ is isomorphic to a subgroup of one of A_4, S_4, A_5 , we conclude $\ell \in \{3, 5\}$ and $m = \ell$.

Now, K_l/\mathbb{Q}_ℓ has a unique quadratic subextension M/\mathbb{Q}_ℓ , and the representation $r: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{C})$ has been chosen in such a way that \bar{r}_ℓ appears in shape

$$\bar{r}_\ell \sim \begin{pmatrix} \alpha & * \\ 0 & 1 \end{pmatrix} \otimes (\text{unramified character})$$

where α is the quadratic character corresponding to M/\mathbb{Q}_ℓ .

So, if M/\mathbb{Q}_ℓ is unramified, that is, if K_l/\mathbb{Q}_ℓ is wildly but not totally ramified, we deduce the contradiction $k = 1$.

On the other hand, if M/\mathbb{Q}_ℓ is ramified, i.e., if K_l/\mathbb{Q}_ℓ is totally and wildly ramified, we must have $\alpha = \chi^{k-1}$. As $k \leq \ell-1$ and α has order 2, we deduce $k = \frac{\ell+1}{2}$. For the proof of part (b) of Theorem 1 in the next subsection, it will be convenient at this point to make an additional remark in the special case that $\ell = 3$: We have then $k = 2$ and this must be the weight attached to ρ by Serre-Edixhoven; referring specifically to Definition 4.3 of [19], we are in case 2(b) of that definition

and $k = 2$ means that K_l/\mathbb{Q}_ℓ is ‘peu ramifié’ in the sense of Serre [38], p.186. We may thus define

$$\mathfrak{W}_\ell := \begin{cases} \emptyset & \text{for } K_l/\mathbb{Q}_\ell \text{ wildly but not totally ramified} \\ \{\frac{\ell+1}{2}\} & \text{if } \ell = 5 \text{ and } K_l/\mathbb{Q}_\ell \text{ totally and wildly ramified,} \end{cases}$$

and for the case $\ell = 3$

$$\mathfrak{W}_3 := \{2\} \quad \text{for } K_l/\mathbb{Q}_3 \text{ totally, wildly ramified, but peu ramifié.}$$

For the proof of part (b) of Theorem 1 it will then be convenient to define additionally for the special case $\ell = 3$:

$$\mathfrak{W}_3 := \{4\} \quad \text{for } K_l/\mathbb{Q}_3 \text{ totally, wildly ramified, and très ramifié.}$$

5.3.4. *Tamely ramified dihedral case.* Suppose finally that K_l/\mathbb{Q}_ℓ is tamely ramified dihedral of order $2m$, $m \in \{2, 3, 4, 5\}$. Then K_l is cyclic of degree m over the unramified quadratic extension M/\mathbb{Q}_ℓ and $\ell \equiv -1 \pmod{m}$. The representation \bar{r}_ℓ has the form $\bar{r}_\ell = \text{Ind}_{M/\mathbb{Q}_\ell}(\beta)$ for a tamely ramified character β on G_M . Thus,

$$(\bar{r}_\ell)|_{I_\ell} \sim \begin{pmatrix} \beta & 0 \\ 0 & \beta^\sigma \end{pmatrix}$$

where σ denotes the non-trivial automorphism of M/\mathbb{Q}_ℓ . We are then necessarily in the supersingular case. The characters β, β^σ are of level 2, we have

$$\beta^\sigma = \beta^\ell$$

and m is the order of the character $\beta^\sigma \beta^{-1} = \beta^{\ell-1}$.

Denote as above by ψ, ψ' the two fundamental characters of level 2. Interchanging ψ and ψ' if necessary we may write

$$\beta = \psi^r (\psi')^s, \quad \beta^\sigma = \psi^s (\psi')^r$$

for integers r, s with $0 \leq r < s \leq \ell - 1$. Then

$$(\bar{r}_\ell \otimes \chi^{-r})|_{I_\ell} \sim \begin{pmatrix} (\psi')^a & 0 \\ 0 & \psi^a \end{pmatrix}$$

with $a := s - r$ which must satisfy $1 \leq a \leq \ell - 2$ because \bar{r}_ℓ is irreducible. Now,

$$(\psi')^a \psi^{-a} = \psi^{a \cdot (\ell-1)}$$

must still have order m and this allows us to determine the possibilities for a : As ψ has order $\ell^2 - 1$ the number a must have the form

$$a = a_0 \cdot \frac{\ell + 1}{m}$$

with $1 \leq a_0 < m$. If $m = 4$ then $a_0 \neq 2$ because $\psi^{a \cdot (\ell-1)}$ would otherwise have order 2.

