2-ADIC PROPERTIES OF CERTAIN MODULAR FORMS AND THEIR APPLICATIONS TO ARITHMETIC FUNCTIONS

KEN ONO AND YUICHIRO TAGUCHI

ABSTRACT. It is a classical observation of Serre that the Hecke algebra acts locally nilpotently on the graded ring of modular forms modulo 2 for the full modular group. Here we consider the problem of classifying spaces of modular forms for which this phenomenon continues to hold. We give a number of consequences of this investigation as they relate to quadratic forms, partition functions, and central values of twisted modular L-functions.

1. Introduction and Statement of Results

Suppose that $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ (throughout let $q := e^{2\pi iz}$) is a holomorphic integer weight modular form with integer coefficients on a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. A famous theorem of Serre [21, 22] implies, for every integer M, that there is an $\alpha(M) > 0$ for which

$$\#\{n \leq X \ : \ a(n) \not\equiv 0 \pmod{M}\} = O\left(\frac{X}{\log^{\alpha(M)} X}\right).$$

In particular, "almost every" coefficient $a(n)$ is a multiple of M.

By making use of congruences between modular forms, Serre's Theorem can often be employed to imply results for the coefficients of non-holomorphic modular forms. For example, consider Klein's modular function

$$j(z) = \sum_{n=-1}^{\infty} C(n)q^n = q^{-1} + 744 + 196884q + \cdots .$$

Although little is known[1] about the parity of the coefficients $C(8n+7)$, it is an elementary fact that $C(n) \equiv 0 \pmod 2$ for every $n \not\equiv 7 \pmod 8$. Serre's result implies much more for those $n \not\equiv 7 \pmod 8$. If $t \geq 1$, then it implies that almost every $n \not\equiv 7 \pmod 8$ has the property that $C(n) \equiv 0 \pmod{2^t}$.

As another example, consider the partition function $Q(n)$ which counts the number of partitions of an integer n into distinct summands. Its generating function is given by

$$\sum_{n=0}^{\infty} Q(n)q^n = \prod_{n=1}^{\infty}(1+q^n) = 1 + q + q^2 + 2q^3 + \cdots .$$

2000 *Mathematics Subject Classification.* 11F11, 11R32, 11S15.

The first author is grateful for the support of the National Science Foundation, the Guggenheim Foundation, the Packard Foundation, and a Romnes Fellowship. The second author thanks YoungJu Choie and Pohang University of Science and Technology for their hospitality during his stay at POSTECH (Sep. 2003 – Feb. 2004) where part of this work was done.

[1]For example, see Remarque (c) of [22].

Although this generating function is not a holomorphic integer weight modular form (note. it is essentially a modular function on $\Gamma_0(1152)$), Gordon and the first author confirmed [9] a speculation of Alladi (see (4.6) of [1]), by proving, for every $t \geq 1$, that almost every n has the property that $Q(n) \equiv 0 \pmod{2^t}$.

Arguing in this way with Serre's Theorem, one can obtain many further results of this type. Here we show how to make such results more precise by making use of the fact that Hecke operators act nilpotently modulo powers of 2 on certain spaces of modular forms. As a special case, we obtain the following theorem for the arithmetic functions $C(n)$, $Q(n)$, and $r_s(n)$, the number of representations of an integer n as a sum of s integral squares.

Theorem 1.1. *Assume the notation above.*

(1) *If $t \geq 1$, then there is a positive integer c such that for every set of distinct odd primes $p_1, p_2, \ldots, p_c$ we have*

$$C(p_1 p_2 \cdots p_c m) \equiv 0 \pmod{2^t},$$

whenever $m \geq 1$ is coprime to $p_1 p_2 \cdots p_c$ and $p_1 p_2 \cdots p_c m \not\equiv 7 \pmod 8$.

(2) *If $t \geq 1$, then there is a positive integer c such that for every set of distinct primes $5 \leq p_1, p_2, \ldots, p_c$ we have*

$$Q\left(\frac{p_1 p_2 \ldots p_c m - 1}{24}\right) \equiv 0 \pmod{2^t},$$

whenever $m \geq 1$ is coprime to $p_1 p_2 \cdots p_c$.

(3) *If $s \geq 2$ is even, then there is a non-negative integer c such that for every positive integer t and every set of distinct odd primes $p_1, p_2, \ldots, p_{c+t}$ we have*

$$r_s(p_1 p_2 \cdots p_{c+t} m) \equiv 0 \pmod{2^t},$$

whenever $m \geq 1$ is coprime to $p_1 p_2 \cdots p_{c+t}$.

Remark. In Theorem 1.1 (1) and (2), observe that the integer c depends on the choice of t. For Theorem 1.1 (2), note that $Q(\alpha) = 0$ if α is not an integer.

Similar arguments can provide information for half-integral weight modular forms modulo 2. In this direction, we consider the 2-divisibility of central values of quadratic twists of certain modular L-functions. By works of Kohnen and Zagier, and Waldspurger (see [11, 12, 29]), these values are essentially the squares of coefficients of half-integral weight Hecke eigenforms. We briefly recall some of the results of Kohnen and Zagier.

Suppose that N is odd and square-free, and suppose that $F(z) \in S_{2k}^{\text{new}}(\Gamma_0(N))$ is an even weight newform. There is a *Kohnen newform*

$$g_F(z) = \sum_{n=1}^{\infty} b(n) q^n \in S_{k+\frac{1}{2}}^{\text{new}}(\Gamma_0(4N)),$$

which is unique up to scalar multiple, whose image under the Shimura correspondence is $F(z)$. We assume that $g_F(z)$ is suitably normalized so that it has Fourier coefficients in the integer ring $\mathcal{O}_L$ of some number field L, and has the additional property that $g_F(z) \not\equiv 0 \pmod{\lambda}$ (i.e. there is an n for which $b(n) \not\equiv 0 \pmod{\lambda}$), where λ is a prime above 2 in $\mathcal{O}_L$.

Let $\nu(N)$ denote the number of prime factors of N, and let $\langle F, F\rangle$ (resp. $\langle g_F, g_F\rangle$) denote the Petersson inner product on $S_{2k}(\Gamma_0(N))$ (resp. $S_{k+\frac{1}{2}}(\Gamma_0(4N))$). If $\ell \mid N$ is prime, then let $w_\ell \in \{\pm 1\}$ be the eigenvalue of the Atkin-Lehner involution

$$F(z) \mid_{2k} W(\ell) = w_\ell F(z).$$

If D is a fundamental discriminant for which $(-1)^k D > 0$, and has the additional property that $\left(\frac{D}{\ell}\right) = w_\ell$ for each prime $\ell \mid N$, then (see Corollary 1 of [11])

$$L(F_D, k) = \frac{\langle F, F\rangle \cdot \pi^k}{2^{\nu(N)}(k-1)!|D|^{k-\frac{1}{2}}\langle g_F, g_F\rangle} \cdot |b(|D|)|^2. \tag{1.1}$$

Here $F_D(z)$ is the newform corresponding to the D-quadratic twist of $F(z)$. For other fundamental discriminants D with $(-1)^k D > 0$, we have $b(|D|) = 0$. For those D for which (1.1) holds, we define $L_{\mathrm{K}}^{\mathrm{alg}}(F_D, k)$, the *Kohnen algebraic part* of $L(F_D, k)$, by

$$L_{\mathrm{K}}^{\mathrm{alg}}(F_D, k) = |b(|D|)|^2. \tag{1.2}$$

These values are predicted, by the Bloch-Kato Conjecture (see [2]), to be quotients of arithmetic invariants associated to Tate-twists of motives for modular forms, and they are often expected to be highly divisible by λ for those D with many prime factors. The simplest case of this phenomenon holds for all newforms of level $N = 1, 3, 5, 7, 15$ or 17.

Theorem 1.2. *Suppose that $F(z) \in S_{2k}^{\mathrm{new}}(\Gamma_0(N))$ is an even weight newform where $N = 1, 3, 5, 7, 15$ or 17. There is a positive integer c with the property that*

$$L_{\mathrm{K}}^{\mathrm{alg}}(F_D, k) \equiv 0 \pmod 4$$

for every D, with at least c odd prime factors, that satisfies (1.1).

Remark. The conclusion of Theorem 1.2 often holds for a higher power of 2. For example, consider the case where $F(z) = \Delta(z) \in S_{12}(\Gamma_0(1))$ and

$$g_\Delta(z) = \sum_{n=1}^{\infty} b(n)q^n = q - 56q^4 + 120q^5 - 240q^8 + 9q^9 + 1440q^{12} - 1320q^{13} - \cdots.$$

For positive fundamental discriminants $D > 1$ (see p. 179 of [12]), it turns out that

$$L_{\mathrm{K}}^{\mathrm{alg}}(\Delta_D, 6) \equiv \begin{cases} 64 \pmod{256} & \text{if } D \equiv 5 \pmod 8 \text{ is prime,} \\ 0 \pmod{256} & \text{otherwise.} \end{cases}$$

These results follow from the nilpotency, modulo powers of 2, of the action of the Hecke operators on certain spaces of modular forms, a phenomenon first observed by Serre for modular forms on $\mathrm{SL}_2(\mathbb{Z})$. To make this notion precise, we begin by fixing notation. For a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ and a subring $\mathcal{O}$ of $\mathbb{C}$, we denote by $S_k(\Gamma; \mathcal{O})$ the $\mathcal{O}$-module of cusp forms of integer weight k with respect to Γ whose Fourier coefficients lie in $\mathcal{O}$. If $\Gamma = \Gamma_0(N)$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is a Dirichlet character, we denote by $S_k(\Gamma_0(N), \chi; \mathcal{O})$ the $\mathcal{O}$-module of cusp forms of weight k and Nebentypus character χ with respect to $\Gamma_0(N)$ whose Fourier coefficients lie in $\mathcal{O}$. Similarly, we denote by $M_k(\Gamma_0(N), \chi; \mathcal{O})$

etc. the spaces of holomorphic modular forms which are not necessarily cusp forms. We write simply $S_k(\Gamma)$, $S_k(\Gamma_0(N),\chi)$, $M_k(\Gamma)$ and $M_k(\Gamma_0(N);\chi)$ for $S_k(\Gamma;\mathbb{C})$, $S_k(\Gamma_0(N),\chi;\mathbb{C})$, $M_k(\Gamma,\mathbb{C})$ and $M_k(\Gamma_0(N),\chi;\mathbb{C})$ respectively. For convenience, we shall drop the dependence of k and χ (in the case of forms with Nebentypus), and we let T_n denote the appropriate nth Hecke operator which will be clear from context. Finally, if λ is a prime of an algebraic number field L, then we let $\mathcal{O}_{L,\lambda}$ be the localization of the integer ring $\mathcal{O}_L$ at λ.

Theorem 1.3. *Let a be a non-negative integer, and let N and k be positive integers. Suppose that $\chi : (\mathbb{Z}/2^aN)^\times \to \mathbb{C}^\times$ is a Dirichlet character with conductor $\mathfrak{f}(\chi)$, and suppose that L is a number field containing the coefficients of all the integer weight k newforms in the spaces $S_k(\Gamma_0(M),\chi)$, for every M with $M \mid 2^aN$ and $\mathfrak{f}(\chi) \mid M$. Let λ be a prime of L lying above 2.*

(1) *If $N = 1, 3, 5, 15$ or 17, then there is an integer $c \geq 0$ such that for every $f(z) \in S_k(\Gamma(2^aN),\chi;\mathcal{O}_{L,\lambda})$ and every $t \geq 1$ we have*

$$f(z) \mid T_{p_1} \mid T_{p_2} \mid \cdots \mid T_{p_{c+t}} \equiv 0 \pmod{\lambda^t}, \tag{1.3}$$

whenever $p_1, p_2, \ldots, p_{c+t}$ are odd primes not dividing N.

(2) *If $N = 7$, then there is an integer $c \geq 0$ such that (1.3) holds for every $f(z) \in S_k(\Gamma_0(2^a \cdot 7),\chi;\mathcal{O}_{L,\lambda})$ and every $t \geq 1$, provided that*

$$p_1, ..., p_{c+t} \equiv \pm 1 \pmod{7}.$$

Furthermore, if χ has 2-power order, then (1.3) holds for every set of primes $p_1, ..., p_{c+t}$ coprime to 14.

