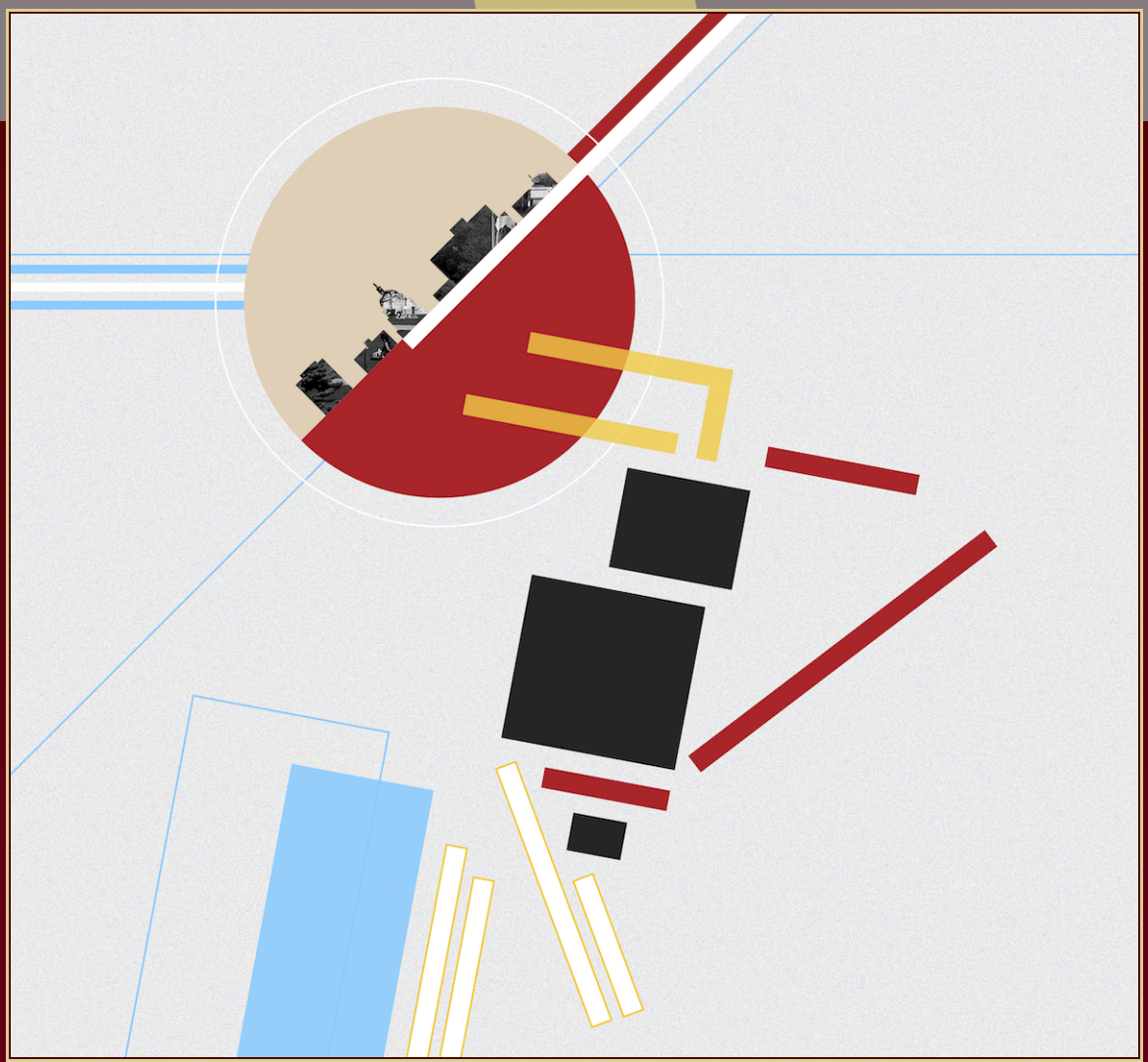
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

Mod-2 dihedral Galois representations of prime conductor

Kiran S. Kedlaya and Anna Medvedovsky



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.325

Mod-2 dihedral Galois representations of prime conductor

Kiran S. Kedlaya and Anna Medvedovsky

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

Kedlaya was supported by NSF (grant DMS-1501214) and UC San Diego (Warschawski Professorship). Medvedovsky was supported by an NSF postdoctoral research fellowship (grant DMS-1703834) and has gratefully enjoyed the hospitality of the Max Planck Institute for Mathematics during the writing of this paper.
MSC2010: 11F33.
Keywords: modular forms, mod 2 Galois representations, elliptic curves, conductor.

These results can be partially explained (see Section 7) by combining the Cohen–Lenstra heuristics [7] 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 [12], and Kida [18] 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].

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 ℓ; 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., [19]) 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 eigenforms 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 [8] and executed to date for $N \leq 400000$ [21]. (The table is also available in `PARI/GP` [27], Magma [25], and Sage [30].)

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 ℓ 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 ℓ, such as $\ell = 2$? Of course, one does not expect the result of computing the kernel of $T_p - a_p$ mod ℓ 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 [15], 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 ℓ, 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

$$\begin{aligned}&(\text{contribution from level } N \text{ newforms})\\ &\quad = (\text{eigenvalue multiplicity of } 0) - \sum_{d<N,\, d|N} \tau(N/d)(\text{contribution from level } d \text{ newforms}),\end{aligned}$$

where $\tau(n)$ is the number of divisors of n; an early abort occurs if this contribution modulo ℓ is zero.

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 [22] but remain largely mysterious for general N (but still tractable for squarefree N, as in the work of Yoo [39]). However, for N prime there is no need to optimize Cremona's method: the method used by Bennett and Rechnitzer [2] to extend the tables of Stein and 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 other situations: one could treat nonprime N, work modulo another prime ℓ, 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 and Sage, 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 Birch [3] as extended by Hein, Tornaría, and Voight [13] (see also [37]). Birch's original method is a variant of the Mestre–Oesterlé method of graphs [24] 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, and Voight generalize to higher weight by considering the action of SO(3) on nonstandard representations. Hein [14] 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.