On the other hand we know that the restriction $(\rho_\ell)|_{I_\ell}$ has the form

$$(\rho_\ell)|_{I_\ell} \sim \begin{pmatrix} (\psi')^{k-1} & 0 \\ 0 & \psi^{k-1} \end{pmatrix}$$

and is the twist by a power of $\chi = \psi^{\ell+1}$ of the above $(\bar{r}_\ell)|_{I_\ell}$. We deduce that $k - 1$ has the form $a + i(\ell + 1)$ or $\ell a + i(\ell + 1)$ for some i , and since $k - 1$ is a number in

$\{1, \dots, \ell - 2\}$ we find that $k = a + 1$ or $k = \ell + 2 - a$ where a is one of the numbers given above. We can then check that $k \in \mathfrak{W}_\ell$ if we define the set \mathfrak{W}_ℓ thus:

$$\mathfrak{W}_\ell = \mathfrak{W}_\ell(K_l/\mathbb{Q}_\ell) := \begin{cases} \left\{ \frac{\ell+3}{2} \right\} & \text{for } m = 2 \\ \left\{ \frac{\ell+4}{3}, \frac{2\ell+5}{3} \right\} & \text{for } m = 3 \\ \left\{ \frac{\ell+5}{4}, \frac{3\ell+7}{4} \right\} & \text{for } m = 4 \\ \left\{ \frac{\ell+6}{5}, \frac{2\ell+7}{5}, \frac{3\ell+8}{5}, \frac{4\ell+9}{5} \right\} & \text{for } m = 5. \end{cases}$$

5.4. This finishes the proof of part (a) of Theorem 1: Starting with the modular mod λ representation ρ cutting out K/\mathbb{Q} with Serre invariants (N, k, ν) , we defined a global character ϕ of order prime to ℓ , and then in sections 5.1 – 5.3 defined the numbers $n_p(K_p/\mathbb{Q}_p, \phi_p)$ and $\delta_p(K_p/\mathbb{Q}_p, \phi_p)$, the characters $\epsilon_p(K_p/\mathbb{Q}_p)$, and the set \mathfrak{W}_ℓ , and in the process verified the conclusions of part (a) of Theorem 1.

5.5. **End of proof.** We now finish the proof of Theorem 1 by proving part (b). So, let ϕ , N , k and ν be given with the properties and relations stated in the theorem. In particular we have that k is a number in the set $\mathfrak{W}_\ell = \mathfrak{W}_\ell(K_l/\mathbb{Q}_\ell)$, and because of our definition of \mathfrak{W}_ℓ we have that K is ramified over ℓ . Choose an embedding $G := \text{Gal}(K/\mathbb{Q}) \hookrightarrow \text{PGL}_2(\mathbb{C})$; this gives us a projective Galois representation

$$\pi: G_{\mathbb{Q}} \longrightarrow \text{PGL}_2(\mathbb{C}).$$

Denote by

$$r: G_{\mathbb{Q}} \longrightarrow \text{GL}_2(\mathbb{C})$$

the lift of π that we specified in section 5.1 above. The hypothesis that K not be totally real implies that r is an odd representation. So, r is modular of weight 1 by Langlands-Tunnell if $G \not\cong A_5$, and by assumption if $G \cong A_5$; cf. remark (3) immediately after the statement of Theorem 1.

Accordingly, the representation \bar{r} defined as the reduction mod λ of r is an irreducible modular mod λ representation. The same is then true of the representation

$$\rho := \bar{r} \otimes \bar{\phi}$$

with $\bar{\phi}$ the reduction mod λ of ϕ . By construction ρ has conductor N and character ν . Now it follows from Ribet's fundamental work [33] on 'level-lowering' as complemented by Diamond in [14], Corollary 1.2, that ρ is the mod λ representation attached to a mod λ cusp form of type (N, k', ν) where k' is the weight attached to ρ by Serre as modified in [19]. Tensoring with some power of χ if necessary, we may further assume that $k' \leq \ell + 1$.