(3) *If $N = 9$, then there is an integer $c \geq 0$ such that (1.3) holds for every $f(z) \in S_k(\Gamma_0(2^a \cdot 9),\chi;\mathcal{O}_{L,\lambda})$ and every $t \geq 1$, provided that*

$$p_1, ..., p_{c+t} \equiv 37, 53, 55, 71 \pmod{72}.$$

Furthermore, if χ has 2-power order, then (1.3) holds for every set of primes $p_1, ..., p_{c+t}$ coprime to 6.

(4) *Suppose that $N = 11$. If the residue degree of λ is not a multiple of 4 or χ has 2-power order, then there is an integer $c \geq 0$ and a set of primes S_{11} (see Section 4), with density $2/3$, such that (1.3) holds for every $f(z) \in S_k(\Gamma_0(2^a \cdot 11),\chi;\mathcal{O}_{L,\lambda})$ and every $t \geq 1$, provided that $p_1, ..., p_{c+t} \in S_{11}$.*

(5) *Suppose that $N = 13$. If the residue degree of λ is odd or χ has 2-power order, then there is an integer $c \geq 0$ and a set of primes S_{13} (see Section 4), with density $2/3$, such that (1.3) holds for every $f(z) \in S_k(\Gamma_0(2^a \cdot 13),\chi;\mathcal{O}_{L,\lambda})$ and every $t \geq 1$, provided that $p_1, ..., p_{c+t} \in S_{13}$.*

Remark. In Theorem 1.3, χ may be trivial. The integer c depends on k, N, χ and L. Furthermore, we note that the primes $p_1, p_2, \ldots, p_{c+t}$ are not required to be distinct.

Remark. Theorem 1.3 can be generalized to the spaces $M_k(\Gamma_0(2^aN),\chi;\mathcal{O}_{L,\lambda})$. To see this, one merely needs to verify that the conclusion holds for the subspace of Eisenstein series. This is easily done using well known formulas for the Fourier expansions of Eisenstein series which are given in terms of generalized divisor functions (for example, see Chapter 7 of [14] or Chapter VII of [19]). The proofs of Theorem 1.1 (1) and (3) require this observation for modular forms on $\Gamma_0(1)$ and $\Gamma_0(4)$.

Remark. We may sometimes want to apply Theorem 1.3 to modular forms with Fourier coefficients in a subfield K of L, and replace the prime λ by the prime λ_0 of K lying below λ. Then we need $c+et$ primes p_i, where e is the ramification index of λ/λ_0. Thus the conclusion (1.3) would be

$$f(z) \mid T_{p_1} \mid T_{p_2} \mid \cdots \mid T_{p_{c+et}} \equiv 0 \pmod{\lambda_0^t}.$$

Serre's ε-Conjecture (cf. e.g. [18]) in characteristic 2 implies that every mod 2 Galois representation associated to a modular form of level 2^aN comes also from a modular form of level N and weight ≤ 4. Consequently, a proof of this conjecture would easily give Theorem 1.3. Although it is known in many cases (cf. [8], [3], [4]), it is not yet known in complete generality. So instead of appealing to the ε-Conjecture, we directly classify mod 2 Galois representations with small Artin conductor $N(\rho)$ outside 2 (see Section 2 for the definition of $N(\rho)$). To state this classification, for a field K, let $\overline{K}$ denote a fixed algebraic closure of K, and let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. Regarding Galois representations, we assume throughout that all representations are continuous with respect to the obvious topology (so in particular their images are always finite in this paper). When we say that an extension of $\mathbb{Q}$ is unramified outside a set of primes, we allow it to be ramified at ∞. In this context, we extend non-existence theorems of Tate and Moon for irreducible mod 2 representations, and we obtain the complete list of semisimple mod 2 representations with $N(\rho) \in \{1, 3, 5, 7, 9, 15, 17\}$ (the cases $N(\rho) = 1$ and $N(\rho) = 3$ are respectively due to Tate [28] and Moon [15]). Assuming GRH, we obtain the $N = 11$ and 13 cases, thereby providing the following conditional classification for $N \leq 17$.

Theorem 1.4. *Assume the notation above, and the definitions of V_n and W_n in Section 2.*

(1) *If $N(\rho) = 1, 3, 5, 7, 15, 17$, then there are no irreducible representations*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2).$$

(2) *There are two isomorphism classes of irreducible representations*

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

with $N(\rho) = 9$. Their images are isomorphic to W_3, and they are defined over $\mathbb{F}_4$. These two representations into $\mathrm{GL}_2(\mathbb{F}_4)$ are $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$-conjugates. If ρ_9^{ε} is a representative of either of these classes, then the extension $K/\mathbb{Q}$ cut out by ρ_9^{ε} contains the quadratic field $\mathbb{Q}(\sqrt{-2})$, and $\det \rho_9^{\varepsilon}$ is a character of conductor 9 and order 3.

(3) *If m is a positive integer with $4 \nmid m$, then there is (up to isomorphism) a unique irreducible representation*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{2^m})$$

with $N(\rho) = 11$. Let ρ_{11} denote a representative of this isomorphism class. It has image isomorphic to $\mathrm{SL}_2(\mathbb{F}_2) \simeq V_3$. The field cut out by ρ_{11} contains the quadratic field $\mathbb{Q}(\sqrt{-11})$, and $\det \rho_{11} = 1$.

(4) *Assuming GRH, in addition to the representation in (3), there are four isomorphism classes of irreducible representations*

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

with $N(\rho) = 11$. *They have images isomorphic to* W_5, *and can be defined over* $\mathbb{F}_{2^4}$. *These representations into* $\mathrm{GL}_2(\mathbb{F}_{2^4})$ *are conjugate to each other under the action of* $\mathrm{Gal}(\mathbb{F}_{2^4}/\mathbb{F}_2)$. *Let* ρ_{11}^{ε} *denote a representative of any one of these isomorphism classes. The field cut out by* ρ_{11}^{ε} *contains the quadratic field* $\mathbb{Q}(\sqrt{-2})$, *and* $\det \rho_{11}^{\varepsilon}$ *is a character of conductor* 11 *and order* 5.

(5) *If* m *is a positive odd integer, then there is (up to isomorphism) a unique irreducible representation*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{2^m})$$

with $N(\rho) = 13$. *Let* ρ_{13} *denote a representative of this isomorphism class. It has image isomorphic to* $\mathrm{SL}_2(\mathbb{F}_2) \simeq V_3$. *The field cut out by* ρ_{13} *contains the quadratic field* $\mathbb{Q}(\sqrt{-26})$, *and* $\det \rho_{13} = 1$.

(6) *Assuming GRH, in addition to the representation in (5), there are two isomorphism classes of irreducible representations*

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

with $N(\rho) = 13$. *They have images isomorphic to* W_3, *and can be defined over* $\mathbb{F}_{2^2}$. *These representations into* $\mathrm{GL}_2(\mathbb{F}_{2^2})$ *are conjugate to each other by the action of* $\mathrm{Gal}(\mathbb{F}_{2^2}/\mathbb{F}_2)$. *Let* ρ_{13}^{ε} *denote a representative of any one of these isomorphism classes. The field cut out by* ρ_{13}^{ε} *contains the quadratic field* $\mathbb{Q}(\sqrt{-1})$, *and* $\det \rho_{13}^{\varepsilon}$ *is a character of conductor* 13 *and order* 3.

In Sections 2 and 3 we prove Theorem 1.4. In Section 4 we recall facts about traces of these representations. In Section 5 we employ Theorem 1.4 to prove Theorem 1.3, and then conclude with the proofs of Theorems 1.1 and 1.2.

Acknowledgements

The authors thank K. Mahlburg, A. Odlyzko, and J.-P. Serre for their comments during the preparation of this paper. The authors are also indebted to H. Moon for making substantial contributions to Sections 2 and 3.

2. Mod 2 Galois representations with small Artin conductor

In this section, we prove Theorem 1.4 except the $N(\rho) = 9$ case. For this purpose[2], q will always be a prime number. For a Galois representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_{\mathbb{F}}(V)$$

on a finite-dimensional vector space V over a discrete field $\mathbb{F}$ of characterisitc ℓ, its Artin conductor $N(\rho)$ outside ℓ is defined by

$$N(\rho) = \prod_{q \neq \ell} q^{n_q(\rho)}, \tag{2.1}$$

[2]When referring to Fourier expansions in other sections, we shall always let $q := e^{2\pi i z}$.

with

$$n_q(\rho) \;=\; \sum_{i=0}^{\infty} \frac{1}{(G_{q,0} : G_{q,i})} \cdot \dim_{\mathbb{F}}(V/V^{G_{q,i}}). \tag{2.2}$$

Here $G_{q,i}$ denotes the ith ramification subgroup of a decomposition subgroup at q of the Galois group $G = \mathrm{Im}(\rho)$. (For background information on ramification groups and conductors, see Chapters IV and V of [24]; see also Section 1.2 of [25].) We note, among other things, the following two facts about $N(\rho)$:

(1) In this paper, we mainly consider the case where $N(\rho)$ is square-free (i.e., $n_q(\rho) = 1$ for all ramified primes $q \neq \ell$). This means in particular that ρ is (i.e. the field extension cut out by ρ is) tamely ramified at q.
(2) If $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ comes from a mod ℓ Hecke eigenform $f(z)$ of level N, then we have that $N(\rho) \mid N$ (see [5] and [13]).

We shall also use the notation $n_q(\rho)$ in the local context (i.e. to denote the exponent of the Artin conductor of a representation of a decomposition group D_q of a prime q, or the Galois group $G_{\mathbb{Q}_q}$ of the local field $\mathbb{Q}_q$). It is also given by (2.2).

We require some further notation to state our results. We shall use the "wild" notation such as $\left(\begin{smallmatrix} 1 & * \\ & * \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} * & * \\ * & * \end{smallmatrix}\right)$ to denote respectively the subgroups

$$\left\{\left(\begin{smallmatrix} 1 & \\ & d \end{smallmatrix}\right) \;:\; d \in \overline{\mathbb{F}}_2^{\times}\right\}, \quad \left\{\left(\begin{smallmatrix} a & \\ & d \end{smallmatrix}\right) \;:\; a, d \in \overline{\mathbb{F}}_2^{\times}\right\}, \quad \left\{\left(\begin{smallmatrix} a & b \\ & d \end{smallmatrix}\right) \;:\; a, d \in \overline{\mathbb{F}}_2^{\times}, b \in \overline{\mathbb{F}}_2\right\}$$

of $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$. Let W be the semidirect product of the diagonal matrices $\left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right)$ and $\left\langle \left(\begin{smallmatrix} 1 & \\ 1 & \end{smallmatrix}\right) \right\rangle$, which is, as a set, equal to $\left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right) \cup \left(\begin{smallmatrix} & * \\ * & \end{smallmatrix}\right)$. It is the wreath product of $\overline{\mathbb{F}}_2^{\times}$ by $\mathbb{Z}/2\mathbb{Z}$ (so that $\mathbb{Z}/2\mathbb{Z}$ acts on $\overline{\mathbb{F}}_2^{\times} \times \overline{\mathbb{F}}_2^{\times}$ by switching the two components), and sits in a short exact sequence

$$1 \to \overline{\mathbb{F}}_2^{\times} \times \overline{\mathbb{F}}_2^{\times} \to W \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

For each odd integer $n \geq 1$, let W_n denote the subgroup of W of order $2n^2$ which is the extension of $\mathbb{Z}/2\mathbb{Z}$ by $\mu_n \times \mu_n$, where μ_n is the group of nth roots of unity in $\overline{\mathbb{F}}_2^{\times}$. As a special case of Theorem 1 of Section 22 of [27], we have the following fact.

Lemma 2.1. *Assume the notation above.*

(1) *Every maximal solvable irreducible subgroup of* $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ *is conjugate to* W.
(2) *If* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ *is an irreducible representation with solvable image, then (after possibly replacing* ρ *by a conjugate)* $\mathrm{Im}(\rho)$ *is contained in* W_n *for some* $n \geq 3$. *Moreover, we have an exact sequence of the form*

$$1 \to H \to \mathrm{Im}(\rho) \to \mathbb{Z}/2\mathbb{Z} \to 1,$$

where H *is a finite subgroup of* $\left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right)$ *which is stable under the action of* $\mathbb{Z}/2\mathbb{Z}$. *The subgroup* H *is the unique maximal normal subgroup of* $\mathrm{Im}(\rho)$.

