MOD-2 DIHEDRAL GALOIS REPRESENTATIONS OF PRIME CONDUCTOR

KIRAN S. KEKLAYA AND ANNA MEDVEDOVSKY

Abstract. For all odd primes $N$ up to 500000, we compute the action of the Hecke operator $T_2$ on the space $S_2(\Gamma_0(N), \mathbb{Q})$ and determine whether or not the reduction mod 2 (with respect to a suitable basis) has 0 and/or 1 as eigenvalues. We then partially explain the results in terms of class field theory and modular mod-2 Galois representations. As a byproduct, we obtain some nonexistence results on elliptic curves and modular forms with certain mod-2 reductions, extending prior results of Setzer, Hadano, and Kida.

1. Introduction

1.1. Computations and theorems. For $N$ a positive integer and $k$ a positive even integer, let $S_k(\Gamma_0(N), \mathbb{Q})$ be the space of weight-$k$ rational cusp forms for the group $\Gamma_0(N)$, equipped with the Hecke operators $T_p$ for all primes $p$ not dividing $N$. For $N$ prime with $2 < N < 500000$, we computed the matrix of $T_2$ acting on some basis of $S_2(\Gamma_0(N), \mathbb{Q})$; this was done using Cremona’s implementation of modular symbols, as documented in [9], via the eclib package in Sage [30]. We then used the m4ri package in Sage, which implements the “method of four Russians” [1, Chapter 9], to compute the rank of the reductions of $T_2$ and $T_2 - 1$ mod 2. These computations took a few CPU-months; we did not make an accurate costing because our method is almost certainly not optimal (see below).

From this data, we observed the following behavior of the mod-2 matrix of $T_2$.

- For $N \equiv 3 \mod 8$, the eigenvalue 0 always occurs if $N > 3$.
- For $N \equiv 1, 3, 5 \mod 8$, the eigenvalue 1 always occurs if $N > 163$.
- For $N \equiv 1 \mod 8$, the eigenvalue 0 occurs with probability 16.8%.
- For $N \equiv 5 \mod 8$, the eigenvalue 0 occurs with probability 42.2%.
- For $N \equiv 7 \mod 8$, the eigenvalue 0 occurs with probability 17.3%.
- For $N \equiv 7 \mod 8$, the eigenvalue 1 occurs with probability 47.9%.

These results can be partially explained (see section 7) by combining the Cohen-Lenstra heuristics [8] with a detailed count of the maximal ideals of the mod-2 Hecke algebra with residue field $\mathbb{F}_2$. The bulk of the paper is devoted to making these counts (Theorems 2 and 12) using class field theory plus the theory of modular Galois representations. As a byproduct, we recover some nonexistence results of Setzer [34], Hadano [14], and Kida [20] for elliptic curves of conductor $N$ or $2N$ with $N$ prime, derived using a totally different approach: a diophantine analysis of discriminants of Weierstrass equations due to Ogg [26].

The first author was supported by NSF (grant DMS-1501214) and UC San Diego (Warschawski Professorship). The second author was supported by an NSF postdoctoral research fellowship (grant DMS-1706834) and has gratefully enjoyed the hospitality of the Max Planck Institute for Mathematics during the writing of this paper.
For $N < 200000$, we also computed the multiplicities of 0 and 1 as generalized eigenvalues of the mod-2 reduction of the matrix of $T_2$. (These multiplicities are independent of the choice of basis.) These are somewhat more complicated to analyze because the self-adjointness of $T_p$ with respect to the Petersson inner product does not guarantee diagonalizability mod $\ell$; hence the computed multiplicity is an upper bound for the count of maximal ideals, and either both are zero or both are nonzero, but more work is needed to explain the full multiplicity. See Conjecture 13 for a step in this direction; existing work on failure of multiplicity one in characteristic 2 (e.g., [21]) suggests that even conjecturally, it may be difficult to formulate a more precise conjecture without allowing for some sporadic exceptions.

1.2. Motivation: tabulation of rational eigenforms. Although these results may be of independent interest, for context we indicate how they were motivated by some considerations around the tabulation of rational eigenforms. Via the modularity theorem, isogeny classes of elliptic curves of conductor $N$ correspond to rational newforms in $S_2(\Gamma_0(N), \mathbb{Q})$: finding rational newforms within $S_2(\Gamma_0(N), \mathbb{Q})$ is the rate-limiting step in Cremona’s algorithm for tabulating rational elliptic curves of a given conductor, as documented in [9] and executed to date for $N \leq 400000$ [13]. (The table is also available in PARI/GP [27], Magma [37], and Sage.)

Within this step of Cremona’s algorithm, the rate-limiting substep is the computation of the kernel of $T_p - a_p$ where $p$ is the smallest prime not dividing $N$ and $a_p$ runs over all integers with $|a_p| \leq 2\sqrt{p}$. Once this step is done, the resulting kernels are typically of much smaller dimension than the original space, so it is of negligible difficulty to diagonalize the restrictions of enough additional Hecke operators to isolate all one-dimensional joint eigenspaces. (The fact that this catches all rational eigenforms is a consequence of self-adjointness and strong multiplicity one.)

Recall that linear algebra over $\mathbb{Q}$ is not generally performed using generic algorithms due to intermediate coefficient explosion; it is better to use a multimodular approach in which one does linear algebra over $\mathbb{F}_\ell$ for various small primes $\ell$ and reconstructs the final answer using the Chinese remainder theorem. In Cremona’s implementation of his algorithm, he uses only the single prime $\ell = 2^{30} - 35$; to date, this has provided enough information to identify the kernel of $T_p - a_p$.

The present work was motivated by a desire to understand the following question: to what extent (if any) can this algorithm be accelerated using linear algebra over $\mathbb{F}_\ell$ for a single small $\ell$, such as $\ell = 2^2$? Of course, one does not expect the result of computing the kernel of $T_p - a_p \mod \ell$ to provide enough information to identify the kernel over $\mathbb{Q}$. However, for $N$ large, the probability that $S_2(\Gamma_0(N), \mathbb{Q})$ admits any rational newforms is relatively small: by analogy with the corresponding estimate for elliptic curves sorted by naïve height [5] or Faltings height [17], one expects that only $O(X^{5/6})$ of positive integers up to $X$ occur as levels of rational newforms. Consequently, there are likely to be many values of $N$ for which $T_p - a_p$ has no kernel at all over $\mathbb{Q}$; if this remains true mod $\ell$, then finding this out would provide an early abort mechanism. A more sophisticated early abort strategy would be to calculate not the rank of $T_p - a_p$, but rather

$$= (\text{eigenvalue multiplicity of 0}) - \sum_{d \mid N, d < N} \tau(N/d)(\text{contribution from level } d \text{ newforms})$$
where \( \tau(n) \) is the number of divisors of \( n \); an early abort occurs if this contribution does not increase under reduction modulo \( \ell \).

The restriction to \( N \) prime in this paper was made for several reasons; notably, a key role in the theoretical analysis is played by Eisenstein ideals, which are well understood for \( N \) prime by the work of Mazur [23] but remain largely mysterious for general \( N \) (but still tractable for squarefree \( N \), as in the work of Yoo [40]). However, for \( N \) prime there is no need to optimize Cremona’s method: the method used by Bennett–Rechnitzer [2] to extend the tables of Stein–Watkins [35] is sufficient to compute (rigorously) a table of elliptic curves of all prime conductors up to \( 10^{10} \). Nonetheless, we hope that a thorough understanding of the present situation will provide a blueprint for extending the analysis; see below.

1.3. Additional questions. We conclude this introduction with discussion of further work to be done in this direction. To begin with, our final analysis of the experimental data remains somewhat incomplete because our analysis of mod-2 Galois representations focuses on the ones with dihedral image; while representations with larger image are somewhat rarer, they do appear to make measurable contributions which we would like to see quantified.

In addition, one could repeat the analysis in alternate situations: one could treat nonprime \( N \), work modulo another prime \( \ell \), consider \( T_p \) for another \( p \), and/or work in some higher weight \( k \). While all of these variants are of intrinsic interest, we would like to point out some developments in the computation of modular forms which draw attention to some particular cases. (Separately, the case of \( N \) prime, \( \ell = 2, p > 2, k = 2 \) has arisen in the context of error-correcting codes [28].)

We first reconsider our choice of method to compute the Hecke actions on \( S_k(\Gamma_0(N), \mathbb{Q}) \). The method of modular symbols is implemented in Magma [37] and Sage [30], and in a specially optimized form for \( k = 2 \) in Cremona’s eclib. The approach used in PARI/GP [27] is based on trace formulas. However, for a large-scale tabulation of rational eigenforms, we believe the best approach is the method of [3] as extended by Hein–Tornaría–Voight [15] (see also [38]). Birch’s original method is a variant of the Mestre–Oesterlé method of graphs [25] in the case where \( k = 2 \) and \( N \) is prime; Birch (partially) described his method for \( k = 2 \) and \( N \) squarefree, in terms of reduction of definite quadratic forms, while Hein–Tornaría–Voight generalize to higher weight by considering the action of \( \text{SO}(3) \) on nonstandard representations. Hein [16] has implemented the method in C++ for \( k = 2 \) and \( N \) squarefree; experimenting with this code reveals several computational benefits.