We shall now proceed to show that $k' \in \mathfrak{W}_\ell(K_l/\mathbb{Q}_\ell)$, though possibly only after tensoring with some power of χ . First notice that if $k' = 1$ then ρ is unramified at ℓ by [8], Corollary 0.2; this is contrary to our assumptions, so $k' \geq 2$.

Suppose that $k' = \ell + 1$. Going through the various cases of Definition 4.3 of [19], we see that we must be in case 2.(b) of that definition, i.e.,

$$\rho|_{I_\ell} \sim \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix},$$

where $* \neq 0$. As we have $k' = \ell + 1$ the definition of k' in this case shows us that we must have $a := \min\{\alpha, \beta\} = 0$, $b := \max\{\alpha, \beta\} = 1$, and that ρ is not finite at ℓ . In particular, we see that $\text{Proj}(\rho)(I_\ell)$ has order $\ell \cdot (\ell - 1)$. On the other hand, this group is a subgroup of one of the groups A_4 , S_4 , or A_5 , so we deduce $\ell = 3$ and that this subgroup is in fact dihedral of order 6; we also see — again by order considerations — that the projectivisation of ρ is totally (wildly) ramified at ℓ . So, K_ℓ is a totally ramified dihedral extension of \mathbb{Q}_3 of order 6. Since ρ is not finite at ℓ , by definition this dihedral extension is ‘très ramifié’ in the sense of Serre, [38], p.186. By definition of $\mathfrak{W}_\ell(K_\ell/\mathbb{Q}_\ell)$ in 5.3.3 above, we have then $\mathfrak{W}_\ell \ni 4 = k'$.

Suppose then that $k' = \ell$ and that we are in the ordinary case. By the theorem of Deligne quoted above in section 5.3 we have then

$$\rho_\ell := (\rho)|_{G_{\mathbb{Q}_\ell}} \sim \begin{pmatrix} u & * \\ 0 & v \end{pmatrix}$$

for some unramified characters u, v . Then $* \neq 0$ again because ρ is ramified at ℓ . We deduce that $\ell \in \{3, 5\}$ and that K_ℓ/\mathbb{Q}_ℓ is either wildly ramified cyclic of order ℓ , or wildly but not totally ramified dihedral of order 2ℓ . Again, this is in contradiction to our assumption $k \in \mathfrak{W}_\ell$ and our definition $\mathfrak{W}_\ell := \emptyset$ in these cases (i.e., we have explicitly excluded these cases via the assumptions of part (b) of Theorem 1).

Assume then $k' = \ell$ but that we are in the supersingular case so that ρ_ℓ has a projective kernel field which is tamely ramified of order $2m$, $m \in \{2, 3, 4, 5\}$. Now, the theorem of Fontaine quoted above implies that we have

$$(\rho_\ell)|_{I_\ell} \sim \begin{pmatrix} (\psi')^{\ell-1} & 0 \\ 0 & \psi^{\ell-1} \end{pmatrix},$$

and we deduce as above in section 5.3 that $\psi^{(\ell-1)^2}$ has order m . On the other hand, this order is $\frac{\ell+1}{2}$, so (m, ℓ) is one of the following: $(2, 3)$, $(3, 5)$, $(4, 7)$. Now, it follows from [19], Proposition 3.3, that for a suitable power χ^j of χ , the representation $\rho \otimes \chi^j$ is modular of weight 3. As one checks that we in fact have $3 \in \mathfrak{W}_\ell$ in each of the 3 cases, we are done.

We may now conclude — possibly after tensoring ρ with a suitable power of χ — that either $k' \in \mathfrak{W}_\ell$ or else $2 \leq k' \leq \ell - 1$. But in the latter case we also have $k' \in \mathfrak{W}_\ell$ by the already proven part (a) of the theorem.

We thus see that our desired conclusion, i.e., the claim of existence of a mod λ cusp form of type (N, k, ν) with associated projective kernel field K is true for at least one number k in the set $\mathfrak{W}_\ell(K_\ell/\mathbb{Q}_\ell)$. In order to finish the proof it then clearly suffices to show the following two statements:

- (1) In case either $\ell = 5$ or K_ℓ/\mathbb{Q}_ℓ has degree not divisible by 5, we must show that (N, \tilde{k}, ν) ‘occurs’ in the above sense for every number $\tilde{k} \in \mathfrak{W}_\ell$ with $2 \leq \tilde{k} \leq \ell - 1$.

