On Seven Conjectures of Kedlaya and Medvedovsky

Noah Taylor*

January 6, 2020

1 Introduction

Let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}(2, \overline{\mathbb{F}}_2)$ be a finite-image two-dimensional mod-2 Galois representation. We say $\overline{\rho}$ is dihedral if the image of $\pi \circ \overline{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}(2, \overline{\mathbb{F}}_2)$ is isomorphic to a finite dihedral group, where $\pi : \mathrm{GL}(2) \to \mathrm{PGL}(2)$ is the usual projection. We say $\overline{\rho}$ is modular of level N if it is the reduction mod 2 of a representation ρ_f associated to a modular eigenform $f \in S_2(\Gamma_0(N), \overline{\mathbb{Z}}_2)$.

We say that a characteristic 0 representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_2)$ is ordinary at 2 if its restriction to the inertia at 2 is reducible. We also say an eigenform f with coefficients in $\overline{\mathbb{Z}}_2$ is ordinary if the coefficient $a(2)$ of q^2 in its q-expansion is a unit mod 2. The terminology is consistent, because by a theorem of Deligne and Fontaine, if $\rho = \rho_f$ is modular, then ρ_f is ordinary if and only if f is ordinary.

In [KM19], Kedlaya and Medvedovsky prove that if a mod 2 representation is dihedral, modular and ordinary of prime level N, then it must be the induction of a character of the class group $\mathrm{Cl}(K)$ of a quadratic extension $K = \mathbb{Q}(\sqrt{\pm N})/\mathbb{Q}$ to $\mathbb{Q}$ [KM19, Section 5.2]. They then analyze all cases of N mod 8 to determine how many distinct mod 2 representations arise from this construction. Finally, they conjecture lower bounds for the number of $\overline{\mathbb{Z}}_2$ eigenforms whose mod 2 representations $\overline{\rho}_f$ are isomorphic to each of the representations obtained above [KM19, Conjecture 13]. The purpose of the current paper is to prove this conjecture, reproduced below.

We let $\mathbb{T}_2^{\mathrm{an}}$ denote the anemic Hecke algebra inside $\mathrm{End}(S_2(\Gamma_0(N), \overline{\mathbb{Z}}_2))$ generated as a $\mathbb{Z}_2$-algebra by the Hecke operators T_k for $(k, 2N) = 1$, and we let $\mathbb{T}_2$ denote the full Hecke algebra, namely $\mathbb{T}_2 = \mathbb{T}_2^{\mathrm{an}}[T_2, U_N]$. Maximal ideals $\mathfrak{m}$ of $\mathbb{T}_2^{\mathrm{an}}$ correspond to classes of mod 2 eigenforms via $\mathbb{T}_2^{\mathrm{an}} \to \mathbb{T}_2^{\mathrm{an}}/\mathfrak{m} \hookrightarrow \overline{\mathbb{F}}_2$, where the image of T_k in the quotient is mapped to the coefficient $a(k)$ of the form. Thus maximal ideals of $\mathbb{T}_2^{\mathrm{an}}$ correspond to modular representations via the Eichler-Shimura construction. We say that $\mathfrak{m}$ is K-dihedral if the representation corresponding to $\mathfrak{m}$ is dihedral in the above sense, and the quadratic extension from which it is an induction is K. (Notice that given $\overline{\rho}$, K is uniquely determined as the quadratic extension of $\mathbb{Q}$ inside the fixed field of the kernel of $\overline{\rho}$ that is ramified at all primes at which $\overline{\rho}$ is ramified.) We write $S_2(N)_{\mathfrak{m}}$ to denote the space of all mod 2 modular forms on which $\mathfrak{m}$ acts nilpotently.

Theorem 1.1 ([KM19, Conjecture 13])**.** *Let N be an odd prime and $\mathfrak{m}$ a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$.*

1. *Suppose $N \equiv 1 \bmod 8$.*
    (a) *If $\mathfrak{m}$ is $\mathbb{Q}(\sqrt{N})$-dihedral, then $\dim S_2(N)_{\mathfrak{m}} \geq 4$.*
    (b) *If $\mathfrak{m}$ is $\mathbb{Q}(\sqrt{-N})$-dihedral, then $\dim S_2(N)_{\mathfrak{m}} \geq h(-N)^{\mathrm{even}}$.*

*The author is supported in part by NSF Grant DMS-1701703.

(c) *If* $\mathfrak{m}$ *is reducible, then* $\dim S_2(N)_{\mathfrak{m}} \geq \frac{h(-N)^{\text{even}}-2}{2}$.

2. *Suppose* $N \equiv 5 \bmod 8$.

   (a) *If* $\mathfrak{m}$ *is ordinary* $\mathbb{Q}(\sqrt{N})$*-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 4$.

   (b) *If* $\mathfrak{m}$ *is* $\mathbb{Q}(\sqrt{-N})$*-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 2$.

3. *Suppose* $N \equiv 3 \bmod 4$ *and* $K = \mathbb{Q}(\sqrt{\pm N})$.

   (a) *If* $\mathfrak{m}$ *is ordinary* K*-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 2$.

The methods we use in proving this conjecture vary somewhat among the cases listed above. Moreover, though part 3 is listed as a single case, we break up its proof into the cases $K = \mathbb{Q}(\sqrt{N})$ and $K = \mathbb{Q}(\sqrt{-N})$. Thus we recognize [KM19, Conjecture 13] as 7 separate conjectures, explaining the title of this note.

1.1 Eigenspace dimension and modular exponent

There is a relation between our work and the problem of understanding the parity of the modular exponent of a modular abelian variety $A = A_f$ as studied in [ARS12]. The problems are not exactly the same, however: the dimension of $S_2(N)_{\mathfrak{m}}$ is greater than 1 if and only if there exists two distinct eigenforms f and f' with $\overline{\rho}_f = \overline{\rho}_{f'} = \overline{\rho}_{\mathfrak{m}}$. On the other hand, the modular degree is even only when there exists a congruence $\bmod \mathfrak{p}$ between eigenforms which are not $G_{\mathbb{Q}}$-conjugate, for some prime $\mathfrak{p}$ above 2. For example, in the case $N = 29$, we know that $S_2(29)$ is 2 dimensional, spanned by $f = q + (-1+\sqrt{2})q^2 + (1-\sqrt{2})q^3 + \ldots$ and $f' = q + (-1-\sqrt{2})q^2 + (1+\sqrt{2})q^3 + \ldots$. These have the same $\bmod 2$ representation; in fact, they are even congruent $\bmod 2$. But the corresponding quotient of $J_0(29)$ is $J_0(29)$ itself, which is simple, so the modular exponent of these forms is 1.