- It is extremely efficient in practice.
- The matrix of \( T_p \) is guaranteed\(^{(1)}\) to be integral (but not symmetric) and optimally sparse, with at most \( p + 1 \) nonzero entries per row.
- It separates eigenspaces for the Atkin-Lehner involutions, thus reducing the complexity of the resulting linear algebra.
- It removes some oldforms, thus again simplifying the linear algebra. For example, if \( N \) is squarefree with an odd number of prime factors, then no oldforms appear; if \( N \) is squarefree with an even number of prime factors, one gets an old subspace from the smallest prime factor of \( N \). For general \( N \), one sees oldforms from levels which differ from \( N \) by a square factor.

\(^{(1)}\)This is not true in Cremona’s setup because projecting onto the minus part of the space of modular symbols could in principle introduce a denominator of 2; we have yet to observe this.
The early abort strategy of computing ranks modulo $\ell$ is potentially even more effective when using the Birch–Hein–Tornaría–Voight method, due to the separation of Atkin–Lehner eigenspaces. However, in order to realize this benefit one must probably take $\ell > 2$, as for $\ell = 2$ the two possible eigenvalues of an involution come together, so there is the chance of some problematic (for our purposes) interaction between the eigenspaces. An analysis of the case $k = 2$, $N$ prime, $\ell = 3$ would be a natural variant of what we have done here.

Moreover, for $k > 2$ the early abort strategy may be of even greater value, as rational newforms in $S_k(\Gamma_0(N), \mathbb{Q})$ correspond to Galois representations for which there is no systematic construction available. Indeed, there is some evidence that there are only finitely many such forms for $k > 4$ \[29\]; extending previous exhaustive searches, particularly in the borderline case $k = 4$, would be a natural next step.

1.4. Acknowledgments. The authors thank Frank Calegari, Fred Diamond, Robert Pollack, Gabor Wiese, and Hwajong Yoo for helpful conversations.

2. Elliptic curves and their 2-torsion

For $K$ a quadratic extension of $\mathbb{Q}$, write $\mathcal{O}_K$ for its ring of integers, $\text{Cl}(K)$ for its class group, $h(K)$ for its class number, and $H(K)$ for its Hilbert class field. Write $\text{Cl}(K, a)$ for the ray class group of $K$ with conductor $a$ and $h(K, a)$ for the order of $\text{Cl}(K, a)$. Let $p(K)$ be a prime of $K$ above $(2)$, and write $\langle p(K) \rangle \subset \text{Cl}(K)$ for the subgroup that $p(K)$ generates. If $K$ is real, let $u(K)$ be a fundamental unit of $K$.

For $E$ an elliptic curve, write $N_E$ for the conductor of $E$. Let $\bar{\rho}_{E, 2} : G_{\mathbb{Q}, 2N_E} \to \text{GL}_2(\mathbb{F}_2)$ be the mod-2 Galois representation associated to $E$; it factors through $G_{K_E}$ where $K_E := \mathbb{Q}(E[2])$ has Galois group contained in $\text{GL}_2(\mathbb{F}_2) \cong S_3$. By considering the subgroups of $S_3$ and their embeddings in $\text{GL}_2(\mathbb{F}_2)$, we see that exactly one of the following alternatives holds.

1. $E[2]$ is reducible as a Galois module, and $K_E$ is either $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$ unramified away from $2N$. In other words, $E$ has at least one rational 2-torsion point.

2. $E[2]$ is irreducible over $\mathbb{F}_2$ but becomes reducible over $\mathbb{F}_4$, and $K_E$ is a cubic Galois extension of $\mathbb{Q}$. In other words, $G_\mathbb{Q}$ permutes the three non-identity points of $E[2]$ cyclically.

3. $E[2]$ is absolutely irreducible over $\mathbb{F}_2$, and $K_E$ is an $S_3$-extension of $\mathbb{Q}$.

Proposition 1. If $N_E = 2^r M$ for some odd squarefree integer $M$ and some $r \geq 0$, then $E[2]$ is either reducible or absolutely irreducible.

Proof. Suppose to the contrary that $K_E$ is cubic. Let $\ell$ be an odd prime dividing $N_E$. Since $\ell$ divides $N_E$ exactly once, $E$ has multiplicative reduction at $\ell$; hence the action of $G_{\mathbb{Q}_\ell}$ on the 2-adic Tate module of $E$ is reducible, and likewise for the action on $E[2]$. However, the (unique) order-3 subgroup of $\text{GL}_2(\mathbb{F}_2)$ is $\{(1 0), (1 1), (1 0)\}$, which acts irreducibly. Therefore the image of $G_{\mathbb{Q}_\ell}$ is trivial in $\text{GL}_2(\mathbb{F}_2)$, and so $K_E$ is unramified at $\ell$. Since this is true for every odd $\ell$ dividing $N_E$, $K_E$ is ramified at most at 2. But there are no cubic extensions of $\mathbb{Q}$ unramified outside 2: the maximal abelian extension unramified outside 2 is $\mathbb{Q}(\zeta_2)$, whose Galois group is pro-2. 

(ii) This happens, for example, for both isogeny classes of elliptic curves of conductor 196 [http://www.lmfdb.org/EllipticCurve/Q/196/] and isogeny classes $a$ and $c$ of conductor 324 [http://www.lmfdb.org/EllipticCurve/Q/324/].
In light of Proposition \[1\] when \( N_E \) is squarefree, we say that \( E \) is reducible if \( E[2] \) is a reducible representation of \( G_Q \) and \( K \)-dihedral, or simply dihedral, if \( K_E \) is an \( S_2 \)-extension containing a quadratic extension \( K \) of \( Q \).

Recall that \( E \) is ordinary (at \( 2 \)) if \( a_2(E) \) is odd, and supersingular (at \( 2 \)) otherwise. By theorems of Deligne and Fontaine (see Theorem \[1\]), \( E \) is ordinary at \( 2 \) if and only if \( \hat{\rho}_{E,2}[G_Q] \) is reducible. In particular, reducible elliptic curves are ordinary.

The following theorem will be proved in section \[5\].

**Theorem 2.** Let \( N \) be an odd prime.

1. Every dihedral elliptic curve of conductor \( N \) is either \( \mathbb{Q}(\sqrt{N}) \)-dihedral or \( \mathbb{Q}(\sqrt{-N}) \)-dihedral.

2. Ordinary dihedral elliptic curves: For \( K = \mathbb{Q}(\sqrt{\pm N}) \), if \( 3 \nmid \frac{h(K)}{\#(p(K))} \), then there are no ordinary \( K \)-dihedral elliptic curves of conductor \( N \).

3. Supersingular elliptic curves.
   - (a) If \( N \equiv 1, 7 \mod 8 \), then there are no supersingular elliptic curves of conductor \( N \).
   - (b) If \( N \equiv 3 \mod 8 \), then every supersingular elliptic curve of conductor \( N \) is \( \mathbb{Q}(\sqrt{-N}) \)-dihedral.
   - (c) If \( N \equiv 5 \mod 8 \), then every supersingular elliptic curve of conductor \( N \) is \( \mathbb{Q}(\sqrt{N}) \)-dihedral. If \( u(K) \neq 1 \mod 2O_K \), then there are no supersingular elliptic curves of conductor \( N \).

4. Reducible elliptic curves: If \( N \neq 1 \mod 8 \), then there are no reducible elliptic curves of conductor \( N \).

For prime \( N \) and \( K = \mathbb{Q}(\sqrt{\pm N}) \), the order of \( \mathfrak{p}(K) \) in \( \text{Cl}(K) \) divides \( 2 \) unless \( N \equiv 1 \mod 8 \), so if \( N \equiv 3, 5, 7 \mod 8 \) then the condition \( 3 \nmid \frac{h(K)}{\#(p(K))} \) in \[2\] is equivalent to \( 3 \nmid h(K) \). Similarly, if \( N \neq 7 \mod 8 \) and \( K = \mathbb{Q}(\sqrt{-N}) \), then the condition \( 3 \nmid \frac{h(K)}{\#(p(K))} \) in \[2\] is equivalent to \( 3 \nmid h(K) \).

Theorem \[2\] includes a theorem of Setzer \[34\] (Theorem 1): if \( N \) is a prime congruent to \( 1 \) or \( 7 \) mod \( 8 \) such that \( 3 \nmid h(\mathbb{Q}(\sqrt{\pm N})) \), then every elliptic curve of conductor \( N \) is reducible. With similar methods, we also recover the following results of Hadano \[14\] (Theorem II, Theorem III) and Kida \[20\] (Theorem 3.3). (Kida’s original statement requires \( N - 64 \) to not be a square; for \( N \neq 17 \), this is equivalent to existence of a reducible elliptic curve of conductor \( N \) \[34\] Theorem 2. See also \[14\] Theorem 1.)