The early abort strategy of computing ranks modulo ℓ is potentially even more effective when using the method of Birch, Hein, Tornaría, and Voight, 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.

2. Elliptic curves and their 2-torsion

For K a quadratic extension of $\mathbb{Q}$, write $\mathcal{O}_K$ for its ring of integers, $\mathrm{Cl}(K)$ for its class group, $h(K)$ for its class number, and $H(K)$ for its Hilbert class field. Write $\mathrm{Cl}(K, \mathfrak{a})$ for the ray class group of K with conductor $\mathfrak{a}$, and $h(K, \mathfrak{a})$ for the order of $\mathrm{Cl}(K, \mathfrak{a})$. Let $\mathfrak{p}(K)$ be a prime of K above (2), and write $\langle \mathfrak{p}(K) \rangle \subset \mathrm{Cl}(K)$ for the subgroup that $\mathfrak{p}(K)$ 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 $\overline{\rho}_{E,2} : G_{\mathbb{Q},2N_E} \to \mathrm{GL}_2(\mathbb{F}_2)$ 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 $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. By considering the subgroups of S_3 and their embeddings in $\mathrm{GL}_2(\mathbb{F}_2)$, we see that exactly one of the following alternatives holds.

(i) $E[2]$ 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.

(ii) $E[2]$ 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 nonidentity points of $E[2]$ cyclically.[2]

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

[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.

[2] This happens, for example, for both isogeny classes of elliptic curves of conductor 196 (lmfdb.org/EllipticCurve/Q/196/) and isogeny classes a and c of conductor 324 (lmfdb.org/EllipticCurve/Q/324/).

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 ℓ be an odd prime dividing N_E. Since ℓ divides N_E exactly once, E has multiplicative reduction at ℓ; 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 $\mathrm{GL}_2(\mathbb{F}_2)$ is $\left\{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)\right\}$, which acts irreducibly. Therefore the image of $G_{\mathbb{Q}_\ell}$ is trivial in $\mathrm{GL}_2(\mathbb{F}_2)$, and so K_E is unramified at ℓ. Since this is true for every odd ℓ 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 $\mathbb{Q}(\zeta_{2^\infty})$, whose Galois group is pro-2. □

In light of Proposition 1, when N_E is squarefree, we say that E is *reducible* if $E[2]$ is a reducible representation of $G_{\mathbb{Q}}$ and *K-dihedral*, or simply *dihedral*, if K_E is an S_3-extension containing a quadratic extension K of $\mathbb{Q}$.

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 11), E is ordinary at 2 if and only if $\overline{\rho}_{E,2}|_{G_{\mathbb{Q}_2}}$ 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.*

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

(ii) *Ordinary dihedral elliptic curves*: *For $K = \mathbb{Q}(\sqrt{\pm N})$, if*

$$3 \nmid \frac{h(K)}{\#\langle \mathfrak{p}(K)\rangle},$$

then there are no ordinary K-dihedral elliptic curves of conductor N.

(iii) *Supersingular elliptic curves*:

(a) *If $N \equiv 1, 7 \bmod 8$, then there are no supersingular elliptic curves of conductor N.*

(b) *If $N \equiv 3 \bmod 8$, then every supersingular elliptic curve of conductor N is $\mathbb{Q}(\sqrt{-N})$-dihedral.*

(c) *If $N \equiv 5 \bmod 8$, then every supersingular elliptic curve of conductor N is $\mathbb{Q}(\sqrt{N})$-dihedral. If $u(K) \not\equiv 1 \bmod 2\mathcal{O}_K$, then there are no supersingular elliptic curves of conductor N.*

(iv) *Reducible elliptic curves*: *If $N \not\equiv 1 \bmod 8$, then there are no reducible elliptic curves of conductor N.*

For prime N and $K = \mathbb{Q}(\sqrt{N})$, the order of $\mathfrak{p}(K)$ in $\mathrm{Cl}(K)$ divides 2 unless $N \equiv 1 \bmod 8$, so if $N \equiv 3, 5, 7 \bmod 8$ then the condition $3 \nmid (h(K)/\#\langle \mathfrak{p}(K)\rangle)$ in (ii) is equivalent to $3 \nmid h(K)$. Similarly, if $N \not\equiv 7 \bmod 8$ and $K = \mathbb{Q}(\sqrt{-N})$, then the condition $3 \nmid (h(K)/\#\langle \mathfrak{p}(K)\rangle)$ in (ii) 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 [12, Theorems II and III] and Kida [18, 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 [12, Theorem I].)

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

(i) *If $N \equiv 1, 7 \bmod 8$, then every elliptic curve of conductor $2N$ is reducible.*

(ii) *If $N \equiv 3, 5 \bmod 8$, there are no elliptic curves of conductor $2N$.*

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

$$h(\mathbb{Q}(\sqrt{\pm N})), \qquad h(\mathbb{Q}(\sqrt{(-1)^{(N-1)/2}N}), 2)$$

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 finite field $\mathbb{F}$ of characteristic p, let G be any group, and let $\rho : G \to \mathrm{GL}_2(\mathbb{F})$ be a semisimple representation. Let $\rho(G) \subset \mathrm{GL}_2(\mathbb{F})$ and $\widetilde{\rho(G)} \subset \mathrm{PGL}_2(\mathbb{F})$ be the image and projective image of ρ, respectively. Then exactly one of the following statements holds [31, Propositions 15–16].

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

(ii) Dihedral case: $\widetilde{\rho(G)}$ is a dihedral group D_n of order $2n$ with $n \geq 2$. In other words, ρ 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.