In some cases, such as when the abelian variety is an ordinary elliptic curve over $\mathbb{Q}$, the problems coincide, and thus this paper is related to (and generalizes) arguments from [CE09]. If A is a (modular) ordinary rational elliptic curve, then there is a corresponding homomorphism $\mathbb{T} \to \mathbb{Z}$. If A has even modular degree, then there certainly exist 2-adic congruences between the modular eigenform f associated to A and other forms, and hence an eigenform $f' \neq f$ with $\overline{\rho}_f = \overline{\rho}_{f'}$. Conversely, suppose that there exists such an f'. Because f has coefficients over $\mathbb{Q}$, the form f' cannot be a Galois conjugate of f. Thus it suffices to show that the equality $\overline{\rho}_f = \overline{\rho}_{f'}$ can be upgraded to a congruence between f and f'. The only ambiguity arises from the coefficients of q^2 and q^N. By Theorem 1.5 below, we see that the coefficient of q^2 is determined up to its inverse by the mod 2 representation. Yet, for A, the coefficient of q^2 is automatically 1 by ordinarity and rationality. We also prove in Lemma 5.1 that U_N is in the Hecke algebra $\mathbb{T}_2^{\text{an}}$, and thus f must be congruent to f'.

1.2 Reduction

Given a maximal ideal $\mathfrak{m}$ of $\mathbb{T}_2^{\text{an}}$, we wish to count the dimension of the space Λ of $\mathbb{Z}_2$-module maps

$$\phi : \mathbb{T}_2 \to \overline{\mathbb{F}}_2 \text{ so that } \mathfrak{m}^k(\phi|_{\mathbb{T}_2^{\text{an}}}) = 0 \text{ for some } k \geq 0$$

as an $\overline{\mathbb{F}}_2$-vector space, where $\mathbb{T}_2^{\text{an}}$ acts on ϕ by $x\phi(y) = \phi(xy)$. We know that $\mathbb{T}_2$ and $\mathbb{T}_2^{\text{an}}$ are finite and flat over $\mathbb{Z}_2$, and thus complete semilocal rings. It then follows that we can write

$$\mathbb{T}_2 = \bigoplus_{\mathfrak{a} \text{ maximal}} \mathbb{T}_{\mathfrak{a}},$$

and a similar statement for $\mathbb{T}_2^{\text{an}}$. We thus study $\mathbb{T}_{\mathfrak{m}}^{\text{an}}$ and remove the restriction that $\mathfrak{m}$ is nilpotent.

Proposition 1.2. *The dimension of* Λ *equals*

$$\sum_{\mathfrak{m}\subseteq\mathfrak{a}}[k_{\mathfrak{a}}:\mathbb{F}_2]\dim_{k_{\mathfrak{a}}}\mathbb{T}_{\mathfrak{a}}/(2),$$

where the sum runs over all maximal ideals $\mathfrak{a}$ *of* $\mathbb{T}_2$ *containing* $\mathfrak{m}$*, and* $k_{\mathfrak{a}}$ *is the residue field corresponding to* $\mathfrak{a}$*.*

Proof. The inclusion of $\mathbb{T}_2^{\mathrm{an}}$ into $\mathbb{T}_2$ induces an inclusion $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$ into $\bigoplus_{\mathfrak{m}\subseteq\mathfrak{a}}\mathbb{T}_{\mathfrak{a}}$, and so the dimension of Λ is the dimension of the $\overline{\mathbb{F}}_2$-space of maps $\phi:\bigoplus_{\mathfrak{m}\subseteq\mathfrak{a}}\mathbb{T}_{\mathfrak{a}}\to\overline{\mathbb{F}}_2$. Any such map can be split into separate maps $\phi_{\mathfrak{a}}$, and all $\phi_{\mathfrak{a}}$ factor through $\mathbb{T}_{\mathfrak{a}}/(2)$. So the dimension of Λ is

$$\dim_{\overline{\mathbb{F}}_2}\mathrm{Hom}_{\mathbb{Z}_2}(\bigoplus_{\mathfrak{m}\subseteq\mathfrak{a}}\mathbb{T}_{\mathfrak{a}},\overline{\mathbb{F}}_2)=\sum_{\mathfrak{m}\subseteq\mathfrak{a}}\dim_{\overline{\mathbb{F}}_2}\mathrm{Hom}_{\mathbb{F}_2}(\mathbb{T}_{\mathfrak{a}}/(2),\overline{\mathbb{F}}_2)=\sum_{\mathfrak{m}\subseteq\mathfrak{a}}\dim_{\mathbb{F}_2}\mathbb{T}_{\mathfrak{a}}/(2)=\sum_{\mathfrak{m}\subseteq\mathfrak{a}}[k_{\mathfrak{a}}:\mathbb{F}_2]\dim_{k_{\mathfrak{a}}}\mathbb{T}_{\mathfrak{a}}/(2).$$

□

The trivial lower bound $\dim_{k_{\mathfrak{a}}}\mathbb{T}_{\mathfrak{a}}/(2)\geq 1$ gives a lower bound on the dimension of Λ. In the case that $\overline{\rho}$ arising from $\mathfrak{m}$ is totally real and absolutely irreducible, we prove a better bound $\dim_{k_{\mathfrak{a}}}\mathbb{T}_{\mathfrak{a}}/(2)\geq 2$. This happens when $\mathfrak{m}$ is $\mathbb{Q}(\sqrt{N})$-dihedral for $N>0$. Let $J_0(N)$ denote the Jacobian of the modular curve $X_0(N)$, so that $\overline{\rho}$ appears as a subrepresentation of the two torsion points $J_0(N)[2]$. For some maximal ideal $\mathfrak{a}$ containing $\mathfrak{m}$, let $A=J_0(N)[\mathfrak{a}]$ be the subscheme of points that are killed by $\mathfrak{a}$. By the main result of [BLR91], A is the direct sum of copies of $\overline{\rho}$. (This holds only when $\overline{\rho}$ is absolutely irreducible, but we cover the reducible case in 2.3 without referring to Proposition 1.3.)

Proposition 1.3. *If* $\mathfrak{m}$ *is a maximal ideal of* $\mathbb{T}_2^{\mathrm{an}}$ *for which the corresponding representation* $\overline{\rho}$ *is totally real, then for any maximal ideal* $\mathfrak{a}$ *of* $\mathbb{T}_2$ *containing* $\mathfrak{m}$*, we have the inequality*

$$\dim_{k_{\mathfrak{a}}}\mathbb{T}_{\mathfrak{a}}/(2)\geq 2\cdot\text{multiplicity of }\overline{\rho}\text{ inside }A.$$

Proof. Since $\overline{\rho}$ is a representation of the Galois group of a totally real field, we know that the points of A are all real. Since A also has a $\mathbb{T}_{\mathfrak{a}}$-action with annihilator $\mathfrak{a}$, A is a $k_{\mathfrak{a}}$-vector space, whose dimension is twice the multiplicity of $\overline{\rho}$. We prove the inequality below, from which the proposition follows quickly.