**Theorem 3** (Hadano). Let \( N \) be a prime such that \( 3 \nmid h(\mathbb{Q}(\sqrt{\pm N})), h(\mathbb{Q}(\sqrt{\pm 2N})) \).

1. If \( N \equiv 1, 7 \mod 8 \), then every elliptic curve of conductor \( 2N \) is reducible.
2. If \( N \equiv 3, 5 \mod 8 \), there are no elliptic curves of conductor \( 2N \).

**Theorem 4** (Kida). Let \( N \) be a prime such that none of

\[
h(\mathbb{Q}(\sqrt{\pm N})), \quad h(\mathbb{Q}(\sqrt{(-1)^{(N-1)/2}N})), \quad 2
\]

is divisible by \( 3 \). Then every elliptic curve of conductor \( N \) is reducible.

3. Representation theory preliminaries

To prepare for the proof of Theorem \[2\] we make some representation-theoretic calculations. Fix a prime \( p \) and a field \( \mathbb{F} \) of characteristic \( p \), let \( G \) be any group, and let \( \rho : G \to \text{GL}_2(\mathbb{F}) \) be a semisimple representation. Let \( \rho(G) \subset \text{GL}_2(\mathbb{F}) \) and
Lemma 5. Let \( \rho(G) \subset PGL_2(\mathbb{F}) \) be the image and projective image of \( \rho \), respectively. Then exactly one of the following statements holds [33 Propositions 15–16].

1. **Reducible case:** \( \overline{\rho(G)} \) is a cyclic group \( C_n \). In other words, \( \rho \) is reducible (over \( \overline{\mathbb{F}} \), a sum of two characters \( \chi \oplus \chi' \), and the order of \( \chi/\chi' \) is \( n \).

2. **Dihedral case:** \( \overline{\rho(G)} \) is a dihedral group \( D_n \) of order \( 2n \) with \( n \geq 2 \). In other words, \( \rho \) is irreducible but there is an index-2 subgroup \( H \) of \( G \), determined uniquely if \( n \geq 3 \), so that \( \rho|_H \) splits as a sum of two characters.

3. **Exceptional case:** \( \overline{\rho(G)} \) is isomorphic to \( A_4 \), \( S_4 \), or \( A_5 \).

4. **Big-image case:** \( \overline{\rho(G)} \) contains \( PSL_2(\mathbb{F}_q) \) for some \( q \geq 5 \), but \( \rho(G) \neq SL_2(\mathbb{F}_5) \).

Call \( \rho \) reducible, dihedral, exceptional, or big-image accordingly.

### 3.1. The dihedral case in detail.

#### 3.1.1. Inducing a character.

Let \( H \subset G \) be a normal subgroup. Any character \( \psi : H \to F^\times \) to a field \( F \) may be twisted by any \( g \in G \) to obtain a new character \( g^\psi \), defined by \( g^\psi(h) := \psi(g^{-1}hg) \). Because \( \psi \) factors though an abelian quotient of \( H \), one can show that \( g^\psi \) depends only on the class \( \bar{g} \) of \( g \) in \( G/H \). We therefore write \( \bar{g}^\psi \) for the twist of \( \psi \) by \( \bar{g} \in G/H \).

Now suppose that \( H \subset G \) has index 2 and take \( \rho \) to be the induced representation \( \text{Ind}^G_H \psi : G \to GL_2(F) \). Let \( \varepsilon_H \) be the (at most quadratic) character of \( G \) that takes \( H \) to 1 and \( G-H \) to \(-1 \). Let \( \bar{g} \) be the nontrivial element of \( G/H \). The following are well-known (e.g., see [32 7.2.1]):

1. \( \rho|_H = \psi \oplus \bar{g}^\psi \);
2. \( \rho \) is an irreducible representation of \( G \) if and only if \( \psi \neq \bar{g}^\psi \);
3. \( \det \rho = \varepsilon_H \cdot \psi(\text{Ver}_{\overline{\rho_H}}^G) \), where \( \text{Ver}_{\overline{\rho_H}}^G : G \to H^{ab} \) is the Verlagerung (transfer) homomorphism taking \( x \in G \) to \( x g^{-1} g^x \).
4. \( \rho(G) \cong D_n \), where \( n \) is the order of \( \bar{g}^\psi/\psi \) (assuming \( \psi \) has finite order).

#### 3.1.2. Dihedral representations.

Conversely, suppose that \( \rho : G \to GL_2(F) \) is a dihedral representation with \( \overline{\rho(G)} = D_n \). If \( n \geq 3 \), then \( D_n \) contains a unique index-2 subgroup isomorphic to \( C_n \). Let \( H \subset G \) be the inverse image of that cyclic subgroup under the map \( G \to GL_2(F) \to PGL_2(F) \). Since \( \overline{\rho(H)} \) is a cyclic group, \( \rho|_H \) is a reducible representation, a sum of two characters, each defined over an at-most-quadratic extension of \( F \). Let \( \psi : H \to F^\times \) be one of these characters. Then Frobenius reciprocity and dimension considerations guarantee that the map \( \text{Ind}^G_H \psi \to \rho \) induced by \( \psi \to \rho|_H \) is an isomorphism.

#### 3.1.3. The image of a dihedral representation.

Suppose further that \( \rho \) is a faithful dihedral representation of \( G \). With \( H \), \( \psi \), and \( \bar{g}^\psi \) as above, we have the following:

**Lemma 5.** (1) \( \ker \psi \cap \ker \bar{g}^\psi = 1 \).

(2) \( H \) is an abelian subgroup of \( G \).

(3) If \( \ker \psi \subset H \) is normal in \( G \), then \( \psi \) is faithful, so \( H \) is cyclic.

---

(iii) The restrictions are explained by exceptional isomorphisms for small primes: \( SL_2(\mathbb{F}_2) \cong D_3 \), \( PSL_2(\mathbb{F}_3) \cong A_4 \), \( PGL_2(\mathbb{F}_3) \cong S_4 \), \( PSL_2(\mathbb{F}_4) = PGL_2(\mathbb{F}_4) \cong A_5 \), and \( PSL_2(\mathbb{F}_5) \cong A_5 \).

(iv) One can show that \( \psi(\text{Ver}_{\overline{\rho_H}}^G) \) takes \( x \in H \) to \( \psi(\bar{g}^\psi(x)) \) and takes \( x \in G-H \) to \( \psi(x^2) \).

(v) For \( n = 2 \), there are three such subgroups. But \( n \) is the order of a character to \( PGL_2(\mathbb{F}_p) \) (see section [32 7.2.1]) and hence prime to \( p \); as we will later restrict to \( p = 2 \), we ignore \( n = 2 \) here.
The proofs are straightforward but not completely standard, so we include them.

Proof.  
(1) Indeed, \( \rho|_H = \psi \oplus \overline{\psi} \) and we have assumed that \( \ker \rho \) is trivial. 
(2) The commutator of any two elements of \( H \) is in both \( \ker \psi \) and \( \overline{\psi}; \) the claim follows from part (1).
(3) By part (2), \( G/H \) acts on \( H \) by conjugation, and \( \ker \overline{\psi} \) is the image of \( \ker \psi \) under the action of the nontrivial element. Now use (1).

□

Note that even if \( \psi \) is faithful and \( H \) is finite cyclic of order \( n \) and the sequence 

\[ 1 \to H \to G \to G/H \to 1 \]

splits (i.e., there is an order-2 element in \( G - H \)), we cannot conclude that \( G \) is isomorphic to \( D_n \); the dicyclic groups give a counterexample for every even \( n \).

3.1.4. Translating to Galois representations. Let \( \rho : G_\mathbb{Q} \to \text{GL}_2(F) \) be a finite-image dihedral representation such that \( \left| \rho(G_\mathbb{Q}) \right| \geq 6 \). Let \( K \) be the quadratic extension of \( \mathbb{Q} \) for which \( \left| \rho(G_\mathbb{Q}) : \rho(G_K) \right| = 2 \), so that \( \rho|_{G_K} \) is reducible. Let \( \psi : G_K \to F^\times \) be a character appearing in \( \rho|_{G_K} \) and let \( L_\psi \) be the fixed field of \( \ker \psi \). If \( L_\psi/\mathbb{Q} \) is Galois, then \( L_\psi = \ker \rho \). Otherwise, writing \( \text{Gal}(K/\mathbb{Q}) = \{1, \sigma\} \), we obtain the twist \( \sigma \psi \); its fixed field \( L_{\sigma \psi} \) is the image \( \overline{\sigma}(L_\psi) \subset \mathbb{Q} \) for any lift \( \overline{\sigma} \) of \( \sigma \) to \( G_K \) and \( \ker \rho =: M \) is the compositum \( L_\psi L_{\sigma \psi} \) (inside \( \mathbb{Q} \)). In particular, it is clear that \( M \) is an abelian extension of \( K \).