(2) In case $\ell \neq 5$ and K_l/\mathbb{Q}_ℓ has degree divisible by 5, we must define a partition $\mathfrak{W}_\ell = \mathfrak{W}_\ell^+ \cup \mathfrak{W}_\ell^-$ and prove the existence of a sign $\mu \in \{+, -\}$ such that (N, \tilde{k}, ν) occurs for every number $\tilde{k} \in \mathfrak{W}_\ell^\mu$ with $2 \leq \tilde{k} \leq \ell - 1$.

This is essentially accomplished via the theory of companion forms [20], [8], and the theory of θ -cycles [22], [19], applied to the ordinary and supersingular cases respectively: Suppose that $|\mathfrak{W}_\ell| > 1$, and that f is a mod λ cusp form of type (N, k, ν) where $k \in \mathfrak{W}_\ell$. Let ρ_f denote the mod λ representation attached to f .

Suppose first that K_l/\mathbb{Q}_ℓ is tamely ramified cyclic of degree m and ramification index $e \mid m$. As $|\mathfrak{W}_\ell| > 1$ we have $e \in \{3, 4, 5\}$. According to the main results of [20] and [8], the form f has a companion form of weight $k_1 := \ell + 1 - k$. One checks that if e is 3 or 4 then \mathfrak{W}_ℓ consists precisely of the numbers k and k_1 . If $e = 5$, we define

$$\mathfrak{W}_\ell^+ := \left\{ \frac{\ell + 4}{5}, \frac{4\ell + 1}{5} \right\}, \quad \mathfrak{W}_\ell^- := \left\{ \frac{2\ell + 3}{5}, \frac{3\ell + 2}{5} \right\}$$

so that

$$\mathfrak{W}_\ell = \mathfrak{W}_\ell^+ \cup \mathfrak{W}_\ell^-,$$

and one checks that if a subset \mathfrak{W}_ℓ^μ contains k , then it also contains k_1 .

Suppose then that K_l/\mathbb{Q}_ℓ is tamely ramified dihedral of order $2m$, so that we are in the supersingular case. As $|\mathfrak{W}_\ell| > 1$ we have $m \in \{3, 4, 5\}$. We then first observe that any number in \mathfrak{W}_ℓ is ≥ 3 except if $\ell = 3$ and $m = 4$; however, in the latter case we have $\mathfrak{W}_\ell = \{2, 4\}$ and there is nothing to show, as $4 > \ell - 1$ in this case. So, we may assume $k \geq 3$. Now the theory of θ -cycles [22], [19], in particular Proposition 3.3 in [19], implies that $\rho_f \otimes \chi^{\ell+1-k}$ is modular of type $(N, \ell + 3 - k, \nu)$ (and obviously with K its projective kernel field). One checks that for $m = 3$ or 4, the sum of the 2 numbers in \mathfrak{W}_ℓ is indeed $\ell + 3$, so we are done in those cases. If $m = 5$ we can split \mathfrak{W}_ℓ into 2 subsets:

$$\mathfrak{W}_\ell = \mathfrak{W}_\ell^+ \cup \mathfrak{W}_\ell^-$$

with

$$\mathfrak{W}_\ell^+ := \left\{ \frac{\ell + 6}{5}, \frac{4\ell + 9}{5} \right\}, \quad \mathfrak{W}_\ell^- := \left\{ \frac{2\ell + 7}{5}, \frac{3\ell + 8}{5} \right\}.$$

As the sum of the two numbers in each \mathfrak{W}_ℓ^μ is $\ell + 3$, we are done.

Thus, the proof of part (b) of Theorem 1 is finished.