Lemma 1.4. *If* W *denotes the Witt vector functor, then*

$$\dim_{k_{\mathfrak{a}}}(A)\leq\mathrm{rank}_{W(k_{\mathfrak{a}})}(\mathbb{T}_{\mathfrak{a}}).$$

Proof. We follow [CE09, Section 3.2]. A proposition of Merel states that the real variety $J_0(N)(\mathbb{R})$ is connected if N is prime [Mer96, Proposition 5]. If g is the genus of $X_0(N)$, then we know that $J_0(N)(\mathbb{C})=(\mathbb{R}/\mathbb{Z})^{2g}$, and therefore $J_0(N)(\mathbb{R})=(\mathbb{R}/\mathbb{Z})^g$. And we also know that

$$J_0(N)[2](\mathbb{R})=(\mathbb{Z}/2\mathbb{Z})^g.$$

Additionally, as we know that $\mathbb{T}_2=\bigoplus_{\mathfrak{a}}\mathbb{T}_{\mathfrak{a}}$, and all $\mathbb{T}_{\mathfrak{a}}$ are free $\mathbb{Z}_2$-modules, say of rank $g(\mathfrak{a})$, we know that

$$\sum_{\mathfrak{a}}g(\mathfrak{a})=\mathrm{rank}_{\mathbb{Z}_2}(\mathbb{T}_2)=g.$$

A lemma of Mazur shows that the $\mathfrak{a}$-adic Tate module, $\varprojlim J_0(N)[\mathfrak{a}^i]$, is a $\mathbb{T}_\mathfrak{a}$-module of rank 2 [Maz77, Lemma 7.7], and therefore a free $\mathbb{Z}_2$-module of rank $2g(a)$, so $J_0(N)[\mathfrak{a}^\infty](\mathbb{C}) = (\mathbb{Q}_2/\mathbb{Z}_2)^{2g(\mathfrak{a})}$. We therefore know that the 2-torsion points of this scheme are

$$J_0(N)[\mathfrak{a}^\infty, 2](\mathbb{C}) = (\mathbb{Z}/2\mathbb{Z})^{2g(\mathfrak{a})}.$$

If σ acting on $J_0(N)(\mathbb{C})$ denotes complex conjugation, then $(\sigma - 1)^2 = 2 - 2\sigma$ kills all 2-torsion, and $\sigma - 1$ itself kills all real points. So within the scheme $J_0(N)[\mathfrak{a}^\infty, 2](\mathbb{C})$, applying $\sigma - 1$ once kills all real points and maps all points to real points, and so

$$\dim_{\mathbb{Z}/2\mathbb{Z}} J_0(N)[\mathfrak{a}^\infty, 2](\mathbb{R}) \geq \frac{1}{2} \dim_{\mathbb{Z}/2\mathbb{Z}} J_0(N)[\mathfrak{a}^\infty, 2](\mathbb{C}) = g(\mathfrak{a}).$$

But $J_0(N)[2](\mathbb{R})$ breaks up into its $\mathfrak{a}^\infty$ pieces, $J_0(N)[2](\mathbb{R}) = \bigoplus_\mathfrak{a} J_0(N)[\mathfrak{a}^\infty, 2](\mathbb{R})$. Taking dimensions on both sides gives

$$g = \sum_\mathfrak{a} \dim_{\mathbb{Z}/2\mathbb{Z}} J_0(N)[\mathfrak{a}^\infty, 2](\mathbb{R}) \geq \sum_\mathfrak{a} g(\mathfrak{a}) = g,$$

so equality must hold everywhere.

Since all points of $A = J_0(N)[\mathfrak{a}]$ are real, we find that

$$\dim_{\mathbb{Z}/2\mathbb{Z}} A \leq \dim_{\mathbb{Z}/2\mathbb{Z}} J_0(N)[\mathfrak{a}^\infty, 2](\mathbb{R}) = g(\mathfrak{a}) = \mathrm{rank}_{\mathbb{Z}_2}(\mathbb{T}_\mathfrak{a}).$$

Dividing both sides by $[k_\mathfrak{a} : \mathbb{Z}/2\mathbb{Z}] = \mathrm{rank}(W(k_\mathfrak{a})/\mathbb{Z}_2)$, we have the result. □

Returning to the proof of Proposition 1.3, we therefore know that

$$\dim_{k_\mathfrak{a}} \mathbb{T}_\mathfrak{a}/(2) = \dim_{W(k_\mathfrak{a})} \mathbb{T}_\mathfrak{a} \geq 2 \cdot \text{multiplicity of } \overline{\rho}.$$

□

For reference, we recall a theorem of Deligne that describes the characteristic 0 representation ρ restricted to the decomposition group at 2:

Theorem 1.5 ([Edi92, Theorem 2.5]). *If ρ_f is an ordinary 2-adic representation corresponding to a weight 2 level $\Gamma_0(N)$ form f, then $\rho_f|_{D_2}$, the restriction of ρ_f to the decomposition group at a prime above 2, is of the shape*

$$\rho|_{D_2} \sim \begin{pmatrix} \chi\lambda^{-1} & * \\ 0 & \lambda \end{pmatrix}$$

for λ the unramified character $G_{\mathbb{Q}_2} \to \mathbb{Z}_2^\times$ taking Frob_2 to the unit root of $X^2 - a_2X + 2$, and χ is the 2-adic cyclotomic character.

2 $N \equiv 1 \bmod 8$

2.1 $K = \mathbb{Q}(\sqrt{N})$

Theorem 2.1. *If $N \equiv 1 \bmod 8$, and $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$ that is $\mathbb{Q}(\sqrt{N})$-dihedral, then $\dim S_2(N)_\mathfrak{m} \geq 4$.*

Proof. Let $K = \mathbb{Q}(\sqrt{N})$ and denote the fixed field of the kernel of $\overline{\rho}$ as L. In this K, the prime (2) factors as $\mathfrak{p}\mathfrak{q}$ for distinct $\mathfrak{p}$ and $\mathfrak{q}$, and $\overline{\rho}$ must be unramified at 2 so Frob_2, as a conjugacy class containing $\mathrm{Frob}_\mathfrak{p}$ and $\mathrm{Frob}_\mathfrak{q}$, must lie in $\mathrm{Gal}(L/K)$. Moreover, $\overline{\rho}$ must be semisimple at 2, because if $\overline{\rho} = \mathrm{Ind}_K^{\mathbb{Q}} \overline{\chi}$ for $\overline{\chi}$ a character of the unramified extension $\mathrm{Gal}(L/K)$, then $\overline{\rho}|_{\mathrm{Gal}(L/K)} = \overline{\chi} \oplus \overline{\chi}^g$ where $g \in \mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(L/K)$.

Theorem 1.5 and this semisimplicity statement tell us that the decomposition group at 2 in the mod 2 representation looks like $\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix}$, because the cyclotomic character is always 1 mod 2. So we find that the polynomial $\det(x \,\mathrm{Id}_2 - \overline{\rho})$ has coefficients that are unramified at 2, and T_2 is a root of $P(x) := \det(x \,\mathrm{Id}_2 - \overline{\rho}(\mathrm{Frob}_2))$. There are thus three cases: either P has no roots already in $k := \mathbb{T}^{\mathrm{an}}/\mathfrak{m}$, or it has distinct roots lying in k, or it has a repeated root.