3.1.5. Artin conductor formulas. We will also make use of the following formula (see, for example, [36, Corollary 1]) for the Artin conductor of \( \text{Ind}_K^Q \psi \) in terms of the Artin conductor of \( \psi \):

\[
\text{cond}(\text{Ind}_K^Q \psi) = |\Delta_K| \cdot N_K^{K/\mathbb{Q}}(\text{cond} \psi),
\]

where \( N_K^{K/\mathbb{Q}} \) is the field norm and \( \Delta_K \) is the discriminant of \( K \).

If \( F \) is a finite extension of \( \mathbb{F}_p \) or a \( p \)-adic field, we will denote the tame or prime-to-\( p \) Artin conductor by \( \text{cond}^{(p)} \). The analogous formula holds:

\[
\text{cond}^{(p)}(\text{Ind}_K^Q \psi) = \left| \Delta_K^{(p)} \right| \cdot N_K^{\psi}(\text{cond}^{(p)} \chi).
\]

Here \( \Delta_K^{(p)} \) is the prime-to-\( p \) part of the discriminant of \( K \).

3.2. Mod-2 dihedral Galois representations. From now on, we work with \( F = \mathbb{F} \), a finite extension of \( \mathbb{F}_2 \). Suppose that \( \rho = \text{Ind}_K^Q \psi : G_Q \to \text{GL}_2(\mathbb{F}) \) is a \( K \)-dihedral representation for some quadratic \( K \) over \( \mathbb{Q} \) and ray class (i.e., Hecke) character \( \psi : G_K \to \mathbb{F}^\times \).

3.2.1. Implications of \( \text{det} \rho = 1 \). Again, let \( L_\psi \) be the fixed field of \( \ker \psi \).

Lemma 6. If \( \text{det} \rho = 1 \), then \( L_\psi \) is Galois over \( \mathbb{Q} \).

Proof. If \( \text{det} \rho = 1 \), then considering \( \text{det} \rho \) on the subgroup \( G_K \), we see that \( \sigma \psi = \psi^{-1} \). Therefore \( L_\psi \) is also the fixed field of \( \ker \sigma \psi \), which means that \( L_\psi/\mathbb{Q} \) is Galois and \( L_\psi \) is the fixed field of \( \ker \rho \). □
3.2.2. The conductor of $\psi$. Let $a$ be the conductor of $\psi$. Since we work in characteristic 2, we are only interested in odd-order $\psi$ here; we thus ignore consideration of any real places of $K$ and view $a$ as an integral ideal of $K$. We have a standard exact sequence relating the class group $\text{Cl}(K)$ to the ray class group $\text{Cl}(K, a)$:

\[ \mathcal{O}_K^\times \to (\mathcal{O}_K/a)^\times \to \text{Cl}(K, a) \to \text{Cl}(K) \to 1 \]

**Lemma 7.** If $a = q^n$ is a power of a prime of $\mathcal{O}_K$ lying over a prime $q$ of $\mathbb{Z}$, then $[\text{Cl}(K, a) : \text{Cl}(K)]$ divides \( \begin{cases} (q-1)q^{k} & \text{for some } k \geq 0 \text{ if } (q) \text{ splits or ramifies in } K, \\ (q^2-1)q^{k} & \text{for some } k \geq 0 \text{ if } (q) \text{ is inert in } K. \end{cases} \)

**Proof.** Immediate from sequence (3) in light of the exact sequence

\[ 1 \to 1 + q^n\mathcal{O}_K \to 1 + q\mathcal{O}_K \to (\mathcal{O}_K/q^n)^\times \to (\mathcal{O}_K/q)^\times \to 1, \]

combined with the fact that $1 + q\mathcal{O}_K$ is pro-$q$. \qed

**Corollary 8.** (1) If 2 ramifies or splits in $K$, then any Hecke character $\psi : G_K \to \mathbb{F}_2^\times$ of modulus $2^n\mathcal{O}_K$ has trivial conductor and hence factors through $\text{Cl}(K)$.

(2) If 2 is inert in $K$, then any Hecke character $\psi : G_K \to \mathbb{F}_2^\times$ of modulus $2^n\mathcal{O}_K$ has conductor dividing $2\mathcal{O}_K$ and hence factors through $\text{Cl}(K, (2))$.

**Proof.** (1) If 2 ramifies in $K$, then this follows immediately from Lemma 7 since $(q-1)q^n$ is a power of 2. If 2 splits as $2\mathcal{O}_K = pp'$, then argue as in Lemma 7 noting that $(\mathcal{O}_K/(2\mathcal{O}_K)^n)^\times = (\mathcal{O}_K/p^n)^\times \times (\mathcal{O}_K/p'^n)^\times$ by the Chinese remainder theorem.

(2) From the proof of Lemma 7 and sequence (4), it’s clear that the only odd contribution to $[\text{Cl}(K, (2)^n) : \text{Cl}(K)]$ comes at $n = 1$. \qed

3.2.3. The local behavior of $\rho$. Fixing an embedding $\iota : G_{\mathbb{Q}_2} \to G_{\mathbb{Q}}$, we can consider the restriction $\rho_2$ of $\rho$ to $G_{\mathbb{Q}_2}$. Let $p$ be the prime of $\mathcal{O}_K$ above 2 corresponding to $\iota$, and let $\psi_2$ be the restriction of $\psi$ to $G_{K_p}$. Then $\rho_2$ is reducible if and only if either

(1) 2 splits in $K$.

(2) 2 is inert or ramified in $K$ and $\sigma\psi_2 = \psi_2$.

(Note that $\sigma$ is in the decomposition group at $p$ in this case.)

3.3. Mod-2 dihedral Galois representations of prime conductor. Retaining the notation $(\mathbb{F}, \rho, K, \psi)$ from the previous subsection, we now additionally suppose that $N$ is an odd prime and $\rho$ has (tame Artin) conductor $N$. The induced tame conductor formula (2) guarantees that either

\[ \Delta^{(2)}_K = (1), \quad \mathcal{N}_\mathbb{Q}^K(\text{cond}^{(2)}\psi) = (N) \quad \text{or} \quad \Delta^{(2)}_K = (N), \quad \mathcal{N}_\mathbb{Q}^K(\text{cond}^{(2)}\psi) = (1). \]

We analyze each scenario in turn.

3.3.1. First scenario: $\Delta^{(2)}_K = (1)$ and $\mathcal{N}_\mathbb{Q}^K(\text{cond}^{(2)}\psi) = (N)$. Here, $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$, and $N$ splits in $K$ as $(N) = qq'$ with $\text{cond}^{(2)}\psi = q$. Hence $\psi$ is a ray class character of conductor $qa$ for some ideal $a$ of $K$ divisible only by primes above 2.

**Lemma 9.** In this scenario, $\det \rho : G_{\mathbb{Q}} \to \mathbb{F}_2^\times$ is a nontrivial character.

**Proof.** Since $\text{cond}\psi$ is not Galois-invariant, $L_\psi$ is not Galois over $\mathbb{Q}$. Lemma 6 then implies the desired conclusion. \qed
3.3.2. Second scenario: $\Delta^{(2)}_K = (N)$ and $N^*_K(\cond(\psi)) = (1)$. Here, $K = \mathbb{Q}(\sqrt{\pm N})$ or $\mathbb{Q}(\sqrt{\pm 2N})$ and $\psi$ is a ray class character of conductor dividing $(2\mathcal{O}_K)^\alpha$.

**Corollary 10.** In this scenario, $\psi$ factors through $\text{Cl}(K)$ unless

- $N \equiv 5 \mod 8$ and $K = \mathbb{Q}(\sqrt{N})$
- $N \equiv 3 \mod 8$ and $K = \mathbb{Q}(\sqrt{-N})$.

in which cases $\psi$ factors through $\text{Cl}(K,(2))$.