(iii) Exceptional case: $\widetilde{\rho(G)}$ is isomorphic to A_4, S_4, or A_5.

(iv) Big-image case: $\widetilde{\rho(G)}$ contains $\mathrm{PSL}_2(\mathbb{F}_q)$ for some $q \geq 5$, but $\rho(G) \neq \mathrm{SL}_2(\mathbb{F}_5)$.[3]

Call ρ *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 ψ factors though an abelian quotient of H, one can show that ${}^g\psi$ depends only on the class $\overline{g}$ of g in G/H. We therefore write ${}^{\overline{g}}\psi$ for the twist of ψ by $\overline{g} \in G/H$.

Now suppose that $H \subset G$ has index 2 and take ρ to be the induced representation $\mathrm{Ind}_H^G \psi : G \to \mathrm{GL}_2(F)$. Let ε_H be the (at most quadratic) character of G that takes H to 1 and $G-H$ to -1. Let $\overline{g}$ be the nontrivial element of G/H. The following are well known (e.g., see [32, 7.2.1]):

(i) $\rho|_H = \psi \oplus {}^{\overline{g}}\psi$;

[3] The restrictions are explained by exceptional isomorphisms for small primes: $\mathrm{SL}_2(\mathbb{F}_2) \cong D_3$, $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$, $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$, $\mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{PGL}_2(\mathbb{F}_4) \cong A_5$, and $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$.

(ii) ρ is an irreducible representation of G if and only if $\psi \neq {}^{\overline{g}}\psi$;

(iii) $\det \rho = \varepsilon_H \cdot \psi(\mathrm{Ver}_H^G)$, where $\mathrm{Ver}_H^G : G \to H^{\mathrm{ab}}$ is the *Verlagerung* (transfer) homomorphism taking $x \in G$ to $xg^{-1}xg$;[4]

(iv) $\widetilde{\rho(G)} \cong D_n$, where n is the order of ${}^{\overline{g}}\psi/\psi$ (assuming ψ has finite order).

3.1.2. *Dihedral representations.* Conversely, suppose that $\rho : G \to \mathrm{GL}_2(F)$ is a dihedral representation with $\widetilde{\rho(G)} = D_n$. If $n \geq 3$, then D_n contains a unique index-2 subgroup isomorphic to C_n.[5] Let $H \subset G$ be the inverse image of that cyclic subgroup under the map $G \to \mathrm{GL}_2(F) \to \mathrm{PGL}_2(F)$. Since $\widetilde{\rho(H)}$ 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 $\psi : H \to \overline{F}^\times$ be one of these characters. Then Frobenius reciprocity and dimension considerations guarantee that the map $\mathrm{Ind}_H^G \psi \to \rho$ induced by $\psi \to \rho|_H$ is an isomorphism.

3.1.3. *The image of a dihedral representation.* Suppose further that ρ is a faithful dihedral representation of G. With H, ψ, and ${}^{\overline{g}}\psi$ as above, we have the following:

Lemma 5. (i) $\ker \psi \cap \ker {}^{\overline{g}}\psi = 1$.

(ii) *H is an abelian subgroup of G.*

(iii) *If $\ker \psi \subset H$ is normal in G, then ψ is faithful, so H is cyclic.*

The proofs are straightforward but not completely standard, so we include them.

Proof. (i) We know that $\rho|_H = \psi \oplus {}^{\overline{g}}\psi$ and we have assumed that $\ker \rho$ is trivial.

(ii) The commutator of any two elements of H is in both $\ker \psi$ and $\ker {}^{\overline{g}}\psi$; now use part (i).

(iii) By part (ii), G/H acts on H by conjugation, and $\ker {}^{\overline{g}}\psi$ is the image of $\ker \psi$ under the action of the nontrivial element. Now use (i). □

Note that even if ψ 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 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ be a finite-image dihedral representation such that $|\widetilde{\rho(G_{\mathbb{Q}})}| \geq 6$. Let K be the quadratic extension of $\mathbb{Q}$ for which $[\widetilde{\rho(G_{\mathbb{Q}})} : \widetilde{\rho(G_K)}] = 2$, 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_ψ be the fixed field of $\ker \psi$. If $L_\psi/\mathbb{Q}$ is Galois, then $L_\psi = \ker \rho$. Otherwise, writing $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$, we obtain the twist ${}^{\sigma}\psi$; its fixed field $L_{\sigma\psi}$ is the image $\tilde{\sigma}(L_\psi) \subset \overline{\mathbb{Q}}$ for any lift $\tilde{\sigma}$ of σ to $G_{\mathbb{Q}}$, and $\ker \rho =: M$ is the compositum $L_\psi L_{\sigma\psi}$ (inside $\overline{\mathbb{Q}}$). In particular, it is clear that M is an abelian extension of K.

[4] One can show that $\psi(\mathrm{Ver}_H^G)$ takes $x \in H$ to $\psi\, {}^{\overline{g}}\psi(x)$ and takes $x \in G - H$ to $\psi(x^2)$.

[5] For $n = 2$, there are three such subgroups. But n is the order of a character to $\overline{\mathbb{F}}_p^\times$ (see Section 3.1.1(iv)) and hence prime to p; as we will later restrict to $p = 2$, we ignore $n = 2$ here.

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 $\mathrm{Ind}_K^{\mathbb{Q}}\,\psi$ in terms of the Artin conductor of ψ:

$$\mathrm{cond}(\mathrm{Ind}_K^{\mathbb{Q}}\,\psi) = |\Delta_K|\,\mathcal{N}_{\mathbb{Q}}^K(\mathrm{cond}\,\psi), \tag{3-1}$$

where $\mathcal{N}_{\mathbb{Q}}^K$ is the field norm and Δ_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 $\mathrm{cond}^{(p)}$. The analogous formula holds:

$$\mathrm{cond}^{(p)}(\mathrm{Ind}_K^{\mathbb{Q}}\,\psi) = |\Delta_K^{(p)}|\,\mathcal{N}_{\mathbb{Q}}^K(\mathrm{cond}^{(p)}\,\chi). \tag{3-2}$$

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 $\rho = \mathrm{Ind}_K^{\mathbb{Q}}\,\psi : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ 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* $\det\rho = 1$. Again, let L_ψ be the fixed field of $\ker\psi$.