If P has no roots in k, then $[k_\mathfrak{a} : k] \geq 2$ for $\mathfrak{a}$ the extension of $\mathfrak{m}$, so Propositions 1.2 and 1.3 say that the dimension of the space is at least

$$[k_\mathfrak{a} : \mathbb{F}_2] \dim_{k_\mathfrak{a}} \mathbb{T}_\mathfrak{a}/(2) \geq [k_\mathfrak{a} : k] \dim_{k_\mathfrak{a}} \mathbb{T}_\mathfrak{a}/(2) \geq 2 \cdot 2 = 4.$$

If P has distinct roots in k, then there are at least 2 extensions of $\mathfrak{m}$ to $\mathbb{T}_2$. Namely, if x_1 and x_2 are lifts of the roots of P to $\mathbb{T}^{\mathrm{an}}_\mathfrak{m}$, the two ideals $\mathfrak{a}_1 = (\mathfrak{m}, T_2 - x_1)$ and $\mathfrak{a}_2 = (\mathfrak{m}, T_2 - x_2)$ are two maximal ideals. So in this case the dimension is at least

$$[k_{\mathfrak{a}_1} : \mathbb{F}_2] \dim_{k_{\mathfrak{a}_1}} \mathbb{T}_{\mathfrak{a}_1}/(2) + [k_{\mathfrak{a}_2} : \mathbb{F}_2] \dim_{k_{\mathfrak{a}_2}} \mathbb{T}_{\mathfrak{a}_2}/(2) \geq \dim_{k_{\mathfrak{a}_1}} \mathbb{T}_{\mathfrak{a}_1}/(2) + \dim_{k_{\mathfrak{a}_2}} \mathbb{T}_{\mathfrak{a}_2}/(2) \geq 2 + 2 = 4.$$

Finally, suppose P has a double root. There is at least one maximal ideal $\mathfrak{a}$ of $\mathbb{T}_2$ above $\mathfrak{m}$. Because we know that $\overline{\rho}|_{D_2}$ is semisimple with determinant 1, the double root must be 1 and $\overline{\rho}|_{D_2}$ is trivial. Then Wiese proves that since all dihedral representations arise from Katz weight 1 modular forms (as Wiese proves in [Wie04]), the multiplicity of $\overline{\rho}$ in A is 2 [Wie07, Corollary 4.5]. In this case the dimension is at least

$$[k_\mathfrak{a} : \mathbb{F}_2] \dim_{k_\mathfrak{a}} \mathbb{T}_\mathfrak{a}/(2) \geq \dim_{k_{\mathfrak{a}_1}} \mathbb{T}_{\mathfrak{a}_1}/(2) \geq 2 \cdot \text{multiplicity of } \overline{\rho} \geq 4.$$

□

2.2 $K = \mathbb{Q}(\sqrt{-N})$

Theorem 2.2. *If $N \equiv 1 \bmod 8$, and $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$ that is $\mathbb{Q}(\sqrt{-N})$-dihedral, then $\dim S_2(N)_\mathfrak{m} \geq 2^e$ where $2^e = \left|\mathrm{Cl}(K)[2^\infty]\right|$.*

Proof. We first recall a well-known proposition of genus theory:

Proposition 2.3. *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with $d > 0$ squarefree.*

(a) *The $\mathbb{F}_2$-dimension of the 2-torsion of the class group of K is one less than the number of primes dividing the discriminant $\Delta_{K/\mathbb{Q}}$.*

(b) *If $d \equiv 5 \bmod 8$ is a prime, then the 2-part of the class group of K is cyclic of order 2.*

(c) *If $d \equiv 1 \bmod 8$ is a prime, then the 2-part of the class group of K is cyclic of order at least 4.*

A proof of the final two parts can be found as [CE05, Proposition 4.1].

We return to the case $N \equiv 1 \bmod 8$. Proposition 2.3 tells us that the 2-part of the class group is cyclic so there is an unramified $\mathbb{Z}/(2^e)$-extension L'/K, say $\mathrm{Gal}(L'/K) = \langle g \rangle$ with $g^{2^e} = \mathrm{Id}$. If we as before denote by L the fixed field of the kernel of $\overline{\rho}$, and we let $M = L \cdot L'$, the character $\overline{\chi}$ of

$\mathrm{Gal}(L/K)$ whose induction equals $\overline{\rho}$ can be extended to a character $\overline{\chi}' : \mathrm{Gal}(M/K) \to \overline{\mathbb{F}}_2[x]/(x^{2^e}-1)$ given by mapping g to x. This can be done because $L \cap L' = K$, because $[L : K]$ is odd, say $[L : K] = n$, and $[L' : K]$ is a power of 2. Then the induction of $\overline{\chi}$ to $\overline{\rho}$ also extends from $\overline{\chi}'$ to $\overline{\rho}' : \mathrm{Gal}(M/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2[x]/(x^{2^e}-1))$. We will prove this representation is modular by describing a q-expansion with coefficients in $\overline{\mathbb{Z}}_2[x]/(x^{2^e}-1)$ whose reduction $\bmod 2$ gives the desired Frobenius traces as coefficients, and proving that the expansion is modular via the embeddings of this coefficient ring into $\mathbb{C}$. Then by the q-expansion principle we will have the result.

Let us suppose we have chosen a 2^eth root of unity $\eta := \zeta_{2^e}$ inside $\overline{\mathbb{Z}}_2$. We may lift $\overline{\chi}$ to a character $\chi : \mathrm{Gal}(L/K) \to \mathbb{Z}_2^{\mathrm{ur}}$. We may therefore also lift $\overline{\chi}'$ to a character $\chi' : \mathrm{Gal}(M/K) \to \mathbb{Z}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$. We may tensor with $\mathbb{Q}_2$, and identifying $\mathbb{Q}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$ with $\bigoplus_{i=0}^{e} \mathbb{Q}_2^{\mathrm{ur}}(\zeta_{2^i})$ by sending x to $\eta^{2^{e-i}}$ gives us $e+1$ representations

$$\chi_i : \mathrm{Gal}(M/K) \to \mathbb{Q}_2^{\mathrm{ur}}(\zeta_{2^i})^\times \text{ and } \rho_i : \mathrm{Gal}(M/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_2^{\mathrm{ur}}(\zeta_{2^i})).$$

These are all finite image odd representations whose coefficients are algebraic and therefore may be compatibly embedded in $\mathbb{C}$. All twists of ρ_i are dihedral or nontrivial cyclic, and therefore all have analytic L-functions. So by the converse theorem of Weil and Langlands (see [Ser77, Theorem 1], for instance), each ρ_i corresponds to a weight 1 eigenform f_i with modulus equal to the conductor of the representation and nebentypus equal to its determinant. Here, the conductor is $4N$ and the nebentypus is the nontrivial character of $\mathrm{Gal}(K/\mathbb{Q})$. This nebentypus, because K has discriminant $4N$, is the character $\lambda_{4N} := \lambda_4\lambda_N$ where λ_4 and λ_N are the nontrivial order 2 characters of $(\mathbb{Z}/4\mathbb{Z})^\times$ and $(\mathbb{Z}/N\mathbb{Z})^\times$; $\lambda_{4N}(p) = 1$ if and only if Frob_p is the identity in $\mathrm{Gal}(K/\mathbb{Q})$ if and only if p splits in K.