**Proof.** Combine Corollary\[^{[3]}\] with the ramification of 2 in $\mathbb{Q}(\sqrt{\pm N})$; see Table\[^{[1]}\].

---

**Table 1.** Class number parity and splitting of 2 in $\mathbb{Q}(\sqrt{\pm N})$ for $N$ prime.

| $N \mod 8$ | $K = \mathbb{Q}(\sqrt{N})$ | $K = \mathbb{Q}(\sqrt{-N})$ |
|------------|----------------------------|----------------------------|
|            | (2) in $K$ | $h(K)$ | $(\#(p(K)))$ | (2) in $K$ | $h(K)$ | $(\#(p(K)))$ |
| 1          | splits     | odd   | varies       | ramifies   | even > 4 | 2         |
| 3          | ramifies   | odd   | 1            | inert      | odd      | 1         |
| 5          | inert      | odd   | 1            | ramifies   | 2-odd    | 2         |
| 7          | ramifies   | odd   | 1            | splits     | odd      | varies    |

---

3.4. Mod-2 modular Galois representations of weight 2. We now suppose that $N$ is an odd integer (not necessarily prime) and $f \in S_2(\Gamma_0(N),\bar{\mathbb{Z}}_2)$ is a normalized weight-2 Hecke eigenform of level $N$. By a theorem of Breuil–Conrad–Diamond–Taylor \[^{[4]}\], such $f$ with coefficients in $\mathbb{Q}$ correspond precisely to isogeny classes of elliptic curves $E$ of conductor $N$, with the $\ell$\textsuperscript{th} Fourier coefficient satisfying $a_\ell(f) = \ell + 1 - \#E(\mathbb{F}_\ell)$ for all primes $\ell \mid 2N$. As for elliptic curves, the form $f$ is *ordinary* or *supersingular* according to whether $a_2(f)$ is a unit in $\mathbb{Z}_2$. Reducing any $G_{\mathbb{Q}}$-stable lattice of the Galois representation associated by Eichler and Shimura to $f$, we obtain a mod-2 representation $\rho_f : G_\mathbb{Q} \rightarrow \text{SL}_2(\mathbb{F}_2)$ which for prime $\ell \mid 2N$ is unramified at $\ell$ and satisfies $\text{Tr } \rho_f(\text{Frob}_\ell) = \bar{a}_\ell(f)$, where $\bar{a}_\ell(f) \in \mathbb{F}_2$ is the mod-2 reduction of $a_\ell(f)$. If $f$ corresponds to an elliptic curve $E$ (up to isogeny), then $\rho_f$ is the representation $\rho_{E,2}$ (up to semisimplification) discussed in section 2.4.

Fixing a prime of $\mathbb{Q}$ above 2, we consider the corresponding decomposition group of $G_{\mathbb{Q}}$, which one can identify with the absolute Galois group $G_{\mathbb{Q}_2} = \text{Gal}(\bar{\mathbb{Q}}_2/\mathbb{Q}_2)$ of the local field $\mathbb{Q}_2$. The following theorem relates the shape of the local representation $\rho_{f,2} := \rho_f|_{G_{\mathbb{Q}_2}}$ to the invertibility of $a_2(f)$. In the statement and the proof, $\mathbb{Q}_{p^2}$ refers to the unique unramified degree-2 extension of $\mathbb{Q}_p$.

**Theorem 11** (Deligne, Fontaine, Edixhoven, Serre). One of the following holds.

1. $\rho_{f,2}$ is reducible, in which case $f$ is ordinary, and

$$\rho_{f,2} \sim \begin{pmatrix} \lambda^{-1} & * \\ 0 & \lambda \end{pmatrix},$$

where $\lambda : G_{\mathbb{Q}_2} \rightarrow \mathbb{F}_2^\times$ is the unramified character sending $\text{Frob}_2$ to $\bar{a}_2(f)$.

Moreover $\rho_{f,2}$ is at most $p$-wildly ramified in the sense of Serre \[^{[3]}\].

---

\[^{[3]}\] An extension $M/\mathbb{Q}_p$ is at most $p$-wildly ramified if $M = M^*\left(\alpha_1^{1/p}, \ldots, \alpha_d^{1/p}\right)$, where $M^*/\mathbb{Q}_p$ is the at most tamely ramified subextension of $M$, and the $\alpha_i$ can be taken to be units in $\mathbb{Q}_p$. 

---
\(\rho_{f,2}\) is irreducible, in which case \(f\) is supersingular. In this case, \(\rho_{f,2}\) is the induction of a character of \(G_{Q_2}\) (the second fundamental character) and is therefore at most tamely ramified.

**Proof.** Write \(p\) in place of 2 to avoid confusion with weight 2. For the shape of \(\rho_{f,p}\), see Edixhoven [11] Theorems 2.5, 2.6. In the ordinary case, since \(f\) has level prime to \(p\) and weight 2, \(\rho_{f,p}\) is finite at \(p\): it arises from a finite flat group scheme over \(\hat{\mathbb{Z}}_p\) (the \(p\)-torsion of a certain abelian variety of GL2-type), forcing \(\rho_{f,p}\) to be at most peu wildly ramified [11, Proposition 8.2]. In the supersingular case, \(\rho_{f,2}\) is at most tamely ramified by [23, Proposition 4]; for the description of \(\rho_{f,p}\) as the induction of the second fundamental character of \(G_{Q_p}\), see [31, §2.2]. \(\Box\)

4. **Mod-2 dihedral representations appearing in weight 2**

Before proving Theorem 2, we state an analogous theorem for cuspforms of weight 2; see Theorem [12] below. As many of the arguments are identical, the two theorems will be proved together in section 5.

For \(N\) an odd squarefree positive integer, we study the distribution of generalized \(T_2\)-eigenvalues on \(S_2(\Gamma_0(N), \bar{\mathbb{F}}_2)^{\text{new}}\). Write \(m(N)\) for the dimension of this space. For \(\alpha \in \bar{\mathbb{F}}_2\), write \(m(N, \alpha)\) for the dimension of the generalized kernel of \(T_2 - \alpha\) on this space (i.e., the dimension of the generalized eigenspace corresponding to \(T_2\)-eigenvalue \(\alpha\)). Let \(m_{\text{ord}}(N) := m(N) - m(N,0)\), the dimension of the ordinary subspace. Our aim will be to give lower bounds on \(m_{\text{ord}}(N)\), \(m(N,1)\), and \(m(N,0)\) by enumerating dihedral forms with multiplicities. Note that, for squarefree \(N\), forms defined over \(\mathbb{F}_2\) will be either dihedral or reducible (that is, the analog of Proposition 1 holds).

To this end, write \(S_2(N) := S_2(\Gamma_0(N), \bar{\mathbb{F}}_2)^{\text{new}}\) and let \(T_2(N) := T_2(N, \bar{\mathbb{F}}_2)^{\text{new}}\) be the shallow Hecke algebra acting on \(S_2(N)\). In other words, \(T_2(N)\) is the (commutative) \(\bar{\mathbb{F}}_2\)-algebra generated inside \(\text{End}_{\bar{\mathbb{F}}_2}(S_2(N))\) by the action of all the Hecke operators \(T_n\) with \(n\) prime to \(2N\). Then \(T_2(N)\) is a semilocal artinian ring whose maximal ideals \(\mathfrak{m}\) correspond to mod-2 Hecke eigensystems appearing in \(S_2(N)\). For \(\ell\) prime to \(2N\), let \(a_{\ell}(\mathfrak{m})\) be the \(T_\ell\)-eigenvalue corresponding to \(\mathfrak{m}\); note that \(\mathfrak{m}\) is generated by the \(T_\ell - a_{\ell}(\mathfrak{m})\) for \(\ell \nmid 2N\). By Serre reciprocity (a/k/a Serre’s conjecture [31], now known by work of Khare–Wintenberger [18, 19], Kisin [22], and Dieulefait [10]), the maximal ideals \(\mathfrak{m}\) also correspond to semisimple Galois representations \(\rho_{\mathfrak{m}} : G_{Q_{2N}} \to \text{SL}_2(\bar{\mathbb{F}}_2)\) that are at most peu wildly ramified at 2. The correspondence is codified by the Eichler-Shimura relation \(a_{\ell}(\mathfrak{m}) = \text{tr}\rho_{\mathfrak{m}}(\text{Frob}_\ell)\).

Theorem 14 implies that given \(\mathfrak{m}\), one can determine whether \(a_{\ell}(\mathfrak{m})\) is 0 or 1; otherwise \(a_{\ell}(\mathfrak{m})\) is only defined up to inverse.\(^{\text{vii}}\)

We decompose \(T_2(N)\) as a product of localizations at its maximal ideals, and correspondingly decompose of \(S_2(N)\) into generalized \(\mathfrak{m}\)-eigenspaces \(S_2(N)_{\mathfrak{m}}:\)

\[
T_2(N) = \prod_{\mathfrak{m}} T_2(N)_{\mathfrak{m}} , \quad S_2(N) = \bigoplus_{\mathfrak{m}} S_2(N)_{\mathfrak{m}} .
\]

\(^{\text{Miv}}\) If \(M\) is still an elementary \(p\)-extension of \(M^p\) but at least one of the \(\alpha_i\) must be a nonunit, then \(M\) is \(\text{très wildly ramified}\). See [31, 2.4.ii]. A representation of \(\text{Gal}(\bar{Q}_p/Q_p)\) as usual inherits the ramification properties of the fixed field of its kernel.

\(^{\text{vii}}\)Note that \(a_{\ell}(\mathfrak{m})\) is not in general the trace of a Frobenius element at 2 of the \(\rho_{\mathfrak{m}}\) corresponding to \(\mathfrak{m}\) (indeed, \(\rho_{\mathfrak{m}}\) may be ramified at 2). Therefore \(a_{\ell}(\mathfrak{m})\) is not a priori determined by \(\mathfrak{m}\). In fact, \(a_{\ell}(\mathfrak{m})\) may not even be defined over the field of definition of \(\rho_{\mathfrak{m}}\). This happens, for example, in level 257 for the \(\mathbb{Q}(\sqrt{257})\)-dihedral Galois orbit of forms.
Note that if \( m \subset \mathbb{T}_2(N) \) is a maximal ideal, then the eigenspace \( S_2(N)[m] \) is nonzero, so that the dimension of the generalized eigenspace \( S_2(N)_m \) is at least 1.