Lemma 6. *If* $\det\rho = 1$, *then* L_ψ *is Galois over* $\mathbb{Q}$.

Proof. If $\det\rho = 1$, then considering $\det\rho$ on the subgroup G_K, we see that ${}^\sigma\psi = \psi^{-1}$. Therefore L_ψ is also the fixed field of $\ker {}^\sigma\psi$, which means that $L_\psi/\mathbb{Q}$ is Galois and L_ψ is the fixed field of $\ker\rho$. □

3.2.2. *The conductor of* ψ. Let $\mathfrak{a}$ be the conductor of ψ. Since we work in characteristic 2, we are only interested in odd-order ψ here; we thus ignore consideration of any real places of K and view $\mathfrak{a}$ as an integral ideal of K. We have a standard exact sequence relating the class group $\mathrm{Cl}(K)$ to the ray class group $\mathrm{Cl}(K,\mathfrak{a})$:

$$\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{a})^\times \to \mathrm{Cl}(K,\mathfrak{a}) \to \mathrm{Cl}(K) \to 1. \tag{3-3}$$

Lemma 7. *If* $\mathfrak{a} = \mathfrak{q}^n$ *is a power of a prime of* $\mathcal{O}_K$ *lying over a prime* q *of* $\mathbb{Z}$, *then*

$$[\mathrm{Cl}(K,\mathfrak{a}) : \mathrm{Cl}(K)] \text{ divides } \begin{cases} (q-1)q^k \text{ for some } k \geq 0 & \text{if } (q) \text{ splits or ramifies in } K, \\ (q^2-1)q^k \text{ for some } k \geq 0 & \text{if } (q) \text{ is inert in } K. \end{cases}$$

Proof. This is immediate from sequence (3-3) in light of the exact sequence

$$1 \to 1 + \mathfrak{q}^n\mathcal{O}_K \to 1 + \mathfrak{q}\mathcal{O}_K \to (\mathcal{O}_K/\mathfrak{q}^n)^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{q})^\times \to 1, \tag{3-4}$$

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

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

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

Proof. (i) 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 $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, then argue as in Lemma 7, noting that by the Chinese remainder theorem, $(\mathcal{O}_K/(2\mathcal{O}_K)^n)^\times = (\mathcal{O}_K/\mathfrak{p}^n)^\times \times (\mathcal{O}_K/\mathfrak{p}'^n)^\times$.

N mod 8	$K=\mathbb{Q}(\sqrt{N})$			$K=\mathbb{Q}(\sqrt{-N})$		
	(2) in K	$h(K)$	$\#\langle\mathfrak{p}(K)\rangle$	(2) in K	$h(K)$	$\#\langle\mathfrak{p}(K)\rangle$
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

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

(ii) From the proof of Lemma 7 and (3-4), it's clear that the only odd contribution to $[\mathrm{Cl}(K,(2)^n):\mathrm{Cl}(K)]$ comes at $n=1$. □

3.2.3. *The local behavior of* ρ. Fixing an embedding $\iota: G_{\mathbb{Q}_2}\hookrightarrow G_{\mathbb{Q}}$, we can consider the restriction ρ_2 of ρ to $G_{\mathbb{Q}_2}$. Let $\mathfrak{p}$ be the prime of $\mathcal{O}_K$ above 2 corresponding to ι, and let ψ_2 be the restriction of ψ to $G_{K_\mathfrak{p}}$. Then ρ_2 is reducible if and only if either

(i) 2 splits in K, or

(ii) 2 is inert or ramified in K and ${}^\sigma\psi_2=\psi_2$. (Note that σ is in the decomposition group at $\mathfrak{p}$ 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 ρ has (tame Artin) conductor N. The induced tame conductor formula (3-2) guarantees that either

$$\Delta_K^{(2)}=(1),\quad \mathcal{N}_{\mathbb{Q}}^K(\mathrm{cond}^{(2)}\,\psi)=(N)\qquad\text{or}\qquad \Delta_K^{(2)}=(N),\quad \mathcal{N}_{\mathbb{Q}}^K(\mathrm{cond}^{(2)}\,\psi)=(1).$$

We analyze each scenario in turn.

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

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

Proof. Since $\mathrm{cond}\,\psi$ is not Galois-invariant, L_ψ is not Galois over $\mathbb{Q}$. Lemma 6 then implies the desired conclusion. □

3.3.2. *Second scenario*: $\Delta_K^{(2)}=(N)$ *and* $\mathcal{N}_{\mathbb{Q}}^K(\mathrm{cond}^{(2)}\,\psi)=(1)$. Here, $K=\mathbb{Q}(\sqrt{\pm N})$ or $\mathbb{Q}(\sqrt{\pm 2N})$ and ψ is a ray class character of conductor dividing $(2\mathcal{O}_K)^n$.

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

- $N\equiv 5 \bmod 8$ *and* $K=\mathbb{Q}(\sqrt{N})$ *or*
- $N\equiv 3 \bmod 8$ *and* $K=\mathbb{Q}(\sqrt{-N})$,

in which cases ψ *factors through* $\mathrm{Cl}(K,(2))$.