6. ADDITIONAL REMARKS.

6.1. The purpose of Theorem 1 is to give the possible Serre invariants (N, k, ν) of mod ℓ representations of one of the exceptional types A_4 , S_4 , or A_5 in terms of local data attached to a fixed projective kernel field K . One may of course reverse the question, i.e., start with a triple (N, k, ν) and ask whether there are any cusp forms with these data and an attached exceptional mod ℓ representation. In connection with this question, the Theorem will immediately give information about whether there are any local Galois theoretic obstructions for this to be the case, and if there are not, will give detailed information about the local structure of possible corresponding projective kernel fields. This information will suffice to determine all

possible candidates for these projective kernel fields, either via class field theory in the A_4 - and S_4 -cases, or via geometry of numbers (or tables) in the A_5 -case. This gives an algorithm which will decide by a finite amount of computation the above question, — again of course under the assumption of the Artin conjecture in the A_5 case. Examples of this were given above in section 3. In these examples the dimension of the space of cusp forms in question was sufficiently low that we could actually ‘point’ to the exceptional form. In general however, the theorem will only inform us about the existence of an exceptional mod ℓ cusp form with the given data (N, k, ν) , though — as was pointed out above — we may in fact count the number of such forms. If one wishes additionally to ‘point’ to these forms one must first realize that all this can mean in general is to give an algorithm that computes their Fourier expansions. We shall now briefly indicate how this can be done.

Starting with an extension K/\mathbb{Q} of A_4 , S_4 or A_5 type, we choose an embedding $\text{Gal}(K/\mathbb{Q}) \hookrightarrow \text{PGL}_2(\mathbb{C})$ and obtain thus a complex projective Galois representation π . The Fourier expansion that we desire is obtained via reduction mod λ — for some prime λ over ℓ — from the L-series of a twist of a lift of π to a linear representation $G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{C})$. If one uses the results the papers [30], [9], [10], and [11], one has an algorithm that computes the L-series of *some* lift r_1 of π (corresponding to a central embedding problem with cyclic kernel of 2-power order). The desired Fourier expansions can be computed from twists of the mod λ reduction ρ_1 of r_1 . Now the problem is that one does not a priori know how the conductor of ρ_1 behaves under twists. However, this can easily be determined by Theorem 1 or rather the proof if it: The representation ρ_1 is a twist of the mod λ reduction ρ of the special linear lift r occurring in the proof of Theorem 1 (section 5 above), say

$$\rho_1 \cong \rho \otimes \xi .$$

If we can determine ξ then because we have complete information about the behavior of ρ with respect to twists, we have determined the Serre invariants of all twists of ρ_1 (essentially parametrized by the conductor of the character by which we are twisting). But ξ is easily determined: Let Σ denote the product of ℓ and the finite primes at which ρ or ρ_1 ramifies. As ρ_1 is given via an explicitly solved embedding problem, one can determine $(\rho_1)|_{I_p}$ for each of the finitely many primes $p \mid \Sigma$. On the other hand $(\rho)|_{I_p}$ is known by construction. Hence, the quantity $\xi_p := \xi|_{I_p}$ can be determined for $p \mid \Sigma$. Identifying ξ_p with a character on U_p , we have ξ explicitly determined as a mod ℓ Dirichlet character by

$$\xi: r \mapsto \prod_{p \mid \Sigma} \xi_p(r)^{-1}, \quad \text{for } (r, \Sigma) = 1 .$$

We can also use the global information obtained by solving an embedding problem to resolve the indeterminacy in part (b) of Theorem 1. In case that $\ell \neq 5$ and K_1/\mathbb{Q}_ℓ has degree divisible by 5, the theorem informs us — under the appropriate modularity assumption — that ρ is mod ℓ modular of type (N, k, ν) with k any of the 2 weights in \mathfrak{W}_ℓ^μ for *some* choice of sign $\mu \in \{+, -\}$. However, since we now know

$$(\rho)|_{I_\ell} \cong (\rho_1 \otimes \xi^{-1})|_{I_\ell}$$

explicitly, we can — as is easily checked — determine μ by looking at this restriction.

6.2. Continuing the above analysis, if we have given a mod ℓ cusp form f of minimal level and weight $k \in \{2, \dots, \ell - 1\}$, and if we know that the Galois representation ρ_f attached to f is irreducible, then we have — under the assumption of the Artin conjecture — an effective procedure which will determine whether ρ_f is of one of the exceptional types A_4, S_4, A_5 . If it is not, the corresponding projective kernel field has Galois group either dihedral or isomorphic to $\mathrm{PSL}_2(\mathbb{F}_{\ell^m})$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^m})$ for some m . Since the dihedral case means that ρ_f is induced from a global 1-dimensional character, it is easy to see — as also noted in the introduction — that it can be effectively decided whether this case prevails. If it does not, we are in the PSL_2 or PGL_2 case and the question arises how we can effectively distinguish between these, and in particular how to determine m computationally. In general, these questions lead to certain not completely trivial considerations that we shall be addressing elsewhere.