We say that a maximal ideal \( m \) of \( \mathbb{T}_2(N) \) is reducible, dihedral, exceptional, or big-image if \( \rho_m \) has the corresponding property. Similarly, we say that \( m \) is supersingular or ordinary if \( \rho_m \) is so at 2.

We determine the fields \( K \) for which there exist \( K \)-dihedral \( m \) occurring in \( \mathbb{T}_2(N) \) for \( N \) prime and how many such \( m \) there are (Theorem 12 below). In section 6, we study the multiplicity of \( S_2(N)_m \) in each case (Conjecture 13 and Proposition 14).

**Theorem 12.** Let \( N \) be an odd prime, and \( m \subset \mathbb{T}_2(N) \) a maximal ideal.  

1. If \( m \) is dihedral, then it is either \( \mathbb{Q}(\sqrt{N}) \)-dihedral or \( \mathbb{Q}(\sqrt{-N}) \)-dihedral.
2. Ordinary dihedrals: For \( K = \mathbb{Q}(\sqrt{N}) \), there are exactly \( \frac{h(K)^{\text{odd}} - 1}{2} \) ordinary \( K \)-dihedral maximal ideals in \( \mathbb{T}_2(N) \). Of these, \( \frac{h(K)^{\text{odd},2\text{-split}} - 1}{2} \) have \( a_2(m) = 1 \).
3. Supersingular dihedrals.  
   (a) If \( m \) is supersingular \( K \)-dihedral, then either \( N \equiv 3 \) mod 8 and \( K = \mathbb{Q}(\sqrt{-N}) \), or \( N \equiv 5 \) mod 8 and \( K = \mathbb{Q}(\sqrt{N}) \).
   (b) Let \( N \equiv 3 \) mod 8 and \( K = \mathbb{Q}(\sqrt{-N}) \). If \( N > 3 \), then there are exactly \( h(K) \) supersingular maximal ideals of \( \mathbb{T}_2(N) \).
   (c) Let \( N \equiv 5 \) mod 8 and \( K = \mathbb{Q}(\sqrt{N}) \). If \( u(K) \equiv 1 \) mod 2\( \mathcal{O}_K \), then there are \( h(K) \) supersingular maximal ideals of \( \mathbb{T}_2(N) \); otherwise, there are none.
4. Reducibles: If \( N \equiv 1 \) mod 8, then there is one reducible maximal ideal of \( \mathbb{T}_2(N) \), generated by \( T_\ell \) for every prime \( \ell \nmid 2N \); otherwise, there are none.

Note that \( h(\mathbb{Q}(\sqrt{N})) \) is always odd, and \( h(\mathbb{Q}(\sqrt{-N})) \) is even only for \( N \equiv 1 \) mod 4.

Note also that a prime \( p \) above 2 of \( K = \mathbb{Q}(\sqrt{\pm N}) \) has order 1 or 2 in the class group unless \( N \equiv \varepsilon \) mod 8 and \( K = \mathbb{Q}(\sqrt{\varepsilon N}) \) for \( \varepsilon = \pm 1 \), so the 2-split condition is vacuous outside those two cases.

## 5. Proofs of theorems

We prove the various parts of Theorems 2 and 12 in parallel. We then adapt the ideas to recover the theorems of Hadano (Theorem 3) and Kida (Theorem 4).

### 5.1. Proof of parts 1

Suppose that \( f \in S_2(N) \) is a \( K \)-dihedral modular form for some quadratic extension \( K \) of \( \mathbb{Q} \) (corresponding to an elliptic curve for Theorem 2 or to a maximal ideal of the Hecke algebra for Theorem 12). Since \( \rho_f \) factors through an extension of \( \mathbb{Q} \) unramified outside of 2 and \( N \), \( K \) must be one of the following:

\[
\mathbb{Q}(\sqrt{N}), \mathbb{Q}(\sqrt{-N}), \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2N}), \mathbb{Q}(\sqrt{-2N}).
\]

If \( K = \mathbb{Q}(\sqrt{\pm 2N}) \), then \( K \) is très wildly ramified at 2 [31 2.6, Exemple], so no modular forms of weight 2 (and in particular no elliptic curves) can be \( K \)-dihedral (Theorem 11). If \( K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \) or \( \mathbb{Q}(\sqrt{2}) \), then we are in the first scenario of subsection 3.3 and Lemma 9 guarantees that a \( K \)-dihedral representation cannot come from a \( \Gamma_0(N) \)-modular form. Thus \( K = \mathbb{Q}(\sqrt{\pm N}) \), as claimed.
5.2. Proof of parts (2). Suppose $K = \mathbb{Q}(\sqrt{\pm N})$ and $f \in S_2(N)$ is a $K$-dihedral ordinary form, with $\rho = \rho_f = \text{Ind}_K^G \psi$ for some character $\psi$ of $G_K$ ramified only at primes above 2 (section 3.3.2). Write $H = H(K)$ and $p = p(K)$. Let $L$ be the fixed field of $\ker \psi$. Since $\det \rho = 1$, by Lemma 6 the extension $L/\mathbb{Q}$ is Galois. Choose a prime $\mathcal{P}$ of $L$ above $p$, and write $\psi_2$ for the restriction of $\psi$ to $\text{Gal}(L_{\mathcal{P}}/K_p)$.

We first show that $\psi$ is in fact unramified at 2, and hence will factor through $H^{\text{odd}}$, the maximal odd-degree subextension of $H$. By Corollary 10 and Table 1 $\psi$ is unramified in all cases except possibly when 2 is inert in $K$. In that case, $\rho_{f,2} = \text{Ind}_K^H \psi_2$, so by 3.1.1 (2) we know that $\psi_2 = \sigma_2 \psi_2$ for $\sigma_2$ a generator of $\text{Gal}(K_p/\mathbb{Q}_2)$. In this case, Theorem 11 (1) tells us that $\psi_2$ is unramified above 2, as then is $\psi$. In fact, the determinant condition further forces $\sigma_2 \psi_2 = \psi_2^{-1}$, which implies $\psi_2 = 1$ because we are in characteristic 2.

Next, from Theorem 11 (1), the condition $a_2(f) = 1$ is equivalent to the condition $\psi_2 = 1$, which exactly means that $\psi$ factors through $H^{\text{odd,2-split}}$, the maximal odd subextension of $H$ over $K$ in which 2 splits completely.

To complete the proof of Theorem 2 (2), we observe that $[H^{\text{odd,2-split}} : K] = \frac{h(K)^{\text{odd}}}{\#(p)}$. If $\rho$ comes from a $K$-dihedral elliptic curve, then it has image $D_3$ so that $\psi$ must have order 3. So a $K$-dihedral elliptic curve of conductor $N$ is only possible if 3 divides $\frac{h(K)^{\text{odd}}}{\#(p)}$, or equivalently $h(K)^{\text{odd}}$. 

To complete the proof of Theorem 12 (2), we recall that in general, $\text{Ind}_K^H \psi = \text{Ind}_K^G \psi'$ if and only if $\psi = \psi'$ or $\sigma \psi = \psi'$ for $\sigma$ a generator of $\text{Gal}(K/\mathbb{Q})$. In our unit-determinant case, $\sigma \psi = \psi^{-1}$. Therefore there are $\frac{h(K)^{\text{odd}}}{2}$ distinct ordinary $K$-dihedral $\rho$, as claimed. The $a_2 = 1$ condition works similarly.

5.3. Proof of parts (3). Suppose that $K = \mathbb{Q}(\sqrt{\pm N})$ and $f \in S_2(N)$ is a $K$-dihedral form with $\rho = \rho_f = \text{Ind}_K^G \psi$ for some character $\psi$ of $G_K$ ramified only at primes above 2. Maintain the notation $H$, $p$, $\sigma$, $\rho_2$ as above. As in the second paragraph of section 5.2 $\psi$ does not factor through $H$ (or else $\rho_2$ would be reducible, contradicting Theorem 11). Therefore $\psi$ must be a character of $\text{Cl}(K,\mathfrak{a})$ for some ideal $\mathfrak{a}$ of $K$ divisible only by primes above 2. By Corollary 8 $\mathfrak{a} = (2)$ and either $N = 3$ mod 8 and $K = \mathbb{Q}(\sqrt{-N})$, or $N = 5$ mod 8 and $K = \mathbb{Q}(\sqrt{N})$.

Now suppose we are in one of these two cases. Since $\sigma \psi = \psi^{-1}$, the character $\sigma \psi$ will also factor through $H(K,(2))$ and not through $H$. This gives exactly $\frac{h(K,(2))}{2} - h(K)$ representations, and hence maximal ideals of $T_3(N)$.