Each f_i is a simultaneous eigenvector for the entirety of the weight 1 Hecke algebra $\mathbb{T}(4N)$, with coefficients in $\mathbb{Q}_2^{\mathrm{ur}}(\zeta_{2^i})$, so by returning to $\mathbb{Q}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$ we obtain a weight 1 form f with coefficients in this ring, which is therefore an eigenform by multiplicity 1 results. We can easily check that the traces of the representation $\rho' = \mathrm{Ind}_K^{\mathbb{Q}} \chi' : \mathrm{Gal}(M/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_2^{\mathrm{ur}}[x]/(x^{2^e}-1))$ correspond to the coefficients of f, and so since χ' and therefore ρ are defined over $\mathbb{Z}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$, f also has coefficients in $\mathbb{Z}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$.

Now we take the characteristic 0 form f and multiply by a modular form of weight 1, level $\Gamma_1(4N)$ and nebentypus χ_{4N} whose q-expansion is congruent to $1 \bmod 2$. That will give us a weight 2 level $\Gamma_0(4N)$ form whose $\bmod 2$ reduction is equal to the q-expansion of a form coming from $\overline{\rho}'$. We find such a form:

Lemma 2.4. *The q-expansion $\sum_{m,n\in\mathbb{Z}} q^{m^2+Nn^2}$ describes a modular form g in $S_1(4N, \mathbb{Z}_2, \chi_{4N})$.*

Proof. This follows from properties of the Jacobi theta function $\vartheta(\tau) = \sum_{k\in\mathbb{Z}} q^{k^2}$, but we give a different proof. Let δ range over all characters of the class group H of K, or equivalently over all unramified characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. By Weil-Langlands, $\mathrm{Ind}_K^{\mathbb{Q}} \delta$ as a representation of $G_{\mathbb{Q}}$ gives us a weight 1 modular form. The determinant of this induction is always equal to $\chi_{K/\mathbb{Q}}$, and the conductor is always equal to $4N$. For two of the characters, δ trivial and δ the nontrivial character of $\mathrm{Gal}(K(i)/K)$, $\mathrm{Ind}_K^{\mathbb{Q}} \delta$ is reducible and the weight 1 modular forms are the Eisenstein series

$$E^{\chi_{4N},\mathbf{1}}(q) = L(\chi_{4N}, 0)/2 + \sum_{m=1}^{\infty} q^m \sum_{d \text{ odd},\ d|m} (-1)^{(d-1)/2} \left(\frac{d}{N}\right)$$

and

$$E^{\chi_N,\chi_4}(q) = \sum_{m=1}^{\infty} q^m \sum_{d \text{ odd},\ de=m} (-1)^{(d-1)/2} \left(\frac{e}{N}\right)$$

respectively. The constant term of the former is, by the class number formula, equal to $h(-N)/2$. Otherwise, the forms are cusp forms f_δ with no constant term.

Lemma 2.5. *The q-expansion of f_δ is given by* $f_\delta = \sum_{m\geq 1} q^m \sum_{I\subseteq \mathcal{O}_K : N(I)=m} \delta(I)$.

Proof. If p is a prime inert in K, then there is no I with $N(I) = p$. In the representation $\mathrm{Ind}_K^{\mathbb{Q}}\,\delta$, Frob_p is antidiagonal, so it has trace 0, which is therefore the Hecke eigenvalue. So for p inert in K, the coefficient is correct. If $p = \mathfrak{p}_1\mathfrak{p}_2$, then $\sum_{I\subseteq\mathcal{O}_K:N(I)=p}\delta(I) = \delta(\mathfrak{p}_1)+\delta(\mathfrak{p}_2)$, and the trace of Frob_p in the representation is also $\delta(\mathfrak{p}_1)+\delta(\mathfrak{p}_2)$ because the restriction of $\mathrm{Ind}_K^{\mathbb{Q}}\,\delta$ to G_K is diagonal with characters δ and δ^g for g a lift of the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ and $\delta^g(h)$ meaning $\delta(ghg^{-1})$. Since all primes over p are conjugate, $\delta^g(\mathfrak{p}_1) = \delta(\mathfrak{p}_2)$ and so the trace of Frob_p is $\delta(\mathfrak{p}_1)+\delta(\mathfrak{p}_2)$ as we needed.

If $p = N$, the ideal over N is principal, and so splits completely in M/K; on inertia invariants, therefore, its Frobenius is trivial and the coefficient of q^N is 1, as is necessary since $\delta((\sqrt{-N})) = 1$ because δ is a character of the class group. And if $p = 2$, the ideal $\mathfrak{p}$ over 2 has order 2 in the class group. The inertia subgroup for some prime over 2 in M is generated by some lift of the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$, and the decomposition group is the product of this group with the subgroup of $\mathrm{Gal}(M/K)$ corresponding to the class of $\mathfrak{p}$. And so on inertia invariants, the eigenvalue of the decomposition group is the eigenvalue of $\mathrm{Frob}_{\mathfrak{p}}$, which is $\delta(\mathfrak{p})$. So the coefficient for q^2 is correct as well.

Finally, we can check using multiplicativity of both Hecke operators and the norm map, as well as the formula for the Hecke operators T_{p^k}, that the coefficients of q^m for composite m are as described also. ☐

We consider $\sum_\delta f_\delta$, cusp forms with their multiplicity (stemming from δ and δ^{-1} giving the same form) and the Eisenstein series once. By independence of characters, for each ideal I where $\delta(I) = 1$ for all δ, that is I is in the identity of the class group, the corresponding term in the sum is $h(-N)$, and for each other nonzero ideal I, the term vanishes in the sum. The sum is thus

$$L(\chi_{4N},0)/2 + h(-N)\sum_{0\neq I=(\alpha)} q^{N(I)} = h(-N)/2 + \frac{h(-N)}{|\mathcal{O}_K^\times|}\sum_{0\neq\alpha=a+b\sqrt{-N}\in\mathcal{O}_K} q^{N(\alpha)}$$
$$= \frac{h(-N)}{2}\left(1+\sum_{(0,0)\neq(a,b)\in\mathbb{Z}} q^{a^2+Nb^2}\right).$$

Dividing by $h(-N)/2$ gives the required form, which we call g. ☐

It turns out that there is a form (not an eigenform) of level $\Gamma_1(N)$ which lifts the Hasse invariant. It is a linear combination of the Eisenstein series $E^{\epsilon,\mathbf{1}}(q)$ for ϵ ranging over all $2^{v_2(N)}$-order characters of $\mathbb{Z}/N\mathbb{Z}^\times$, and has the correct nebentypus when reduced because all 2-power roots of unity are $1 \bmod$ the maximal ideal over 2 in $\mathbb{Z}[\eta]$. This form is described by MathOverflow user Electric Penguin in [hp].