Proof. Combine Corollary 8 with the ramification of 2 in $\mathbb{Q}(\sqrt{\pm N})$: see Table 1. □

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

Fixing a prime of $\overline{\mathbb{Q}}$ above 2, we consider the corresponding decomposition group of $G_{\mathbb{Q}}$, which one can identify with the absolute Galois group $G_{\mathbb{Q}_2} = \mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ 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.*

(i) *$\rho_{f,2}$ is reducible, in which case f is ordinary, and*

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

where $\lambda : G_{\mathbb{Q}_2} \to \overline{\mathbb{F}}_2^\times$ is the unramified character sending Frob_2 to $\bar{a}_2(f)$.
Moreover $\rho_{f,2}$ is at most peu wildly ramified in the sense of Serre.[6]

(ii) *$\rho_{f,2}$ is irreducible, in which case f is supersingular. In this case, $\rho_{f,2}$ is the induction of a character of $G_{\mathbb{Q}_4}$ (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 [10, Theorems 2.5 and 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 $\overline{\mathbb{Z}}_p$ (the p-torsion of a certain abelian variety of GL_2-type), forcing $\rho_{f,p}$ to be at most peu wildly ramified [10, Proposition 8.2]. In the supersingular case, $\rho_{f,2}$ is at most tamely ramified, by [31, Proposition 4]; for the description of $\rho_{f,p}$ as the induction of the second fundamental character of $G_{\mathbb{Q}_{p^2}}$, see [33, §2.2]. □

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.

[6] An extension $M/\mathbb{Q}_p$ is *at most peu wildly ramified* if $M = M^{\mathrm{tr}}(\alpha_1^{1/p}, \ldots, \alpha_d^{1/p})$, where $M^{\mathrm{tr}}/\mathbb{Q}_p$ is the at most tamely ramified subextension of M, and the α_i can be taken to be units in M^{tr}. If M is still an elementary p-extension of M^{tr} but at least one of the α_i must be a nonunit, then M is *très wildly ramified*. See [33, 2.4.ii]. A representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ as usual inherits the ramification properties of the fixed field of its kernel.

For N an odd squarefree positive integer, we study the distribution of generalized T_2-eigenvalues on $S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)^{\text{new}}$. Write $m(N)$ for the dimension of this space. For $\alpha \in \overline{\mathbb{F}}_2$, 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 α). 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 $S_2(N) := S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)^{\text{new}}$ and let $\mathbb{T}_2(N) := \mathbb{T}_2(N, \overline{\mathbb{F}}_2)^{\text{new}}$ be the shallow Hecke algebra acting on $S_2(N)$. In other words, $\mathbb{T}_2(N)$ is the (commutative) $\overline{\mathbb{F}}_2$-algebra generated inside $\text{End}_{\overline{\mathbb{F}}_2}(S_2(N))$ by the action of all the Hecke operators T_n with n prime to $2N$. Then $\mathbb{T}_2(N)$ is a semilocal artinian ring whose maximal ideals $\mathfrak{m}$ correspond to mod-2 Hecke eigensystems appearing in $S_2(N)$. For ℓ prime to $2N$, let $a_\ell(\mathfrak{m}) \in \overline{\mathbb{F}}_2$ be the T_ℓ-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 (that is, Serre's conjecture [33], now known by work of Khare and Wintenberger [16; 17], Kisin [20], and Dieulefait [9]), the maximal ideals $\mathfrak{m}$ also correspond to semisimple Galois representations $\rho_\mathfrak{m} : G_{\mathbb{Q},2N} \to \text{SL}_2(\overline{\mathbb{F}}_2)$ 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 11 implies that, given $\mathfrak{m}$, one can determine whether $a_2(\mathfrak{m})$ is 0 or 1; otherwise $a_2(\mathfrak{m})$ is only defined up to inverse.[7]

We decompose $\mathbb{T}_2(N)$ as a product of localizations at its maximal ideals, and correspondingly decompose $S_2(N)$ into generalized $\mathfrak{m}$-eigenspaces $S_2(N)_\mathfrak{m}$:

$$\mathbb{T}_2(N) = \prod_\mathfrak{m} \mathbb{T}_2(N)_\mathfrak{m}, \qquad S_2(N) = \bigoplus_\mathfrak{m} S_2(N)_\mathfrak{m}.$$

Note that if $\mathfrak{m} \subset \mathbb{T}_2(N)$ is a maximal ideal, then the eigenspace $S_2(N)[\mathfrak{m}]$ is nonzero, so that the dimension of the generalized eigenspace $S_2(N)_\mathfrak{m}$ is at least 1.

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

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

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

(i) *If $\mathfrak{m}$ is dihedral, then it is either $\mathbb{Q}(\sqrt{N})$-dihedral or $\mathbb{Q}(\sqrt{-N})$-dihedral.*

(ii) *Ordinary dihedrals: For $K = \mathbb{Q}(\sqrt{\pm N})$, there are exactly $\frac{1}{2}(h(K)^{\text{odd}} - 1)$ ordinary K-dihedral maximal ideals in $\mathbb{T}_2(N)$. Of these, $\frac{1}{2}(h(K)^{\text{odd,2-split}} - 1)$ have $a_2(\mathfrak{m}) = 1$.*

[7] Note that $a_2(\mathfrak{m})$ 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 $a_2(\mathfrak{m})$ is not a priori determined by $\mathfrak{m}$. In fact, $a_2(\mathfrak{m})$ 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.