6.3. **Acknowledgements.** The authors wish to thank Gebhard Böckle for drawing their attention to the possibility of using the theorem of Fong–Swan in the proof of Proposition 1 (originally we split up the discussion according to whether $\ell \nmid \#G$ or not). This led to a nice streamlining of the argument.

We also thank Kenneth Ribet for a number of constructive suggestions and comments that were very helpful in improving the presentation.

REFERENCES

- [1] J. Basmaji, I. Kiming: ‘A table of A_5 -fields.’ On Artin’s conjecture for odd 2-dimensional representations, Lecture Notes in Math., Vol. 1585, Springer, 1994, pp. 37–46 and 122–141.
- [2] P. Bayer, G. Frey: ‘Galois representations of octahedral type and 2-coverings of elliptic curves.’ Math. Z. **207** (1991), 395–408.
- [3] M. Boylan: *Exceptional congruences for the coefficients of certain eta-product newforms*, J. Number Theory **98** (2003), 377–389.
- [4] J. P. Buhler: *Icosahedral Galois representations*, Lecture Notes in Mathematics **654**, (Springer, 1978).
- [5] K. M. Buzzard: ‘The levels of modular representations.’ Thesis, Cambridge 1995.
- [6] K. M. Buzzard, M. Dickinson, N. Shepherd-Barron, R. Taylor: ‘On icosahedral Artin representations.’ Duke Math. J. **109** (2001), 283–318.
- [7] H. Carayol: ‘Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires.’ Duke Math. J. **59** (1989), 785–801.
- [8] R. F. Coleman, J. F. Voloch: ‘Companion forms and Kodaira–Spencer theory.’ Invent. Math. **110** (1992), 263–281.
- [9] T. Crespo: ‘Central extensions of the alternating group as Galois groups.’ Acta Arith. **66** (1994), 229–236.
- [10] T. Crespo: ‘Galois realization of central extensions of the symmetric group with kernel a cyclic 2-group.’ Acta Arith. **70** (1995), 183–192.
- [11] T. Crespo: ‘Construction of $2^m S_n$ -fields containing a C_{2^m} -field.’ J. Algebra **201** (1998), 233–242.
- [12] P. Deligne: ‘Formes modulaires et représentations ℓ -adiques’, Sémin. Bourbaki 355 (1968/69), lecture Notes in Mathematics 179, 139–172, Springer-Verlag, 1971.
- [13] P. Deligne, J.-P. Serre: ‘Formes modulaires de poids 1’, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530.