So we take fg and reduce the coefficients mod the maximal ideal over 2 and get a form $h \in S_2(\overline{\mathbb{F}}_2[x]/(x^{2^e}-1), \Gamma_0(4N))$. We know that h remains an eigenform because for odd primes, $p \equiv 1 \bmod 2$ so increasing the weight doesn't change the Hecke action on the coefficients, and for 2 increasing the weight does not change the action of U_2 on q-expansions. Because h is an eigenform, if $\mathbb{T}(4N)$ now represents the Hecke algebra acting on weight 2 forms of level $\Gamma_0(4N)$, we get a ring homomorphism $\overline{\gamma} : \mathbb{T}(4N) \to \overline{\mathbb{F}}_2[x]/(x^{2^e}-1)$. The image of this map tensored with $\overline{\mathbb{F}}_2$ is the entirety of $\overline{\mathbb{F}}_2[x]/(x^{2^e}-1)$: we have prime ideals of K in all elements of the class group, so if μ is some nonzero element in the image of $\overline{\chi}$ not equal to 1, then both $\mu x + \mu^{-1}x^{-1}$ and $\mu x^{-1} + \mu^{-1}x$ are in the image of $\overline{\gamma}$, so that

$$\mu^{-1}(\mu x^{-1} + \mu^{-1}x) + \mu(\mu x + \mu^{-1}x^{-1}) = (\mu^2 + \mu^{-2})x$$

is in the $\overline{\mathbb{F}}_2$ vector space generated by the image of $\overline{\gamma}$, and hence x is also. And since $\overline{\gamma}$ is a ring homomorphism, all powers of x lie in the filled out image.

As described in [CE09, Section 3.3], we may find a representation

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2[x]/(x^{2^e}-1)),$$

in the following way: we let $\mathfrak{a}'$ denote the kernel of $\mathbb{T}(4N) \xrightarrow{\overline{\gamma}} \overline{\mathbb{F}}_2[x]/(x^{2^e}-1) \xrightarrow{x\mapsto 1} \overline{\mathbb{F}}_2$, and we let $\mathbb{T}(4N)_{\mathfrak{a}'}$ denote the completion of $\mathbb{T}(4N)$ with respect to that ideal. The Galois action on $J_0(4N)[\mathfrak{a}']$ breaks into isomorphic 2-dimensional representations $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}(4N)/\mathfrak{a}')$, and Carayol constructs a lift $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}(4N)_{\mathfrak{a}'})$ [Car94, Theorem 3]. We pushforward this map along $\mathbb{T}(4N)_{\mathfrak{a}'} \to \overline{\mathbb{F}}_2[x]/(x^{2^e}-1)$ which also has full image to get a representation $G_{\mathbb{Q}} \to \overline{\mathbb{F}}_2[x]/(x^{2^e}-1)$. It's clear that this representation is isomorphic to $\overline{\rho}' = \mathrm{Ind}_K^{\mathbb{Q}}\overline{\chi}'$ by looking at traces. So $\overline{\rho}'$ is modular of level $\Gamma_0(4N)$.

We know that h is an eigenform for U_2, and the operator U_2 lowers the level from $4N$ to $2N$. So $h = U_2 h$ is an eigenform of level $\Gamma_0(2N)$. We recall the level lowering theorem of Calegari and Emerton; here A is an Artinian local ring of residue field k of characteristic 2.

Theorem 2.6 ([CE09, Theorem 3.14])**.** *If $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$ is a modular Galois representation of level $\Gamma_0(2N)$, such that*

1. *$\overline{\rho}$ is (absolutely) irreducible,*
2. *$\overline{\rho}$ is ordinary and ramified at 2, and*
3. *ρ is finite flat at 2,*

then ρ arises from an A-valued Hecke eigenform of level N.

Our $\overline{\rho}'$, pushed forward through the map $\overline{\mathbb{F}}_2[x]/(x^{2^e}-1) \to \overline{\mathbb{F}}_2$ and restricting to its true image, is irreducible, ordinary and ramified. All that remains in order to apply the theorem is to check that $\overline{\rho}'$ is finite flat at 2. It's enough to show this after restricting to $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2^{\mathrm{ur}})$. But the representation has only degree two ramification, so the image of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2^{\mathrm{ur}})$ is order 2. And furthermore, it's easy to see that it arises as the generic fiber of $D^{\oplus 2^e}$ over $\mathbb{Z}_2^{\mathrm{ur}}$, where D is the nontrivial extension of $\mathbb{Z}/2\mathbb{Z}$ by μ_2 discussed in [Maz77, Proposition 4.2], represented for example by $\mathbb{Z}_2[x,y]/(x^2-x, y^2+2x-1)$ with comultiplication

$$x \to x_1 + x_2 - 2x_1x_2 \text{ and } y \to y_1y_2 - 2x_1x_2y_1y_2.$$

So we may apply Theorem 2.6, and deduce that our modular form h is a modular form of level N.

We have therefore constructed a surjective map $\mathbb{T}_{\mathfrak{m}} \otimes_{\mathbb{Z}_2} \overline{\mathbb{F}}_2 \to \overline{\mathbb{F}}_2[x]/(x^{2^e}-1)$, so the $\overline{\mathbb{F}}_2$-dimension of $S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)_{\mathfrak{m}}$ must be at least 2^e. Note that Proposition 2.3 shows that this dimension is at least 4. □

2.3 $\mathfrak{m}$ is reducible

Theorem 2.7. *If $N \equiv 1 \bmod 8$, and $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$ for which $\overline{\rho}_{\mathfrak{m}}$ is reducible, then* $\dim S_2(N)_{\mathfrak{m}} \geq \frac{h(-N)^{\mathrm{even}}-2}{2}$.

Proof. We know that $\mathfrak{m} \subseteq \mathbb{T}^{\mathrm{an}}$ is generated by T_ℓ and 2 for all primes $\ell \not| 2N$. In [CE05, Corollary 4.9] and the discussion after Proposition 4.11, Calegari and Emerton prove that $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}/(2)$ must be isomorphic to $\mathbb{F}_2[x]/(x^{2^{e-1}})$, where $2^e = h(-N)^{\mathrm{even}}$. They accomplish this by setting up a deformation problem, namely deformations of $(\overline{V}, \overline{L}, \overline{\rho})$ where $\overline{\rho}$ is the mod-2 representation $\left(\begin{smallmatrix} 1 & \phi \\ 0 & 1 \end{smallmatrix}\right)$, ϕ is the additive character $G_{\mathbb{Q}} \to \mathbb{F}_2$ that arises as the nontrivial character of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, and $\overline{L}$ is a line in $\overline{V}$ not fixed by $G_{\mathbb{Q}}$. With the conditions set on the deformation, they find that it is representable by some $\mathbb{Z}_2$-algebra R.

Next, they prove an $R = \mathbb{T}$-type theorem, namely that $R = \mathbb{T}$ where $\mathbb{T}$ is the completion at the Eisenstein ideal of the Hecke algebra acting on all modular forms of level $\Gamma_0(N)$, including the Eisenstein series. Finally they study $R/2$ which represents the deformation functor to characteristic 2 rings, and show that if ρ^{univ} is the universal deformation, then ρ^{univ} factors through the largest unramified 2-extension of K. This combined with their fact that a map $R \to \mathbb{F}_2[x]/(x^n)$ can be surjective if and only if $n \leq 2^{e-1}$ proves that $R/2 = \mathbb{F}_2[x]/(x^{2^{e-1}})$.