(iii) *Supersingular dihedrals*:
   (a) *If* $\mathfrak{m}$ *is supersingular* K*-dihedral, then either* $N \equiv 3 \bmod 8$ *and* $K = \mathbb{Q}(\sqrt{-N})$, *or* $N \equiv 5 \bmod 8$ *and* $K = \mathbb{Q}(\sqrt{N})$.
   (b) *Let* $N \equiv 3 \bmod 8$ *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* $N \equiv 5 \bmod 8$ *and* $K = \mathbb{Q}(\sqrt{N})$. *If* $u(K) \equiv 1 \bmod 2\mathcal{O}_K$, *then there are* $h(K)$ *supersingular maximal ideals of* $\mathbb{T}_2(N)$; *otherwise, there are none.*

(iv) *Reducibles*: *If* $N \equiv 1 \bmod 8$, *then there is one reducible maximal ideal of* $\mathbb{T}_2(N)$, *generated by* T_ℓ *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 $N \equiv 1 \bmod 4$. Note also that a prime $\mathfrak{p}$ above 2 of $K = \mathbb{Q}(\sqrt{\pm N})$ has order 1 or 2 in the class group unless $N \equiv \varepsilon \bmod 8$ 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 part (i).*** 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 ρ_f factors through an extension of $\mathbb{Q}$ unramified outside of 2 and N, K must be one of the following:

$$\mathbb{Q}(\sqrt{N}), \quad \mathbb{Q}(\sqrt{-N}), \quad \mathbb{Q}(\sqrt{-1}), \quad \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{-2}), \quad \mathbb{Q}(\sqrt{2N}), \quad \mathbb{Q}(\sqrt{-2N}).$$

If $K = \mathbb{Q}(\sqrt{\pm 2})$ or $\mathbb{Q}(\sqrt{\pm 2N})$, then K is très wildly ramified at 2 [33, §2.6, Exemple], so no modular form of weight 2 (and in particular no elliptic curve) can be K-dihedral (Theorem 11). If $K = \mathbb{Q}(\sqrt{-1})$, then we are in the first scenario of Section 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 part (ii).*** Suppose $K = \mathbb{Q}(\sqrt{\pm N})$ and $f \in S_2(N)$ is a K-dihedral ordinary form, with $\rho = \rho_f = \mathrm{Ind}_K^{\mathbb{Q}} \psi$ for some character ψ of G_K ramified only at primes above 2 (Section 3.3.2). Write $H = H(K)$ and $\mathfrak{p} = \mathfrak{p}(K)$. 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 $\mathfrak{p}$, and write ψ_2 for the restriction of ψ to $\mathrm{Gal}(L_{\mathcal{P}}/K_{\mathfrak{p}})$.

We first show that ψ is in fact unramified at 2, and hence will factor through H^{odd}, the maximal odd-degree subextension of H. By Corollary 10 and Table 1, ψ is unramified in all cases except possibly when 2 is inert in K. In that case, $\rho_{f,2} = \mathrm{Ind}_{K_{\mathfrak{p}}}^{\mathbb{Q}_2} \psi_2$, so by 3.1.1(ii) we know that $\psi_2 = {}^{\sigma_2}\psi_2$ for σ_2 a generator of $\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_2)$. In this case, Theorem 11(i) tells us that ψ_2 is unramified above 2, as then is ψ. 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(i), the condition $a_2(f) = 1$ is equivalent to the condition $\psi_2 = 1$, which exactly means that ψ 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(ii), we observe that $[H^{\text{odd,2-split}} : K] = h(K)^{\text{odd}}/\#\langle\mathfrak{p}\rangle$. If ρ comes from a K-dihedral elliptic curve, then it has image D_3, so ψ must have order 3. So a K-dihedral elliptic curve of conductor N is only possible if 3 divides $h(K)^{\text{odd}}/\#\langle\mathfrak{p}\rangle$, or equivalently $h(K)/\#\langle\mathfrak{p}\rangle$.

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

5.3. ***Proof of part*** **(iii).** Suppose that $K = \mathbb{Q}(\sqrt{\pm N})$ and that $f \in S_2(N)$ is a K-dihedral form with $\rho = \rho_f = \text{Ind}_K^{\mathbb{Q}}\,\psi$ for some character ψ of G_K ramified only at primes above 2. Maintain the notation H, $\mathfrak{p}$, σ, ρ_2 as above. As in the second paragraph of Section 5.2, ψ does not factor through H (or else ρ_2 would be reducible, contradicting Theorem 11). Therefore ψ 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 $N \equiv 3 \bmod 8$ and $K = \mathbb{Q}(\sqrt{-N})$, or $N \equiv 5 \bmod 8$ 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 $\frac{1}{2}(h(K, (2)) - h(K))$ representations, and hence maximal ideals of $\mathbb{T}_2(N)$.

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

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

for ω 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 (3-3) 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 $N = 3$, 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 $\mathcal{O}_K = \{\pm 1\} \times u^{\mathbb{Z}}$ for some fundamental unit $u = u(K)$, and therefore we similarly have the two cases

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

5.4. ***Proof of part*** **(iv).** If $N \not\equiv 1 \bmod 8$, then 2 is not an Eisenstein prime for N (see Mazur [22] or Mazur and Serre [23]), so there are no cuspforms in $S_2(N, \overline{\mathbb{Z}})$ congruent to the Eisenstein series $E_{2,N}$ modulo 2, which carries the unique reducible maximal ideal in squarefree level. In particular, there are no rational newforms whose associated mod-2 Galois representation is reducible.

This completes the proof of Theorem 2 and Theorem 12.

5.5. ***Proof of Theorem 4.*** By Theorem 12(ii), the condition $3 \nmid h(\mathbb{Q}(\sqrt{\pm N}))$ 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(iii), $K = \mathbb{Q}(\sqrt{(-1)^{(N-1)/2}N})$ and ψ is a nontrivial order-3 character of $H(K, (2))$; this is ruled out by assuming that $3 \nmid h(K, (2))$. This completes the proof of Theorem 4.

5.6. ***Proof of Theorem 3.*** We now change notation to address Theorem 3. Let N be a prime such that $3 \nmid h(K)$ for $K = \mathbb{Q}(\sqrt{\pm N})$, $\mathbb{Q}(\sqrt{\pm 2N})$, and let E be an elliptic curve of conductor $2N$. Let $f \in S_2(2N)$ be the corresponding modular form and let $\mathfrak{m} \subseteq \mathbb{T}_2(2N)$ be the corresponding maximal ideal. Since E has multiplicative reduction at 2, f is ordinary and the conclusion of Theorem 11(i) holds. By Proposition 1, $\mathfrak{m}$ is either reducible or ordinary dihedral.