The formulations in part (3b) of Theorem 12 and part (3c) of both theorems come from analyzing the sequence (3) from the proof of Lemma 7. For $N$ congruent to 3 modulo 8, we have $K = \mathbb{Q}(\sqrt{-N})$, so that

$$\mathcal{O}_K = \begin{cases} \{\pm 1\} & \text{if } N > 3 \\ \{\pm 1, \pm \omega, \pm \omega^2\} & \text{if } N = 3 \end{cases}$$

for $\omega$ a cube root of unity in $\mathbb{Q}(\sqrt{-3})$. Since (2) is inert in $K$, we have $\mathcal{O}_K/(2) = \mathbb{F}_4$. Therefore, for $N > 3$ (still congruent to 3 modulo 8), sequence (3) becomes

$$\{\pm 1\} \to \mathbb{F}_4^\times \to H(K,(2)) \to H(K) \to 1,$$

so that $h(K,(2)) = 3h(K)$. For $N = 3$, on the other hand, the global units exactly cancel out the mod-(2) units, so that $h(K,(2)) = h(K)$. For $N$ congruent to 5
modulo 8, we still have \( \mathcal{O}_K/(2) = \mathbb{F}_4 \), but this time \( \mathcal{O}_K = \{ \pm 1 \} \times u^Z \) for some fundamental unit \( u = u(K) \), and therefore we similarly have the two cases

\[
h(K, (2)) = \begin{cases} 3h(K) & \text{if } u \text{ maps to } 1 \text{ in } (\mathcal{O}_K/(2))^\times \\ h(K) & \text{otherwise}. \end{cases}
\]

5.4. **Proof of parts [4]**. If \( N \not\equiv 1 \mod 8 \), then 2 is not an Eisenstein prime for \( N \) (see Mazur [23] or Mazur–Serre [24]), so there are no cuspforms in \( S_2(N, Z) \) congruent to the Eisenstein series \( E_2 \); this is ruled out by assuming that \( 3 \nmid h(K) \); this completes the proof of Theorem 3. Let \( \rho_T \) be an order-3 character of \( T \) corresponding to 1 in \( \mathcal{O}_K/(2)^\times \), and let \( \psi \) be a nontrivial order-3 character of \( H(K, (2)) \); this completes the proof of Theorem 4.

5.5. **Proof of Theorem 4.** By Theorem 12 (2), the condition \( 3 \nmid h(K) \) rules out the existence of an ordinary elliptic curve of conductor \( N \). For a supersingular elliptic curve, with notation as in the proof of Theorem 12 (3), \( K = \mathbb{Q}(\sqrt{-1})^{(N-1)/2} \) and \( \psi \) is a nontrivial order-3 character of \( H(K, (2)) \); this is ruled out by assuming that \( 3 \nmid h(K) \) holds. By Proposition [1] \( m \) is either reducible or ordinary dihedral.

In the reducible case, \( m \) is an Eisenstein ideal; by the proof of [40, Theorem 6.1], the difference of the cusps of \( X_0(2N) \) corresponding to \( 1, 1/2 \in \mathbb{P}^1(\mathbb{Q}) \) must have even order in the Jacobian. By [40, Theorem 1.3] this order is the numerator of \((N^2 - 1)/8\), forcing \( N \equiv 1, 7 \mod 8 \).

In the ordinary dihedral case, by Lemma [8] we must be in the second scenario of subsection 3.3 that is, that is, \( \rho_T = \text{Ind}_K^H \psi \) where \( K \) is one of \( \mathbb{Q}(\sqrt{\pm N}) \) and \( \psi \) is an order-3 character of \( G_K \) ramified only at primes above 2. As in subsection 5.2 we see that \( \psi \) is also unramified at 2 and so factors through \( \text{Cl}(K) \); however, this contradicts the hypothesis that \( 3 \nmid h(K) \).

This completes the proof of Theorem 4.

6. **Multiplicities of mod-2 dihedral cuspforms in weight 2**

The following conjecture complements Theorem 12. Note that the fact that \( m \subset T_2(N) \) is a maximal ideal automatically implies that \( \dim S_2(N)_m \geq 1 \).

**Conjecture 13.** Let \( N \) be an odd prime and \( m \) a maximal ideal of \( T_2(N) \).

1. Suppose \( N \equiv 1 \mod 8 \).
   (a) If \( m \) is \( \mathbb{Q}((\sqrt{N}) \)-dihedral, then \( \dim S_2(N)_m \geq 4 \).
   (b) If \( m \) is \( \mathbb{Q}(\sqrt{-N}) \)-dihedral, then \( \dim S_2(N)_m \geq h(-N)^{\text{even}} \).
   (c) If \( m \) is reducible, then \( \dim S_2(N)_m \geq \frac{h(-N)^{\text{even}} - 2}{2} \).
2. Suppose \( N \equiv 5 \mod 8 \).
   (a) If \( m \) is ordinary \( \mathbb{Q}(\sqrt{N}) \)-dihedral, then \( \dim S_2(N)_m \geq 4 \).
   (b) If \( m \) is \( \mathbb{Q}(\sqrt{-N}) \)-dihedral, then \( \dim S_2(N)_m \geq 2 \).
3. Suppose \( N \equiv 3 \mod 4 \) and \( K = \mathbb{Q}(\sqrt{\pm N}) \).
(a) If \( m \) is ordinary \( K \)-dihedral, then \( \dim S_2(N)_m \geq 2 \).

In the case that \( N \equiv 9 \mod 16 \), part (1c) has been proved by Calegari and Emerton [6, Theorem 1.1]: indeed, they establish that \( \dim S_2(N)_m = \frac{k(-N)^{even}-2}{2} \) for the unique reducible \( m \) in this case.

**Proposition 14.** Part (3) of Conjecture [12] is true when \( K = \mathbb{Q}(\sqrt{-N}) \).

**Proof.** If \( K = \mathbb{Q}(\sqrt{-N}) \), and \( N \equiv 3 \mod 4 \) is a prime, and \( \varepsilon = \varepsilon_K \), then there are exactly \( h(-N)^{-1} \) distinct \( K \)-dihedral forms in \( S_1(N,\varepsilon,\mathbb{C}) \) corresponding to inductions of characters \( \psi : \text{Gal}(H(K)/K) \to \mathbb{C}^\times \) (see, for example, [32] §8.1.I for details). Since \( h(-N) \) is odd, all of these reduce to distinct representations modulo 2, so that \( S_1(N,\varepsilon_K,\overline{\mathbb{F}}_2) \) is a direct sum of \( \frac{h(-N)}{2} \) non-isomorphic one-dimensional lines spanned by ordinary forms. The two maps \( S_1(\Gamma_1(N),\mathbb{F}_2) \to S_2(\Gamma_1(N),\mathbb{F}_2) \) given by \( f \to f^2 \) and \( f \to E_{1,\varepsilon,f} \) preserve Hecke eigenspaces (the former because we are in characteristic 2; the latter because \( E_{1,\varepsilon} \) in characteristic zero lifts the Hasse invariant: see user Electric Penguin’s answer to MathOverflow question 228497[viii]) and are linearly independent.

Since \( \varepsilon \) is quadratic, we obtain a Hecke equivariant embedding \( (S_1(N,\varepsilon,\overline{\mathbb{F}}_2)_{K\text{-dih}})^2 \to S_2(N,\overline{\mathbb{F}}_2) \) that doubles the eigenspace. \( \square \)

7. Comparison with experimental results

To conclude, we compare our results to the empirical assertions about the mod-2 reduction of \( T_2 \) acting on \( S_2(\Gamma_0(N),\mathbb{Q}) \) for \( N \) prime from the introduction.

- For \( N \equiv 3 \mod 8 \), the eigenvalue 0 always occurs if \( N > 3 \).
- For \( N \equiv 1,3,5 \mod 8 \), the eigenvalue 1 always occurs if \( N > 163 \).
- For \( N \equiv 1 \mod 8 \), the eigenvalue 0 occurs with probability 16.8%.
- For \( N \equiv 5 \mod 8 \), the eigenvalue 0 occurs with probability 42.2%.
- For \( N \equiv 7 \mod 8 \), the eigenvalue 0 occurs with probability 17.3%.
- For \( N \equiv 7 \mod 8 \), the eigenvalue 1 occurs with probability 47.9%.

Of these, the first assertion is implied by part (3) of Theorem [12] and the second assertion is implied by part (2) of Theorem [12]. Combining the other parts of Theorem [12] with the Cohen-Lenstra heuristics yields the following statements.