Therefore, the same holds for the Eisenstein Hecke algebra $\mathbb{T}/2$. So we know that $\mathbb{T}$ is a free $\mathbb{Z}_2$-module of rank $\frac{h(-N)^{\mathrm{even}}}{2}$. But we may split off a one-dimensional subspace corresponding to the Eisenstein series, so that the cuspidal Hecke algebra $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$ has rank one less, and therefore has rank $\frac{h(-N)^{\mathrm{even}}}{2} - 1$. (In fact, the full Hecke algebra is determined also, because in any reducible mod 2 representation, T_2 and U_N must both map to 1, as U_N is unipotent and T_2 maps to the image of Frobenius under a mod 2 character unramified at every prime not equal to 2. But there are no nontrivial such characters.) And therefore the dimension of the space $S_2(N)_{\mathfrak{m}}$ is the dimension of the space $\mathrm{Hom}(\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}, \overline{\mathbb{F}}_2)$, which is dimension $\frac{h(-N)^{\mathrm{even}}}{2} - 1$, as desired. □

[KM19] partially prove this theorem using [CE05], doing the case of $N \equiv 9 \bmod 16$. As we see, the method works equally well for $N \equiv 1 \bmod 16$. The only difference between the two cases is that [CE05] prove that for $N \equiv 9 \bmod 16$, the Hecke algebra $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$ is a discrete valuation ring, and therefore a domain, but that plays no role here.

3 $N \equiv 5 \bmod 8$

3.1 $K = \mathbb{Q}(\sqrt{N})$

Theorem 3.1. *If $N \equiv 5 \bmod 8$, and $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$ that is $\mathbb{Q}(\sqrt{N})$-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 4$.

Proof. Because 2 is inert in $\mathbb{Q}(\sqrt{N})$, we know that $\overline{\rho}|_{D_2}$ is of size 2. Then the image of $\overline{\rho}$ is a subgroup of a 2-Sylow subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$, and therefore is isomorphic to an upper-triangular idempotent representation $\overline{\rho}|_{D_2} \simeq \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. If we compare to Theorem 1.5, we find that in an eigenform for all T_p including T_2 that corresponds to this representation, $a_2 = 1$. So the three methods of section 2.1 do not work.

Recall Proposition 1.3 that says if the representation $\overline{\rho}$ was totally real, then $\dim_{k_{\mathfrak{a}}} \mathbb{T}_{\mathfrak{a}}/(2) \geq 2 \cdot$ multiplicity of $\overline{\rho}$, so if this multiplicity is at least 2, we're done. So we assume that $\overline{\rho}$ occurs once in $J_0(N)[\mathfrak{a}]$. However, we know by [Wie07, Theorem 4.4] that since $\overline{\rho}$ comes from a Katz modular form of weight 1 and level N, and the multiplicity of $\overline{\rho}$ on $J_0(N)[\mathfrak{a}]$ is 1, that the multiplicity of

$\overline{\rho}$ in $J_0(N)[\mathfrak{m}]$ is 2. So by the proof as in Proposition 1.3, we know the dimension of $\mathbb{T}_\mathfrak{m}/(2)$ has dimension at least twice 2, or dimension 4, and so $\dim S_2(N)_\mathfrak{m} \geq 4$ as required. $\square$

3.2 $K = \mathbb{Q}(\sqrt{-N})$

Theorem 3.2. *If $N \equiv 5 \bmod 8$, and $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$ that is $\mathbb{Q}(\sqrt{-N})$-dihedral, then $\dim S_2(N)_\mathfrak{m} \geq 2$.*

This follows in a similar way to Theorem 2.2. Proposition 2.3 proves that the 2 part of the class group of K is order 2, so applying the results of section 2.2 proves the theorem in this case. The only difficulties are in verifying the conditions of Theorem 2.6; that is, $\overline{\rho}$ is absolutely irreducible, ordinary, and ramified, and ρ itself is finite flat at 2. It's clear that the first three conditions hold, and the final condition holds because $\mathbb{Q}_2^{\mathrm{ur}}(\sqrt{-N}) = \mathbb{Q}_2^{\mathrm{ur}}(i)$ even though $N \equiv 5 \bmod 8$. So the group scheme in this case is the same as the group scheme in section 2.2, and we have verified all necessary conditions.

4 $N \equiv 3 \bmod 4$

4.1 $K = \mathbb{Q}(\sqrt{N})$

Theorem 4.1. *If $N \equiv 3 \bmod 4$, and $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$ that is $\mathbb{Q}(\sqrt{N})$-dihedral, then $\dim S_2(N)_\mathfrak{m} \geq 2$.*

Proof. We let $\mathfrak{a}$ be a prime of $\mathbb{T}_2$ containing $\mathfrak{m}$. Then again recalling Proposition 1.3, since K and therefore $\overline{\rho}$ are totally real, we calculate that the dimension is at least

$$\dim_{k_\mathfrak{a}} \mathbb{T}_\mathfrak{a}/(2) \geq 2 \cdot \text{multiplicity of } \overline{\rho} \geq 2$$

as required. $\square$

4.2 $K = \mathbb{Q}(\sqrt{-N})$

Theorem 4.2. *If $N \equiv 3 \bmod 4$, and $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$ that is $\mathbb{Q}(\sqrt{-N})$-dihedral, then $\dim S_2(N)_\mathfrak{m} \geq 4$.*

Proof. This was shown in [KM19, Proposition 14] using essentially the same method as we use in sections 2.2 and 3.2. The only differences are that $K/\mathbb{Q}$ is unramified at 2 so the Artin conductor of $\overline{\rho}'$ is N, not $4N$, so no level-lowering is required; and that we obtain a second eigenspace from our modular form f coming from the reduction of f^2. $\square$

5 The effect of U_N

In none of our proofs did we ever exploit the fact that U_N is not defined to be in $\mathbb{T}_2^{\mathrm{an}}$ as we did with T_2, and the following gives an explanation why.

Lemma 5.1. *There is an inclusion $U_N \in \mathbb{T}_2^{\mathrm{an}}$, so $\mathbb{T}_2 = \mathbb{T}_2^{\mathrm{an}}[T_2]$.*

Proof. Since $\mathbb{T}_2^{\mathrm{an}} = \bigoplus_\mathfrak{m} \mathbb{T}_\mathfrak{m}^{\mathrm{an}}$, it suffices to prove that $U_N \in \mathbb{T}_\mathfrak{m}^{\mathrm{an}}$ for each maximal ideal $\mathfrak{m}$. Let

$$\overline{\rho} = \overline{\rho}_\mathfrak{m} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{T}_\mathfrak{m}^{\mathrm{an}}/\mathfrak{m}) \subseteq \mathrm{GL}_2(\overline{\mathbb{F}}_2)$$

denote the residual representation associated to $\mathfrak{m}$. If $\overline{\rho}$ is not irreducible, then it is Eisenstein. The Eisenstein ideal $\mathfrak{I} \subseteq \mathbb{T}_2$ is generated by $1 + \ell - T_\ell$ for $\ell \neq N$ and by $U_N - 1$. Let $\mathfrak{a} = (2, \mathfrak{I})$ denote the corresponding maximal ideal of $\mathbb{T}_2$. By [Maz77, Proposition 17.1], the ideal $\mathfrak{a}$ is actually generated by $\eta_\ell := 1 + \ell - T_\ell$ for a suitable good prime $\ell \neq 2, N$. But this implies that $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}} = \mathbb{T}_{\mathfrak{a}}$ and that U_N (and T_2) lie in $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$. Hence we assume that $\overline{\rho}$ is irreducible.