- [14] F. Diamond: 'The refined conjecture of Serre.' *Elliptic curves, modular forms, & Fermat's last theorem* (Hong Kong, 1993), 22–37, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.
- [15] F. Diamond, R. Taylor: 'Non-optimal levels of mod ℓ modular representations.' *Invent. Math.* **115** (1994), 435–462.
- [16] L. E. Dickson: *Linear groups with an exposition of the Galois field theory*, (Teubner, Leipzig 1901).
- [17] L. Dieulefait, N. Vila: 'Projective linear groups as Galois groups over \mathbb{Q} via modular representations.' *J. Symbolic Comput.* **30** (2000), 799–810.
- [18] D. Doud: ' S_4 and \tilde{S}_4 extensions of \mathbb{Q} ramified at only one prime.' *J. Number Theory* **75** (1999), 185–197.
- [19] B. Edixhoven: 'The weight in Serre's conjectures on modular forms.' *Invent. Math.* **109** (1992), 563–594.
- [20] B. Gross: 'A tameness criterion for Galois representations associated to modular forms (mod p).' *Duke Math. J.* **61** (1990), 445–517.
- [21] K. Haberland: 'Perioden von Modulformen einer Variabler und Gruppenkohomologie, III.' *Math. Nachr.* **112** (1983), 297–315.
- [22] N. Jochnowitz: 'A study of the local components of the Hecke algebra mod ℓ .' *Trans. Amer. Math. Soc.* **270** (1982), 253–267.
- [23] I. Kiming: 'On the liftings of 2-dimensional projective Galois representations over \mathbb{Q} .' *J. Number Theory* **56** (1996), 12–35.
- [24] I. Kiming, X. Wang: 'Examples of 2-dimensional, odd Galois representations of A_5 -type over \mathbb{Q} satisfying the Artin conjecture.' *On Artin's conjecture for odd 2-dimensional representations*, Lecture Notes in Math., Vol. **1585**, Springer, 1994, pp. 109–121.
- [25] J. C. Lagarias, H. L. Montgomery, A. M. Odlyzko: 'A bound for the least prime ideal in the Chebotarev density theorem.' *Invent. Math.* **54** (1979), 271–296.
- [26] R. P. Langlands: 'Base Change for $GL(2)$.' *Ann. of Math. Stud.* **96**, Princeton University Press, 1980.
- [27] R. Livné: 'On the conductors of mod ℓ Galois representations coming from modular forms.' *J. Number Theory* **31** (1989), 133–141.
- [28] F. Momose: 'On the ℓ -adic representations attached to modular forms.' *J. Fac. Sci. Univ. Tokyo* **28** (1981), 89–109.
- [29] PARI/GP, Bordeaux, <http://pari.math.u-bordeaux.fr/>.
- [30] J. Quer: 'Liftings of projective 2-dimensional Galois representations and embedding problems.' *J. Algebra* **171** (1995), 541–566.
- [31] K. A. Ribet: 'On ℓ -adic representations attached to modular forms.' *Invent. Math.* **28** (1975), 245–275.
- [32] K. A. Ribet: 'On ℓ -adic representations attached to modular forms. II.' *Glasgow Math. J.* **27** (1985), 185–194.
- [33] K. A. Ribet: 'On modular representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms.' *Invent. Math.* **100** (1990), 431–476.
- [34] K. A. Ribet: 'Images of semistable Galois representations.' *Pacific J. Math.* **181** (1997), 277–297.
- [35] J.-P. Serre: 'Représentations linéaires des groupes finis.' Hermann, Paris, 1967.
- [36] J.-P. Serre: 'Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer].' *Séminaire Bourbaki*, 24e année (1971/1972), Exp. No. 416, 319–338. Oeuvres III, pp. 74–88.
- [37] J.-P. Serre: 'Modular forms of weight one and Galois representations.' *Algebraic number fields: L -functions and Galois properties* (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 193–268. Academic Press, London, 1977.
- [38] J.-P. Serre: 'Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.' *Duke Math. J.* **54** (1987), 179–230.
- [39] O. Schreier, B. L. van der Waerden: 'Die Automorphismen der Projektiven Gruppen.' *Abh. Math. Sem. Univ. Hamburg* **6** (1928), 303–322.
- [40] J. Sturm: 'On the congruence of modular forms.' *Number Theory*, New York, 1984–85, Lecture Notes in Math., Vol. **1240**, Springer, 1987, pp. 275–280.
- [41] H. P. F. Swinnerton-Dyer: 'On ℓ -adic representations and congruences for coefficients of modular functions.' *Modular functions of one variable, III*, Lecture Notes in Math., Vol. **350**, Springer, Berlin, 1973, pp. 1–55.

- [42] H. P. F. Swinnerton-Dyer: 'On ℓ -adic representations and congruences for coefficients of modular forms. II.' Modular functions of one variable, V, Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977, pp. 63–90.
- [43] R. Taylor: 'On icosahedral Artin representations II.' Preprint, 2000.
- [44] J. Tunnell: 'Artin's conjecture for representations of octahedral type.' Bull. Amer. Math. Soc. (N.S.) 5 (1981), 173–175.
- [45] A. Weil: 'Exercices dyadiques.' Invent. Math. 27 (1974), 1–22.
- [46] E.-W. Zink: 'Ergänzungen zu Weils Exercises dyadiques.' Math. Nachr. 92 (1979), 163–183.

(Ian Kiming) DEPT. OF MATHEMATICS, UNIVERSITY OF COPENHAGEN, UNIVERSITETSPARKEN 5,
2100 COPENHAGEN Ø, DENMARK

E-mail address: kiming@math.ku.dk

(Helena A. Verrill) DEPT. OF MATHEMATICS, LOUISIANA STATE UNIVERSITY, BATON ROUGE,
LOUISIANA 70803-4918, USA

E-mail address: verrill@math.lsu.edu