- For \( N \equiv 5 \mod 8 \), the eigenvalue 0 occurs for “dihedral reasons” when \( u(N) \equiv 1 \mod 2\mathcal{O}(N) \). The three possible nonzero reductions of \( u(N) \) mod \( 2\mathcal{O}(N) \) being equally likely, this should occur with probability \( \frac{1}{4} = 25% \).
- For \( N \equiv 7 \mod 8 \), the eigenvalue 1 occurs for “dihedral reasons” when \( h(N) > 1 \) or \( h(-N)^{odd,2\text{-split}} > 1 \). Each of these is modeled by the probability that a random finite abelian group, modulo the subgroup generated by a random element, yields a nontrivial quotient; this probability is

\[
1 - \prod_{p>2} \prod_{j=1}^{\infty} \left( 1 - \frac{1}{p^{j+1}} \right) = 0.2455 \ldots
\]

Since the two events are presumed to be independent, at least one should occur with probability 43.1%.

Removing these cases leaves the following occurrence of eigenvalues arising from exceptional or big-image maximal ideals.

[viii] https://mathoverflow.net/questions/228497
• For $N \equiv 1 \mod 8$, the eigenvalue 0 occurs with probability 16.8%.
• For $N \equiv 5 \mod 8$, the eigenvalue 0 occurs with probability 13.3%.
• For $N \equiv 7 \mod 8$, the eigenvalue 0 occurs with probability 17.3%.
• For $N \equiv 7 \mod 8$, the eigenvalue 1 occurs with probability 8.4%.

It would of course be desirable to explain these probabilities also. This will require combining some analysis of the corresponding representations with Wood’s non-abelian analogue of the Cohen-Lenstra heuristics [39], which for a given pair of finite groups $G, G'$ predicts the probability that a quadratic number field $K$ admits a Galois $G$-extension $L$ for which $L/Q$ is a Galois $G'$-extension.

For $N < 200000$ prime, we also checked whether Theorem 12 and Conjecture 13 together give a sharp lower bound on the eigenvalue multiplicities of 0 and 1. For each residue mod 8, the percentage of cases where this fails is shown in Table 2.

**Table 2.** Frequency of unexplained eigenvalue multiplicity in the mod-2 reduction of $T_2$ on $S_2(\Gamma_0(N), \mathbb{Q})$ for $N < 200000$ prime.

| $N \mod 8$ | excess multiplicity of 0 | excess multiplicity of 1 |
|------------|--------------------------|--------------------------|
| 1          | 16.4%                    | 43.8%                    |
| 3          | 53.0%                    | 45.7%                    |
| 5          | 22.5%                    | 45.8%                    |
| 7          | 17.3%                    | 39.0%                    |

Note that these percentages include both uncounted (exceptional or big-image) maximal ideals and non-sharpness in Conjecture 13. The preceding calculation suggests that excess multiplicity of 0 for $N \equiv 1, 7 \mod 8$ arises almost entirely from uncounted maximal ideals, but in other cases Conjecture 13 may need to be refined.

**References**

[1] G. Bard, *Algebraic Cryptanalysis*, Springer, Dordrecht, 2009.
[2] M. Bennett and A. Rechnitzer, Computing elliptic curves over $\mathbb{Q}$: bad reduction at one prime, in *Recent progress and modern challenges in applied mathematics, modeling and computational science*, Fields Inst. Commun., 79, Springer, New York, 2017, 387–415.
[3] B. Birch, Hecke actions on classes of ternary quadratic forms, *Computational number theory (Debrecen, 1989)*, de Gruyter, Berlin, 1991, 191–212.
[4] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* 14 (2001), 843–939.
[5] A. Brumer, The average rank of elliptic curves, I, *Invent. Math.* 109 (1992), 445–472.
[6] F. Calegari and M. Emerton, On the ramification of Hecke algebras at Eisenstein primes, *Invent. Math.* 160 (2005), 97–144.
[7] F. Calegari and M. Emerton, Elliptic curves of odd modular degree, *Israel J. Math.* 169 (2009), 417–444.
[8] H. Cohen and H.W. Lenstra, Jr., Heuristics on class groups, *Number theory (New York, 1982)*, Lecture Notes in Math. 1052, Springer, Berlin, 1984, 26–36.
[9] J.E. Cremona, *Algorithms for Modular Elliptic Curves*, second edition, Cambridge Univ. Press, 1997; [http://homepages.warwick.ac.uk/~masgaj/book/fulltext/index.html](http://homepages.warwick.ac.uk/~masgaj/book/fulltext/index.html)
[10] L. Dieulefait, Remarks on Serre’s modularity conjecture, *Manuscr. Math.* 139 (2012), 71–89.
[11] Bas Edixhoven, The weight in Serre’s conjecture on modular forms, *Invent. Math.* 109 (1992), 563–594.
[12] B. Edixhoven, Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one, *J. Inst. Math. Jussieu* 5 (2006), 1–34.
[13] The LMFDB Collaboration, *L-Functions and Modular Forms Database*, [http://www.lmfdb.org](http://www.lmfdb.org) (retrieved February 2018).
[14] T. Hadano, On the conductor of an elliptic curve with a rational point of order 2, *Nagoya Math. J.* 53 (1974), 199–210.
[15] J. Hein, Orthogonal modular forms: an application to a conjecture of Birch, algorithms and computations, PhD thesis, Dartmouth College, 2016.
[16] J. Hein, *git* repository [https://github.com/jefferyphein/ternary-birch](https://github.com/jefferyphein/ternary-birch) (retrieved February 2018).
[17] R. Hortsch, Counting elliptic curves of bounded Faltings height, *Acta Arith.* 173 (2016), 239–253.
[18] C. Khare and J.-P. Wintenberger, Serre’s modularity conjecture (I), *Invent. Math.* 178 (2009), 485–504.
[19] C. Khare and J.-P. Wintenberger, Serre’s modularity conjecture (II), *Invent. Math.* 178 (2009), 505–586.
[20] M. Kida, Ramification in the division fields of an elliptic curve, *Abh. Math. Sem. Univ. Hamburg* 73 (2003), 195–207.
[21] L.J.P. Kilford and G. Wiese, On the failure of the Gorenstein property for Hecke algebras of prime weight, *Exper. Math.* 17 (2008), 37–52.
[22] M. Kisin, Modularity of 2-adic Barsotti-Tate representations, *Invent. Math.* 178 (2009), 587–634.
[23] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHÉS* 47 (1977), 33–186.
[24] B. Mazur and J.-P. Serre, Points rationnels des courbes modulaires $X_0(N)$ (d’après A. Ogg), *Séminaire Bourbaki* (1974/1975), Exp. No. 408, Lecture Notes in Math. 514, Springer, Berlin, 1976, 238–255.
[25] J.-F. Mestre, La méthode des graphes. Exemples et applications, in *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields* (Katata, 1986), Nagoya Univ., Nagoya, 1986, 217–242.
[26] A. Ogg, Abelian curves of small conductor, *J. reine angew Math.* 226 (1967), 204–215.
[27] The PARI group, *PARI/GP* [http://pari.math.u-bordeaux.fr/](http://pari.math.u-bordeaux.fr/) version 2.9.4 (2017).
[28] H. Randriam, Hecke operators with odd determinant and binary frameproof codes beyond the probabilistic bound?, *2010 IEEE Information Theory Workshop* , Dublin, 2010, 1–5.
[29] D. Roberts, Newforms with rational coefficients, *Ramanujan J.* 38 (2016), 267–275.
[30] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\text{Gal}({\overline{\mathbb{Q}}}/{\mathbb{Q}})$, *Duke Math. J.* 54 (1987), 179–230.
[31] J.-P. Serre, Modular forms of weight one and Galois representations, *Algebraic Number Fields* (A. Fröhlich, ed.), Academic Press (1977), pp.193–268.
[32] J.-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972), 259–331.
[33] B. Setzer, Elliptic curves of prime conductor, *J. London Math. Soc.* 10 (1975), 367–378.
[34] W.A. Stein and M. Watkins, A database of elliptic curves-first report, *Algorithmic number theory* (Sydney, 2002), Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002, 267–275.
[35] Yuichiro Taguchi, Induction formula for the Artin conductors of mod $\ell$ Galois representations, *Proc. Amer. Math. Soc.* 130 (2002), 2865–2869.
[36] The University of Sydney Computational Algebra Group, *Magma* [http://magma.maths.usyd.edu.au/magma/](http://magma.maths.usyd.edu.au/magma/) version 2.23-8 (2018).
[37] J. Voight, Computing classical modular forms as orthogonal modular forms, *Lecture Notes in Comput. Sci.* 8540, Springer, Berlin, 2014, 267–275.
[38] M.M. Wood, Nonabelian Cohen-Lenstra moments, [arXiv:1702.04644v1](http://arxiv.org/abs/1702.04644v1) (2017).
[39] H. Yoo, On Eisenstein ideals and the cuspidal group of $J_0(N)$, *Israel J. Math.* 214 (2016), 359–377.

**Univ. of California, San Diego, 9500 Gilman Drive #0112, La Jolla, CA 92093 USA**

**E-mail address:** kedlaya@ucsd.edu

**URL:** [http://kskedlaya.org/](http://kskedlaya.org/)

**Department of Mathematics and Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215 USA**

**E-mail address:** medved@gmail.com