Let V_n denote the dihedral group[3] of order $2n$. Note that the projective image (= the image in $\mathrm{PGL}_2(\overline{\mathbb{F}}_2)$) of W_n is isomorphic to V_n, and that every irreducible subgroup G of W_n has projective image isomorphic to V_m for some $m \leq n$. For example, if $G \simeq V_n$, then it contains no non-trivial scalar matrix, and its projective image is also isomorphic to V_n.

[3]We use this notation to distinguish dihedral groups from decomposition groups.

We require one further group theoretic lemma.

Lemma 2.2. *Assume the notation above.*

(1) *If $n \geq 3$ is odd, then there are $\varphi(n)^2/2$ isomorphism classes of faithful representations*

$$\rho : W_n \to \mathrm{GL}_2(\overline{\mathbb{F}}_2),$$

where $\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times$. They are defined over $\mathbb{F}_{2^m}$, where m is the least integer for which $n \mid (2^m - 1)$.

(2) *Let I be a non-trivial subgroup of the subgroup $\mu_n \times \{1\}$ of W_n. There are $\varphi(n)$ isomorphism classes of faithful representations*

$$\rho : W_n \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$$

for which $\dim V^{\rho(I)} = 1$, where $V = \overline{\mathbb{F}}_2 \oplus \overline{\mathbb{F}}_2$ is the representation space of ρ. They are $\mathrm{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)$-conjugate to each other.

Proof. By Lemma 2.1, after conjugation, we may assume that $\mathrm{Im}(\rho)$ is contained in the subgroup W of $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$. If ρ is faithful, then $\mathrm{Im}(\rho)$ coincides with the subgroup W_n of W. In particular, such ρ is automatically irreducible. Fix a generator ζ of μ_n. For the moment, denote the diagonal matrix $\left(\begin{smallmatrix}\xi & \\ & \eta\end{smallmatrix}\right)$ by (ξ, η). Suppose that ρ maps the elements $(\zeta, 1), (1, \zeta) \in \mu_n \times \mu_n \subset W_n$ to $(\zeta^a, \zeta^b), (\zeta^c, \zeta^d)$, respectively, where $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$. Since ρ is compatible with the involution $\tau : (\zeta^x, \zeta^y) \mapsto (\zeta^y, \zeta^x)$, we must have $a = d$ and $b = c$. Indeed, we have $\rho(\zeta^x, \zeta^y) = (\zeta^{ax+cy}, \zeta^{bx+dy})$ and $\rho(\zeta^y, \zeta^x) = (\zeta^{ay+cx}, \zeta^{by+dx})$. But we have also

$$\rho(\zeta^y, \zeta^x) = \rho((\zeta^x, \zeta^y)^\tau) = (\rho(\zeta^x, \zeta^y))^\tau = (\zeta^{bx+dy}, \zeta^{ax+cy}).$$

Therefore, we have that $(\zeta^{ay+cx}, \zeta^{by+dx}) = (\zeta^{bx+dy}, \zeta^{ax+cy})$ for all $x, y \in \mathbb{Z}/n\mathbb{Z}$, and hence that $a = d$ and $b = c$.

Conversely, for each $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^2$, we have a representation

$$\rho_{a,b} : W_n \to W_n \subset \mathrm{GL}_2(\overline{\mathbb{F}}_2)$$

which maps $(\zeta, 1)$ to (ζ^a, ζ^b). It is defined over $\mathbb{F}_{2^m}$ if $\mu_n \subset \mathbb{F}_{2^m}$ (i.e. if $n \mid (2^m - 1)$). It induces on the subgroup $\mu_n \times \mu_n$ of W_n a $(\mathbb{Z}/n\mathbb{Z})$-module endomorphism which is represented by the matrix $\left(\begin{smallmatrix}a & b \\ b & a\end{smallmatrix}\right)$. Hence $\rho_{a,b}$ is faithful if and only if $a^2 - b^2 \in (\mathbb{Z}/n\mathbb{Z})^\times$. Such pairs $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^2$ are parametrized by $(u, v) \in (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ as $a + b = u$, $a - b = v$, so that there are $\varphi(n)^2$ such pairs (a, b). Also, we have $\rho_{a',b'} \simeq \rho_{a,b}$ if and only if $(a', b') = (a, b)$ or (b, a). Thus there are just $\varphi(n)^2/2$ isomorphism classes of such representations $\rho_{a,b}$. This proves (1).

Now we prove (2). The condition $\dim V^{\rho_{a,b}(I)} = 1$ means that a or b is 0. There are just $\varphi(n)$ isomorphism classes of such representations. Since $\mathrm{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)$ acts transitively on the set $\{\zeta^a \ : \ a \in (\mathbb{Z}/n\mathbb{Z})^\times\}$ of primitive nth roots of unity, the representations $\rho_{a,0}$ are mapped to each other by elements of $\mathrm{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)$. □

Using these preliminary facts, in this section we shall prove Theorem 1.4 (1), (3-6), and we defer the proof of Theorem 1.4 (2) to Section 3.

Remark. Note that all the representations in Theorem 1.4 have solvable images.

The proof of these cases of Theorem 1.4 depends on the analysis of the ramification of the representations ρ at each prime $q \mid 2N(\rho)$. For each prime q, let D_q ($\subset G_{\mathbb{Q}}$) be the decomposition subgroup for a choice of an extension $\mathfrak{q}$ of the prime ideal (q) to $\overline{\mathbb{Q}}$, and I_q its inertia subgroup. By the embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{\mathfrak{q}}$, we identify D_q with the absolute Galois group $G_{\mathbb{Q}_q}$ of the q-adic field $\mathbb{Q}_q$. For a representation

$$\rho : D_q \to \mathrm{GL}_2(\mathbb{F})$$

over any discrete field $\mathbb{F}$, let $e_q = e_q(\rho)$ denote its ramification index (i.e. the ramification index of the extension $K/\mathbb{Q}_q$ cut out by ρ, or equivalently the order of $\rho(I_q)$).

We first consider the case where $q = 2$. The following proposition improves Tate's discriminant bound at 2 (Formula $(*)$ on p. 154 of [28]); it reduces the valuation by $1/2$ in the "general" case.

Proposition 2.3. *Let $\rho : D_2 \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be a 2-dimensional representation of D_2 over $\overline{\mathbb{F}}_2$.*

(1) *The ramification index e_2 of ρ is either a power of 2, or is an odd integer.*
(2) *Suppose that ρ is wildly ramified, and has ramification index 2^m with $m \geq 1$. Let $K/\mathbb{Q}_2$ be the extension cut out by ρ, and let $\mathcal{D}_{K/\mathbb{Q}_2}$ be its different. Then we have*

$$v_2(\mathcal{D}_{K/\mathbb{Q}_2}) \;=\; \begin{cases} 1 \text{ or } 3/2 & \text{if } \rho \text{ is abelian and } m = 1, \\ 2 & \text{if } \rho \text{ is abelian and } m = 2, \\ 2 - 1/2^{m-1} & \text{if } \rho \text{ is non-abelian,} \end{cases}$$

where v_2 is the valuation of K normalized by $v_2(2) = 1$.

Remark. In the proposition above, we say that ρ is abelian if $\mathrm{Im}(\rho)$ is an abelian group. If ρ is wildly ramified and abelian, then note that the only possible values of m are 1 and 2. If ρ is wildly ramified and non-abelian, then we have $m \geq 2$.

Proof. Suppose ρ is wildly ramified (i.e. e_2 is even). The wild inertia subgroup G_1 of $G = \rho(D_2)$ is then a non-trivial 2-group. After conjugation, we may assume that G_1 is contained in $\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$. Since G_1 is normal in G and the normalizer of $\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ is $\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)$, it follows that ρ is reducible. Suppose that

$$\rho = \begin{pmatrix} \psi_1 & * \\ & \psi_2 \end{pmatrix},$$

where $\psi_i : D_2 \to \overline{\mathbb{F}}_2^{\times}$ are characters of D_2. By local class field theory, the inertia subgroup of $D_2^{\mathrm{ab}} = \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/\mathbb{Q}_2)$ is identified with $\mathbb{Z}_2^{\times}$, which is a pro-2 group. Hence the ψ_i must be unramified, and ρ has a 2-power ramification index. This proves (1).

To calculate the different of $K/\mathbb{Q}_2$, let K_0 be the maximal unramified subextension of $K/\mathbb{Q}_2$. We shall calculate the different $\mathcal{D}_{K/K_0}$ of K/K_0, which is equal to $\mathcal{D}_{K/\mathbb{Q}_2}$. Suppose first that $\psi_1 = \psi_2$. This is equivalent to saying that ρ is abelian (cf. Lemma 3.1 below). Then K is the compositum of K_0 and a totally ramified abelian extension K_1 over $\mathbb{Q}_2$ with Galois group isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$. Such a K_1 is contained in $\mathbb{Q}_2(\zeta_8)$, where ζ_8 is a primitive

8th root of unity. Then we have $m = 1$ or 2, and

$$v_2(\mathcal{D}_{K/K_0}) \;=\; v_2(\mathcal{D}_{K_1/\mathbb{Q}_2}) \;=\; \begin{cases} 1 & \text{if } K_1 = \mathbb{Q}_2(\sqrt{-1}), \\ 3/2 & \text{if } K_1 = \mathbb{Q}_2(\sqrt{\pm 2}), \\ 2 & \text{if } K_1 = \mathbb{Q}_2(\zeta_8). \end{cases}$$

To analyze the case where $\psi_1 \neq \psi_2$, let $X = \mathrm{Hom}(\mathrm{Gal}(K/K_0), \mathbb{C}^\times)$ be the character group of $\mathrm{Gal}(K/K_0)$. By assumption, we have $X \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus m}$. If A denotes the valuation ring $\mathcal{O}_{K_0}$ of K_0, then by local class field theory, X can be identified with a subgroup of $\mathrm{Hom}(A^\times/(A^\times)^2, \mathbb{C}^\times)$, and then the subgroup X_i of X consisting of the characters with conductor dividing 2^i is identified with a subgroup of $\mathrm{Hom}(A^\times/(1+2^iA)^\times(A^\times)^2, \mathbb{C}^\times)$. It is easy to see that

$$X = X_3 \supset X_2 \supset X_1 = X_0 = \{1\}.$$

Moreover, Tate showed ([28], p. 155; see also the proof of Theorem 3 of [16]) that $(X_3 : X_2) = 1$ or 2.

Let $\sigma \in D_2$ be a lifting of the Frobenius element of D_2/I_2 ($\simeq \mathrm{Gal}(\overline{\mathbb{F}}_2/\mathbb{F}_2)$). It acts on $A^\times$ and $\mathrm{Gal}(K/K_0)$ in a way compatible with the reciprocity map. Also we let σ act on X by $\chi \mapsto \chi \circ \sigma$. Since the action of σ on A is a ring automorphism of A, it preserves the filtration $(1+2^iA)_{i\geq 1}$, and hence the action of σ on X preserves the filtration $X_3 \supset X_2 \supset X_1 = X_0$. In terms of the image of ρ, the action of σ on $\mathrm{Gal}(K/K_0) = \rho(I_2)$ can be visualized as follows (cf. [16], Sect. 1). Write $\rho(\sigma) = \left(\begin{smallmatrix} a_1 & b \\ & a_2 \end{smallmatrix}\right)$, and note that it acts on the subgroup $\rho(I_2) \subset \left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$ by conjugation:

$$\begin{pmatrix} a_1 & b \\ & a_2 \end{pmatrix} \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} a_1 & b \\ & a_2 \end{pmatrix}^{-1} \;=\; \begin{pmatrix} 1 & a_1 a_2^{-1} x \\ & 1 \end{pmatrix}.$$

Set $\alpha = a_1 a_2^{-1} \in \overline{\mathbb{F}}_2^\times$. The above formula shows that, if α has order f as an element of $\overline{\mathbb{F}}_2^\times$, then each non-trivial element of X is in a unique $\langle\alpha\rangle$-orbit which has cardinality f. Suppose $\psi_1 \neq \psi_2$ (i.e. $a_1 \neq a_2$), so that α has order $f \geq 3$. If $(X_3 : X_2) = 2$, then $X_3 \smallsetminus X_2$ has just 2^{m-1} elements, and is at the same time a disjoint union of $\langle\alpha\rangle$-orbits of odd cardinality $f \geq 3$; this is a contradiction. Thus we have that $X = X_2$ (i.e. all non-trivial $\chi \in X$ have conductor 4). By the Führerdiskriminantenproduktformel, we have

$$v_2(\mathcal{D}_{K/K_0}) \;=\; \frac{1}{2^m} v_2\left(\prod_{\chi \in X} \mathfrak{f}(\chi)\right) \;=\; \frac{(2^m - 1) \times 2}{2^m} \;=\; 2 - \frac{1}{2^{m-1}},$$

where $\mathfrak{f}(\chi)$ is the conductor of χ. This completes the proof of Proposition 2.3. □

Remark. The proof of Proposition 2.3 depends on the fact that $X_3 \smallsetminus X_2$ has 2-power order if it is non-empty. This phenomenon does not hold in general for representations $\rho : D_\ell \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ when ℓ is an odd prime. To see this, note that the set of characters of maximal conductor has cardinality $\ell^{m-1}(\ell-1)$, which is not a power of ℓ for odd primes ℓ (for example, see the proof of Theorem 3 in [16]).