If $\overline{\rho}$ is irreducible but not absolutely irreducible, then its image would have to be cyclic of degree prime to 2. Since the image of inertia at N is unipotent it has order dividing 2. Thus this would force $\overline{\rho}$ to be unramified at N. There are no nontrivial odd cyclic extensions of $\mathbb{Q}$ ramified only at 2, and thus this does not occur, and we may assume that $\overline{\rho}$ is absolutely irreducible.

Tate proved in [Tat94] the following theorem:

Theorem 5.2 (Tate)**.** *Let G be the Galois group of a finite extension $K/\mathbb{Q}$ which is unramified at every odd prime. Suppose there is an embedding $\rho : G \hookrightarrow \mathrm{SL}_2(k)$, where k is a finite field of characteristic 2. Then $K \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ and $\mathrm{Tr}\,\rho(\sigma) = 0$ for each $\sigma \in G$.*

If $\overline{\rho}$ is unramified at N, then $\det \overline{\rho}$ is a character of odd order unramified outside 2, which by Kronecker-Weber must be trivial, so $\overline{\rho}$ maps to $\mathrm{SL}_2(k)$. We may apply Theorem 5.2 to determine that $\overline{\rho}$ has unipotent image, which therefore is not absolutely irreducible. Hence we may assume that $\overline{\rho}$ is ramified at N. By local-global compatibility at N, the image of inertia at N of $\overline{\rho}$ is unipotent. Because it is nontrivial, it thus has image of order exactly 2.

Let $\{f_i\}$ denote the collection of $\overline{\mathbb{Q}}_2$-eigenforms such that $\overline{\rho}_{f_i} = \overline{\rho}$. Associated to each f_i is a field E_i generated by the eigenvalues T_l for $l \neq 2, N$. There exists a corresponding Galois representation:

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}} \otimes \mathbb{Q}) = \prod \mathrm{GL}_2(E_i).$$

The traces of ρ at Frobenius elements land inside $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$, and hence the traces of all elements land inside $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$. By a result of Carayol, there exists a choice of basis so that ρ is valued inside $\mathrm{GL}_2(\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}})$; that is, there exists a free $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$-module of rank 2 with a Galois action giving rise to ρ. Each representation ρ_{f_i} has the property that, locally at N, the image of inertia is unipotent. In particular, $\rho|_{G_{\mathbb{Q}_N}}$ is tamely ramified. Let $\langle \sigma, \tau \rangle$ denote the Galois group of the maximal tamely ramified extension of $\mathbb{Q}_N$, where σ is a lift of Frobenius and τ a pro-generator of tame inertia, so $\sigma\tau\sigma^{-1} = \tau^N$. We claim that there exists a basis of $(\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}})^2$ such that

$$\overline{\rho}|_{G_{\mathbb{Q}_N}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Note, first of all, that it is true modulo $\mathfrak{m}$ by assumption (because $\overline{\rho}$ is ramified). Choose a lift $e_2 \in (\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}})^2$ of a vector which is not fixed by $\overline{\rho}(\tau)$, and then let $e_1 = (\rho(\tau) - 1)e_2$. Since the reduction of e_1 and e_2 generate $(\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}/\mathfrak{m})^2$, by Nakayama's lemma they generate $(\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}})^2$. Finally we have $(\rho(\tau) - 1)^2 = 0$ since $(\rho_{f_i}(\tau) - 1)^2 = 0$ for each i.

Now consider the image of σ. Writing

$$\rho(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}),$$

the condition that $\rho(\sigma)\rho(\tau) = \rho(\tau)^N \rho(\sigma)$ forces $c = 0$. But then if

$$\rho(\sigma) = \begin{pmatrix} * & * \\ 0 & x \end{pmatrix} \in \mathrm{GL}_2(\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}),$$

then for every specialization ρ_{f_i}, the action of Frobenius on the unramified quotient is x. But for each ρ_{f_i}, the action of Frobenius on the unramified quotient is the image $U_N(f_i)$ of U_N. Hence this implies that $x = U_N$, and thus that $U_N \in \mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$. □

6 Acknowledgments

The author would like to thank Frank Calegari for the many useful conversations leading toward the proofs in sections 1 through 4, and from whom the proof of Lemma 5.1 was communicated.

References

[ARS12] Amod Agashe, Kenneth A. Ribet, and William A. Stein. The modular degree, congruence primes, and multiplicity one. In *Number theory, analysis and geometry*, pages 19–49. Springer, New York, 2012.

[BLR91] Nigel Boston, Hendrik W. Lenstra, Jr., and Kenneth A. Ribet. Quotients of group rings arising from two-dimensional representations. *C. R. Acad. Sci. Paris Sér. I Math.*, 312(4):323–328, 1991.

[Car94] Henri Carayol. Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, volume 165 of *Contemp. Math.*, pages 213–237. Amer. Math. Soc., Providence, RI, 1994.

[CE05] Frank Calegari and Matthew Emerton. On the ramification of Hecke algebras at Eisenstein primes. *Invent. Math.*, 160(1):97–144, 2005.

[CE09] Frank Calegari and Matthew Emerton. Elliptic curves of odd modular degree. *Israel J. Math.*, 169:417–444, 2009.

[Edi92] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

[hp] Electric Penguin (https://mathoverflow.net/users/85372/electric penguin). Lifting the hasse invariant mod 2. MathOverflow. URL:https://mathoverflow.net/q/228596 (version: 2017-02-13).

[KM19] Kiran Kedlaya and Anna Medvedovsky. Mod-2 dihedral galois representations of prime conductor. *The Open Book Series*, 2(1):325–342, jan 2019.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Mer96] Loïc Merel. L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$. *J. Reine Angew. Math.*, 477:71–115, 1996.

[Rib90] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[Ser77] J.-P. Serre. Modular forms of weight one and Galois representations. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 193–268, 1977.

[Tat94] John Tate. The non-existence of certain Galois extensions of $\mathbf{Q}$ unramified outside 2. In *Arithmetic geometry (Tempe, AZ, 1993)*, volume 174 of *Contemp. Math.*, pages 153–156. Amer. Math. Soc., Providence, RI, 1994.

[Wie04] Gabor Wiese. Dihedral Galois representations and Katz modular forms. *Doc. Math.*, 9:123–133, 2004.

[Wie07] Gabor Wiese. Multiplicities of Galois representations of weight one. *Algebra Number Theory*, 1(1):67–85, 2007. With an appendix by Niko Naumann.