In the reducible case, $\mathfrak{m}$ is an Eisenstein ideal; by the proof of [39, 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 [39, Theorem 1.3] this order is the numerator of $(N^2 - 1)/8$, forcing $N \equiv 1, 7 \bmod 8$.

In the ordinary dihedral case, by Lemma 9 we must be in the second scenario of Section 3.3; that is, $\rho_f = \mathrm{Ind}_K^{\mathbb{Q}} \psi$ where K is one of $\mathbb{Q}(\sqrt{\pm N})$ or $\mathbb{Q}(\sqrt{\pm 2N})$ and ψ is an order-3 character of G_K ramified only at primes above 2. As in Section 5.2, we see that ψ is also unramified at 2 and so factors through $\mathrm{Cl}(K)$; however, this contradicts the hypothesis that $3 \nmid h(K)$.

This completes the proof of Theorem 3.

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

The following conjecture[8] complements Theorem 12. Note that the fact that $\mathfrak{m} \subset \mathbb{T}_2(N)$ is a maximal ideal automatically implies that $\dim S_2(N)_{\mathfrak{m}} \geq 1$.

Conjecture 13. *Let N be an odd prime and $\mathfrak{m}$ a maximal ideal of $\mathbb{T}_2(N)$.*

(i) *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* $\dim S_2(N)_{\mathfrak{m}} \geq h(-N)^{\mathrm{even}}$.
  (c) *If $\mathfrak{m}$ is reducible, then* $\dim S_2(N)_{\mathfrak{m}} \geq \frac{1}{2}(h(-N)^{\mathrm{even}} - 2)$.

(ii) *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* $\dim S_2(N)_{\mathfrak{m}} \geq 2$.

(iii) *Suppose $N \equiv 3 \bmod 4$ and $K = \mathbb{Q}(\sqrt{\pm N})$.*
  (a) *If $\mathfrak{m}$ is ordinary K-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 2$.

In the case that $N \equiv 9 \bmod 16$, part (i c) has been proved by Calegari and Emerton [6, Theorem 1.1]: indeed, they establish that $\dim S_2(N)_{\mathfrak{m}} = \frac{1}{2}(h(\mathbb{Q}(\sqrt{-N}))^{\mathrm{even}} - 2)$ for the unique reducible $\mathfrak{m}$ in this case.

Proposition 14. *Part (iii) of Conjecture 13 is true when $K = \mathbb{Q}(\sqrt{-N})$.*

[8] Added in proof: Frank Calegari reports that some progress towards these conjectures has been made by Noah Taylor.

Proof. If $K = \mathbb{Q}(\sqrt{-N})$, and $N \equiv 3 \bmod 4$ is a prime, and $\varepsilon = \varepsilon_K$, there are exactly $\frac{1}{2}(h(K)-1)$ distinct K-dihedral forms in $S_1(N, \varepsilon, \mathbb{C})$ corresponding to inductions of characters $\psi : \mathrm{Gal}(H(K)/K) \to \mathbb{C}^\times$ (see, for example, [32, §8.1.I] for details). Since $h(K)$ is odd, all of these reduce to distinct representations modulo 2, so that $S_1(N, \varepsilon_K, \overline{\mathbb{F}}_2)^{K\text{-dih}}$ splits as a Hecke module into a direct sum of $\frac{1}{2}(h(K)-1)$ nonisomorphic one-dimensional lines spanned by ordinary forms. The two maps $S_1(\Gamma_1(N), \mathbb{F}_2) \hookrightarrow S_2(\Gamma_1(N), \mathbb{F}_2)$ given by $f \mapsto f^2$ and $f \mapsto E_{1,\varepsilon} f$ preserve Hecke eigenspaces (the former because we are in characteristic 2; the latter because $E_{1,\varepsilon}$ in characteristic zero lifts the Hasse invariant[9]) and are linearly independent [11, Proposition 4.4]. Since ε is quadratic, we obtain a Hecke equivariant embedding $(S_1(N, \varepsilon, \overline{\mathbb{F}}_2)^{K\text{-dih}})^2 \hookrightarrow S_2(N, \overline{\mathbb{F}}_2)$ that doubles the eigenspace. □

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

Of these, the first assertion is implied by part (iii b) of Theorem 12 and the second assertion is implied by part (ii) of Theorem 12. Combining the other parts of Theorem 12 with the Cohen–Lenstra heuristics yields the following statements.

- For $N \equiv 5 \bmod 8$, the eigenvalue 0 occurs for "dihedral reasons" when $u(N) \equiv 1 \bmod 2\mathcal{O}(N)$. The three possible nonzero reductions of $u(N) \bmod 2\mathcal{O}(N)$ being equally likely, this should occur with probability $\frac{1}{3} = 33.3\%$.
- For $N \equiv 7 \bmod 8$, the eigenvalue 1 occurs for "dihedral reasons" when $h(\mathbb{Q}(\sqrt{-N}))^{\text{odd,2-split}} > 1$ or $h(\mathbb{Q}(\sqrt{N})) > 1$. 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%.

[9] See user Electric Penguin's answer to MathOverflow question 228497.

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%

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.

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

- For $N \equiv 1 \bmod 8$, the eigenvalue 0 occurs with probability 16.8%.
- For $N \equiv 5 \bmod 8$, the eigenvalue 0 occurs with probability 13.3%.
- For $N \equiv 7 \bmod 8$, the eigenvalue 0 occurs with probability 17.3%.
- For $N \equiv 7 \bmod 8$, 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 nonabelian analog of the Cohen–Lenstra heuristics [38], 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 $L/\mathbb{Q}$ 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.