Next we consider ramification at primes $q \neq 2$. The following general lemma, which improves on Lemma 2 of [16], suffices for our purposes.

Lemma 2.4. *Let ℓ and q be distinct primes, and let m be a positive integer. If $\rho : D_q \to \mathrm{GL}_2(\mathbb{F}_{\ell^m})$ has $n_q(\rho) = 1$, then ρ is reducible, and its ramification index e_q either equals ℓ or divides $\gcd(q-1, \ell^m - 1)$. If $e_q \neq \ell$, then the representation ρ is completely reducible (i.e. diagonalizable).*

Proof. Since $n_q(\rho) = 1$, the inertia subgroup $\rho(I_q)$ fixes a subspace of dimension one. Since $\rho(I_q)$ is normal in $\rho(D_q)$, this subspace is stable under $\rho(D_q)$ (i.e. ρ is reducible). Then we may assume that ρ is of the form

$$\rho = \begin{pmatrix} \psi_1 & * \\ & \psi_2 \end{pmatrix}, \qquad \psi_i : D_q \to \mathbb{F}_{\ell^m}^\times,$$

and where ψ_1 is unramified. The restriction of ψ_2 to I_q factors through the inertia subgroup of $D_q^{\mathrm{ab}} = \mathrm{Gal}(\mathbb{Q}_q^{\mathrm{ab}}/\mathbb{Q}_q)$, which is identified by local class field theory with $\mathbb{Z}_q^\times$. Since ψ_2 is at most tamely ramified, it factors through $(\mathbb{Z}_q/q\mathbb{Z}_q)^\times$. Thus $\psi_2(I_q)$ has order dividing $\gcd(q-1, \ell^m - 1)$. Also, the ℓ-primary part of the abelian group $\rho(I_q)$ has order at most ℓ, because the tame inertia group is cyclic (in fact, the maximal pro-ℓ quotient of I_q is isomorphic to $\mathbb{Z}_\ell$ (cf. [23], Sect. 1)), while the group $\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$ is ℓ-torsion. Thus $\rho(I_q)$ has order dividing $\ell \cdot \gcd(q-1, \ell^m - 1)$. But since $\rho(I_q)$ is abelian, it cannot have order strictly divisible by ℓ, whence the conclusion. Indeed, suppose there are elements σ, $\tau \in \rho(I_q)$ of orders s, ℓ, respectively, where $s > 1$ and is prime to ℓ. They must be of the form

$$\sigma = \begin{pmatrix} 1 & b \\ & d \end{pmatrix} \quad \text{with } d \neq 1, \quad \text{and} \quad \tau = \begin{pmatrix} 1 & t \\ & 1 \end{pmatrix} \quad \text{with } t \neq 0.$$

These do not commute.

Suppose $e_q \neq \ell$. If ρ is not completely reducible, then there is an element $\tau \in \rho(D_q) \smallsetminus \rho(I_q)$ of order ℓ (cf. (1) of Lemma 3.1). Then $\langle \tau \rangle$ is the unique ℓ-Sylow subgroup of $\rho(D_q)$. Since $\rho(I_q)$ is also non-trivial and normal in $\rho(D_q)$, these two subgroups commute. But this is a contradiction, as can be seen in a similar way to the above arguments. Hence ρ is completely reducible. □

Example. Here we provide some values of q, m, and e_q, when $\ell = 2$. Apart from the case where $q = 257$, we shall require these values later.

(1) If $q = 3, 5, 17, 257$, then $\gcd(q-1, 2^m - 1) = 1$. Consequently, Lemma 2.4 implies that $e_q = 2$ for all $m \geq 1$.
(2) If $q = 7$ or 13, then $\gcd(q-1, 2^m - 1) = \gcd(3, 2^m - 1) = 1$ or 3, depending on whether m is odd or even. Hence, Lemma 2.4 implies that

$$e_q = \begin{cases} 2 & \text{if } m \text{ is odd,} \\ 2 \text{ or } 3 & \text{if } m \text{ is even.} \end{cases}$$

(3) If $q = 11$, then a similar argument easily implies that

$$e_q = \begin{cases} 2 & \text{if } 4 \nmid m, \\ 2 \text{ or } 5 & \text{if } 4 \mid m. \end{cases}$$

Proof of Theorem 1.4 (1), (3-6). All of these cases are proved almost simultaneously. Suppose there is an irreducible representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ with $N(\rho) = N$, where $N = 1, 3, 5, 7, 11, 13, 15$ or 17. Since the cases where $N(\rho) = 1, 3$ are handled respectively in [28] and [15], we only consider the remaining cases. As in [28], we distinguish the two cases where $G = \mathrm{Im}(\rho)$ is solvable and non-solvable. Let $K/\mathbb{Q}$ be the extension cut out by ρ, so that we have $G = \mathrm{Gal}(K/\mathbb{Q})$.

First we deal with the solvable cases. If G is solvable, then after conjugation, it is contained in W_n for some odd $n \geq 3$, and it sits in the exact sequence from Lemma 2.1 (2):

$$1 \to H \to G \to \mathbb{Z}/2\mathbb{Z} \to 1, \qquad H \subset (\overline{\mathbb{F}}_2^{\times})^2.$$

Hence, K is an abelian extension of odd degree over the quadratic field F corresponding to H. Since K is unramified outside $2N$, so is F, and it is a quadratic subfield of $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{N})$ if $N \neq 15$ (resp. $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5})$ if $N = 15$). By Lemma 2.4, the ramification index e_q of ρ at $q \mid N$ is either 2 or an odd factor of $q - 1$. Hence if $N = 5, 15$ or 17, we have $e_q = 2$ for all $q \mid N$.

We first assume that $e_q = 2$ also for the other N. Suppose $N = 5, 7, 11$ or 17. Since each quadratic subfield F of $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{N})$ has class number dividing 4, the ideal class group of F does not contribute to the abelian extension K/F of odd degree. Since K/F is unramified at $q = N$, by Lemma 2.4 together with the assumption that $e_q = 2$, the Galois group $\mathrm{Gal}(K/F)$ is, by class field theory, a quotient of the unit group $\mathcal{O}_{F,2}^{\times}$ of the 2-adic completion $\mathcal{O}_{F,2} = \mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_2$ of $\mathcal{O}_F$. Its prime-to-2 quotient has order at most 3, which is possible only when 2 is inert in $F/\mathbb{Q}$. Since $G = \mathrm{Im}(\rho)$ has to be embedded irreducibly into $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$, it must be isomorphic to $\mathrm{SL}_2(\mathbb{F}_2) \simeq V_3 \simeq S_3$. According to [10], if $N = 5, 7$ or 17, there are no S_3-extensions $K/\mathbb{Q}$ which are unramified outside $2N$ and have $e_2 = 3$ and $e_N = 2$; and if $N = 11$, there exists only one such extension, which is the splitting field of the polynomial $x^3 - x^2 + x + 1$. It contains the quadratic field $F = \mathbb{Q}(\sqrt{-11})$.

Suppose $N = 13$. Three of the quadratic subfields F of $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{13})$ which ramify at 13 have class number 1 or 2, and the rest, $\mathbb{Q}(\sqrt{-26})$, has class number 6. If $F/\mathbb{Q}$ is unramified at 2, then $F = \mathbb{Q}(\sqrt{13})$, and 2 is inert there. Then $\mathcal{O}_{F,2}^{\times}$ has prime-to-2 quotient of order 3, but according to [10], there are no S_3-extension $K/\mathbb{Q}$ which are unramified outside $\{2, 13\}$ and have ramification index $e_2 = $ odd and $e_{13} = 2$. If $F/\mathbb{Q}$ is ramified at 2, then by Proposition 2.3 (1), K/F must be unramified everywhere, and K must be a cyclic extension of degree 3 of $F = \mathbb{Q}(\sqrt{-26})$. According to [10], there is just one S_3-extension of $\mathbb{Q}$ which is unramified outside $\{2, 13\}$ and has ramification index $e_2 = e_{13} = 2$, which is the splitting field of the polynomial $x^3 - x - 2$ and is an unramified extension of $F = \mathbb{Q}(\sqrt{-26})$.

Suppose $N = 15$. If $F/\mathbb{Q}$ is unramified at 2, then $F = \mathbb{Q}(\sqrt{-15})$. It has class number 2, and the prime 2 splits in $F/\mathbb{Q}$. Thus K/F must be trivial. If $e_2 = 2$, then $F = \mathbb{Q}(\sqrt{15})$ or $\mathbb{Q}(\sqrt{\pm 30})$, which has class number 2 or 4. By Lemma 2.4, K/F must be unramified everywhere, and hence the extension must be trivial.

Suppose next that $q = N = 7, 11$ or 13 and e_q is odd. Then since $F/\mathbb{Q}$ is ramified only at 2, the quadratic field F is either $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, or $\mathbb{Q}(\sqrt{-2})$. Since $\rho(D_q)$ is of odd order

by Lemma 2.4, the prime q splits in $F/\mathbb{Q}$, and hence we have

$$F = \begin{cases} \mathbb{Q}(\sqrt{2}) & \text{if } q = 7, \\ \mathbb{Q}(\sqrt{-2}) & \text{if } q = 11, \\ \mathbb{Q}(\sqrt{-1}) & \text{if } q = 13. \end{cases}$$

If $(q) = \mathfrak{q}_1\mathfrak{q}_2$ in $\mathcal{O}_F$, then one of the two inertia subgroups of $\mathfrak{q}_1$ and $\mathfrak{q}_2$ is mapped into $\left(\begin{smallmatrix} 1 & * \\ & \end{smallmatrix}\right)$ and the other into $\left(\begin{smallmatrix} * & \\ & 1 \end{smallmatrix}\right)$. They are exchanged by the action of $\mathrm{Gal}(F/\mathbb{Q}) \simeq \langle \left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right) \rangle$. These subgroups are described explicitly as follows: By Proposition 2.3 (1), K/F is ramified only at $q = N$. Since F has class number 1, by class field theory, $\mathrm{Gal}(K/F)$ is a quotient of $\mathcal{O}_{F,q}^\times/\mathcal{O}_F^\times(1 + q\mathcal{O}_{F,q})^\times \simeq (\mathbb{F}_q^\times \times \mathbb{F}_q^\times)/(\text{Image of } \mathcal{O}_F^\times)$, where $\mathcal{O}_{F,q} := \mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_q$. Note that $\mathrm{Gal}(K/F)$ is of odd order. The odd part of $\mathbb{F}_q^\times \times \mathbb{F}_q^\times$ is isomorphic to

$$\begin{cases} (\mathbb{Z}/3\mathbb{Z})^2 & \text{if } N = 7, 13, \\ (\mathbb{Z}/5\mathbb{Z})^2 & \text{if } N = 11. \end{cases}$$

Hence $\mathrm{Im}(\rho)$ is isomorphic to W_3 (resp. W_5) and $\rho(I_q)$ is identified with its subgroup $\mu_3 \times \{1\}$ (resp. $\mu_5 \times \{1\}$) if $N = 7, 13$ (resp. 11). But if $N = 7$, there does not exist such a ρ. Indeed, if there were a Galois extension $K/\mathbb{Q}$ with Galois group W_n, then it has a subextension with Galois group isomorphic to $V_n \simeq W_n/\{(\xi, \xi) |\ \xi \in \mu_n\}$. According to [10], there are no V_3-extensions of $\mathbb{Q}$ unramified outside $\{2, 7\}$.

If $N = 11$ (resp. 13), there do exist representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ with $N(\rho) = N$ and $\mathrm{Im}(\rho) \simeq W_5$ (resp. W_3). These are what we call ρ_{11}^{ε} and ρ_{13}^{ε}.

The part of the theorem concerning the number of isomorphism classes, and the Galois conjugacy of ρ with image isomorphic to W_n follows from Lemma 2.2 on representations of the finite group W_n.

The determinants of the representations ρ are known as follows: For $\rho = \rho_{11}$ and ρ_{13}, it is trivial to see that $\det \rho = 1$. If $\rho = \rho_{11}^{\varepsilon}$ (resp. ρ_{13}^{ε}), the character $\det \rho : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_2^\times$ factors through the maximal quotient of $(\mathbb{Z}/11\mathbb{Z})^\times$ (resp. $(\mathbb{Z}/13\mathbb{Z})^\times$) of odd order, which is of order 5 (resp. 3) (cf. [25], §1.3; see also the remark at the beginning of §4 below). On the other hand, as we saw above, $\det \rho(I_q)$ has order 5 (resp. 3). Hence $\det \rho$ is a character of conductor 11 (resp. 13) and of order 5 (resp. 3).

Next we prove the non-solvable case. This is done, as in [28], [15], [16], by the comparison of the Tate and Odlyzko bounds for discriminants. Suppose there exists a non-solvable representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ with $N(\rho) = N$, where $= 5, 7, 11, 13, 15$ or 17. Let $K/\mathbb{Q}$ be the extension cut out by ρ. We denote by $d_{K/\mathbb{Q}}$ the discriminant of $K/\mathbb{Q}$, and $d_K^{1/n} = |d_{K/\mathbb{Q}}|^{1/n}$ the root discriminant of K, where $n = [K : \mathbb{Q}]$. We compare the Tate and Odlyzko bounds for $d_K^{1/n}$ and deduce a contradiction.

Let $d_{K,q}$ be the q-primary part of $|d_{K/\mathbb{Q}}|$, and write $d_K^{1/n} = \prod_q d_{K,q}^{1/n}$. We have $(d_{K,q}) = \prod_{v|q} N_{K_v/\mathbb{Q}_q}(\mathcal{D}_{K_v/\mathbb{Q}_q})$, where K_v is the v-adic completion of K at a prime v of K lying above q, $\mathcal{D}_{K_v/\mathbb{Q}_q}$ the different of $K_v/\mathbb{Q}_q$, and $N_{K_v/\mathbb{Q}_q}$ is the norm map of $K_v/\mathbb{Q}_q$. For each q, we shall calculate $d_{K,q}^{1/n}$ as $q^{v_q(\mathcal{D}_{K_v/\mathbb{Q}_q})}$, for any $v \mid q$. For $q = 2$, this is done by Proposition 2.3 (2). For $q \mid N$, since $K_v/\mathbb{Q}_q$ is tamely ramified, we have $v_q(\mathcal{D}_{K_v/\mathbb{Q}_q}) = (e_q - 1)/e_q$ if e_q denotes the ramification index of $K_v/\mathbb{Q}_q$, and the value of e_q is given by Lemma 2.4.

To apply Lemma 2.4, we shall twist ρ by a character so that it lands on as small a subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ as possible. We have canonical isomorphisms $\mathrm{SL}_2(\overline{\mathbb{F}}_2) = \mathrm{PSL}_2(\overline{\mathbb{F}}_2) = \mathrm{PGL}_2(\overline{\mathbb{F}}_2)$, and an isomorphism

$$\begin{aligned} \mathrm{GL}_2(\overline{\mathbb{F}}_2) &\xrightarrow{\sim} \mathrm{SL}_2(\overline{\mathbb{F}}_2) \times \overline{\mathbb{F}}_2^{\times} \\ g &\mapsto (g\delta(g)^{-1}, \delta(g)), \end{aligned}$$

where we set $\delta(g) = \det(g)^{1/2}$. This maps $\mathrm{GL}_2(\mathbb{F}_{2^m})$ to $\mathrm{SL}_2(\mathbb{F}_{2^m}) \times \mathbb{F}_{2^m}^{\times}$, for each $m \geq 1$. The character $\delta : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_2^{\times}$ is tamely ramified at $q \mid N$, and factors through the maximal quotient of $(\mathbb{Z}/N\mathbb{Z})^{\times}$ of odd order. By Sections 251–253 of [7], the projective image of ρ (i.e. the image of $\mathrm{Im}(\rho)$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_2)$) is conjugate in $\mathrm{PGL}_2(\overline{\mathbb{F}}_2)$ to $\mathrm{PGL}_2(\mathbb{F}_{2^\mu}) = \mathrm{PSL}_2(\mathbb{F}_{2^\mu})$, where 2^μ is the order of the 2-Sylow subgroup of $\mathrm{Im}(\rho)$. Since we assume $\mathrm{Im}(\rho)$ is non-solvable, we have $\mu \geq 2$. After replacing ρ by a conjugate, we may assume that

$$\rho_0 := \rho \otimes \delta^{-1} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$$

has values in $\mathrm{GL}_2(\mathbb{F}_{2^\mu})$, and its image is the simple group $\mathrm{SL}_2(\mathbb{F}_{2^\mu})$. Then ρ has values in $\mathrm{GL}_2(\mathbb{F}_{2^m})$, where $\mathbb{F}_{2^m} := \mathbb{F}_{2^\mu}(\mathrm{Im}(\det\rho))$. Note that μ divides m.

Suppose there is a ρ with $\mu = 2$. Then there should be an A_5-extension $K_0/\mathbb{Q}$ cut out by $\rho_0 : G_{\mathbb{Q}} \to \mathrm{SL}_2(\mathbb{F}_4) \simeq A_5$ which is unramified outside $2N$. According to [10], there are no such extensions if $N = 7, 11$ or 13. If $N = 15$ (resp. 17), then there are 51 (resp. one) such extensions, but none of them have ramification index $e_q = 2$ at $q \mid N$, as required by Lemma 2.4. Thus we have $\mu \geq 3$.

Suppose there is a ρ with $\mu \geq 3$. By Proposition 2.3, Lemma 2.4 and the examples following it, we have:

$$d_K^{1/n} \leq \begin{cases} 4 \cdot 5^{1/2} = 8.9442... & \text{if } N = 5, \\ 4 \cdot 7^{2/3} = 14.6372... & \text{if } N = 7, \\ 4 \cdot 11^{1/2} = 13.2664... & \text{if } N = 11 \text{ and } 4 \nmid m, \\ 4 \cdot 11^{4/5} = 27.2379... & \text{if } N = 11 \text{ and } 4 \mid m, \\ 4 \cdot 13^{1/2} = 14.4222... & \text{if } N = 13 \text{ and } 2 \nmid m, \\ 4 \cdot 13^{2/3} = 22.1150... & \text{if } N = 13 \text{ and } 2 \mid m, \\ 4 \cdot 15^{1/2} = 15.4919... & \text{if } N = 15, \\ 4 \cdot 17^{1/2} = 16.4924... & \text{if } N = 17. \end{cases} \tag{2.3}$$

If $n = [K : \mathbb{Q}]$ is equal to or larger than $|\mathrm{SL}_2(\mathbb{F}_{2^3})| = 504$, then the Odlyzko bound [17] gives unconditionally

$$d_K^{1/n} > 20.023, \tag{2.4}$$

and under the GRH gives

$$d_K^{1/n} > 26.485. \tag{2.5}$$

These inequalities provide a contradiction unconditionally if either $N = 5, 7, 15, 17$, or $N = 13$ and m is odd (resp. under the GRH if $N = 13$ and m is even).

The $N = 11$ case is a bit more involved. Recall that $\mathbb{F}_{2^m} = \mathbb{F}_{2^\mu}(\mathrm{Im}(\det\rho))$. Suppose first that $\det\rho$ is trivial. Then we have $m = \mu$. If $4 \nmid m$, then (2.3) contradicts (2.4). If $4 \mid m$, then the Odlyzko bound gives under the GRH that, for $n \geq |\mathrm{SL}_2(\mathbb{F}_{2^4})| = 4080$,

$$d_K^{1/n} \ > \ 31.645, \tag{2.6}$$

which contradicts (2.3).

If $\det\rho$ is non-trivial, then since it factors through a quotient of $(\mathbb{Z}/11\mathbb{Z})^\times$ of odd order, its image has order 5 (so we have $4 \mid m$). This implies the ramification index $e_{11}(\rho)$ of ρ at 11 is divisible by 5. By Lemma 2.4, we have that $e_{11}(\rho) = 5$. Then $e_{11}(\rho_0)$ divides $e_{11}(\rho) = 5$. By [28], ρ_0 cannot be unramified at 11. Hence $e_{11}(\rho_0) = 5$. In particular, $\mathrm{Im}(\rho_0) = \mathrm{SL}_2(\mathbb{F}_{2^\mu})$ has order divisible by 5. Hence μ must be even. Since we assumed $\mu \geq 3$, we have $\mu \geq 4$. Then under the GRH, (2.3) and (2.6) contradict each other. Now the proof is complete. □

3. Mod 2 representations of conductor 9

To complete the proof of Theorem 1.4, we must handle the case where $N(\rho) = 9$ (i.e. Theorem 1.4 (2)). Here we prove this remaining case. We require two preliminary lemmas.

Lemma 3.1. *Let G be a finite subgroup of $\mathrm{GL}_2(\mathbb{F})$, where $\mathbb{F}$ is a field of characteristic $\ell > 0$.*

1. *If the representation $G \hookrightarrow \mathrm{GL}_2(\mathbb{F})$ is reducible and the order of G is not divisible by ℓ, then G is diagonalizable (i.e. it is conjuate to a subgroup of $\left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right)$).*
2. *If G is abelian and its order is divisible by ℓ, then G is the direct product of a subgroup H of scalar matrices and a subgroup U of unipotent matrices (i.e. it is conjugate to a subgroup of $\left\{\left(\begin{smallmatrix} a & b \\ & a \end{smallmatrix}\right) \middle|\ a \in \mathbb{F}^\times, b \in \mathbb{F}\right\}$).*

Proof. Conclusion (1) is a basic fact in the theory of linear representations of finite groups. Namely, every finite-dimensional representation of G over a field of characteristic $\ell \nmid |G|$ is completely reducible (for example, see [20]).

To prove (2), we may assume that the ℓ-Sylow subgroup of G is contained in $\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$, and then that $G \subset \left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)$. Since $\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$ is the unique maximal ℓ-torsion subgroup of $\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)$, the subgroup G of $\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)$ has a unique ℓ-Sylow subgroup $U := G \cap \left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$. Let $\tau = \left(\begin{smallmatrix} 1 & t \\ & 1 \end{smallmatrix}\right) \in U$ be a non-trivial element. Then the commutant in $\mathrm{GL}_2(\mathbb{F})$ of $\langle\tau\rangle$ is $\left\{\left(\begin{smallmatrix} a & b \\ & a \end{smallmatrix}\right) \ : \ a \in \mathbb{F}^\times, b \in \mathbb{F}\right\} = \left\{\left(\begin{smallmatrix} a & \\ & a \end{smallmatrix}\right) \ : \ a \in \mathbb{F}^\times\right\} \times \left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$, of which the first factor has no ℓ-torsion and the second factor is of ℓ-torsion. As a subgroup, G has a similar structure. □

Lemma 3.2. *If $\rho : D_3 \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ has $n_3(\rho) = 2$, then the following are both true.*

1. *We have that ρ is wildly ramified, and possibly after conjugation, we have $\rho(D_3) \subset \left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right)$ and $\rho(I_3) \subset \left(\begin{smallmatrix} 1 & \\ & * \end{smallmatrix}\right)$. If G_i denotes the ith ramification subgroup of $\rho(D_3)$, then $G_0 = G_1 \simeq \mathbb{Z}/3\mathbb{Z}$ and $G_2 = \{1\}$.*
2. *Let $K/\mathbb{Q}_3$ be the extension cut out by ρ, and let $\mathcal{D}_{K/\mathbb{Q}_3}$ be its different. Then we have*

$$v_3(\mathcal{D}_{K/\mathbb{Q}_3}) \ = \ \frac{4}{3},$$

where v_3 is the valuation of K normalized by $v_3(3) = 1$.

Proof. Suppose ρ is irreducible. Then by Lemma 2.1, after conjugation, its image $G = \rho(D_3)$ sits in the exact sequence in Lemma 2.1 (2):

$$1 \to H \to G \to \mathbb{Z}/2\mathbb{Z} \to 1,$$

where H is a subgroup of $\left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right)$, and G is a semidirect product of H and the subgroup generated by $\tau = \left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right)$. By Lemma 3.1 (2), G is not abelian. In particular, the inertia subgroup $G_0 = \rho(I_3)$ of G is non-trivial. Since G_0 is normal in G and ρ is assumed irreducible, the fixed subspace of $V = \overline{\mathbb{F}}_2 \oplus \overline{\mathbb{F}}_2$ by G_0 is $\{0\}$. It then follows from the assumption $n_3(\rho) = 2$ that ρ is tamely ramified. Suppose $G_0 \not\subset H$; thus G_0 maps surjectively onto $\mathbb{Z}/2\mathbb{Z}$, so that there is an element τ' of G_0 of order 2. Then $\langle \tau' \rangle$, being the unique 2-Sylow subgroup of the tame inertia, is normal in G, and hence G is the direct product of H and $\langle \tau' \rangle$. In particular, G is abelian. This is a contradiction, and hence $G_0 \subset H$. Thus H is the Galois group of a tamely ramified abelian extension of the unramified quadratic extension F of $\mathbb{Q}_3$. By local class field theory, there is a surjective homomorphism $F^\times \to H$, and the tame inertia subgroup G_0 is isomorphic to a quotient of $\mathbb{F}_9^\times \simeq \mathbb{Z}/8\mathbb{Z}$. Since G_0 is a subgroup of $\left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right) \simeq \overline{\mathbb{F}}_2^\times \times \overline{\mathbb{F}}_2^\times$, it must be $\{1\}$, and hence G is abelian. This is again a contradiction. Thus ρ cannot be irreducible in any event, and we may assume that

$$\rho \;=\; \begin{pmatrix} \psi_1 & * \\ & \psi_2 \end{pmatrix},$$

where $\psi_i : D_3 \to \overline{\mathbb{F}}_2^\times$ are characters. Since $\psi_i(I_3)$ is of odd order, by local class field theory, the restriction of ψ_i to I_3 factors through $(1 + 3\mathbb{Z}_3)^\times$ (i.e. ψ_i is either unramified or wildly ramified). The condition that

$$n_3(\rho) \;=\; \dim(V/V^{G_0}) + \dim(V/V^{G_1})/(G_0 : G_1) + \cdots \;=\; 2$$

implies that ψ_1 is unramified, and that ψ_2 is wildly ramified with $n_3(\psi_2) = 2$ (if $\rho|_{I_3}$ is completely reducible, the role of ψ_1 and ψ_2 may be switched). By Lemma 3.1 (1), the wild inertia subgroup G_1 of G_0 is, after conjugation, contained in $\left(\begin{smallmatrix} 1 & \\ & * \end{smallmatrix}\right)$. Since the normalizer in $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ of any non-trivial subgroup of $\left(\begin{smallmatrix} 1 & \\ & * \end{smallmatrix}\right)$ is $\left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right)$, and since G_1 is normal in G, we have $G \subset \left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right)$. Thus we have

$$\rho \;=\; \begin{pmatrix} \psi_1 & \\ & \psi_2 \end{pmatrix},$$

in which ψ_1 is unramified and $n_3(\psi_2) = 2$. It then follows also that $G_0 = G_1 \simeq \mathbb{Z}/3\mathbb{Z}$ and $G_2 = \{1\}$. This proves claim (1).

To prove claim (2), observe that there are two non-trivial $\mathbb{C}^\times$-valued characters of G_0, both of which have conductor 3^2. By the Führerdiskriminantenproduktformel, we have

$$v_3(\mathcal{D}_{K/\mathbb{Q}_3}) \;=\; \frac{1}{3}(2 \times 2) \;=\; \frac{4}{3}.$$

□

Proof of Theorem 1.4 (2). Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be an irreducible representation with $N(\rho) = 9$. Again, we consider the solvable and non-solvable cases separately.

Suppose $\mathrm{Im}(\rho)$ is solvable. Then $\mathrm{Im}(\rho)$ sits in the exact sequence in Lemma 2.1 (2):

$$1 \to H \to \mathrm{Im}(\rho) \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

Let $K/\mathbb{Q}$ be the extension cut out by ρ, so that $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Im}(\rho)$, and let F be the quadratic subfield of K corresponding to H. By assumption, $K/\mathbb{Q}$ is unramified outside $\{2,3\}$. By Lemma 3.2, the prime 3 splits in $F/\mathbb{Q}$, and hence $F = \mathbb{Q}(\sqrt{-2})$. It has class number 1. By class field theory and the condition $N(\rho) = 3^2$, the Galois group $H = \mathrm{Gal}(K/F)$ is isomorphic to a quotient of

$$\mathcal{O}_{F,3}^{\times}/\mathcal{O}_F^{\times}(1+3^2\mathcal{O}_{F,3})^{\times} \simeq (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}.$$

Since H must fit into the above exact sequence, and since $\rho(D_3)$ is as described in Lemma 3.2, we have that

$$H = H_1 \times H_2,$$

where $H_i \simeq \mathbb{Z}/3\mathbb{Z}$, and the two factors H_i are exchanged by the action of $\mathrm{Gal}(F/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ (note. Each factor H_i of H corresponds to the inertia subgroup of one of the two primes of F lying above 3). Hence $\mathrm{Im}(\rho)$ is isomorphic to W_3. By Lemma 2.2, there are two isomorphism classes of such ρ which are defined over $\mathbb{F}_4$, and they are $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$-conjugate to each other. Arguing as in the previous section, it turns out that $\det\rho$, for these representations ρ, are characters of conductor 9 and order 3.

Next suppose that there is a representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ with non-solvable image. By Proposition 2.3, we have $v_2(\mathcal{D}_{K/\mathbb{Q}}) \leq 2$. By Lemma 3.2, we have $v_3(\mathcal{D}_{K/\mathbb{Q}}) = 4/3$. Hence the root discriminant $d_K^{1/n}$ of $K/\mathbb{Q}$ satisfies

$$d_K^{1/n} \leq 2^2 \cdot 3^{4/3} = 17.3069\cdots.$$

If $n \geq 504 = |\mathrm{SL}_2(\mathbb{F}_{2^3})|$, then the Odlyzko bound [17] implies unconditionally that

$$d_K^{1/n} > 20.023.$$

Hence there are no such ρ with $\mu \geq 3$, where 2^μ is the order of the 2-Sylow subgroup of $\mathrm{Im}(\rho)$. If $\mu = 2$, then there must be a Galois extension $K/\mathbb{Q}$ with Galois group isomorphic to $\mathrm{SL}_2(\mathbb{F}_4) \simeq A_5$ which is unramified outside $\{2,3\}$. According to [10], there are no such extensions. If $\mu = 1$, then $\mathrm{Im}(\rho)$ is solvable. □

4. Traces of mod 2 representations

In this section, we study the traces of representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$. First recall the following fact on characters of $G_{\mathbb{Q}}$ (cf. [25], §1.3): Let

$$\psi : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_\ell^{\times}$$

be a character with $N(\psi) = N$. By class field theory, it factors through the map $G_{\mathbb{Q}} \to (\mathbb{Z}/\ell^a N\mathbb{Z})^{\times}$ for some $a \geq 0$ which maps a Frobenius element Frob_p to the class of p (mod $\ell^a N$). We have $(\mathbb{Z}/\ell^a N\mathbb{Z})^{\times} \simeq (\mathbb{Z}/\ell^a\mathbb{Z})^{\times} \times (\mathbb{Z}/N\mathbb{Z})^{\times}$, and since $\overline{\mathbb{F}}_\ell^{\times}$ has no non-trivial elements of ℓ-power order, ψ factors through the maximal prime-to-ℓ quotient of $(\mathbb{Z}/\ell\mathbb{Z})^{\times} \times (\mathbb{Z}/N\mathbb{Z})^{\times}$. In particular, if $\ell = 2$, then it factors through the maximal quotient of $(\mathbb{Z}/N\mathbb{Z})^{\times}$ of odd order.

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be a reducible representation with $N(\rho) = N$. We may assume that

$$\rho = \begin{pmatrix} \psi_1 & * \\ & \psi_2 \end{pmatrix},$$

where $\psi_i : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_2^{\times}$ are characters. By the definition of the exponent of Artin conductor (2.2), we have $n_q(\psi_1) + n_q(\psi_2) \leq n_q(\rho)$ for each $q \mid N$. As remarked above, they factor through the maximal quotient of $(\mathbb{Z}/N\mathbb{Z})^{\times}$ of odd order. Furthermore, for each prime $q \mid N$, if $n_q(\rho) = 1$, then one of the ψ_i is unramified and the other is at most tamely ramified at q. Also, if $n_q(\rho) = 2$ and ρ is wildly ramified at q, then one of the ψ_i is unramified and the other has the exponent of Artin conductor 2. In general, if ρ is not completely reducible, the restriction $\rho|_{I_q}$ could be completely reducible, and then the choice of i for which ψ_i is unramified may vary for different q. But if N is a prime power (as is the case below), then one of the ψ_i is an everywhere unramified character of $G_{\mathbb{Q}}$, and hence trivial by Minkowski.

Lemma 4.1. *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be a reducible representation with $N(\rho) = N$, and let ρ^{ss} denote its semisimplification.*

(1) *If $N = 3^a 5^b 17^c 257^d 65537^e$ with $a, b, c, d, e = 0$ or 1, then ρ^{ss} is trivial, and*
$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 0$$
for every prime $p \nmid 2N$.

(2) *If $N = 7, 9, 11, 13$, then either ρ^{ss} is trivial or $\rho^{\mathrm{ss}} \simeq 1 \oplus \psi$, where 1 is the trivial character of $G_{\mathbb{Q}}$ and ψ is a character of conductor N and order $3, 3, 5, 3$ respectively. If ρ^{ss} is trivial, then $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 0$ for every prime $p \nmid 2N$. If $\rho^{\mathrm{ss}} \simeq 1 \oplus \psi$, then for every prime $p \nmid 2N$ we have*
$$\mathrm{Tr}(\rho(\mathrm{Frob}_p) = 0 \iff \begin{cases} p \equiv \pm 1 \pmod{N} & \text{if } N = 7, 9, 11, \\ p \equiv \pm 1, \pm 5 \pmod{N} & \text{if } N = 13. \end{cases}$$

Proof. First we prove (1). In these cases, $(\mathbb{Z}/N\mathbb{Z})^{\times}$ has 2-power order, and so the characters ψ_i are both trivial. Hence $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 1 + 1 = 0$ for every prime $p \nmid 2N$.

Now we prove (2). For $N = 7, 11, 13$, by the above discussion, one of the characters, say ψ_1, is trivial and the other has $n_q(\psi_2) \leq 1$. If ψ_2 is unramified, then it is trivial as a character of $G_{\mathbb{Q}}$, and so ρ^{ss} is trivial. So we may assume $n_q(\psi_2) = 1$. If $N = 9$, then ρ is wildly ramified by Lemma 3.2. By the above discussion, we have ψ_1 trivial and $n_q(\psi_2) = 2$. In all cases, we have $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 1 + \psi_2(\mathrm{Frob}_p) = 0$ if and only if $\psi_2(\mathrm{Frob}_p) = 1$. Since the maximal odd quotient of $(\mathbb{Z}/N\mathbb{Z})^{\times}$ has order 3 (resp. 5), if $N = 7, 9, 13$ (resp. $N = 11$), we have $\psi_2(\mathrm{Frob}_p) = 1$ if and only if p is a 3rd (resp. 5th) power in $(\mathbb{Z}/N\mathbb{Z})^{\times}$. □

Next we consider irreducible representations. Recall that the projective image of an irreducible solvable representation is a dihedral group (see the remark after Lemma 2.1).

Lemma 4.2. *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be an irreducible solvable representation. If the projective image of ρ has order $2n$, then the set $S(\rho)$ of primes $p \nmid 2N(\rho)$ for which $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 0$ has density $\frac{1}{2} + \frac{1}{2n}$.*

Proof. Possibly after conjugation, we may assume that $\mathrm{Im}(\rho) \subset \left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right) \cup \left(\begin{smallmatrix} & * \\ * & \end{smallmatrix}\right)$. Then for $g \in \mathrm{Im}(\rho)$, we have $\mathrm{Tr}(g) = 0$ if and only if $g \in \left(\begin{smallmatrix} & * \\ * & \end{smallmatrix}\right)$, or g is a scalar matrix. If c denotes the number of scalar matrices in $\mathrm{Im}(\rho)$, then $\mathrm{Im}(\rho)$ has $2cn$ elements and $\mathrm{Im}(\rho) \cap \left(\begin{smallmatrix} & * \\ * & \end{smallmatrix}\right)$ has cn elements. By the Chebotarev Density Theorem, the density of the set $S(\rho)$ is
$$\frac{cn + c}{2cn} = \frac{1}{2} + \frac{1}{2n}.$$

□

Let ρ be one of the representations

$$\rho_{11}, \qquad \rho_{11}^{\varepsilon}, \qquad \rho_{13}, \qquad \rho_{13}^{\varepsilon}, \qquad \rho_{9}^{\varepsilon}, \tag{4.1}$$

from Theorem 1.4. Respectively, they have images which are isomorphic to

$$V_3, \qquad W_5, \qquad V_3, \qquad W_3, \qquad W_3. \tag{4.2}$$

For these ρ, let

$$S_{11}, \qquad S_{11}^{\varepsilon}, \qquad S_{13}, \qquad S_{13}^{\varepsilon}, \qquad S_{9}^{\varepsilon} \tag{4.3}$$

denote the corresponding set of primes $p \nmid 2N(\rho)$ for which $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 0$. By Lemma 4.2, these sets of primes have density $2/3$ or $3/5$. They can be calculated explicitly by finding a newform to which the ρ is associated (see Proposition 4.5 for more details).

In each case, these sets contain a natural subset of primes with density $1/2$ which are distinguished by simple congruence conditions. To see this, assume that $\mathrm{Im}(\rho) \subset \left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right) \cup \left(\begin{smallmatrix} & * \\ * & \end{smallmatrix}\right)$. The extension $K/\mathbb{Q}$ cut out by ρ contains a unique quadratic subfield F. A prime $p \nmid 2N(\rho)$ is split (resp. inert) in $F/\mathbb{Q}$ if and only if $\rho(\mathrm{Frob}_p)$ maps to the trivial (resp. non-trivial) element of $\mathrm{Gal}(F/\mathbb{Q})$ (i.e. if and only if $\rho(\mathrm{Frob}_p)$ is in $\left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right)$ (resp. $\left(\begin{smallmatrix} & * \\ * & \end{smallmatrix}\right)$)). In particular, we have the following lemma.

Lemma 4.3. *Assume the notation and hypotheses in the preceding discussion. If a prime p is inert in $F/\mathbb{Q}$, then $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 0$.*

For the representations ρ in (4.1), the corresponding quadratic fields F are:

$$\mathbb{Q}(\sqrt{-11}), \qquad \mathbb{Q}(\sqrt{-2}), \qquad \mathbb{Q}(\sqrt{-26}), \qquad \mathbb{Q}(\sqrt{-1}), \qquad \mathbb{Q}(\sqrt{-2}). \tag{4.4}$$

This discussion is summarized by the following proposition which classifies the representations ρ of small conductor in terms of the set $S(\rho)$. Here and elsewhere, for two representations $\rho, \rho' : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$, we write $\rho \underset{G_{\mathbb{F}_2}}{\sim} \rho'$ when the two representations are equal up to isomorphism and $\mathrm{Gal}(\overline{\mathbb{F}}_2/\mathbb{F}_2)$-conjugacy.

Proposition 4.4. *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be a representation with $N(\rho) = N$.*

1. *If $N = 1, 3, 5, 15, 17$, then $S(\rho)$ consists of all the primes $p \nmid 2N$, and the semisimplification ρ^{ss} of ρ is trivial.*
2. *If $N = 7$, then there are two possibilities.*
   (a) *The set $S(\rho)$ consists of all primes $p \nmid 14$, and ρ^{ss} is trivial.*
   (b) *The set $S(\rho)$ consists of the primes $p \equiv \pm 1 \pmod 7$. In this case, we have*
   $$\rho^{\mathrm{ss}} \underset{G_{\mathbb{F}_2}}{\sim} 1 \oplus \varepsilon_7^2,$$
   where $\varepsilon_7^2 : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_2^{\times}$ is a character of conductor 7 and order 3.
   Furthermore, if $\det \rho = 1$, then the case (b) does not occur.
3. *If $N = 9$, then there are three possibilities.*
   (a) *The set $S(\rho)$ consists of all primes $p \nmid 6$, and ρ^{ss} is trivial.*

(b) *The set* $S(\rho)$ *consists of the primes* $p \equiv \pm 1 \pmod 9$. *In this case, we have*

$$\rho^{\mathrm{ss}} \simeq 1 \oplus \varepsilon_9^2,$$

where $\varepsilon_9^2 : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_2^{\times}$ *is a character of conductor* 9 *and order* 3.

(c) *The set* $S(\rho)$ *contains the primes* $p \equiv 5, 7 \pmod 8$. *In this case,* $S(\rho)$ *has density* $2/3$, *and we have* $\rho \underset{G_{\mathbb{F}_2}}{\sim} \rho_9^{\varepsilon}$.

Furthermore, if $\det \rho = 1$, *then the cases (b) and (c) do not occur.*

(4) *Assuming GRH, if* $N = 11$, *then there are four possibilities.*

(a) *The set* $S(\rho)$ *consists of all primes* $p \nmid 22$, *and* ρ^{ss} *is trivial.*

(b) *The set* $S(\rho)$ *consists of the primes* $p \equiv \pm 1 \pmod{11}$. *In this case, we have*

$$\rho^{\mathrm{ss}} \underset{G_{\mathbb{F}_2}}{\sim} 1 \oplus \varepsilon_{11}^2,$$

where $\varepsilon_{11}^2 : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_2^{\times}$ *is a character of conductor* 11 *and order* 5.

(c) *The set* $S(\rho)$ *contains the primes* $p \equiv 2, 6, 7, 8, 10 \pmod{11}$. *In this case,* $S(\rho)$ *has density* $2/3$, *and we have* $\rho \simeq \rho_{11}$.

(d) *The set* $S(\rho)$ *contains the primes* $p \equiv 5, 7 \pmod 8$. *In this case,* $S(\rho)$ *has density* $3/5$, *and we have* $\rho \underset{G_{\mathbb{F}_2}}{\sim} \rho_{11}^{\varepsilon}$.

Furthermore, if $\det \rho = 1$, *then the cases (b) and (d) do not occur. If* ρ *is defined over* $\mathbb{F}_{2^m}$, *where* $4 \nmid m$, *then we do not need to assume the GRH, and the cases (b) and (d) do not occur.*

(5) *Assuming GRH, if* $N = 13$, *then there are four possibilities.*

(a) *The set* $S(\rho)$ *consists of all primes* $p \nmid 26$, *and* ρ^{ss} *is trivial.*

(b) *The set* $S(\rho)$ *consists of the primes* $p \equiv \pm 1, \pm 5 \pmod{13}$, *and we have*

$$\rho^{\mathrm{ss}} \simeq 1 \oplus \varepsilon_{13}^4,$$

where $\varepsilon_{13}^4 : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_2^{\times}$ *is a character of conductor* 13 *and order* 3.

(c) *The set contains the primes*

$$\begin{aligned} p \equiv\ & 11, 19, 23, 29, 33, 41, 53, 55, 57, 59, 61, 67, \\ & 69, 73, 77, 79, 83, 87, 89, 95, 97, 99, 101, 103 \pmod{104}. \end{aligned}$$

In this case, $S(\rho)$ *has density* $2/3$, *and we have* $\rho \simeq \rho_{13}$.

(d) *The set* $S(\rho)$ *contains the primes* $p \equiv 3 \pmod 4$. *In this case,* $S(\rho)$ *has density* $2/3$, *and we have* $\rho \underset{G_{\mathbb{F}_2}}{\sim} \rho_{13}^{\varepsilon}$.

Furthermore, if $\det \rho = 1$, *then the cases (b) and (d) do not occur. If* ρ *is defined over* $\mathbb{F}_{2^m}$, *where* $2 \nmid m$, *then we do not need to assume the GRH, and the cases (b) and (d) do not occur.*

Remark. Note that the condition $\det \rho = 1$ follows if we assume that ρ is defined over $\mathbb{F}_{2^m}$, when $2 \nmid m$ and $N = 7, 9, 13$ (resp. $4 \nmid m$ and $N = 11$).

Now we illustrate the implications of Proposition 4.4 for modular forms. To make this precise, we recall important facts regarding modular Galois representations. Let $N \leq 17$ be

odd. Suppose that $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_k(\Gamma_0(2^aN), \chi; \mathcal{O}_{L,\lambda})$ is a newform of some level $M \mid 2^aN$. By Deligne [6], there is a Galois representation

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2),$$

associated to $f(z)$, which has the property that

$$\begin{aligned} \mathrm{Tr}(\rho_f(\mathrm{Frob}_p)) &= a(p) \pmod{\lambda}, \\ \det(\rho_f(\mathrm{Frob}_p)) &= p^{k-1}\chi(p) \pmod{\lambda}, \end{aligned} \tag{4.5}$$

for every prime $p \nmid 2M$. Note that if the character χ has 2-power order, then $\det \rho_f = 1$. In particular, such a ρ_f cannot be ρ_{11}^{ε}, ρ_{13}^{ε} or ρ_9^{ε}. Note also that χ has 2-power order if the prime λ has residue degree m not divisible by 2 (resp. 4) when $N = 7, 9, 13$ (resp. 11). Since $f(z)$ is a newform, for primes $p \nmid 2M$ we have

$$f(z) \mid T_p = a(p)f(z).$$

Combining this fact with (4.5) and Proposition 4.4, we immediately obtain the following proposition.

Proposition 4.5. *Suppose that $a \geq 0$, and that L is a number field and λ a prime of L lying above 2. Let $f(z) \in S_k(\Gamma_0(2^aN), \chi; \mathcal{O}_{L,\lambda})$ be a newform of some level $M \mid 2^aN$.*

(1) *If $N = 1, 3, 5, 15$, or 17, then for every prime $p \nmid 2N$ we have*
$$f(z) \mid T_p \equiv 0 \pmod{\lambda}.$$
(2) *If $N = 7$, then one of the following holds.*
   (a) *For every prime $p \nmid 14$, we have $f(z) \mid T_p \equiv 0 \pmod{\lambda}$.*
   (b) *For every prime $p \nmid 14$, we have $f(z) \mid T_p \equiv 0 \pmod{\lambda}$ if and only if*
   $$p \equiv \pm 1 \pmod{7}.$$
   Furthermore, if χ has 2-power order, then the case (b) does not occur.
(3) *If $N = 9$, then one of the following holds.*
   (a) *For every prime $p \nmid 6$, we have $f(z) \mid T_p \equiv 0 \pmod{\lambda}$.*
   (b) *For every prime $p \nmid 6$, we have $f(z) \mid T_p \equiv 0 \pmod{\lambda}$ if and only if*
   $$p \equiv \pm 1 \pmod{9}.$$
   (c) *For every prime $p \nmid 6$, we have $f(z) \mid T_p \equiv 0 \pmod{\lambda}$ if and only if $p \in S_9^{\varepsilon}$.*
   Furthermore, if χ has 2-power order, then the cases (b) and (c) do not occur.
(4) *Assuming GRH, if $N = 11$, then one of the following holds.*
   (a) *For every prime $p \nmid 22$, we have $f(z) \mid T_p \equiv 0 \pmod{\lambda}$.*
   (b) *For every prime $p \nmid 22$, we have $f(z) \mid T_p \equiv 0 \pmod{\lambda}$ if and only if*
   $$p \equiv \pm 1 \pmod{11}.$$
   (c) *For every prime $p \nmid 22$, we have $f(z) \mid T_p \equiv 0 \pmod{\lambda}$ if and only if $p \in S_{11}$.*
   (d) *For every prime $p \nmid 22$, we have $f(z) \mid T_p \equiv 0 \pmod{\lambda}$ if and only if $p \in S_{11}^{\varepsilon}$.*
   Furthermore, if χ has 2-power order, then the cases (b) and (d) do not occur. In addition, if λ has residue degree not divisible by 4, then the classification above is unconditional, and the cases (b) and (d) do not occur.
(5) *Assuming GRH, if $N = 13$, then one of the following holds.*

(a) *For every prime* $p \nmid 26$, *we have* $f(z) \mid T_p \equiv 0 \pmod{\lambda}$.
(b) *For every prime* $p \nmid 26$, *we have* $f(z) \mid T_p \equiv 0 \pmod{\lambda}$ *if and only if*

$$p \equiv \pm 1, \pm 5 \pmod{13}.$$

(c) *For every prime* $p \nmid 26$, *we have* $f(z) \mid T_p \equiv 0 \pmod{\lambda}$ *if and only if* $p \in S_{13}$.
(d) *For every prime* $p \nmid 26$, *we have* $f(z) \mid T_p \equiv 0 \pmod{\lambda}$ *if and only if* $p \in S_{13}^{\varepsilon}$.
Furthermore, if χ *has 2-power order, then the cases (b) and (d) do not occur. In addition, if* λ *has odd residue degree, then the classification above is unconditional, and the cases (b) and (d) do not occur.*

5. Proofs of Theorems 1.1, 1.2 and 1.3

In this section, we prove Theorems 1.1, 1.2 and 1.3 of the Introduction.

Proof of Theorem 1.3. Let $f_1(z), \dots, f_r(z)$ be the newforms in $S_k^{\text{new}}(\Gamma_0(M), \chi; \mathcal{O}_{L,\lambda})$, where $M \mid 2^a N$ and $\mathfrak{f}(\chi) \mid M$. For each $f_i(z)$, let M_i denote its level, and denote its Fourier expansion by

$$f_i(z) = \sum_{n=1}^{\infty} a_i(n) q^n. \tag{5.1}$$

The theory of newforms implies that each $f(z) \in S_k(\Gamma_0(2^a N), \chi; \mathcal{O}_{L,\lambda})$ can be written as

$$f(z) \ = \ \sum_{i=1}^{r} \sum_{d \mid \frac{2^a N}{M_i}} a_{i,d} f_i(dz),$$

with $a_{i,d} \in L$. Since the $\mathcal{O}_{L,\lambda}$-module

$$\sum_{i=1}^{r} \sum_{d \mid \frac{2^a N}{M_i}} \mathcal{O}_{L,\lambda} \cdot f_i(dz)$$

is of finite index in $S_k(\Gamma_0(2^a N), \chi; \mathcal{O}_{L,\lambda})$, there is an integer $c \geq 0$ such that for all such $f(z)$ we have $\text{ord}_\lambda(a_{i,d}) \geq -c$.

By Proposition 4.5, for every relevant prime $p \nmid 2N$, we have

$$f_i(z) \mid T_p \ = \ a_i(p) f_i(z) \ = \ \lambda b_{i,p} f_i(z) \quad \text{with some} \quad b_{i,p} \in \mathcal{O}_{L,\lambda}.$$

In some cases, determining the set of relevant primes requires Lemma 4.3 and the fields in (4.4). If we abuse notation and let λ also be a uniformizer of $\mathcal{O}_{L,\lambda}$, then we have

$$f(z) \mid T_p \ = \ \sum_{i=1}^{r} \sum_{d \mid \frac{2^a N}{M_i}} a_{i,d} f_i(dz) \mid T_p \ = \ \sum_{i=1}^{r} \sum_{d \mid \frac{2^a N}{M_i}} a_{i,d} \lambda b_{i,p} f_i(dz).$$

Applying T_p's repeatedly, we see that

$$f(z) \mid T_{p_1} \mid \cdots \mid T_{p_{c+t}} \ \equiv \ 0 \pmod{\lambda^t}$$

for any $c + t$ such primes $p_1, ..., p_{c+t}$. □

To prove Theorem 1.1, we require an elementary proposition regarding the combinatorial properties of Hecke operators acting on holomorphic modular forms $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$. For primes $p \nmid N$, the Hecke operator T_p is a linear endomorphism on $M_k(\Gamma_0(N), \chi)$ (resp. $S_k(\Gamma_0(N), \chi)$), and it is defined by

$$f(z) \mid T_p = \sum_{n=0}^{\infty} \left(a(pn) + \chi(p)p^{k-1}a(n/p)\right) q^n. \tag{5.2}$$

Note that $a(\alpha) = 0$ if $\alpha \notin \mathbb{Z}$.

Proposition 5.1. *Suppose that $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi; \mathcal{O}_{L,\lambda})$, where L is a number field and λ is a prime of L. If t is a positive integer and $p_1, p_2, \ldots, p_c$ are distinct primes coprime to N for which*

$$f(z) \mid T_{p_1} \mid T_{p_2} \mid \cdots \mid T_{p_c} \equiv 0 \pmod{\lambda^t},$$

then we have $a(p_1p_2 \cdots p_c m) \equiv 0 \pmod{\lambda^t}$, for every $m \geq 1$ coprime to $p_1p_2 \cdots p_c$.

Proof. For integers $1 \leq j \leq c$, define algebraic integers $b_j(n) \in \mathcal{O}_L$ by

$$\sum_{n=0}^{\infty} b_j(n)q^n = f(z) \mid T_{p_1} \mid \cdots \mid T_{p_j}.$$

In particular, for $j = c$ we have

$$\sum_{n=0}^{\infty} b_c(n)q^n = f(z) \mid T_{p_1} \mid T_{p_2} \mid \cdots \mid T_{p_c} \equiv 0 \pmod{\lambda^t}.$$

By (5.2), if m is a positive integer coprime to $p_1p_2 \cdots p_c$, then $0 \equiv b_c(m) \pmod{\lambda^t}$ and $b_c(m) = b_1(p_2p_3 \cdots p_c m) = a(p_1p_2 \cdots p_c m)$. This completes the proof. □

Proof of Theorem 1.1. Here we prove Theorem 1.1 (1), (2) and (3).

(1) Théorème 5.2 of [22] implies that

$$j^*(z) := \sum_{n \not\equiv 7 \pmod 8} C(n)q^n = 744 + 196884q + \cdots$$

is a weight zero 2-adic modular form. This implies, for every power of 2, say 2^t, that there is a holomorphic modular integer weight k modular form, say

$$F(z) = \sum_{n=0}^{\infty} C_t(n)q^n \quad \in M_k(\mathrm{SL}_2(\mathbb{Z}); \mathbb{Z}),$$

for which $F(z) \equiv j^*(z) \pmod{2^t}$. Since the Hecke eigenvalues of the Eisenstein series on $\mathrm{SL}_2(\mathbb{Z})$ are even for every T_p where p is an odd prime, conclusion (1) follows from the $N = 1$ case of Theorem 1.3 and Proposition 5.1.

(2) By the proof of Theorem 1 of [9], for every $t \geq 1$ there is an integer weight cusp form $F(z) \in S_k(\Gamma_0(1152); \mathbb{Z})$ with trivial Nebentypus character for which

$$F(z) \equiv \sum_{n=0}^{\infty} Q(n)q^{24n+1} \pmod{2^t}.$$

Since $1152 = 2^7 \cdot 9$, and since the trivial character has 2-power order, conclusion (2) follows from Proposition 5.1 and the $N = 9$ case of Theorem 1.3.
(3) Since $\Theta(z) = \sum_{n=-\infty}^{\infty} q^{n^2}$ is a holomorphic modular form of weight $1/2$ on $\Gamma_0(4)$ and since $s \geq 2$ is even, it follows that

$$\sum_{n=0}^{\infty} r_s(n) q^n = \Theta(z)^s \in \mathbb{Z}[[q]]$$

is an integer weight modular form on $\Gamma_0(4)$. It is a classical fact that the phenomenon in (1.3) holds for the integer weight Eisenstein series on $\Gamma_0(4)$ (cf. Remark after Theorem 1.3). Consequently, the desired conclusion follows from the $N = 1$ case of Theorem 1.3 and Proposition 5.2. □

Proof of Theorem 1.2. As before, let $\Theta(z) = 1 + 2q + 2q^4 + \cdots \equiv 1 \pmod 2$ be the weight $1/2$ Jacobi theta function on $\Gamma_0(4)$. Using the notation from the introduction, we have

$$g_F(z)\Theta(z) \equiv g_F(z) \pmod 2,$$

and is an integer weight modular form with level $4, 12, 20, 28, 60$ or 68. The conclusion now follows from (1.2), Theorems 1.3 and Proposition 5.2. □

References

[1] K. Alladi, *A combinatorial correspondence related to Göllnitz's (BIG) partition theorem and applications*, Trans. Amer. Math. Soc. **349** (1997), 2721-2735.
[2] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festchrift - Vol. 1, Prog. in Math., Birkhäuser, Boston, 1990, 333-400.
[3] K. Buzzard, *On level-lowering for mod* 2 *representations*, Math. Res. Lett. **7** (2000), 95–110
[4] K. Buzzard, *A mod ℓ multiplicity one result*, Appendix to: K. Ribet and W. Stein, *Lectures on Serre's conjectures*, in: "Arithmetic Algebraic Geometry", IAS/Park City Math. Ser. 9, A.M.S., Providence, 2001, pp. 223–225
[5] H. Carayol, *Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires*, Duke Math. J. **59** (1989), 785–801
[6] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Séminaire Bourbaki, 1968/69, Exp. 355, Lect. Notes in Math. **179**, Springer-Verlag, 1971
[7] L. E. Dickson, *Linear Groups*, Teubner, 1901, Leibzig
[8] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), 563–594
[9] B. Gordon and K. Ono, *Divisibility properties of certain partition functions by powers of primes*, Ramanujan J. **1**, (1997), 25-35.
[10] J. Jones, *Tables of Number Fields with Prescribed Ramification*, `http://math.la.asu.edu/~jj/numberfields/`
[11] W. Kohnen, *Fourier coefficients of modular forms of half-integral weight*, Math. Ann. **271** (1985), 237-268.
[12] W. Kohnen and D. Zagier, *Values of L-series of modular forms at the center of the critical strip*, Invent. Math. **64** (1981), 173-198.
[13] R. Livné, *On the conductors of mod ℓ Galois representations coming from modular forms*, J. Number Theory **31** (1989), 133–141
[14] T. Miyake, *Modular Forms*, Springer-Verlag, New York, 1989.
[15] H. Moon, *The non-existence of certain mod p Galois representations*, Bull. Korean Math. Soc. **40** (2003), 537–544

[16] H. Moon, Y. Taguchi, *Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations*, Documenta Math. Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 641–654
[17] A. M. Odlyzko, *Discriminant bounds*, November 29, 1976, in: Some unpublished materials, at `http://www.dtc.umn.edu/~odlyzko/unpublished/index.html`
[18] K. Ribet, *Report on mod ℓ representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/Q)$, in: "Motives", Proc. Sympos. Pure Math. **55**, Part 2, A.M.S., Providence, 1994, pp. 639–676
[19] B. Schoeneberg, *Elliptic modular functions, An introduction*, Springer-Verlag, Berlin, 1974.
[20] J.-P. Serre, *Représentations Linéaires des Groupes Finis*, Hermann, Paris, 1971
[21] J.-P. Serre, *Valeurs propres des opérateurs de Hecke modulo ℓ*, Asterisque **24-25** (1975), 109-117
[22] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, L'Enseignement Math. **22** (1976), 227-260
[23] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331
[24] J.-P. Serre, *Corps Locaux* (3ème éd.), Hermann, Paris, 1980
[25] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230
[26] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan 11, Iwanami Shoten and Princeton Univ. Press, 1971
[27] D. A. Suprunenko, *Matrix Groups*, A.M.S., Providence, 1976
[28] J. Tate, *The non-existence of certain Galois extensions of* $\mathbb{Q}$ *unramified outside* 2, Contemp. Math. **174**, A.M.S., Providence, 1994, pp. 153–156
[29] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pure et Appl. **60** (1981), 375-484.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: `ono@math.wisc.edu`

Graduate School of Mathematics, Kyushu University 33, Fukuoka 812-8581, Japan
E-mail address: `taguchi@math.kyushu-u.ac.jp`