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

Acknowledgments

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

References

[1] Gregory V. Bard, *Algebraic cryptanalysis*, Springer, 2009. MR 2838791

[2] Michael A. Bennett and Andrew Rechnitzer, *Computing elliptic curves over* $\mathbb{Q}$*: Bad reduction at one prime*, Recent progress and modern challenges in applied mathematics, modeling and computational science, Fields Inst. Commun., no. 79, Springer, 2017, pp. 387–415. MR 3700057

[3] B. J. Birch, *Hecke actions on classes of ternary quadratic forms*, Computational number theory, de Gruyter, Berlin, 1991, pp. 191–212. MR 1151865

[4] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* **Q***: Wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939. MR 1839918

[5] Armand Brumer, *The average rank of elliptic curves, I*, Invent. Math. **109** (1992), no. 3, 445–472. MR 1176198

[6] Frank Calegari and Matthew Emerton, *On the ramification of Hecke algebras at Eisenstein primes*, Invent. Math. **160** (2005), no. 1, 97–144. MR 2129709

[7] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups*, Number theory, Lecture Notes in Math., no. 1052, Springer, 1984, pp. 26–36. MR 750661

[8] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997. MR 1628193

[9] Luis Dieulefait, *Remarks on Serre's modularity conjecture*, Manuscripta Math. **139** (2012), no. 1-2, 71–89. MR 2959671

[10] Bas Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594. MR 1176206

[11] ———, *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), no. 1, 1–34. MR 2195943

[12] Toshihiro Hadano, *On the conductor of an elliptic curve with a rational point of order 2*, Nagoya Math. J. **53** (1974), 199–210. MR 0354673

[13] Jeffery Hein, *Orthogonal modular forms*: *An application to a conjecture of Birch, algorithms and computations*, Ph.D. thesis, Dartmouth College, Ann Arbor, MI, 2016, p. 169. MR 3553638

[14] Jeffrey Hein, *ternary-birch*, git repository, retrieved February 2018.

[15] Ruthi Hortsch, *Counting elliptic curves of bounded Faltings height*, Acta Arith. **173** (2016), no. 3, 239–253. MR 3512854

[16] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture, I*, Invent. Math. **178** (2009), no. 3, 485–504. MR 2551763

[17] ———, *Serre's modularity conjecture, II*, Invent. Math. **178** (2009), no. 3, 505–586. MR 2551764

[18] M. Kida, *Ramification in the division fields of an elliptic curve*, Abh. Math. Sem. Univ. Hamburg **73** (2003), 195–207. MR 2028514

[19] L. J. P. Kilford and Gabor Wiese, *On the failure of the Gorenstein property for Hecke algebras of prime weight*, Experiment. Math. **17** (2008), no. 1, 37–52. MR 2410114

[20] Mark Kisin, *Modularity of 2-adic Barsotti–Tate representations*, Invent. Math. **178** (2009), no. 3, 587–634. MR 2551765

[21] The LMFDB Collaboration, *The L-functions and modular forms database*, electronic reference, retrieved February 2018.

[22] Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186. MR 488287

[23] Barry Mazur and Jean-Pierre Serre, *Points rationnels des courbes modulaires $X_0(N)$ (d'après A. Ogg)*, Séminaire Bourbaki (1974/1975), Lecture Notes in Math., no. 514, Springer, 1976, [exposé] 469, pp. 238–255. MR 0485882

[24] J.-F. Mestre, *La méthode des graphes*: *Exemples et applications*, Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields (Nagoya), Nagoya Univ., 1986, pp. 217–242. MR 891898

[25] The University of Sydney Computational Algebra Group, *Magma*, 2018, version 2.23-8.

[26] A. P. Ogg, *Abelian curves of small conductor*, J. Reine Angew. Math. **226** (1967), 204–215. MR 0210706

[27] PARI group, *PARI/GP*, 2017, version 2.9.4.

[28] H. Randriam, *Hecke operators with odd determinant and binary frameproof codes beyond the probabilistic bound?*, IEEE Information Theory Workshop, 2010.

[29] David P. Roberts, *Newforms with rational coefficients*, Ramanujan J. **46** (2018), no. 3, 835–862. MR 3826758

[30] The Sage Development Team, *SageMath, the Sage Mathematics Software System*, 2017, version 8.1.

[31] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR 0387283

[32] ———, *Modular forms of weight one and Galois representations*, Algebraic number fields: L-functions and Galois properties (London), Academic Press, 1977, pp. 193–268. MR 0450201

[33] ———, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230. MR 885783

[34] Bennett Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. **10** (1975), 367–378. MR 0371904

[35] William A. Stein and Mark Watkins, *A database of elliptic curves—first report*, Algorithmic number theory, Lecture Notes in Comput. Sci., no. 2369, Springer, 2002, pp. 267–275. MR 2041090

[36] Yuichiro Taguchi, *Induction formula for the Artin conductors of mod l Galois representations*, Proc. Amer. Math. Soc. **130** (2002), no. 10, 2865–2869. MR 1908909

[37] J. Voight, *Computing classical modular forms as orthogonal modular forms*, lecture notes.

[38] Melanie Matchett Wood, *Nonabelian Cohen–Lenstra moments*, preprint, 2017. arXiv 1702.04644v1

[39] Hwajong Yoo, *On Eisenstein ideals and the cuspidal group of $J_0(N)$*, Israel J. Math. **214** (2016), no. 1, 359–377. MR 3540618

Received 2 Mar 2018. Revised 26 Aug 2018.

KIRAN S. KEDLAYA: kedlaya@ucsd.edu
Department of Mathematics, University of California, San Diego, La Jolla, CA, United States

ANNA MEDVEDOVSKY: medved@gmail.com
Department of Mathematics and Statistics, Boston University, Boston, MA, United States

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine