THE UNIVERSITY OF CHICAGO

LIFTS OF MODULAR FORMS COMING FROM MOD 2 GALOIS REPRESENTATIONS

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY
NOAH TAYLOR

CHICAGO, ILLINOIS
JUNE 2021

To my parents.

"There are five elementary arithmetical operations: addition, subtraction, multiplication, division, and... modular forms."

Martin Eichler (Apocryphal)

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGMENTS

This thesis wouldn't have been possible without a whole host of supportive people. First and foremost, I would like to thank my advisor Frank Calegari for all his patience and helpfulness when I would set myself deadlines and then inevitably break them. He has imparted so much knowledge to me, both through our meetings and through his classes, that I wouldn't be here without him. Additionally, I'd like to thank Matt Emerton for being a great secondary advisor, giving me important feedback and thoughts on my papers, and providing Number Theory lunch with great conversation.

I would like to thank all my friends here in Chicago who have helped make grad school a great time: Ronno Das for his shirts and his interest in all mathematics, no matter how atypical; Dylan Quintana for taking the role as my doppelgänger seriously and for providing useful board game stress release nights; Eric Stubley for always being available to bounce ideas off of; Karl Schaefer for his softball, REU, and teaching leadership; Tim Black for sticking around in Chicago long enough to watch your favorite class graduate, as well as sharing my interest in Groundhog Day; Ben O'Connor for being a great friend from my first year of undergrad through Knots and Graphs, Ross, and office mates here in Chicago; Nat Mayer and Isabella Scott for enjoyable movie nights and for walking home with me when others lived too far away; and Mariya Sardarli and Alan Chang for keeping with the "Crossword Crew" tradition which made me wake up on time more than I should mention. I'd like to thank Weinan Lin, Shuo Pang and Bingjin Liu for being great roommates and philosophical discussion partners for a majority of my time in Chicago. I'd also like

to thank the Histones for providing me an outlet once a week to hang out and sing with people who aren't in the math department.

I would like to thank my family: my parents Doug Taylor and Jill Schellhase, my brothers Adam Taylor and Andy Taylor and my sisters-in-law Lizzie Taylor and Anne McAlister, and my sister Anna Taylor. Even if y'all haven't understood any of the math I'm doing, the smiles and head-nodding have been appreciated, as well as the support, banter and jokes in our text conversations.

I would also like to thank the contingent of Jacob's Porch friends: Chris Tavenor, Kim Tavenor, Brian Timm, Ethan Sprunger, Amanda Martin, Danny Darvish, Dana Martin, Carolyn May, Michael Behrendt, and the rest of the Porchites who made my undergrad years fun and make my trips back to Columbus more exciting.

Finally, I would like to thank all the professors and math teachers that have helped me along the way: Kirk Keller, Melissa Balko, Mike Ouimet, Trisha Cores, Sasha Leibman, Vitaly Bergelson, Warren Sinnott, Sergei Chmutov, Dan Shapiro, Jim Fowler, and Kazuya Kato.

ABSTRACT

This thesis is made up of 3 separate pieces of work in two themes. In the first half, we prove a few cases of the Sato-Tate conjecture, which says that for an abelian surface A over a totally real field F, the Frobenius elements Frob_λ acting on the ℓ-adic Tate module (or more precisely its dual) can be formed into a compatible system of elements over all ℓ, viewed (up to twist) as lying in a compact subgroup of $\mathrm{GL}_4(\mathbb{C})$, and have traces that are equidistributed according to the smallest such compact subgroup possible. To do so, we use a result of [1] which proves automorphy of certain ℓ-adic representations, and in another case we construct a new decomposition of the ℓ-adic Tate module representation as a tensor product of a finite-image representation and a 2-dimensional representation easily handled by earlier methods. Then we consider the final remaining cases and prove some partial results on the distribution of the traces of the Frobenii, and conversely explain precisely why we can't say any more without further automorphy theorems.

In the latter half of this thesis, we consider the question of how the odd-power coefficients of a modular form control the even-power coefficients in the space of modular forms of weight 2 level $\Gamma_0(N)$ with N prime, from two different angles. We first study a question of Kedlaya and Medvedovsky about the number of modular lifts of a mod 2 dihedral representation, and give lower bounds for the number of such lifts depending on N mod 8 and whether the representation is totally real. We use multiple different methods to construct lifts: in some cases, we are able to use the connectedness of the real points of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ to double the dimension; in other cases, we are able to use the class group of

the fixed field of the representation to manually construct weight 1 forms that can be multiplied by a lift of the Hasse Invariant to give weight 2 forms of the correct level and Nebentypus.

We then prove that the difference between the anemic Hecke algebra that excludes T_2 and the full Hecke algebra including T_2 is exactly described by the space of Katz forms in characteristic 2, weight 1 and level $\Gamma_0(N)$. We prove first that the difference is encompassed in the space of mod 2 forms with only even-power terms, which then arise from weight 1 forms by squaring. We then prove that there are no weight 2 level $\Gamma_0(N)$ Katz forms, so every form arising from weight 1 is a classical form, completing the bijection between the Katz forms in weight 1 and the weight 2 forms with only even-power monomials, and hence with the quotient $\mathbb{T}/\mathbb{T}^{\mathrm{an}}$. Finally, we end with questions about the proportion of primes N for which $\mathbb{T}$ of level N is equal to $\mathbb{T}^{\mathrm{an}}$; if $N \equiv 3 \bmod 4$ there are only finitely many examples, but for $N \equiv 1 \bmod 4$ we observe that it's probable there are a positive proportion of such primes.

This thesis is a compilation of three papers: [39], [38] and [40]. They have been lightly edited to eliminate redundant or internal citations, and some irrelevant asides have been removed, but otherwise they remain intact. In particular, notation is introduced at the start of each chapter that corresponds to that particular chapter's usage; while it has mostly been synchronized, in case of discrepancy we shall refer to the specific notations of the chapter.

CHAPTER 1

SATO-TATE DISTRIBUTIONS ON ABELIAN SURFACES

1.1 Introduction

Let C be a genus g curve over a number field F. Given a prime v of F, with residue field $\mathbb{F}_v$ of size q_v, a theorem of Hasse says that the number N_v of $\mathbb{F}_v$ points on C is between $q_v + 1 - 2g\sqrt{q_v}$ and $q_v + 1 + 2g\sqrt{q_v}$, so that

$$a_v := \frac{q_v + 1 - N_v}{\sqrt{q_v}} \in [-2g, 2g].$$

The Sato-Tate conjecture asks for the distribution of the a_v in $[-2g, 2g]$ as $q_v \to \infty$, and predicts that they are equidistributed (after passing to a finite extension F'/F) with respect to a measure depending on the Mumford-Tate group of the Jacobian of C. For example, if E is an elliptic curve with CM, the distribution is given either by the pushforward of the Haar measure of SO(2) or of O(2) under the trace map. It has also been proven in [19] and [5] that if F is totally real and E does not have CM, then the distribution is the pushforward of the Haar measure of SU(2).

We look at genus $g = 2$ curves and 2-dimensional abelian surfaces. In complete analogy with the elliptic curve case, [15] describes 52 possible subgroups of USp(4) whose pushforwards describe the normalized point counts a_v for a genus 2 curve, and notes that it is likely possible to prove the Sato-Tate conjecture in many cases with a similar method to that of the elliptic curve case. [20] uses the powerful potential automorphy theorem of [4] to prove the conjecture for all but five of the non-generic cases that occur over totally real fields. In this paper we will use a more powerful potential automorphy theorem of [1] to extend the proof in [20], and then we extend [20]'s work to prove the conjecture for four other subgroups. Of course, given the Jacobian $J(C)$ of a genus 2 curve C, we can obtain the numbers a_v directly from $J(C)$, by taking the normalized trace of the action of Frob_v, so we may forget about the curve C entirely and work directly with abelian surfaces.

The theorems we prove are as follows:

Theorem 1.3.4. *If A/F is an abelian surface, F a totally real field, which has a two-dimensional real endomorphism ring defined over a quadratic extension of F which is either totally real or CM, then the Sato-Tate conjecture holds for A.*

Theorem 1.3.6. *If A/F is a (not necessarily simple) abelian surface, F a totally real field, which has quaternionic multiplication defined over a dihedral extension, then the Sato-Tate conjecture holds for A.*

These two theorems are equidistribution results, so we know the exact distributions of the a_v. However, we cannot currently prove the Sato-Tate conjecture for A if the endomorphism ring of A is $\mathbb{Z}$, or if the quadratic extension described in Theorem 1.3.4 is neither totally real or CM. In these cases, we prove lesser results:

Theorem 1.4.1. *If A/F is an abelian surface, F a totally real field, then for any $\varepsilon > 0$, $a_v < -\dfrac{2}{3} + \varepsilon$ for a positive proportion of primes v, and $a_v > \dfrac{2}{3} - \varepsilon$ for a positive proportion of primes v.*

Theorem 1.4.3. *If A/F is an abelian surface over a totally real field which has a two-dimensional real endomorphism ring defined over a quadratic extension of F,* *then $a_v < -2.47$ for a positive proportion of primes and $a_v > 2.47$ for a positive proportion of primes.*

The paper is divided as follows: In section 1.2, we set up the terminology and state the Sato-Tate conjecture precisely. Section 1.3 is devoted to proving Theorems 1.3.4 and 1.3.6 above, and the goal of section 1.4 is to prove the asymptotics in Theorems 1.4.1 and 1.4.3, as well as others in Theorems 1.4.2 and 1.4.4.

1.2 Setup

1.2.1 The Conjecture

To set up the Sato-Tate conjecture, we follow [15, Section 2]. Fix a number field F, an embedding into $\overline{\mathbb{Q}}$, and an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$. Let A be an abelian variety of dimension 2 over F. We choose a polarization of A. Given a prime ℓ, this allows the identification of the ℓ-adic Tate module with the etale and singular homologies

$$V_\ell(A) \simeq H_{1,\mathrm{et}}(A_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell) \simeq H_{1,\mathrm{et}}(A_{\mathbb{C}}, \mathbb{Q}_\ell) \simeq H_1(A_{\mathbb{C}}^{\mathrm{top}}, \mathbb{Q}_\ell) \simeq H_1(A_{\mathbb{C}}^{\mathrm{top}}, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

The Weil pairing on the dual of the Tate module $\widehat{V_\ell(A)}$ corresponds to the cup product pairing on the cohomologies, so it is a nondegenerate alternating pairing and, given a symplectic basis of $\widehat{V_\ell(A)}$, induces a continuous map $\rho_{A,\ell} : G_F \to \mathrm{GSp}_4(\overline{\mathbb{Q}_\ell})$. We let G_ℓ be the image of this map, and G_ℓ^{Zar} be the Zariski closure in $\mathrm{GSp}_4(\overline{\mathbb{Q}_\ell})$. Then we let G_F^1 be the kernel of the cyclotomic character $\chi_\ell : G_F \to \mathbb{Z}_\ell^\times$, so that $g \in G_F^1$ acts trivially on the Weil pairing. Then G_ℓ^1 is the image of G_F^1 under

$\rho_{A,\ell}$ and $G_\ell^{1,\mathrm{Zar}}$ is the Zariski closure. Because G_F^1 acts trivially on the Weil pairing, reconsidering it as a pairing on the vector space, $G_\ell^{1,\mathrm{Zar}}$ is the kernel of the similitude character

$$\psi : G_\ell^{\mathrm{Zar}} \to \mathbb{Z}_\ell^\times, \langle hv, hw\rangle = \psi(h)\langle v, w\rangle.$$

Fix an isomorphism $\iota : \overline{\mathbb{Q}_\ell} \to \mathbb{C}$ for this ℓ. We then define $G = G_\ell^{\mathrm{Zar}} \otimes_{\overline{\mathbb{Q}_\ell}} \mathbb{C}$ and $G^1 = G_\ell^{1,\mathrm{Zar}} \otimes_{\overline{\mathbb{Q}_\ell}} \mathbb{C}$; then $G/G^1 \simeq \mathbb{C}$ via the similitude character. We look at the image of Frob_v in this quotient for v a prime of F with residue field $\mathbb{F}_{q_v}$. Certainly $\mathrm{Frob}_v(\zeta_{\ell^n}) = \zeta_{\ell^n}^{q_v}$ so Frob_v maps to q_v. An argument of Deligne, summarized in [33, Section 8.3.2], shows that the center of the original GSp(4) lies in the center of G, so we may divide $\rho_{A,\ell}(\mathrm{Frob}_v)$ by $q_v^{\frac{1}{2}}$ to get an element g_v in G^1 whose eigenvalues have norm 1 because of the Weil conjectures.

Definition 1.2.1. The Sato-Tate group ST_A of A is a maximal compact Lie subgroup of G^1 inside USp(4), which depends on ℓ and the embedding ι.

The element g_v has eigenvalues of norm 1 so its semisimple component (and even itself, because as described in the errata to [15], g_v is already semisimple) lies in some conjugate of ST_A; we let $s(v)$ denote its conjugacy class. The Sato-Tate conjecture is as follows:

Conjecture 1.2.2. *The elements $s(v)$ are equidistributed among the conjugacy classes of ST_A, under the pushforward of the Haar measure from ST_A.*

We record that the Sato-Tate group has a common model over $\mathbb{Q}$ over all ℓ, as in [15, Theorem 2.16], but it's not known whether the conjugacy classes $s(v)$ themselves are independent of ℓ.

1.2.2 Proof strategy

Suppose S is the set of primes outside of which $\rho_{A,\ell}$ is unramified. The general idea for proof is laid out in [32]; therein the following theorem is shown.

Theorem 1.2.3. *Suppose that, for any irreducible representation r of ST_A, the L-function*

$$L^S(r,s) = \prod_{v \notin S} \frac{1}{\det(1 - r(s(v))q_v^{-s})}$$

has a meromorphic extension to the half-plane $Re(s) \geq 1$, with no poles or zeroes except possibly at $s = 1$. Then the elements $s(v)$ are equidistributed in the conjugacy classes of ST_A if and only if the L-functions $L^S(r,s)$ for irreducible nontrivial r have no zero or pole at $s = 1$.

We denote the property of having no zeroes or poles on a region invertibility. The L-function has factors at primes of S as well, but their factors do not add poles or zeroes so we ignore them. To show invertibility of these L-functions, the only known method is to equate them to L-functions of automorphic forms, a la [41], [19]. [20] covers most cases using [4, Theorem 5.4.1]; we introduce a new more widely applicable theorem of [1]. We refer to [4, Section 5.1] for the definition of a weakly compatible system.

Definition 1.2.4. A weakly compatible system of representations of G_F is a 5-tuple $(M, S, \{Q_v(x)\}, \{r_\lambda\}, \{H_\tau\})$ with S a finite set of F-primes satisfying

- M is a number field, and $\{r_\lambda : G_f \to \mathrm{GL}_n(\overline{M}_\lambda)\}$ is a set of representations of G_F indexed over the primes λ of M. If $v \notin S$ is a prime of F, then for λ not over the same rational prime p as v, r_λ is unramified at v.

- The polynomials $Q_v(x)$ have rational coefficients and the characteristic polynomial of $r_\lambda(\mathrm{Frob}_v)$ is equal to $Q_v(x)$, independent of λ.

- If v and λ are over the same rational prime p, then r_λ is de Rham at v; furthermore, if $v \notin S$, then r_λ is crystalline at v.

- For each embedding $\tau : F \hookrightarrow \overline{M}$, the Hodge-Tate weights of r_λ are given by the multiset H_τ, and are in fact independent of λ.

Theorem 1.2.5 ([1, Corollary 7.1.11])**.** *Suppose that F is a CM field and that the 5-tuple $\mathcal{R} = (M, S, \{Q_v(x)\}, \{r_\lambda\}, \{H_\tau\})$ is a rank 2 weakly compatible system of l-adic representations of G_F such that $H_\tau = \{0, 1\}$ for all τ and such that $\mathcal{R}$ is strongly irreducible. If m is a nonnegative integer, then there exists a finite CM extension F_m/F with $F_m/\mathbb{Q}$ Galois such that the weakly compatible system $Symm^m\mathcal{R}|_{G_{F_m}}$ is automorphic.*

We recall that a strongly irreducible system is one where each representation is irreducible even after restricting to finite-index subgroups of G_F.

Remark 1.2.6. The difference between this theorem and [4, Theorem 5.4.1] that we take advantage of is that [4, Theorem 5.4.1] requires all towers to be either CM or totally real. In contrast, [1, Corollary 7.1.11] allows us to base-change from our totally real field F to a CM field F', find an extension F_m over which the compatible system $\mathrm{Symm}^m\mathcal{R}|_{G_{F_m}}$ is automorphic, and be allowed the added condition that F_m/F is Galois. This is not possible with the theorem of [4]; in asking that F_m/F be Galois, we are only allowed base-change to totally real F'.

1.3 Sato-Tate for certain ST_A

We introduce the cases of the Sato-Tate conjecture we will prove. Let A be an abelian surface defined over a field F. If L is the smallest field over which all endomorphisms of A are defined, we define the Galois type of A to be the pair $(\mathrm{End}_L(A) \otimes \mathbb{R}, \mathrm{Gal}(L/F))$ of a real algebra and a group with an action on the algebra. [15, Theorem 4.3] proves that there is a correspondence between the Sato-Tate group and the Galois type of an abelian surface with the following property: if the type (E, G) corresponds to the Sato-Tate group K, then the algebra E corresponds bijectively to the identity component K_0 of K, and G is isomorphic to the component group K/K_0.

Therefore, we can equivalently divide the conjecture into cases indexed by the connected component of the Sato-Tate group or by the endomorphism algebra $\mathrm{End}_L(A) \otimes \mathbb{R}$, which can then be further subdivided by including the component group. There are 6 possible endomorphism algebras laid out in [15, Theorem 4.3] listed below, along with the corresponding Sato-Tate connected component and its embedding into USp(4):

- **A**: $\mathrm{End}_L(A) \otimes \mathbb{R} = \mathbb{R}$, corresponding to $ST_A^0 = \mathrm{USp}(4)$
- **B**: $\mathrm{End}_L(A) \otimes \mathbb{R} = \mathbb{R} \times \mathbb{R}$, corresponding to $ST_A^0 = \mathrm{SU}(2) \times \mathrm{SU}(2)$ via $M_1 \times M_2 \to \left(\begin{smallmatrix} M_1 & 0 \\ 0 & M_2 \end{smallmatrix}\right)$.
- **C**: $\mathrm{End}_L(A) \otimes \mathbb{R} = \mathbb{R} \times \mathbb{C}$, corresponding to $ST_A^0 = \mathrm{SU}(2) \times \mathrm{U}(1)$ via $M \times z \to \left(\begin{smallmatrix} M & & \\ & z & \\ & & \overline{z} \end{smallmatrix}\right)$

- **D**: $\mathrm{End}_L(A) \otimes \mathbb{R} = \mathbb{C} \times \mathbb{C}$, corresponding to $ST_A^0 = \mathrm{U}(1) \times \mathrm{U}(1)$ via $z \times w \to \begin{pmatrix} z & & & \\ & \overline{z} & & \\ & & w & \\ & & & \overline{w} \end{pmatrix}$
- **E**: $\mathrm{End}_L(A) \otimes \mathbb{R} = M_2(\mathbb{R})$, corresponding to $ST_A^0 = \mathrm{SU}(2)$ via $M \to \begin{pmatrix} M & 0 \\ 0 & \overline{M} \end{pmatrix}$
- **F**: $\mathrm{End}_L(A) \otimes \mathbb{R} = M_2(\mathbb{C})$, corresponding to $ST_A^0 = \mathrm{U}(1)$ via $z \to \begin{pmatrix} z \cdot I_2 & 0 \\ 0 & \overline{z} \cdot I_2 \end{pmatrix}$

Further subdividing this list, we obtain 52 distinct Galois types, corresponding to 52 distinct Sato-Tate groups. Of these, 35 arise as the Sato-Tate group of an abelian surface defined over a totally real field, and 34 of those arise from an abelian surface defined over $\mathbb{Q}$. Almost nothing is known about the single group of type **A**; in [20], the Sato-Tate conjecture was fully proven for all groups of types **D** and **F**, for all totally real abelian surfaces giving rise to groups of type **C**, and for all totally real abelian surfaces giving rise to one of two groups of type **B** and six of ten groups of type **E**. In addition, assuming that L was also totally real, all other cases were proven. We describe the remaining cases and prove them with a weakened hypothesis on L.

1.3.1 Preliminaries

Before we discuss specific Sato-Tate groups, let us recall standard facts about Galois representations coming from the abelian varieties we study.

Definition 1.3.1. Suppose A is an abelian variety defined over F. We say A is of GL_2-type if it is isogenous over F to a product $A_1 \times A_2 \times \ldots A_k$ of simple abelian varieties, each also defined over F, and with a field $K_i \hookrightarrow \mathrm{End}_F(A_i) \otimes \mathbb{Q}$ with $[K_i : \mathbb{Q}] = \dim(A_i)$.

Given a simple abelian surface A/F of GL_2-type with field K and a rational prime ℓ, the dual of the ℓ-adic Tate module T_ℓ gives rise to an ℓ-adic Galois representation $G_F \to \mathrm{GL}_4(\mathbb{Q}_\ell)$, isomorphic to the ℓ-adic etale cohomology of A. The image lands in $\mathrm{GL}_2(\mathbb{Q}_\ell \otimes K)$. For each embedding $\lambda : K \to \overline{\mathbb{Q}_\ell}$, we get a map from this image to $\mathrm{GL}_2(K_\lambda)$ for K_λ the completion of K at λ. Thus for each embedding of K into $\overline{\mathbb{Q}_\ell}$ for each ℓ we obtain a representation $\rho_{A,\lambda} : G_F \to \mathrm{GL}_2(K_\lambda)$. These form a weakly compatible system $(\rho_{A,\lambda})_\lambda$.

Theorem 1.3.2 ([30, Theorems 3.1, 3.2])**.** *The weakly compatible system $(\rho_{A,\lambda})_\lambda$ is regular of Hodge-Tate weights 0 and 1, totally odd and pure of weight 1. If K is a real quadratic field, then $\det \rho_{A,\lambda} = \chi_\ell$, the ℓ-adic cyclotomic character; if K is imaginary quadratic, then $\det \rho_{A,\lambda} = \epsilon \otimes \chi_\ell$ for some finite-image character ϵ independent of ℓ.*

In each case below, we will consider the irreducible representations of the Sato-Tate group. We will extend these in a natural way to representations of G^1. These will be algebraic representations of G^1, so that we get compatible systems of representations of $G_\ell^{1,\mathrm{Zar}}$. We can then obtain representations of G_ℓ^{Zar} by extending to the central $\mathbb{G}_m$. Finally obtaining this, we get a compatible system of representations of the Galois group G_F, and we can thus use Theorem 1.2.5 above, combined with Rankin-Selberg theory, to show that the original L-function is invertible, as required. This method will be detailed further in the subsections below.

1.3.2 $\boldsymbol{B}[C_2]$

When we discuss $\mathbf{B}[C_2]$, the Sato-Tate group is $\langle \mathrm{SU}(2) \times \mathrm{SU}(2), J\rangle$ where $J = \begin{pmatrix} & & & 1 \\ & & \text{-1} & \\ & \text{-1} & & \\ 1 & & & \end{pmatrix}$. This corresponds to either the case where A is isogenous to a direct sum of nonisogenous elliptic curves, each without CM, or when A is simple but has multiplication by a real quadratic field. In these cases, $\mathbb{Q} \otimes \mathrm{End}_{\overline{\mathbb{Q}}}(A)$ is either $\mathbb{Q} \times \mathbb{Q}$ or real quadratic. Conjecture 1.2.2 in the first case has been proven as [18, Theorem 5.4] assuming a few "Expected Theorems". These have been proven since the writing of the paper; see [5] for a discussion. We henceforth assume $\mathbb{Q} \otimes \mathrm{End}_{\overline{\mathbb{Q}}}(A) = K$ is a real quadratic field. Because we're in the $\mathbf{B}[C_2]$ case, A is not of GL_2 type over F, but is of GL_2 type over a quadratic extension.

We look first at representations of $ST_A^0 = \mathrm{SU}(2) \times \mathrm{SU}(2)$ which is an index 2 subgroup of ST_A. The irreducible representations of SU(2) are $\mathrm{Sym}^k(St)$ for St the standard 2-dimensional representation and $k \geq 0$; hence the irreducible representations of $\mathrm{SU}(2) \times \mathrm{SU}(2)$ are $r_{k,l} = \mathrm{Sym}^k(St) \otimes \mathrm{Sym}^l(St)$ for $k, l \geq 0$. We deduce the representations of ST_A using the following standard theorem of Clifford theory (in this form found as [20, Lemma 23], the proof being the author's own):

Theorem 1.3.3. *If $H \leq G$ is an index 2 subgroup, and r is a finite-dimensional irreducible representation of H, then r extends to a representation of G if and only if r is isomorphic to r^x, where r^x is the representation of H defined as $r^x(h) = r(xhx^{-1})$ for $x \in G\backslash H$. If this is the case, then r extends to exactly two nonisomorphic irreducible representations r_0 and $r_0 \otimes \chi$ for χ the nontrivial character $G/H \to \{\pm 1\}$. The irreducible representations are exactly those arising from such r, along with the inductions $\mathrm{Ind}_H^G \rho$ of all representations ρ of H that do not satisfy the above property.*

Proof. Suppose $r \simeq r^x$. This means that there is some endomorphism U with $r^x(h) = Ur(h)U^{-1}$ for each $h \in H$; we can clearly set $r_0(x) = U$ and $r_0(h) = r(h)$, giving a representation of G. Conversely, if r extends to r_0, $r_0(x)r(h)r_0(x)^{-1} = r^x(h)$ shows that $r \simeq r^x$. If these two conditions hold, Frobenius Reciprocity shows that there can be at most two distinct representations that restrict to r on H, and we have found two already, r_0 and $r_0 \otimes \chi$.

Now given any irreducible representation s of G, either $s|_H$ is irreducible or not. If so we're in the case above; if not, say s_1 is a subrepresentation of $s|_H$. Then by the universal property of Ind, since we have an H-equivariant map from s_1 into s, there must be a G-equivariant map $\mathrm{Ind}_H^G s_1 \to s$; by Schur's lemma and counting dimensions, we must have $\mathrm{Ind}_H^G s_1 = s$. □

We apply this theorem with $G = ST_A = \langle \mathrm{SU}(2) \times \mathrm{SU}(2), J \rangle$ and $H = \mathrm{SU}(2) \times \mathrm{SU}(2)$. Given the representation $r_{k,l}$ we choose $x = J$ and find that

$$J(A, B)J^{-1} = (-J_0BJ_0, -J_0AJ_0) = (J_0BJ_0^{-1}, J_0AJ_0^{-1}) = (J_0, J_0)(B, A)(J_0, J_0)^{-1}$$

where $J_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ so that $J = \begin{pmatrix} 0 & J_0 \\ -J_0 & 0 \end{pmatrix}$. Because $\begin{pmatrix} J_0 & 0 \\ 0 & J_0 \end{pmatrix} \in \mathrm{SU}(2) \times \mathrm{SU}(2)$, we find that $r_{k,l}^J \simeq r_{l,k}$. The representations $r_{k,l}$ are nonisomorphic for distinct pairs (k, l) so the representation $r_{k,l}$ extends only for $k = l$, say to r_k^1 and r_k^2; otherwise we obtain only the induced representation, which makes no distinction between (k,l) and (l,k). Hence all irreducible representations of ST_A are

$$r_k^1 \text{ and } r_k^2 \text{ for } k \geq 0 \text{ and } \mathrm{Ind}_{ST_A^0}^{ST_A} r_{k,l} \text{ for } k > l \geq 0.$$

As discussed above and by [15, Proposition 2.17], because ST_A has two components, the field L over which all endomorphisms are defined, $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathrm{End}_L(A)$, is a quadratic extension of F, and ST_{A_L}, the Sato-Tate group of A as a variety over L, is just the identity connected component $ST_A^0 = \mathrm{SU}(2) \times \mathrm{SU}(2)$ of ST_A.

Theorem 1.3.4. *If L is either a totally real field or a CM field, then Conjecture 1.2.2 is true for A over F.*

Proof. If L is a totally real field, this was proven already in [20, Proposition 24], so suppose L is a CM field; we proceed in a similar fashion. We must show that for each representation given above, the L-function in Theorem 1.2.3 is invertible at 1. Let us first look at a representation $\mathrm{Ind}_{ST_A^0}^{ST_A} r_{k,l}$. It follows from a theorem of Artin that if $s'(v')$ denotes the normalized image of Frobenius for prime v' in G_L, then

$$\begin{aligned} L^S(\mathrm{Ind}_{ST_A^0}^{ST_A} r_{k,l}, s) &= \prod_{v \notin S} \frac{1}{\det(1 - \mathrm{Ind}_{ST_A^0}^{ST_A} r_{k,l}(s(v)) q_v^{-s})} \\ &= \prod_{v' \notin S'} \frac{1}{\det(1 - r_{k,l}(s'(v')) q_{v'}^{-s})} \\ &= L^{S'}(r_{k,l}, s) \end{aligned}$$

so that we may prove invertibility of this new L-function.

From here, we cease mention of F and work solely with L. Let us extend $r_{k,l}$ from a representation of $\mathrm{SU}(2) \times \mathrm{SU}(2)$ to a representation $R_{k,l}$ of $G(L)$, the algebraic group coming from G_L instead of G_F; we naturally do this by restricting $\mathrm{Sym}^k(St) \otimes \mathrm{Sym}^l(St)$ from $\mathrm{GL}(2) \times \mathrm{GL}(2)$ to $G(L)$. In fact, we get a representation of $G_\ell^{\mathrm{Zar}}(L) \subseteq \mathrm{GL}_2(\overline{\mathbb{Q}_\ell}) \times \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$, which we can also call $R_{k,l}$. Thus finally we get a representation of G_L, namely $R_{k,l} \circ \rho_{A_L,\ell}$. Looking at where $\mathrm{Frob}_{v'}$ is sent, the L-function is

$$\begin{aligned} L^{S'}(r_{k,l}, s) &= L^{S'}(R_{k,l} \circ \rho_{A_L,\ell}, s + (k+l)/2) \\ &= \prod_{v' \notin S'} \det(1 - R_{k,l} \circ \rho_{A_L,\ell}(\mathrm{Frob}_{v'}) q_{v'}^{-(s+(k+l)/2)})^{-1}. \end{aligned}$$

As discussed before the statement of Theorem 1.3.2, the two embeddings λ_1, λ_2 of $K = \mathrm{End}_L^0(A)$ into $\overline{\mathbb{Q}_\ell}$ give the decomposition of $\rho_{A_L,\ell}$ into $\rho_{A_L,\lambda_1} \oplus \rho_{A_L,\lambda_2}$, and these give the further decomposition of the L-function into

$$L^{S'}(\mathrm{Sym}^k(\rho_{A_L,\lambda_1}) \otimes \mathrm{Sym}^l(\rho_{A_L,\lambda_2}), s + (k+l)/2);$$

this is finally what we must prove to be holomorphic and invertible.

We look at the weakly compatible system $(\rho_{A_L,\lambda})_\lambda$. The Hodge-Tate weights of these are all 0 and 1. Since the image of $\rho_{A_L,\lambda}$ is open in $G_\lambda^{\mathrm{Zar}} = \mathrm{GL}_2(\overline{\mathbb{Q}_p})$, there is no subgroup of G_L for which $\rho_{A_L,\lambda}$ becomes reducible. So we may apply Theorem 1.2.5 to get some CM field L'_m over which the compatible system $(\mathrm{Sym}^m(\rho_{A_L,\lambda}))_\lambda$ is automorphic.

The theory of cyclic base change in [2] shows that $(\mathrm{Sym}^m(\rho_{A_L,\lambda}))_\lambda$ is automorphic over all E where L'_m/E is cyclic, and hence solvable; we can apply the Rankin-Selberg method as in the proof of [18, Theorem 5.3] to the field $L' = L'_k L'_l$, over which the two compatible systems $(\mathrm{Sym}^k(\rho_{A_L,\lambda}))_\lambda$ and $(\mathrm{Sym}^l(\rho_{A_L,\lambda}))_\lambda$ are both automorphic, to show that

$$L^{S'}(\mathrm{Sym}^k(\rho_{A_L,\lambda_1}|_{G_E}) \otimes \mathrm{Sym}^l(\rho_{A_L,\lambda_2}|_{G_E}), s + (k+l)/2)$$

is invertible along the central line, assuming that the representations $\mathrm{Sym}^k(\rho_{A_L,\lambda_1}|_{G_E})$ and $\mathrm{Sym}^l(\rho_{A_L,\lambda_2}|_{G_E})$ are not dual. But $k \neq l$, so a dimension count shows that they cannot be dual. So

$$L^{S'}(\mathrm{Sym}^k(\rho_{A_L,\lambda_1}|_{G_E}) \otimes \mathrm{Sym}^l(\rho_{A_L,\lambda_2}|_{G_E}), s + (k+l)/2)$$

is invertible for all E solvable subfields of L'; Brauer's theorem applies to the Galois groups $\mathrm{Gal}(L'/E) \subseteq \mathrm{Gal}(L'/L)$, and we get that the L-function for the representation over L is an integer power combination of those over E, and therefore is also invertible.

Next, we look at the representations r_k^i for $i = 1, 2$ and $k \geq 1$. Recall that they are the two distinct extensions of $\mathrm{Sym}^k \otimes \mathrm{Sym}^k$ to representations of $N(\mathrm{SU}(2) \times \mathrm{SU}(2)) = \langle \mathrm{SU}(2) \times \mathrm{SU}(2), J \rangle$. As before, let us extend r_k^i to an algebraic representation of $G \subseteq \langle \mathrm{GL}(2) \times \mathrm{GL}(2), J \rangle$ by restricting $\mathrm{Sym}^k \otimes \mathrm{Sym}^k$ and leaving the image of J alone. This again gives us a representation R_k^i of G_ℓ^{Zar}, and then composing with $\rho_{A,\ell}$ finally gives us a Galois representation. The L-function attached to r_k^i is

$$L^S(r_k^i, s) = \prod_{v \notin S} \frac{1}{\det(1 - r_k^i(s(v)) q_v^{-s})} = \prod_{v \notin S} \frac{1}{\det(1 - R_k^i \circ \rho_{A,\ell}(\mathrm{Frob}_v) q_v^{-(s+k)})}.$$

This L-function being invertible follows if the L-functions for $R_k^i \circ \rho_{A,\ell}|_{G_E}$ for L'/E solvable are, where $L' = L'_k$ is the field from Theorem 1.2.5. For a given E, either $L \subseteq E$ or $L \not\subseteq E$. If $L \subseteq E$, then $R_k^i \circ \rho_{A,\ell}|_{G_E} = \mathrm{Sym}^k(\rho_{A,\lambda_1}|_{G_E}) \otimes \mathrm{Sym}^k(\rho_{A,\lambda_2}|_{G_E})$ as before. Then we can apply Rankin-Selberg, except dimension count doesn't work. We want

$$\begin{aligned}&L(\mathrm{Sym}^k(\rho_{A,\lambda_1}|_{G_E}) \otimes \mathrm{Sym}^k(\rho_{A,\lambda_2}|_{G_E}), s+k)\\ =&L(\mathrm{Sym}^k(\rho_{A,\lambda_1}|_{G_E}) \otimes \mathrm{Sym}^k(\rho_{A,\lambda_2}|_{G_E}) \otimes \chi_\ell^{-k}, s)\end{aligned}$$

to be invertible, so we require that $\mathrm{Sym}^k(\rho_{A,\lambda_1}|_{G_E})$ and $\mathrm{Sym}^k(\rho_{A,\lambda_2}|_{G_E}) \otimes \chi_\ell^{-k}$ not be dual. But $\rho_{A,\lambda_1}|_{G_E}$ is essentially self-dual via the Weil pairing; in fact, $\rho_{A,\lambda_1}|_{G_E} \simeq \rho^\vee_{A,\lambda_1}|_{G_E} \otimes \chi_\ell$. Therefore, we require that $\mathrm{Sym}^k(\rho_{A,\lambda_2}|_{G_E}) \otimes \chi_\ell^{-k}$ not be isomorphic to $\mathrm{Sym}^k(\rho_{A,\lambda_1}|_{G_E}) \otimes \chi_\ell^{-k}$. But if this happened, then $\rho_{A,\lambda_2}|_{G_{E'}} \simeq \rho_{A,\lambda_1}|_{G_{E'}}$ for some finite extension E'. This contradicts the fact that $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = K$, so we're done in this case.

Otherwise, $L \not\subseteq E$, and E is therefore a totally real subfield of L'. But if $L = F(\sqrt{\alpha})$, then let $E' = E(\sqrt{\alpha})$ to get a degree 2 CM extension containing L. $(\mathrm{Sym}^k(\rho_{A,\lambda}|_{G_{E'}}))_\lambda$ is cuspidal automorphic as before, and the L-function of the G_E representation is just the Asai L-function of the associated automorphic representation of this system, in the terminology of [17]. By [17, Theorem 4.3], this Asai L-function is nonzero and holomorphic on the right half-plane, if the automorphic representation is not self-dual. In fact, it's always nonzero, so it's holomorphic for both r_k^1 and r_k^2 if and only if the product of the two Asai L-functions is holomorphic.

But the product is

$$L(r_k^1|_{G_E}, s)L(r_k^2|_{G_E}, s) = L(\mathrm{Sym}^k(\rho_{A,\lambda_1}|_{G_{E'}}) \otimes \mathrm{Sym}^k(\rho_{A,\lambda_2}|_{G_{E'}}), s+k),$$

which as before is holomorphic. So each of these two Asai L-functions is holomorphic.

Finally, we look at the nontrivial finite representation r_0^2. This takes J to -1 and the connected component of the identity ST_A^0 to 1. But the L-function is

$$\prod_{v \notin S} \frac{1}{1 - \chi(\mathrm{Frob}_v) q_v^{-s}},$$

where χ is the Hecke character coming from $\mathrm{Gal}(L/F)$, and this is hence its L-function. It's thus clear that this L-function is invertible. So we've shown that, for every representation, the L-function is invertible along the line $\Re s = 1$, so we're done. $\square$

Remark 1.3.5. Notice that this proves the Sato-Tate conjecture in this case when $F = \mathbb{Q}$ because all quadratic extensions are either totally real or CM.

1.3.3 $\boldsymbol{E}[D_{2n}]$, $n = 2, 3, 4, 6$

We look now at the Sato-Tate groups

$$ST_A = \left\langle \begin{pmatrix} B & \\ & \overline{B} \end{pmatrix}_{B \in \mathrm{SU}(2)}, E_n := \begin{pmatrix} e^{\frac{\pi i}{n}} \mathrm{Id}_2 & \\ & e^{-\frac{\pi i}{n}} \mathrm{Id}_2 \end{pmatrix}, J \right\rangle,$$

with identity component ST_A^0 the embedded copy of SU(2) and component group D_{2n}. These arise from abelian varieties A whose endomorphism ring $\mathrm{End}_M^0(A)$ is a quaternion algebra for a large enough field extension M/F. Either A is potentially the sum of two elliptic curves without CM whose ℓ-adic representations are twists of each other by a finite-order character, or A is simple with quaternionic multiplication. If we view A as defined over L, where G_L is the index-2 subgroup of the Galois group G_F corresponding to the cyclic subgroup of the component group D_{2n} under the correspondence given in [15, Theorem 2.17], the endomorphism ring is not yet a quaternion algebra. It is, however, a quadratic field K, as proven in [15, Theorem 4.7]; we note that while the statement in [15] is constructed for the direct sum of elliptic curves case, there is no use of this in the proof, so we may apply it here as well.

To prove Conjecture 1.2.2 in this case, our strategy is to decompose the representation $\rho_{A,\ell}$ into a tensor $s \otimes \delta$ where δ is a finite-image dihedral representation and s is a two-dimensional representation. We do this by manually constructing a 2-cocycle in a certain cohomology group that obstructs a representation lift from G_L to G_F, then use the fact that the cohomology is 0 to obtain a coboundary description, which allows us to lift. Then we check that s acts solely on the identity component and δ acts on the component group times $\pm\,\mathrm{Id}$, and finally use Rankin-Selberg and Theorem 1.2.5 again.

As in the previous case, we may decompose the representation $\rho_{A,\ell}|_{G_L}$ into two 2-dimensional pieces $\rho_{A,\lambda}$ and $\rho_{A,\overline{\lambda}}$ via the two embeddings of K into $\overline{\mathbb{Q}_\ell}$, and as in the previous case, Theorem 1.3.2 says that $(\rho_{A,\lambda})_{\lambda \in S'}$ is a compatible system of representations. But unlike the previous case, we get the isomorphism $\rho_{A,\lambda} \otimes \epsilon \simeq \rho_{A,\overline{\lambda}}$ for some finite-image character ϵ. We notice that $\mathrm{Ind}_{G_L}^{G_K} \rho_{A,\lambda} = \rho_{A,\ell}$ by Frobenius reciprocity, and so $\rho_{A,\ell}|_{G_L} = \rho_{A,\lambda} \oplus \rho_{A,\lambda}^g$ for $g \in G_F \backslash G_L$; therefore, $\rho_{A,\lambda} \otimes \epsilon \simeq \rho_{A,\overline{\lambda}} \simeq \rho_{A,\lambda}^g$. (Notationally, from here we will assume that any group element g with or without subscript is in $G_F \backslash G_L$ and any group element h is in G_L, so as to repeatedly omit this statement.)

Because of [15, Proposition 2.17], we know that if M is the smallest field with $\mathrm{End}_M^0(A)$ being the full quaternion algebra, then $\mathrm{Gal}(M/F) = D_{2n}$, and that $\mathrm{Gal}(M/L) = C_n$. Because

$$(\rho_{A,\lambda} \oplus (\rho_{A,\lambda} \otimes \epsilon))|_{G_M} = \rho_{A_M,\lambda} \oplus (\rho_{A_M,\lambda} \otimes \epsilon|_{G_M})$$

has a four-dimensional real endomorphism ring only if $\epsilon|_{G_M}$ is trivial, we must have ϵ being a character of $\mathrm{Gal}(M/L)$. In particular, $\epsilon(h) = 1$ if $h \in G_M$. But because of the structure of D_{2n}, we know that $g \in G_F \backslash G_L$ has $g^2 \in G_M$. So $\epsilon(g^2) = 1$.

In addition, we know

$$\rho_{A,\lambda}^g \simeq \rho_{A,\lambda} \otimes \epsilon, \text{ so } \rho_{A,\lambda} \simeq \rho_{A,\lambda}^g \otimes \epsilon^g \simeq \rho_{A,\lambda} \otimes \epsilon \otimes \epsilon^g$$

and hence we conclude that $\epsilon(ghg^{-1})\epsilon(h) = 1$.

We let c be such that

$$c(h_1, h_2) = c(g_1, h_2) = 1, c(h_1, g_2) = c(g'h_1, g_2) = \epsilon(h_1)$$

for all g_1, g_2, h_1, h_2, and fixed $g' \in G_F \backslash G_L$. Then the above statements are enough to exhaustively prove that c is a cocycle in $H^2(G_F, \overline{K_\lambda}^\times)$ with $\overline{K_\lambda}^\times$ having the trivial action and discrete topology. But it's a theorem of Tate that $H^2(G_F, \overline{K_\lambda}^\times)$ is trivial, so this cocycle must be a coboundary. That means there is a continuous (i.e. finite-image) cochain $\gamma : G_F \to \overline{K_\lambda}^\times$ with $c(g_1, g_2) = \frac{\gamma(g_1)\gamma(g_2)}{\gamma(g_1 g_2)}$, and so on through all combinations of g_i and h_i.

We can check via the above the following equations:

$$\begin{aligned}
\gamma(\mathrm{Id}) &= 1 \\
\gamma(g)\gamma(g^{-1}) &= c(g, g^{-1}) = \epsilon(g'^{-1}g) \\
\gamma(g)\gamma(hg^{-1}) &= \gamma(ghg^{-1})c(g, hg^{-1}) = \gamma(ghg^{-1})\epsilon(g'^{-1}g) = \gamma(ghg^{-1})\gamma(g)\gamma(g^{-1}) \\
\gamma(h)\gamma(g^{-1}) &= \gamma(hg^{-1})c(h, g^{-1}) = \gamma(hg^{-1})\epsilon(h) = \gamma(ghg^{-1})\gamma(g^{-1})\epsilon(h)
\end{aligned}$$

so that $\gamma(h) = \gamma(ghg^{-1})\epsilon(h)$ for every pair (g, h). Further, γ is a character of G_L; from here we only remember the domain of γ being G_L. Therefore, if we let $s_{A,\lambda} = \rho_{A,\lambda} \otimes \gamma$, then

$$s^g_{A,\lambda} = \rho^g_{A,\lambda} \otimes \gamma^g \simeq \rho_{A,\lambda} \otimes \epsilon \otimes \gamma^g \simeq \rho_{A,\lambda} \otimes \gamma = s_{A,\lambda}$$

so that we may extend $s_{A,\lambda}$ to be a representation of G_F, by Theorem 1.3.3, with basis $\{s_1, s_2\}$. And there is a clear G_L-equivariant map $\rho_{A,\lambda} \to s_{A,\lambda} \otimes \mathrm{Ind}_{G_L}^{G_F} \gamma^{-1}$ given by sending v to $v \otimes 1$; therefore, there is a G_F-equivariant map $\rho_{A,\ell} = \mathrm{Ind}_{G_L}^{G_F} \rho_{A,\lambda} \to s_{A,\lambda} \otimes \mathrm{Ind}_{G_L}^{G_F} \gamma^{-1}$. By dimension count, they must be isomorphic. Therefore, we are able to write $\rho_{A,\ell}$ as $s_{A,\lambda} \otimes \delta$, where δ is finite-image with vector space having basis $\{v_1, v_2\}$, and in fact has image isomorphic to a dihedral group. Notice that the way we devised γ, we didn't use anything about λ, and ϵ is independent of λ by Theorem 1.3.2; so γ is independent of λ as is V, so since $(\rho_{A,\lambda})_\lambda$ is a weakly compatible system, so too is $(s_{A,\lambda})_\lambda$.

Theorem 1.3.6. *If F is a totally real field and A is an abelian variety defined over F which has Galois type $\boldsymbol{E}[D_n]$ for $n = 2, 3, 4, 6$, then the Sato-Tate conjecture holds for A.*

Proof. As before, we must show that for each representation r of the Sato-Tate group, the L-function $\prod_{v \notin S} \det(1 - r(s(v))q_v^{-s})^{-1}$ is holomorphic and invertible for $\Re s \geq 1$ where $s(v)$ is the conjugacy class given by dividing the image of Frob_v by $q_v^{1/2}$. The Sato-Tate group ST_A is given by $\mathrm{SU}(2) \times D_{4n}/\langle(-\mathrm{Id}_2, E_n^n)\rangle$, so that any representation of ST_A is given by a representation of $\mathrm{SU}(2)$ tensored with a representation of D_{4n} whose signs agree on their centers. Of course the irreducible representations of $\mathrm{SU}(2)$ are $\mathrm{Sym}^k(St)$ and there are 4 one-dimensional and $n-1$ two-dimensional representations of D_{4n}.

Our goal now is to describe where $s_{A,\lambda}$ and δ send Frob_v inside ST_A. As written before, the Sato-Tate group is represented as the matrices in

$$\left\langle \begin{pmatrix} B & \\ & \overline{B} \end{pmatrix}_{B \in \mathrm{SU}(2)}, \begin{pmatrix} e^{\frac{\pi i}{n}} \mathrm{Id}_2 & \\ & e^{-\frac{\pi i}{n}} \mathrm{Id}_2 \end{pmatrix}, J \right\rangle .$$

These are inside $\mathrm{Sp}(4)$ where the alternating form is $\begin{pmatrix} & & 1 & \\ & & & 1 \\ -1 & & & \\ & -1 & & \end{pmatrix}$. However, we instead view it with the alternating form $\begin{pmatrix} &&&-1\\ &&1&\\ &-1&&\\ 1&&& \end{pmatrix}$. That is, we conjugate the Sato-Tate group by $\begin{pmatrix} 1&&&\\ &1&&\\ &&&1\\ &&-1& \end{pmatrix}$ to get the new group

$$\left\langle \begin{pmatrix} B & \\ & B \end{pmatrix}_{B \in \mathrm{SU}(2)}, \begin{pmatrix} e^{\frac{\pi i}{n}}\,\mathrm{Id}_2 & \\ & e^{-\frac{\pi i}{n}}\,\mathrm{Id}_2 \end{pmatrix}, \begin{pmatrix} & \mathrm{Id}_2 \\ \mathrm{Id}_2 & \end{pmatrix} \right\rangle.$$

Writing it in this form, because the Zariski closure of SU(2) is SL(2), we know that G^1 must contain all matrices $\left(\begin{smallmatrix} A & \\ & A \end{smallmatrix}\right)$ where $A \in \mathrm{SL}(2)$. But as above, the theorem of Deligne says that the scalar multiples of the identity must be in the Zariski closure of the image of $\rho_{A,\ell}$, so that means that G must contain all matrices of the form above, where A is now in GL(2). Now G is the image under ι of G_ℓ^{Zar}, the Zariski closure of the image of $\rho_{A,\ell}$, which is the Kronecker product of the Zariski closure of the image of $s_{A,\lambda}$ with the image of δ. If we look at the closure of $\rho_{A,\ell}(\ker \delta)$, this is a finite index subgroup of G_ℓ^{Zar}. Because the connected component of the identity $G_\ell^{\mathrm{Zar},0}$ is isomorphic to GL(2) and thus is Zariski irreducible, the closure of $\rho_{A,\ell}(\ker \delta)$ cannot be smaller than this.

But also it cannot be larger than this: it is contained in the centralizer of a 4-dimensional vector space inside $M_4(\overline{\mathbb{Q}_\ell})$, namely $\left(\begin{smallmatrix} a\cdot \mathrm{Id} & b\cdot \mathrm{Id} \\ c\cdot \mathrm{Id} & d\cdot \mathrm{Id} \end{smallmatrix}\right)$ in the basis $s_1 \otimes v_1, s_2 \otimes v_1, s_1 \otimes v_2, s_2 \otimes v_2$, but $G_\ell^{\mathrm{Zar},0}$ is already such a centralizer: it centralizes $\left(\begin{smallmatrix} a\cdot \mathrm{Id} & b\cdot \mathrm{Id} \\ c\cdot \mathrm{Id} & d\cdot \mathrm{Id} \end{smallmatrix}\right)$ in the usual basis. Therefore the closure of $\rho_{A,\ell}(\ker \delta)$ is equal to this connected component $\left\{\left(\begin{smallmatrix} A & \\ & A \end{smallmatrix}\right) : A \in \mathrm{GL}(2)\right\}$.

On the other hand, G_F can act on the vector space for the representation $\rho_{A,\ell}$

solely through δ. The image of this representation commutes with the kernel of δ above, but as we observed, all such matrices are of the form $\left(\begin{smallmatrix} a\cdot\mathrm{Id} & b\cdot\mathrm{Id} \\ c\cdot\mathrm{Id} & d\cdot\mathrm{Id}\end{smallmatrix}\right)$. So the image of G_F acting via δ alone lands in this vector space. In order for the image to land in GSp(4), we can calculate that either $b = c = 0$ or $a = d = 0$. Recall also that its image is dihedral and irreducible, so it must essentially give some dihedral representation. Each matrix in a 4-dimensional finite-image representation is unitary, so each of them already appears in the Sato-Tate group. But the only matrices of this form in the Sato-Tate group were in the group $\langle E_n, J\rangle$, so this must be the image of G_F acting through δ.

We have therefore shown that the image of δ is exactly D_{4n}, and the closure of the image of $s_{A,\lambda}$ is GL(2). Recall from above that a representation of the Sato-Tate group is given by the tensor product of a representation of D_{4n} with a representation of SU(2) with the same sign. Given such a representation, say $\eta \otimes \mathrm{Sym}^k(St)$, the L-function is

$$\begin{aligned} &\prod_{v \notin S} \det(1 - \mathrm{Sym}^k(s(v)) \otimes \eta(s(v)) q_v^{-s})^{-1} \\ =&\prod_{v \notin S} \det(1 - (\mathrm{Sym}^k \circ \iota \circ s_{A,\lambda})(\mathrm{Frob}_v) \otimes (\eta \circ \delta)(\mathrm{Frob}_v) q_v^{-s-k/2})^{-1}. \end{aligned}$$

We may apply Theorem 1.2.5 to $(s_{A,\lambda})_\lambda$, or in fact we may even apply [4, Theorem 5.4.1] to find a field F'/F for which $(s_{A,\lambda}|_{G_{F'}})_\lambda$ is cuspidal automorphic, assuming $k \geq 1$. Then as before, cyclic base change tells us that $(s_{A,\lambda}|_{G_E})_\lambda$ is cuspidal automorphic where F'/E is solvable so that $L(\mathrm{Sym}^k|_{G_E}, s)$ is invertible, and then Brauer's theorem tells us that $L(\mathrm{Sym}^k, s)$ is invertible as well. We know that $\eta \circ \delta$ is cuspidal automorphic already if η is nontrivial, because $\eta \circ \delta$ is either a 1-dimensional representation, a nontrivial Hecke character, or a 2-dimensional dihedral representation, which is induced from a nontrivial Hecke character of G_L and whose automorphy and cuspidality is established in [2, Theorem 6.2]. So $L(\eta, s)$ is invertible and the Rankin-Selberg method as before tells us that the L-function we wanted,

$$L(\mathrm{Sym}^k \otimes \eta, s) = \prod_{v \notin S} \det(1 - (\mathrm{Sym}^k \circ s_{A,\lambda})(\mathrm{Frob}_v) \otimes (\eta \circ \delta)(\mathrm{Frob}_v) q_v^{-s-k/2})^{-1},$$

is invertible as long as Sym^k and η are not dual. For $k \geq 1$ this is obvious by cardinality, and for $k = 0$ and η nontrivial, this is just the Artin L-function for a representation of $\mathrm{Gal}(L'/F)$ where L' is the fixed field of the kernel of δ. Since this is a solvable group, we know the L-function is invertible. □

1.4 Other asymptotics

So far our goal has been to show that the normalized Frobenius conjugacy classes are equidistributed within the Sato-Tate group, and from this we can deduce the distributions of the normalized traces of Frobenius in the interval $[-4, 4]$. We have done this by proving that all nontrivial irreducible representations' L-functions are invertible. Unfortunately, the current state of affairs does not allow this in the two cases **A** or **B**$[C_2]$, so we set our sights a little lower. We'd like to be able to show that for some positive fraction of primes, the trace of Frobenius is positive (resp. negative), but even this is beyond our elementary methods. A theorem of Boxer, Calegari, Gee and Pilloni helps us in this regard, as well as a theorem of Taïbi and Gee. Let A be any abelian surface over a totally real field F, and suppose that for some good prime v, the characteristic polynomial of the normalized Frobenius $\frac{\mathrm{Frob}_v}{\sqrt{q_v}}$ in its compatible system of representations is

$$\mathrm{Char}_{\frac{\mathrm{Frob}_v}{\sqrt{q_v}}}(X) = (X-\alpha)(X-\alpha^{-1})(X-\beta)(X-\beta^{-1}) = X^4 - a_1X^3 + a_2X^2 - a_1X + 1.$$

We first define $a_{1,\min}$ as the number for which zero proportion of primes v have $a_1 < a_{1,\min}$ but for any $\epsilon > 0$ a positive proportion of v have $a_1 < a_{1,\min} - \epsilon$. Let us define $a_{1,\max}, a_{2,\min}$ and $a_{2,\max}$ similarly. We'll be able to prove the following theorems:

Theorem 1.4.1. *If A/F is a generic abelian surface, i.e.* $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}$*, then $a_{1,\min} \leq -\frac{2}{3}$ and $a_{1,\max} \geq \frac{2}{3}$.*

Theorem 1.4.2. *If A/F is a generic abelian surface, then $a_{2,\min} \leq \frac{4}{5}$ and $a_{2,\max} \geq \frac{4}{3}$.*

Theorem 1.4.3. *If A/F is an abelian surface of type $\boldsymbol{B}[C_2]$, then $a_{1,\min} \leq -2.47$ and $a_{1,\max} \geq 2.47$.*

Theorem 1.4.4. *If A/F is an abelian surface of type $\boldsymbol{B}[C_2]$, then $Fa_{2,\min} \leq 0.43$ and $a_{2,\max} \geq 3.57$.*

The first two theorems above are the "best of their kind", so to speak; that is, given the L-functions we currently know to be invertible, there are probability distributions of α and β on the unit circle for which $a_1 \geq -\frac{2}{3}$, and yet the Tauberian statistics of these L-functions are not violated.

1.4.1 The generic case

Let us state the results of Boxer-Calegari-Gee-Pilloni and Gee-Taïbi.

Theorem 1.4.5 ([7, Theorem 9.2.8])**.** *Let A be a challenging abelian surface over a totally real field F. Then A is potentially modular.*

Challenging in the above theorem just means being in case $\mathbf{A}$ or $\mathbf{B}[C_2]$.

Suppose that $(\rho_{A,\ell}, V)$ is the dual of the ℓ-adic Tate module representation of A. Suppose that v_1, v_2, v_3, v_4 are a symplectic basis of V under the Weil pairing; that is, $\langle v_1, v_2\rangle = \langle v_3, v_4\rangle = 1$ and all other pairs of vectors are 0 under the pairing. The Weil pairing on V then becomes a direct-sum split of $\wedge^2 V$:

$$\wedge^2 V = \mathbb{Q}_\ell(1) \oplus W$$

where $\mathbb{Q}_\ell(1)$ is spanned by $v_1 \wedge v_2 + v_3 \wedge v_4$. It is not difficult to show that if A is generic, then W is irreducible.

Theorem 1.4.6 ([16])**.** *If $\rho_{A,\ell}$ is strongly irreducible, there is a cuspidal automorphic form Π on $\mathrm{GL}(5)$ corresponding to the W above.*

Sketch. Suppose that π is the automorphic representation corresponding to A. By [25, Theorem A], we know that $\wedge^2\pi$ is automorphic, and is the induction of the tensor product of cuspidal automorphic representations of GL_{n_i} for $\sum n_i = 6$. We know further that π is symplectic, so we may take $n_1 = 1$.

It then suffices to show that $n_1 = 1$ and $n_2 = 5$. The occurrence of more than one $n_i = 1$ is ruled out by [34, Theorem 1.1], and the possibility that $n_1 = 1$, $n_2 = 2$, and $n_3 = 3$ is ruled out by [3, Prop 4.2]. Therefore, $\Pi_2 = \Pi$ is cuspidal. □

To prove Theorems 1.4.1 and 1.4.2, it suffices to prove them when looking at A/E where E/F is any field extension. This is for the following reasons: if a prime v of F splits in E, the Frobenius element does not change, and neither does the size of the residue field, so that the normalized trace of Frobenius is unchanged. Also, a set of primes of E of density 1 lie above split primes of F, so looking at the set of primes of E described in 1.4.1 or 1.4.2, almost all of them lie above a split prime of F. So a positive proportion of the split primes of F, which is a positive proportion of all primes of F, satisfy the inequalities.

Thus after Theorem 1.4.5 we may assume that A/F is modular, and so $\rho_{A,\ell}$ corresponds to a cuspidal automorphic representation. We continue to assume F totally real, as this is a further allowance in [7]. We also assume that we are in the generic case **A**. Therefore, as usual we know $L(V, s)$ is holomorphic and nonzero on $\Re(s) \geq 1$ (where the L-function is shifted so that the critical line is $\Re(s) = \frac{1}{2}$ and all the eigenvalues have norm 1, as in the previous section). In addition, since W corresponds to a cuspidal representation, $L(W, s)$ is also holomorphic and nonzero on the same set. And by Rankin-Selberg, since $V \simeq V^* \otimes \mathbb{Q}_\ell(1)$ and so $V \otimes V$ contains one copy of the cyclotomic character, $L(V \otimes V, s)$ has a simple pole at $s = 1$ and is holomorphic everywhere else on $\Re(s) \geq 1$ (where again the L-function is normalized in the standard way). The same holds for W; that is, since W is irreducible and essentially self-dual, $L(W \otimes W, s)$ has a simple pole at $s = 1$ and is holomorphic nonzero everywhere else on the half-plane. And finally, since V and W are distinct irreducible representations, $L(V \otimes W, s)$ is holomorphic nonzero everywhere on the half plane, again by Rankin-Selberg.

Now that we have these five L-functions and their poles at 1, we look back at Serre.

Theorem 1.4.7 ([32]). *Given a Dirichlet series*

$$L(\rho, s) = \prod_v \frac{1}{\det(1 - \rho(x_v) q_v^{-s})}$$

with a pole of order c at $s = 1$ and holomorphic nonzero elsewhere on $\Re(s) \geq 1$, then

$$\sum_{q_v \leq n} \operatorname{Tr} \rho(x_v) = c \left(\frac{n}{\log n} \right) + o(n/\log n).$$

We apply this to the five L-functions above, with the normalized image of Frob_v in V having eigenvalues $\alpha_v, \alpha_v^{-1}, \beta_v, \beta_v^{-1}$, to get

$$\sum_{q_v \leq n} (\alpha_v + \alpha_v^{-1} + \beta_v + \beta_v^{-1}) = o(n/\log n)$$

and four other asymptotic equations. Combining with the statement of Serre's theorem for the trivial representation (namely, $\sum_{q_v \leq n} 1 = n/\log n + o(n/\log n)$), and letting $s_v = \alpha_v + \alpha_v^{-1}$ and $t_v = \beta_v + \beta_v^{-1}$ for convenience, we find the system

$$\sum_{q_v \le n} s_v + t_v = o(n/\log n)$$

$$\sum_{q_v \le n} s_v t_v + 1 = o(n/\log n)$$

$$\sum_{q_v \le n} s_v^2 + 2s_v t_v + t_v^2 - 1 = o(n/\log n) \qquad \Rightarrow \sum_{q_v \le n} s_v^2 + t_v^2 - 3 = o(n/\log n)$$

$$\sum_{q_v \le n} s_v^2 t_v + s_v t_v^2 + s_v + t_v = o(n/\log n) \qquad \Rightarrow \sum_{q_v \le n} s_v^2 t_v + s_v t_v^2 = o(n/\log n)$$

$$\sum_{q_v \le n} s_v^2 t_v^2 + 2s_v t_v = o(n/\log n) \qquad \Rightarrow \sum_{q_v \le n} s_v^2 t_v^2 - 2 = o(n/\log n)$$

Proof of Theorem 1.4.1. The identity

$$(2-s)(2-t)(3s+3t+2-\varepsilon) = (8-4\varepsilon)+(8+2\varepsilon)(s+t)-6(s^2+t^2)-(10+\varepsilon)st+3(s^2t+st^2)$$

holds, so

$$\begin{aligned}
&\sum_{q_v \le n} (2-s_v)(2-t_v)(3s_v+3t_v+2-\varepsilon) \\
&= \sum_{q_v \le n} (8-4\varepsilon) + (8+2\varepsilon)(s_v+t_v) - 6(s_v^2+t_v^2) - (10+\varepsilon)s_v t_v + 3(s_v^2 t_v + s_v t_v^2) \\
&= \sum_{q_v \le n} 3(s_v^2 t_v + s_v t_v^2) - (10+\varepsilon)(s_v t_v + 1) - 6(s_v^2 + t_v^2 - 3) + (8+2\varepsilon)(s_v+t_v) - 3\varepsilon \\
&= (-3\varepsilon + o(1))\frac{n}{\log n}.
\end{aligned}$$

So if $-\frac{2}{3} < a_{1,\min} = -\frac{2}{3}+\frac{\varepsilon}{3}$, then a zero proportion of primes v have $a_1 = s_v + t_v <$

$-\frac{2}{3}+\frac{\varepsilon}{3}$. And the Weil bounds on the eigenvalues hold, meaning that the sum of the left side should be positive for large enough n, but the right side is negative for large enough n. So it's impossible for $a_{1,\min} > -\frac{2}{3}$. The same idea holds for $a_{1,\max}$; the asymptotics above are invariant under the transformation $(s_v, t_v) \to (-s_v, -t_v)$, so if it's impossible for most primes to have their a_1's lie above $-\frac{2}{3}+\frac{\varepsilon}{3}$, then it's also impossible for most primes to have their a_1's lie below $\frac{2}{3}-\frac{\varepsilon}{3}$. □

Proof of Theorem 1.4.2. Similarly, the following two equations hold:

$$(3st+2+\varepsilon)(st+4) = 3s^2t^2 + (14+\varepsilon)st + (8+4\varepsilon)$$

$$(5st+6-\varepsilon)(4-st) = -5s^2t^2 + (14+\varepsilon)st + (24-4\varepsilon),$$

so

$$\begin{aligned}\sum_{q_v \le n} (3s_vt_v+2+\varepsilon)(s_vt_v+4) &= \sum_{q_v \le n} (8+4\varepsilon) + (14+\varepsilon)s_vt_v + 3s_v^2t_v^2 \\ &= \sum_{q_v \le n} 3(s_v^2t_v^2-2) + (14+\varepsilon)(s_vt_v+1) + 3\varepsilon \\ &= (3\varepsilon + o(1))\frac{n}{\log n}\end{aligned}$$

and

$$\begin{aligned}\sum_{q_v \le n} (5s_vt_v + 6 - \varepsilon)(4 - s_vt_v) &= \sum_{q_v \le n} (24 - 4\varepsilon) + (14 + \varepsilon)s_vt_v - 5s_v^2t_v^2 \\ &= \sum_{q_v \le n} -5(s_v^2t_v^2 - 2) + (14 + \varepsilon)(s_vt_v + 1) - 5\varepsilon \\ &= (-5\varepsilon + o(1))\frac{n}{\log n}\end{aligned}$$

If $s_vt_v \le -\frac{2}{3} - \frac{\varepsilon}{3}$ for all but a density zero set of primes v, then in the first equation the left side would be negative for large n, but the right side is positive for large n, impossible. So $s_vt_v > -\frac{2}{3} - \frac{\varepsilon}{3}$ a positive proportion of the time for every positive ε, and hence $a_2 = 2 + s_vt_v > \frac{4}{3} - \frac{\varepsilon}{3}$ for a positive proportion of the time. Thus $a_{2,\max} \ge \frac{4}{3}$.

And if $s_vt_v \ge -\frac{6}{5} + \frac{\varepsilon}{5}$ for all but a density zero set of primes v, then in the second equation the left side would be positive for large n, but the right side is negative for large n, impossible. So $s_vt_v < -\frac{6}{5} + \frac{\varepsilon}{5}$ a positive proportion of the time for every positive ε, and hence $a_2 = 2 + s_vt_v < \frac{4}{5} + \frac{\varepsilon}{5}$ for a positive proportion of the time. Thus $a_{2,\min} \le \frac{4}{5}$. □

As stated in the introduction, these are the best possible theorems we may obtain with the asymptotics arising from Serre's method; namely, if

$$\begin{aligned} s_v = 0 \text{ and } t_v = 2 &\text{ for } \frac{1}{6} \text{ of all primes,} \\ s_v = -\frac{3}{2} \text{ and } t_v = 2 &\text{ for } \frac{4}{21} \text{ of all primes, and} \\ s_v = \frac{-1-\sqrt{7}}{3} \text{ and } t_v = \frac{-1+\sqrt{7}}{3} &\text{ for } \frac{9}{14} \text{ of all primes,} \end{aligned}$$

then

$$\begin{aligned} \sum_{q_v \le n} s_v + t_v &= \frac{(1+o(1))n/\log n}{6}(0+2) + \frac{(4+o(1))n/\log n}{21}\left(-\frac{3}{2}+2\right) \\ &+ \frac{(9+o(1))n/\log n}{14}\left(\frac{-1-\sqrt{7}}{3}+\frac{-1+\sqrt{7}}{3}\right) \\ &= \left(\frac{2}{6}+\frac{2}{21}-\frac{6}{14}+o(1)\right)\frac{n}{\log n} = o\left(\frac{n}{\log n}\right) \end{aligned}$$

and similar equalities hold for the other four asymptotics as well. Because $a_{1,v}$ can only ever be $-\frac{2}{3}$, $\frac{1}{2}$ or 2, $a_{1,\min}$ is $-\frac{2}{3}$, and we cannot prove anything stronger.

A mirror equality case holds in calculating $a_{1,\max}$, and similar equality cases hold in the cases of $a_{2,\min}$ and $a_{2,\max}$. If

$$\begin{aligned} s_v = -2 \text{ and } t_v = 2 &\text{ for } \frac{1}{10} \text{ of all primes,} \\ s_v = -\frac{1}{3} \text{ and } t_v = 2 &\text{ for } \frac{9}{35} \text{ of all primes, and} \\ s_v = \frac{-1-\sqrt{7}}{3} \text{ and } t_v = \frac{-1+\sqrt{7}}{3} &\text{ for } \frac{9}{14} \text{ of all primes,} \end{aligned}$$

then the equalities all hold as above, and $a_{2,\max} = \frac{4}{3}$ for this set. And if

$$\begin{aligned} s_v = 2 \text{ and } t_v = 2 &\text{ for } \frac{1}{52} \text{ of all primes,} \\ s_v = -2 \text{ and } t_v = -2 &\text{ for } \frac{1}{52} \text{ of all primes,} \\ s_v = -\frac{3}{5} \text{ and } t_v = 2 &\text{ for } \frac{125}{767} \text{ of all primes, and} \\ s_v = \frac{-5-\sqrt{1495}}{35} \text{ and } t_v = \frac{-5+\sqrt{1495}}{35} &\text{ for } \frac{1225}{1534} \text{ of all primes,} \end{aligned}$$

it is not difficult to again check that all asymptotics above hold, and $a_{2,\min} = \frac{4}{5}$ for this set.

Therefore, with our current knowledge of modularity lifting theorems, we cannot say more than these theorems.

Remark 1.4.8. While Theorems 1.4.1 and 1.4.2 do the job of bounding $a_{1,\min}$, etc., from above or below, they are rather weak. We expect $a_{1,\min}$ to be equal to -4, yet we can only currently show that $a_{1,\min} \leq -\frac{2}{3}$, and similarly for $a_{1,\max}$. We also expect $a_{2,\max} = 6$, but we can only show that $a_{2,\max} \geq \frac{4}{3}$; and we expect $a_{2,\min} = -2$, but we can only show that $a_{2,\min} \leq \frac{4}{5}$.

Notice also that we used heavily the fact that $\mathbf{A}$ was generic, because if it were not, neither the 4-dimensional representation V nor the 5-dimensional representation W would need be irreducible. Because we know the Sato-Tate conjecture in all cases except $\mathbf{A}$ and $\mathbf{B}[C_2]$, we can calculate $a_{1,\min/\max}$ and $a_{2,\min/\max}$ for abelian surfaces of these types; for any abelian surface in cases $\mathbf{E}$ or $\mathbf{F}$, where the normalized eigenvalues of Frobenius are always 2 copies of α and 2 copies of α^{-1}, $a_{2,\max}$ is still 6 as expected, but $a_2 = 4 + \alpha^2 + \alpha^{-2}$, so we expect (and deduce) that $a_{2,\min} = 2$, so Theorem 1.4.2 doesn't hold if our abelian surface is not generic.

1.4.2 The case $\boldsymbol{B}[C_2]$

We now suppose our abelian variety A over totally real field F has Sato-Tate group $\langle \mathrm{SU}(2) \times \mathrm{SU}(2), J\rangle$. We may still apply Theorem 1.4.5, so that A is potentially modular. We base change to a totally real field extension F' where A is modular and the Tate module representation is cuspidal. Then, as before, the representation $\rho_{A,\ell}$ is induced from a representation $\rho_{A_L,\lambda}$. This means that $\rho_{A,\ell} \simeq \rho_{A,\ell} \otimes \chi_{L/K}$. On the level of automorphic representations, this means that the cuspidal representation Π coming from ρ also satisfies $\Pi \simeq \Pi \otimes \chi_{L/K}$. But this means that Π is the base change of some cuspidal representation π of $\mathrm{GL}(2)$ over L.

This representation π arises from the compatible system of representations $(\rho_{A,\lambda})_\lambda$, and since these have big image because we're in case $\mathbf{B}[C_2]$, we know that the representations $\rho_{A,\lambda}$, and more generally $\mathrm{Sym}^k \rho_{A,\lambda}$ for any $k \geq 1$, are not induced from any character. This means that $\mathrm{Sym}^k \rho_{A,\lambda} \not\simeq \mathrm{Sym}^k \rho_{A,\lambda} \otimes \chi$ for any character χ. We recall theorems of Kim-Shahidi:

Theorem 1.4.9 ([26] Theorem 2.2.2)**.** *Let π be a cuspidal automorphic representation of $\mathrm{GL}(2, \mathbb{A}_L)$, let ω_π denote the central character, and let $A^i(\pi) = \mathrm{Sym}^i(\pi) \otimes \omega_\pi^{-1}$. Then $A^3(\pi)$ is not cuspidal if and only if there exists a nontrivial grössencharacter μ such that $A^2(\pi) \simeq A^2(\pi) \otimes \mu$.*

Theorem 1.4.10 ([26] Theorem 3.3.7)**.** *With notation as above, $A^4(\pi)$ is a cuspidal representation of $\mathrm{GL}(5, \mathbb{A}_L)$ unless*

(1) There is some nontrivial grössencharacter η with $\pi \otimes \eta \simeq \pi$

(2) $A^3(\pi)$ is not cuspidal

(3) $A^3(\pi)$ is cuspidal, but there is some nontrivial quadratic grössencharacter η with
$A^3(\pi) \simeq A^3(\pi) \otimes \eta$

Therefore, $A^2(\pi), A^3(\pi)$ and $A^4(\pi)$ are all automorphic. And because $\mathrm{Sym}^k \rho_{A,\lambda}$ is not isomorphic to its own twist, neither is $\mathrm{Sym}^k \pi$. So we obtain that $A^2(\pi), A^3(\pi)$ and $A^4(\pi)$ are cuspidal.

In the same way as above, if α_v, α_v^{-1} are the eigenvalues of $\rho_{A_L,\lambda}(\mathrm{Frob}_v){q_v}^{-1/2}$ for primes v of L, and β_v, β_v^{-1} are the eigenvalues of $\rho_{A_L,\overline{\lambda}}(\mathrm{Frob}_v){q_v}^{-1/2}$, and for simplicity we denote $x_v = \alpha_v + \alpha_v^{-1}$ and $y_v = \beta_v + \beta_v^{-1}$, then via Rankin-Selberg we find that if $0 \leq k, l \leq 4$ or if one of k, l equals 0 and the other is at most 8, then

$$\sum_{q_v<n} x_v^k y_v^l = \begin{cases} (C_{k/2}C_{l/2} + o(1))\frac{n}{\ln n}, & k, l \text{ both even} \\ \frac{o(1)n}{\ln n}, & \text{one of } k, l \text{ odd} \end{cases}$$

where $C_n = \frac{1}{n+1}\binom{2n}{n}$ is the n'th Catalan number.

Proof of Theorem 1.4.3. Let

$$\begin{aligned}Q(x,y) = &-12.543(x+y) + 53.838(x^2+y^2) - 12.954(x^3+y^3) - 13.063(x^4+y^4)\\ &- 7.914(x^5+y^5) - 2.9(x^6+y^6) + 3.607(x^7+y^7) + 1.575(x^8+y^8)\\ &+ 124.68xy - 183.789(x^2y+y^2x) + 1.878(x^3y+y^3x) + 50.255(x^4y+y^4x)\\ &+ 117.628x^2y^2 + 73.149(x^3y^2+y^3x^2) - 48.646(x^4y^2+y^4x^2) - 65.928x^3y^3\\ &+ 8.734(x^4y^3+y^4x^3) + 1.098x^4y^4\end{aligned}$$

(All decimals are exact, unless otherwise noted.) It's easy to check that the minimum of $Q(x,y)$ on the set $\{x, y \in [-2,2] : x+y \geq -2.47\}$ is when $x \approx -1.81913$ and $y \approx 0.644208$, giving a minimum of approximately -1.93656, and yet the sum

$$\sum_{q_v<n} Q(x_v, y_v) = \frac{(-2.04+o(1))n}{\ln n}.$$

So it is impossible for $x_v + y_v$ to always be ≥ -2.47, and therefore $a_{1,\text{min}} \leq -2.47$. And each asymptotic above is invariant under $(x,y) \to (-x,-y)$, so a mirror polynomial proves that $a_{1,\text{max}} \geq 2.47$. (A more precise polynomial proves that $a_{1,\text{min}} \leq -2.4763827913319$, and as in Theorem 1.4.1 we can find points (x,y) and probabilities that prohibit any further improvements.) □

Proof of Theorem 1.4.4. Let

$$
\begin{aligned}
R(x,y) &= -24.04(x^2+y^2) + 39.64(x^4+y^4) - 13.14(x^6+y^6) \\
&\quad + 3.82(x^8+y^8) - 15.76xy - 119.88(x^3y+y^3x) + 484.32x^2y^2 \\
&\quad - 153.28(x^4y^2+y^4x^2) + 192.44x^3y^3 + 8.2x^4y^4
\end{aligned}
$$

It's easy to check that the minimum of $R(x,y)$ on the set $\{x,y \in [-2,2] : xy \geq -1.57\}$ is when $x \approx 0.907648$ and $y \approx 0.188967$, for a minimum of approximately -8.32369, and yet the sum

$$\sum_{q_v<n} R(x_v,y_v) = \frac{(-9.96+o(1))n}{\ln n}.$$

So it is impossible for $x_v y_v$ to always be ≥ -1.57, and therefore $a_{2,\min} \leq -1.57+2 = 0.43$. And each asymptotic above is invariant under $(x,y) \to (-x,y)$, so a mirror polynomial proves that $a_{2,\max} \geq 3.57$. (A more precise polynomial proves that $a_{2,\min} \leq 0.421451779353951$, and as in Theorem 1.4.1 we can find points (x,y) and probabilities that prohibit any further improvements.) □

CHAPTER 2
FORMS COMING FROM DIHEDRAL REPRESENTATIONS

2.1 Introduction

Let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}(2, \overline{\mathbb{F}}_2)$ be a finite-image two-dimensional mod 2 Galois representation. (Here and for the rest of this thesis, we assume all representations, finite or not, are continuous.) We say $\overline{\rho}$ is dihedral if the image of $\pi \circ \overline{\rho} : G_{\mathbb{Q}} \to \mathrm{PGL}(2, \overline{\mathbb{F}}_2)$ is isomorphic to a finite dihedral group, where $\pi : \mathrm{GL}(2) \to \mathrm{PGL}(2)$ is the usual projection. We say $\overline{\rho}$ is modular of level N if it is the reduction of a representation ρ_f associated to a modular eigenform $f \in S_2(\Gamma_0(N), \overline{\mathbb{Z}}_2)$ mod the maximal ideal of $\overline{\mathbb{Z}}_2$ (call this ideal $\mathfrak{M}$). Here, ρ is associated to a normalized eigenform f if, for all $\ell \nmid 2N$, the coefficient a_ℓ equals the trace $\mathrm{Tr}\,\rho(\mathrm{Frob}_\ell)$. (When we write $S_2(\Gamma_0(N), R)$ we will always mean $S_2(\Gamma_0(N), \mathbb{Z}) \otimes R$, so for example we exclude Katz forms that are not reductions of characteristic 0 forms.) Additionally, reduction of a representation mod $\mathfrak{M}$ makes sense because given a characteristic 0 representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(V)$ where V is a vector space over $\overline{\mathbb{Q}}_2$, we may choose an invariant lattice isomorphic to $\overline{\mathbb{Z}}_2^2$ inside V, so that the image of ρ is inside $\mathrm{GL}_2(\overline{\mathbb{Z}}_2)$ and reduction mod $\mathfrak{M}$ is defined (independent of the choice of lattice up to semisimplification).

We say that ρ is ordinary at 2 if its restriction to the inertia at 2 is reducible. We also say a normalized eigenform f with coefficients in $\overline{\mathbb{Z}}_2$ is ordinary if the coefficient a_2 of q^2 in its q-expansion is a unit mod $\mathfrak{M}$. The terminology is consistent, because by theorems of Deligne and Fontaine, if $\rho = \rho_f$ is modular, then ρ_f is ordinary if and only if f is ordinary.

In [23], Kedlaya and Medvedovsky prove that if a characteristic 2 representation is dihedral, modular and ordinary of prime level N, then it must be the induction of a nontrivial odd-order character of the class group $\mathrm{Cl}(K)$ of a quadratic extension $K = \mathbb{Q}(\sqrt{\pm N})/\mathbb{Q}$ to $\mathbb{Q}$ [23, Section 5.2]. They then analyze all cases of $N \bmod 8$ to determine how many distinct mod 2 representations arise from this construction. Finally, they conjecture lower bounds for the number of $\overline{\mathbb{Z}}_2$ eigenforms whose mod $\mathfrak{M}$ representations $\overline{\rho}_f$ are isomorphic to each of the representations obtained above [23, Conjecture 13]. The purpose of the current chapter is to prove this conjecture, reproduced below.

We let $\mathbb{T}_2^{\mathrm{an}}$ denote the anemic Hecke algebra inside $\mathrm{End}(S_2(\Gamma_0(N), \overline{\mathbb{Z}}_2))$ generated as a $\mathbb{Z}_2$-algebra by the Hecke operators T_k for $(k, 2N) = 1$, and we let $\mathbb{T}_2$ denote the full Hecke algebra, namely $\mathbb{T}_2 = \mathbb{T}_2^{\mathrm{an}}[T_2, U_N]$. Ring homomorphisms $\mathbb{T}_2^{\mathrm{an}} \to \overline{\mathbb{F}}_2$ correspond to classes of mod 2 eigenforms, up to the coefficients of even and divisible-by-N powers of q, where the image of T_k is mapped to the coefficient a_k of the form. The kernel of such a map is a maximal ideal which determines the map up to Galois conjugation of the image. Thus maximal ideals of $\mathbb{T}_2^{\mathrm{an}}$ correspond to Galois-conjugate classes of modular representations via the Eichler-Shimura construction, and we attach properties of the representation such as ordinariness or reducibility to the maximal ideal, which are invariant under Galois-conjugation and hence well-defined properties of the ideal. We say that $\mathfrak{m}$ is K-dihedral if the representation corresponding to $\mathfrak{m}$ is dihedral in the above sense, and the quadratic extension from which it is an induction is K. (Notice that given $\overline{\rho}$, K is uniquely determined as the quadratic extension of $\mathbb{Q}$ inside the fixed field of the kernel of $\overline{\rho}$ that is ramified at all primes at which $\overline{\rho}$ is ramified.) We write $S_2(N)_{\mathfrak{m}} = S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)_{\mathfrak{m}}$ to denote the space of all mod 2 modular forms on which $\mathfrak{m}$ acts nilpotently.

Theorem 2.1.1 ([23, Conjecture 13])**.** *Let N be an odd prime and $\mathfrak{m}$ a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$.*

1. *Suppose $N \equiv 1 \bmod 8$.*

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

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

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

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

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

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

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

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

2.1.1 Reduction

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

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

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

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

and a similar statement for $\mathbb{T}_2^{\mathrm{an}}$, where $\mathbb{T}_{\mathfrak{a}}$ is the localization (or equivalently completion) of $\mathbb{T}_2$ at the ideal $\mathfrak{a}$. We thus study $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$ and remove the restriction that $\mathfrak{m}$ is nilpotent.

Proposition 2.1.2. *The dimension of* Λ *equals*

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

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

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

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

□

The trivial lower bound $\dim_{k_{\mathfrak{a}}} \mathbb{T}_{\mathfrak{a}}/(2) \geq 1$ gives a lower bound on the dimension of Λ. In the case that $\overline{\rho}$ arising from $\mathfrak{m}$ is totally real and absolutely irreducible, we prove a better bound $\dim_{k_{\mathfrak{a}}} \mathbb{T}_{\mathfrak{a}}/(2) \geq 2$. This happens when $\mathfrak{m}$ is $\mathbb{Q}(\sqrt{N})$-dihedral for $N > 0$. Let $J_0(N)$ denote the Jacobian of the modular curve $X_0(N)$, so that $\overline{\rho}$ appears as a subrepresentation of the 2-torsion points $J_0(N)[2]$. For some maximal ideal $\mathfrak{a}$ containing $\mathfrak{m}$, let $A = J_0(N)[\mathfrak{a}]$ be the subscheme of points that are killed by $\mathfrak{a}$. By the main result of [6], if $\overline{\rho}$ is absolutely irreducible, A is the direct sum of copies of $\overline{\rho}$.

Proposition 2.1.3. *If $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\text{an}}$ for which the corresponding representation $\overline{\rho}$ is absolutely irreducible and totally real, then for any maximal ideal $\mathfrak{a}$ of $\mathbb{T}_2$ containing $\mathfrak{m}$, we have the inequality*

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

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

Lemma 2.1.4. *If W denotes the Witt vector functor, then*

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

Proof. We follow [9, Section 3.2]. A proposition of Merel states that the real variety

$J_0(N)(\mathbb{R})$ is connected if N is prime [29, Proposition 5]. If g is the genus of $X_0(N)$, then we know that $J_0(N)(\mathbb{C}) = (\mathbb{R}/\mathbb{Z})^{2g}$, and therefore $J_0(N)(\mathbb{R}) = (\mathbb{R}/\mathbb{Z})^g$. And we also know that

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

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

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

A lemma of Mazur shows that the $\mathfrak{a}$-adic Tate module, $\varprojlim J_0(N)[\mathfrak{a}^i]$, is a $\mathbb{T}_{\mathfrak{a}}$-module of rank 2 [28, Lemma 7.7], and therefore a free $\mathbb{Z}_2$-module of rank $2g(\mathfrak{a})$, so $J_0(N)[\mathfrak{a}^\infty](\mathbb{C}) = (\mathbb{Q}_2/\mathbb{Z}_2)^{2g(\mathfrak{a})}$. We therefore know that the 2-torsion points of this scheme are

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

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

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

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

Taking dimensions on both sides gives

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

so equality must hold everywhere.

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

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

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

Returning to the proof of Proposition 2.1.3, we therefore know that

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

□

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

Theorem 2.1.5 ([45, Theorem 2])**.** *If ρ_f is an ordinary 2-adic representation corresponding to a weight 2 level $\Gamma_0(N)$ form f, then $\rho_f|_{D_2}$, the restriction of ρ_f to the decomposition group at a prime above 2, is of the shape*

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

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

2.2 $N \equiv 1 \bmod 8$

2.2.1 $K = \mathbb{Q}(\sqrt{N})$

Theorem 2.2.1. *If $N \equiv 1 \bmod 8$, and $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$ that is $\mathbb{Q}(\sqrt{N})$-dihedral, then* $\dim S_2(N)_\mathfrak{m} \geq 4$.

Proof. Let $K = \mathbb{Q}(\sqrt{N})$ and denote the fixed field of the kernel of $\overline{\rho}$ as L. In this K, the prime (2) factors as $\mathfrak{p}\mathfrak{q}$ for distinct $\mathfrak{p}$ and $\mathfrak{q}$, and $\overline{\rho}$ must be unramified at 2 so Frob_2, as a conjugacy class containing $\mathrm{Frob}_\mathfrak{p}$ and $\mathrm{Frob}_\mathfrak{q}$, must lie in $\mathrm{Gal}(L/K)$. Moreover, $\overline{\rho}$ must be semisimple at 2, because if $\overline{\rho} = \mathrm{Ind}_K^\mathbb{Q} \overline{\chi}$ for $\overline{\chi}$ a character of the unramified extension $\mathrm{Gal}(L/K)$, then $\overline{\rho}|_{\mathrm{Gal}(L/K)} = \overline{\chi} \oplus \overline{\chi}^g$ for some fixed $g \in \mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(L/K)$ and $\overline{\chi}^g(h) = \overline{\chi}(ghg^{-1})$ for $h \in \mathrm{Gal}(L/K)$.

Theorem 2.1.5 and this semisimplicity statement tell us that the decomposition group at 2 in the mod 2 representation looks like $\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix}$, because the cyclotomic character is always 1 mod 2. So we find that the polynomial $\det(x \,\mathrm{Id}_2 - \overline{\rho})$ has coefficients that are unramified at 2, and a_2 is a root of $P(x) := \det(x \,\mathrm{Id}_2 - \overline{\rho}(\mathrm{Frob}_2))$. There are thus three cases: either P has no roots already in $k := \mathbb{T}^{\mathrm{an}}/\mathfrak{m}$, or it has distinct roots lying in k, or it has a repeated root.

If P has no roots in k, then $[k_\mathfrak{a} : k] \geq 2$ for $\mathfrak{a}$ the extension of $\mathfrak{m}$, so Propositions 2.1.2 and 2.1.3 say that the dimension of the space is at least

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

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

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

Finally, suppose P has a double root. There is at least one maximal ideal $\mathfrak{a}$ of $\mathbb{T}_2$ above $\mathfrak{m}$. Because we know that $\overline{\rho}|_{D_2}$ is semisimple with determinant 1, the double root must be 1 and $\overline{\rho}|_{D_2}$ is trivial. Then Wiese proves that since all dihedral representations arise from Katz weight 1 modular forms (as Wiese proves in [42]), the multiplicity of $\overline{\rho}$ in A is 2 [43, Corollary 4.5]. In this case the dimension is at least

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

□

2.2.2 $K = \mathbb{Q}(\sqrt{-N})$

Theorem 2.2.2. *If $N \equiv 1 \bmod 8$, and $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$ that is $\mathbb{Q}(\sqrt{-N})$-dihedral, then $\dim S_2(N)_{\mathfrak{m}} \geq 2^e$ where $2^e = \big|\operatorname{Cl}(K)[2^\infty]\big|$.*

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

Proposition 2.2.3. *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with $d > 0$ squarefree.*

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

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

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

A proof of the final two parts can be found as [8, Proposition 4.1].

We return to the case $N \equiv 1 \bmod 8$. Proposition 2.2.3 tells us that the 2-part of the class group is cyclic so there is an unramified $\mathbb{Z}/(2^e)$-extension L'/K, say $\operatorname{Gal}(L'/K) = \langle g \rangle$ with $g^{2^e} = \mathrm{Id}$. If we as before denote by L the fixed field of the kernel of $\overline{\rho}$, and we let $M = L \cdot L'$, the character $\overline{\chi}$ of $\operatorname{Gal}(L/K)$ whose induction equals $\overline{\rho}$, and which is nontrivial by definition of a dihedral ideal, can be extended to a character $\overline{\chi}' : \operatorname{Gal}(M/K) \to \overline{\mathbb{F}}_2[x]/(x^{2^e} - 1)^\times$ given by mapping g to x. This can be done because $L \cap L' = K$, because $[L : K]$ is odd and $[L' : K]$ is a power of 2. Then the induction of $\overline{\chi}$ to $\overline{\rho}$ also extends from $\overline{\chi}'$ to $\overline{\rho}' : \operatorname{Gal}(M/\mathbb{Q}) \to$

$\mathrm{GL}_2(\overline{\mathbb{F}}_2[x]/(x^{2^e}-1))$. We will prove this representation is modular by describing a q-expansion with coefficients in $\overline{\mathbb{Z}}_2[x]/(x^{2^e}-1)$ whose reduction mod 2 gives the desired Frobenius traces as coefficients, and proving that the expansion is modular via the embeddings of this coefficient ring into $\mathbb{C}$. Then by the q-expansion principle we will have the result.

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

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

These are all finite image odd dihedral representations whose coefficients are algebraic and therefore may be compatibly embedded in $\mathbb{C}$. All twists of ρ_i are dihedral or nontrivial cyclic, and therefore all have analytic L-functions. So by the converse theorem of Weil and Langlands (see [31, Theorem 1], for instance), each ρ_i corresponds to a weight 1 eigenform f_i with level equal to the conductor of the representation and nebentypus equal to its determinant. Here, the conductor is $4N$ and the nebentypus is the nontrivial character of $\mathrm{Gal}(K/\mathbb{Q})$. This nebentypus, because K has discriminant $4N$, is the character $\lambda_{4N} := \lambda_4\lambda_N$ where λ_4 and λ_N are the nontrivial order 2 characters of $(\mathbb{Z}/4\mathbb{Z})^\times$ and $(\mathbb{Z}/N\mathbb{Z})^\times$; $\lambda_{4N}(p) = 1$ if and only if Frob_p is the identity in $\mathrm{Gal}(K/\mathbb{Q})$ if and only if p splits in K.

Each f_i is a simultaneous eigenvector for the entirety of the weight 1 Hecke algebra

$\mathbb{T}(4N)$, with coefficients in $\mathbb{Q}_2^{\mathrm{ur}}(\zeta_{2^i})$, so by returning to $\mathbb{Q}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$ we obtain a weight 1 form f with coefficients in this ring, which is therefore an eigenform by multiplicity 1 results. (Remember that we defined $S_1(\Gamma_0(4N), \mathbb{Q}_2^{\mathrm{ur}}[x]/(x^{2^e}-1))$ to equal $S_1(\Gamma_0(4N), \mathbb{Z}) \otimes \mathbb{Q}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$, so this eigenform is only a formal linear combination of holomorphic weight 1 forms with coefficients in $\mathbb{Q}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$, and may be better understood as corresponding to a ring map $\mathbb{T}(4N) \to \mathbb{Q}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$.) We can easily check that the traces of the representation $\rho' = \mathrm{Ind}_K^{\mathbb{Q}} \chi' : \mathrm{Gal}(M/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_2^{\mathrm{ur}}[x]/(x^{2^e}-1))$ correspond to the coefficients of f, and so since χ' and therefore ρ' are defined over $\mathbb{Z}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$, f also has coefficients in $\mathbb{Z}_2^{\mathrm{ur}}[x]/(x^{2^e}-1)$.

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

Lemma 2.2.4. *The q-expansion $\sum_{m,n\in\mathbb{Z}} q^{m^2+Nn^2}$ describes a (non-cuspidal) modular form g in $M_1(\Gamma_1(4N), \mathbb{Z}_2, \lambda_{4N})$.*

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

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

and

$$E^{\lambda_N,\lambda_4}(q) = \sum_{m=1}^{\infty} q^m \sum_{d \text{ odd}, \, de=m} (-1)^{(d-1)/2} \left(\frac{e}{N}\right)$$

respectively. The constant term of the former is, by the class number formula, equal to $h(-N)/2$ where $h(-N) = |\mathrm{Cl}(\mathbb{Q}(\sqrt{-N}))|$ is the class number of $\mathbb{Q}(\sqrt{-N})$. Otherwise, the forms are cusp forms f_δ with no constant term.

Lemma 2.2.5. *The q-expansion of f_δ is given by* $f_\delta = \sum_{m \geq 1} q^m \sum_{I \subseteq \mathcal{O}_K : N(I) = m} \delta(I)$.

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

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

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

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

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

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

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

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

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

As described in [9, Section 3.3], we may find a representation

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

in the following way: we let $\mathfrak{a}'$ denote the kernel of $\mathbb{T}(4N) \xrightarrow{\overline{\gamma}} \overline{\mathbb{F}}_2[x]/(x^{2^e}-1) \xrightarrow{x \mapsto 1} \overline{\mathbb{F}}_2$, and we let $\mathbb{T}(4N)_{\mathfrak{a}'}$ denote the completion of $\mathbb{T}(4N)$ with respect to that ideal. The Galois action on $J_0(4N)[\mathfrak{a}']$ breaks into isomorphic 2-dimensional representations $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}(4N)/\mathfrak{a}')$, and Carayol constructs a lift $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}(4N)_{\mathfrak{a}'})$ [10, Theorem 3]. We pushforward this map along $\mathbb{T}(4N)_{\mathfrak{a}'} \to \overline{\mathbb{F}}_2[x]/(x^{2^e} - 1)$ which also has full image to get a representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2[x]/(x^{2^e}-1))$. It's clear that this representation is isomorphic to $\overline{\rho}' = \mathrm{Ind}_K^{\mathbb{Q}} \overline{\chi}'$ by looking at traces. So $\overline{\rho}'$ is modular of level $\Gamma_0(4N)$.

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

Theorem 2.2.6 ([9, Theorem 3.14])**.** *If $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$ is a modular Galois representation of level $\Gamma_0(2N)$, such that*

1. *$\overline{\rho}$ is (absolutely) irreducible,*

2. *$\overline{\rho}$ is ordinary and ramified at 2, and*

3. *ρ is finite flat at 2,*

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

Our $\overline{\rho}'$, pushed forward through the map $\overline{\mathbb{F}}_2[x]/(x^{2^e} - 1) \to \overline{\mathbb{F}}_2$ and restricting to its true image, is irreducible, ordinary and ramified. All that remains in order to apply the theorem is to check that $\overline{\rho}'$ is finite flat at 2. It's enough to show this after restricting to $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2^{\mathrm{ur}})$. But the representation has only degree two ramification, so the image of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2^{\mathrm{ur}})$ is order 2. And furthermore, it's easy to see that it arises as the generic fiber of $D^{\oplus 2^e}$ over $\mathbb{Z}_2^{\mathrm{ur}}$, where D is the nontrivial extension of $\mathbb{Z}/2\mathbb{Z}$ by μ_2 discussed in [28, Proposition 4.2], represented for example by $\mathbb{Z}_2[x, y]/(x^2 - x, y^2 + 2x - 1)$ with comultiplication

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

So we may apply Theorem 2.2.6, and deduce that our modular form h is a modular form of level N.

We have therefore constructed a surjective map $\mathbb{T}_{\mathfrak{m}} \otimes_{\mathbb{Z}_2} \overline{\mathbb{F}}_2 \to \overline{\mathbb{F}}_2[x]/(x^{2^e} - 1)$, so the $\overline{\mathbb{F}}_2$-dimension of $S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)_{\mathfrak{m}}$ must be at least 2^e. Note that Proposition 2.2.3 shows that this dimension is at least 4. □

2.2.3 $\mathfrak{m}$ is reducible

Theorem 2.2.7. *If $N \equiv 1 \bmod 8$, and $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_2^{\mathrm{an}}(N)$ for which $\overline{\rho}_{\mathfrak{m}}$ is reducible, then* $\dim S_2(N)_{\mathfrak{m}} \geq \frac{h(-N)^{\mathrm{even}}-2}{2}$.

Proof. We know that $\mathfrak{m} \subseteq \mathbb{T}^{\mathrm{an}}$ is generated by T_ℓ and 2 for all primes $\ell \nmid 2N$. In [8, Corollary 4.9] and the discussion after Proposition 4.11, Calegari and Emerton prove that $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}/(2)$ must be isomorphic to $\mathbb{F}_2[x]/(x^{2^{e-1}})$, where $2^e = h(-N)^{\mathrm{even}}$. They accomplish this by setting up a deformation problem, namely deformations of $(\overline{V}, \overline{L}, \overline{\rho})$ where $\overline{\rho}$ is the mod 2 representation $\begin{pmatrix} 1 & \phi \\ 0 & 1 \end{pmatrix}$, ϕ is the additive character $G_{\mathbb{Q}} \to \mathbb{F}_2$ that arises as the nontrivial character of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, and $\overline{L}$ is a line in $\overline{V}$ not fixed by $G_{\mathbb{Q}}$. With the conditions set on the deformation, they find that it is representable by some $\mathbb{Z}_2$-algebra R.

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

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

[23] partially prove this theorem using [8], doing the case of $N \equiv 9 \bmod 16$. As we see, the method works equally well for $N \equiv 1 \bmod 16$. The only difference between the two cases is that [8] prove that for $N \equiv 9 \bmod 16$, the Hecke algebra $\mathbb{T}^{\text{an}}_{\mathfrak{m}}$ is a discrete valuation ring, and therefore a domain, but that plays no role here.

2.3 $N \equiv 5 \bmod 8$

2.3.1 $K = \mathbb{Q}(\sqrt{N})$

Theorem 2.3.1. *If* $N \equiv 5 \bmod 8$, *and* $\mathfrak{m}$ *is a maximal ideal of* $\mathbb{T}^{\text{an}}_2(N)$ *that is* $\mathbb{Q}(\sqrt{N})$*-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 4$.

Proof. Because 2 is inert in $\mathbb{Q}(\sqrt{N})$, we know that $\overline{\rho}|_{D_2}$ is of size 2. Then the image of $\overline{\rho}$ is a subgroup of a 2-Sylow subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$, and therefore is isomorphic to an upper-triangular idempotent representation $\overline{\rho}|_{D_2} \simeq \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. If we compare to Theorem 2.1.5, we find that in an eigenform for all T_p including T_2 that corresponds to this representation, $a_2 = 1$. So the three methods of section 2.2.1 do not work.

Recall Proposition 2.1.3 that says if the representation $\overline{\rho}$ is totally real, then $\dim_{k_{\mathfrak{a}}} \mathbb{T}_{\mathfrak{a}}/(2) \geq 2 \cdot$multiplicity of $\overline{\rho}$, so if this multiplicity is at least 2 inside $J_0(N)[\mathfrak{a}]$ for some $\mathfrak{a}$ containing $\mathfrak{m}$, we're done. So we assume that $\overline{\rho}$ occurs once in every $J_0(N)[\mathfrak{a}]$. However, we know by [43, Theorem 4.4] that since $\overline{\rho}$ comes from a Katz modular form of weight 1 and level N, and the multiplicity of $\overline{\rho}$ on $J_0(N)[\mathfrak{a}]$ is 1, that the multiplicity of $\overline{\rho}$ in $J_0(N)[\mathfrak{m}]$ is 2. So by Propositions 2.1.2 and 2.1.3, we know the dimension of $\mathbb{T}_{\mathfrak{m}}/(2)$ has dimension at least twice 2, or dimension 4, and so $\dim S_2(N)_{\mathfrak{m}} \geq 4$ as required. □

2.3.2 $K = \mathbb{Q}(\sqrt{-N})$

Theorem 2.3.2. *If* $N \equiv 5 \bmod 8$*, and* $\mathfrak{m}$ *is a maximal ideal of* $\mathbb{T}_2^{\mathrm{an}}(N)$ *that is* $\mathbb{Q}(\sqrt{-N})$*-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 2$.

This follows in a similar way to Theorem 2.2.2. Proposition 2.2.3 proves that the 2 part of the class group of K is order 2, so applying the results of section 2.2.2 proves the theorem in this case. The only difficulties are in verifying the conditions of Theorem 2.2.6; that is, $\overline{\rho}$ is absolutely irreducible, ordinary, and ramified, and ρ itself is finite flat at 2. It's clear that the first three conditions hold, and the final condition holds because $\mathbb{Q}_2^{\mathrm{ur}}(\sqrt{-N}) = \mathbb{Q}_2^{\mathrm{ur}}(i)$ even though $N \equiv 5 \bmod 8$, as $\mathbb{Q}_2(\sqrt{N}) = \mathbb{Q}_2(\sqrt{5})$ is unramified over $\mathbb{Q}_2$. So the group scheme in this case is the same as the group scheme in section 2.2.2, and we have verified all necessary conditions.

2.4 $N \equiv 3 \bmod 4$

2.4.1 $K = \mathbb{Q}(\sqrt{N})$

Theorem 2.4.1. *If* $N \equiv 3 \bmod 4$*, and* $\mathfrak{m}$ *is a maximal ideal of* $\mathbb{T}_2^{\mathrm{an}}(N)$ *that is* $\mathbb{Q}(\sqrt{N})$*-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 2$.

Proof. We let $\mathfrak{a}$ be a prime of $\mathbb{T}_2$ containing $\mathfrak{m}$. Then again recalling Proposition 2.1.3, since K and therefore $\overline{\rho}$ are totally real, we calculate that the dimension is at least

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

as required. □

2.4.2 $K = \mathbb{Q}(\sqrt{-N})$

Theorem 2.4.2. *If* $N \equiv 3 \bmod 4$*, and* $\mathfrak{m}$ *is a maximal ideal of* $\mathbb{T}_2^{\mathrm{an}}(N)$ *that is* $\mathbb{Q}(\sqrt{-N})$*-dihedral, then* $\dim S_2(N)_{\mathfrak{m}} \geq 4$.

Proof. This was shown in [23, Proposition 14] using essentially the same method as we use in sections 2.2.2 and 2.3.2. The only differences are that $K/\mathbb{Q}$ is unramified at 2 so the Artin conductor of $\overline{\rho}'$ is N, not $4N$, so no level-lowering is required; and that we obtain a second eigenspace from our modular form f coming from the reduction of f^2. □

2.5 The effect of U_N

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

Lemma 2.5.1. *There is an inclusion $U_N \in \mathbb{T}_2^{\mathrm{an}}$, so $\mathbb{T}_2 = \mathbb{T}_2^{\mathrm{an}}[T_2]$.*

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

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

denote the residual representation associated to $\mathfrak{m}$. If $\overline{\rho}$ is not irreducible, then it is Eisenstein. The Eisenstein ideal $\mathfrak{I} \subseteq \mathbb{T}_2$ is generated by $1 + \ell - T_\ell$ for $\ell \neq N$ and by $U_N - 1$. Let $\mathfrak{a} = (2, \mathfrak{I})$ denote the corresponding maximal ideal of $\mathbb{T}_2$. By [28, Proposition 17.1], the ideal $\mathfrak{a}$ is actually generated by $\eta_\ell := 1 + \ell - T_\ell$ for a suitable good prime $\ell \neq 2, N$. But this implies that $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}} = \mathbb{T}_{\mathfrak{a}}$ and that U_N (and T_2) lie in $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$. Hence we assume that $\overline{\rho}$ is irreducible.

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

Tate proved in [37] the following theorem:

Theorem 2.5.2 (Tate)**.** *Let G be the Galois group of a finite extension $K/\mathbb{Q}$ which is unramified at every odd prime. Suppose there is an embedding $\rho : G \hookrightarrow \mathrm{SL}_2(k)$,* *where k is a finite field of characteristic 2. Then $K \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ and $\operatorname{Tr} \rho(\sigma) = 0$ for each $\sigma \in G$.*

If $\overline{\rho}$ is unramified at N, then $\det \overline{\rho}$ is a character of odd order unramified outside 2, which by Kronecker-Weber must be trivial, so $\overline{\rho}$ maps to $\mathrm{SL}_2(k)$. We may apply Theorem 2.5.2 to determine that $\overline{\rho}$ has unipotent image, which therefore is not absolutely irreducible. Hence we may assume that $\overline{\rho}$ is ramified at N. By local-global compatibility at N, the image of inertia at N of $\overline{\rho}$ is unipotent. Because it is nontrivial, it thus has image of order exactly 2.

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

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

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

We claim that there exists a basis of $(\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}})^2$ such that

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

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

Now consider the image of σ. Writing

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

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

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

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

CHAPTER 3

THE INDEX OF $\mathbb{T}^{\mathrm{an}}$ IN $\mathbb{T}$

3.1 Introduction

Let N be a prime number and let $S_2(\Gamma_0(N), \mathbb{Z})$ denote the modular forms of weight 2 and level $\Gamma_0(N)$ with integer coefficients, and for any other ring R, we denote $S_2(\Gamma_0(N), R) = S_2(\Gamma_0(N), \mathbb{Z}) \otimes R$. If R is a characteristic p ring, we define the space $S_2(\Gamma_0(N), R)^{\mathrm{Katz}}$ to be the R-module of Katz forms as defined in [21, Section 1.2], and define similar notation for the spaces of weight 1 forms. For $N \nmid n$, let T_n denote the nth Hecke operator inside $\mathrm{End}(S_2(\Gamma_0(N), \overline{\mathbb{Z}}))$, and let U_N denote the Nth Hecke operator. We let $\mathbb{T}^{\mathrm{an}}$ denote $\mathbb{Z}[T_3, T_5, \ldots]$, the algebra generated by T_n for $(2N, n) = 1$, and we denote $\mathbb{T}^{\mathrm{an}}[T_2, U_N]$ by $\mathbb{T}$. The goal of this chapter is to compute the index of $\mathbb{T}^{\mathrm{an}}$ inside $\mathbb{T}$. Specifically, we prove the following theorem in sections 3.3 and 3.4:

Theorem 3.1.1. *The quotient $\mathbb{T}/\mathbb{T}^{\mathrm{an}}$ is purely 2-torsion, and*

$$\dim_{\mathbb{F}_2} \mathbb{T}/\mathbb{T}^{\mathrm{an}} = \dim_{\mathbb{F}_2} S_1(\Gamma_0(N), \mathbb{F}_2)^{\mathrm{Katz}}.$$

In other words, if $c = \dim_{\mathbb{F}_2} S_1(\Gamma_0(N), \mathbb{F}_2)^{\mathrm{Katz}}$ is the dimension of the weight 1 level $\Gamma_0(N)$ Katz forms over $\mathbb{F}_2$, then the index of $\mathbb{T}^{\mathrm{an}}$ in $\mathbb{T}$ is equal to 2^c.

The setup of this chapter is as follows. In section 3.2, we introduce some facts from the literature about modular forms and establish a duality theorem between modular forms and Hecke algebras. In section 3.3 we prove the first half of the theorem, that $\mathbb{T}^{\mathrm{an}}$ contains $2\mathbb{T}$ as submodules of $\mathbb{T}$, so the quotient $\mathbb{T}/\mathbb{T}^{\mathrm{an}}$ is purely 2-torsion. Then in section 3.4 we use a theorem of Katz to relate the extra elements of $\mathbb{T}$ to weight 1 modular forms using the duality, and finally establish the equality of Theorem 3.1.1 between dimensions. In section 3.5 we conclude with some examples, and some theorems and conjectures we propose based on the work of Cohen-Lenstra and Bhargava.

3.2 Preliminaries

3.2.1 From $\mathbb{Z}$ to $\mathbb{Z}_2$

We start by proving that $U_N \in \mathbb{T}^{\mathrm{an}}$, thereby reducing our work to considering $\mathbb{T}^{\mathrm{an}} \subseteq \mathbb{T}^{\mathrm{an}}[T_2]$.

Theorem 3.2.1. *$U_N \in \mathbb{T}^{\mathrm{an}}$.*

Proof. It is enough to check that $U_N \in \mathbb{T}^{\mathrm{an}} \otimes \mathbb{Z}_p$ for every p: if $\mathbb{T}^{\mathrm{an}}$ and $\mathbb{T}^{\mathrm{an}}[U_N]$ have different ranks as $\mathbb{Z}$-modules, then the $\mathbb{Z}_p$-ranks of $\mathbb{T}^{\mathrm{an}} \otimes \mathbb{Z}_p$ and $\mathbb{T}^{\mathrm{an}}[U_N] \otimes \mathbb{Z}_p = \mathbb{T}^{\mathrm{an}} \otimes \mathbb{Z}_p[U_N]$ are also different for every p, contradiction. On the other hand, if $\mathrm{rank}(\mathbb{T}^{\mathrm{an}}) = \mathrm{rank}(\mathbb{T}^{\mathrm{an}}[U_N])$, then the quotient $\mathbb{T}^{\mathrm{an}}[U_N]/\mathbb{T}^{\mathrm{an}}$ is finite. If it's nontrivial, then for any prime p dividing its order, there is a surjective map $(\mathbb{T}^{\mathrm{an}}[U_N] \otimes \mathbb{Z}_p)/(\mathbb{T}^{\mathrm{an}} \otimes \mathbb{Z}_p) \twoheadrightarrow (\mathbb{T}^{\mathrm{an}}[U_N]/\mathbb{T}^{\mathrm{an}}) \otimes \mathbb{Z}_p$ with nontrivial image. So for this p, $\mathbb{T}^{\mathrm{an}}[U_N] \otimes \mathbb{Z}_p \neq \mathbb{T}^{\mathrm{an}} \otimes \mathbb{Z}_p$. Therefore, we will only check whether $\mathbb{T}^{\mathrm{an}} \otimes \mathbb{Z}_p$ contains U_N. Further, as $\mathbb{T}^{\mathrm{an}} \otimes \mathbb{Z}_p$ is a complete semi-local ring, it splits as a direct sum of its completions at maximal ideals, so it's further enough to check that U_N is in $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$ for the completion $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$ at each maximal ideal $\mathfrak{m}$.

We proved as Lemma 2.5.1 that $U_N \in \mathbb{T}^{\text{an}} \otimes \mathbb{Z}_2 = \mathbb{T}_2^{\text{an}}$, so the statement is true for all maximal ideals over 2. So let ℓ be an odd prime, $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}^{\text{an}}$ over ℓ, and $\mathfrak{a}$ be a maximal ideal of $\mathbb{T}$ containing $\mathfrak{m}$.

Let $\mathbb{T}_{\mathfrak{a}}$ be the completion of $\mathbb{T}$ with respect to $\mathfrak{a}$, and let A be the integral closure of $\mathbb{T}_{\mathfrak{a}}$ over $\mathbb{Z}_\ell$, which can be written as $A = \oplus_i \mathcal{O}_i$ for $\mathcal{O}_i$ finite extensions of $\mathbb{Z}_\ell$. The maps

$$\pi_i : \mathbb{T} \to \mathbb{T}_{\mathfrak{a}} \to A \to \mathcal{O}_i$$

produce conjugacy classes of eigenforms with coefficients in $\mathcal{O}_i$, with the coefficient $a_{i,j}$ of q^j equal to $\pi_i(T_j)$ if $(j, N) = 1$, or $\pi_i(U_j)$ if $N|j$. These are newforms as N is prime, and there are no weight 2 level 1 forms. By Eichler-Deligne-Shimura-Serre there are representations $\rho_i : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_i)$, unramified away from ℓN, so that $\mathrm{Tr}(\rho_i(\mathrm{Frob}_\ell)) = a_{i,p}$ for all primes $p \nmid \ell N$.

[12, Theorem 3.1(e)] describes the shape of the local-at-N representation:

$$\rho_i|_{G_{\mathbb{Q}_N}} = \begin{pmatrix} \epsilon\chi & * \\ 0 & \chi \end{pmatrix}$$

where χ is the unramified representation taking Frob_N to $a_{i,N}$ and ϵ is the N-adic cyclotomic character. Additionally, $\det \rho_i = \epsilon$, so χ^2 is identically 1 and $a_{i,N}$ is equal to 1 or -1 for each i. We show that $a_{i,N}$ is equal among all i over all $\mathfrak{a}$ containing $\mathfrak{m}$, so that the image of U_N in $\mathbb{T}_{\mathfrak{a}}$ is constantly 1 or -1 over all $\mathfrak{a}$, and hence, in $\mathbb{T}_{\mathfrak{m}} = \oplus_{\mathfrak{m} \subseteq \mathfrak{a}} \mathbb{T}_{\mathfrak{a}}$, is inside $\mathbb{T}_{\mathfrak{m}}^{\text{an}}$.

By the Chebotarev density theorem, a representation is determined up to semisimplification and conjugation by its trace on the Frobenius elements of unramified primes. The $\rho_i(\mathrm{Frob}_p)$ have trace equal to $a_{i,p}$, which is the image of T_p under π_i. Because $\mathfrak{m}$ is contained in $\mathfrak{a}$ for all $\mathfrak{a}$, the image of T_p under reduction of $\mathbb{T}^{\mathrm{an}}$ mod $\mathfrak{m}$ is the same as the reduction of $a_{i,p}$ mod $\mathfrak{a}$. Therefore, the semisimplifications of the reductions of ρ_i over all i and all $\mathfrak{a}$ are all isomorphic. But we can deduce the value of $a_{i,N}$ from the reduction of ρ_i mod $\mathfrak{a}$, because $\rho_i|_{G_{\mathbb{Q}_N}}$ has an unramified quotient and a ramified subspace, and the same is true for the reduction mod $\mathfrak{a}$ as $\ell \neq 2$. So the image of the Frobenius on the unramified quotient is either 1 or -1 for one (and hence every) ρ_i, and therefore $a_{i,N}$ does not depend on i or $\mathfrak{a}$, only on $\mathfrak{m}$. So U_N lies in $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$ for all $\mathfrak{m}$, and we're done. □

We can now reduce from forms over $\overline{\mathbb{Z}}$ to forms over $\overline{\mathbb{Z}}_2$. With a similar argument to the proof of Theorem 3.2.1, we can check that T_2 is contained in all completions at maximal ideals of $\mathbb{T}^{\mathrm{an}}\left[\frac{1}{2}\right]$. This is true as 2 is unramified in, and T_2 is a trace of, the modular representations over primes other than 2, so Chebotarev and completeness of $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$ show that $T_2 \in \mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$. So only at the prime 2 are $\mathbb{T}$ and $\mathbb{T}^{\mathrm{an}}$ different. We can calculate the index of $\mathbb{T}^{\mathrm{an}} \otimes \mathbb{Z}_2$ inside $\mathbb{T} \otimes \mathbb{Z}_2$, and by abuse of notation begin to call these $\mathbb{T}^{\mathrm{an}}$ and $\mathbb{T}$ instead. We know that $\mathbb{T}$ and $\mathbb{T}^{\mathrm{an}}$ are semi-local rings, and as such, they can be written as a direct sum of their completions:

$$\mathbb{T} = \bigoplus_{\mathfrak{a} \subset \mathbb{T}} \mathbb{T}_{\mathfrak{a}}, \qquad \text{and} \qquad \mathbb{T}^{\mathrm{an}} = \bigoplus_{\mathfrak{m} \subset \mathbb{T}^{\mathrm{an}}} \mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}.$$

Additionally, because the $\mathbb{Z}_2$-ranks of $\mathbb{T}$ and $\mathbb{T}^{\mathrm{an}}$ are equal, $T_2 \in \mathbb{T} \otimes \mathbb{Q}_2 = \mathbb{T}^{\mathrm{an}} \otimes \mathbb{Q}_2 = \mathbb{T}^{\mathrm{an}}\left[\frac{1}{2}\right]$, and hence maps $\mathbb{T}^{\mathrm{an}} \to K$ where K is a finite extension of $\mathbb{Q}_2$

can be uniquely extended to maps $\mathbb{T} \to K$. This means that modular forms are rigid in characteristic 0: we can determine the image of T_2 from the image of the remaining operators, and hence from any modular representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(K)$ we may determine the entire form f. We say that ρ is ordinary if the restriction $\rho|_{D_2}$ of ρ to the decomposition group at 2 is reducible, and we say that an eigenform is ordinary if a_2 is a unit mod 2.

3.2.2 A Duality Theorem

In this section, we will compute the Pontryagin dual of one of the summands in $\mathbb{T}$ with the following lemma. Let $\mathfrak{a}$ be any maximal ideal of $\mathbb{T}$ and let

$$S_2(\Gamma_0(N), \mathbb{Z}_2)_{\mathfrak{a}} = e \cdot S_2(\Gamma_0(N), \mathbb{Z}_2)$$

where e is the projector $\mathbb{T} \to \mathbb{T}_{\mathfrak{a}}$.

Lemma 3.2.2. *The Pontryagin dual of* $\mathbb{T}_{\mathfrak{a}}$ *is* $M = \varinjlim S_2(\Gamma_0(N), \mathbb{Z}_2)_{\mathfrak{a}}/(2^n)$ *where the transition maps are multiplication by* 2*.*

Proof. First, we note that $\mathbb{T}_{\mathfrak{a}}$ acts on M because $\mathbb{T}_{\mathfrak{a}}$ acts compatibly on each level. If any element $T \in \mathbb{T}_{\mathfrak{a}}$ acts trivially on M, then on any given modular form in $S_2(\Gamma_0(N), \mathbb{Z}_2)_{\mathfrak{a}}$, it acts by arbitrarily high powers of 2, and hence acts as 0. Then T acts trivially on the rest of $S_2(\Gamma_0(N), \mathbb{Z}_2)$, so T is the 0 endomorphism. Therefore, M is a faithful $\mathbb{T}_{\mathfrak{a}}$-module.

We also know that $M[\mathfrak{a}]$, the elements of M killed by all of $\mathfrak{a}$, is a subspace of $S_2(\Gamma_0(N), \mathbb{Z}_2)_{\mathfrak{a}}/(2) = S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{a}}$. It is a vector space over $\mathbb{T}/\mathfrak{a}$, although through the action of $\mathbb{T}$, not by multiplication on the coefficients. We explain why it's a 1-dimensional $\mathbb{T}/\mathfrak{a}$-vector space. The map

$$S_2(\Gamma_0(N), \mathbb{F}_2) \to \operatorname{Hom}(\mathbb{T}, \mathbb{F}_2), \quad f \mapsto \phi_f : T_n \to a_n$$

is injective by the q-expansion principle. The forms killed by $\mathfrak{a}$ must correspond to maps factoring through $\mathbb{T}/\mathfrak{a}$, so the space of forms is at most the dimension of $\operatorname{Hom}(\mathbb{T}/\mathfrak{a}, \mathbb{F}_2) = \dim_{\mathbb{F}_2} \mathbb{T}/\mathfrak{a}$. So the dimension as a $\mathbb{T}/\mathfrak{a}$-vector space is at most 1.

On the other hand, there is at least 1 form in $M[\mathfrak{a}]$, because we may take the form $T_1 q + T_2 q^2 + T_3 q^3 + \ldots \in S_2(\Gamma_0(N), \mathbb{T}/\mathfrak{a})$ and consider its image under the trace map $\mathbb{T}/\mathfrak{a} \to \mathbb{F}_2$. This is nonzero because the trace map is nondegenerate, and because the Hecke operators generate $\mathbb{T}$ additively. This is in the kernel of $\mathfrak{a}$ because the trace of a form is just the sum of its conjugates, and for any expression in $\mathfrak{a}$ in terms of the Hecke operators with coefficients in $\mathbb{F}_2$, because its application to the original form is 0 by definition, its application to any of the form's conjugates must also be 0 (because the Hecke operators act $\mathbb{F}_2$-linearly on a form's coefficients and hence commute with Galois conjugation), and so too must its application to the sum. Because the trace form has coefficients in $\mathbb{F}_2$, we've found a nontrivial form in $M[\mathfrak{a}]$, and this must be dimension 1 as required.

We consider the Pontryagin dual of M: as M is a $\mathbb{Z}_2$-module, the image of any map $M \to \mathbb{Q}/\mathbb{Z}$ must land in $\mathbb{Q}_2/\mathbb{Z}_2$. So let $M^\vee = \operatorname{Hom}_{\mathbb{Z}_2}(M, \mathbb{Q}_2/\mathbb{Z}_2)$. We endow this with a $\mathbb{T}_\mathfrak{a}$-module structure by letting $(T\phi)(f) = \phi(Tf)$. Because $S_2(\Gamma_0(N), \mathbb{Z}_2)_\mathfrak{a} \simeq \mathbb{Z}_2^k$ for some k because it is torsion free, $M \simeq (\mathbb{Q}_2/\mathbb{Z}_2)^k$ as a $\mathbb{Z}_2$ module. So if $\phi(f) = 0$ for all $\phi \in M^\vee$, we know that $f = 0$. If $T\phi = 0$ for all ϕ, then $\phi(Tf) = 0$ for all ϕ and f, and so $Tf = 0$ for all f, and $T = 0$. So $M^\vee$ is also a faithful $\mathbb{T}_\mathfrak{a}$-module.

Further, $\mathbb{T}_\mathfrak{a}$ injects into $M^\vee$: we can rewrite

$$M = \varinjlim \frac{1}{2^n} S_2(\Gamma_0(N), \mathbb{Z}_2)_\mathfrak{a} / S_2(\Gamma_0(N), \mathbb{Z}_2)_\mathfrak{a}$$

where the transition maps are inclusion. Then the $\mathbb{T}_\mathfrak{a} \times M \to \mathbb{Q}_2/\mathbb{Z}_2$ as $(T, f) \to a_1(Tf)$ defines the injection. By Nakayama's lemma and the duality of $M[\mathfrak{a}]$ and $M^\vee/\mathfrak{a}$, the minimal number of generators of $M^\vee$ as a $\mathbb{T}_\mathfrak{a}$-module is 1. So we've proven that $M^\vee \simeq \mathbb{T}_\mathfrak{a}$. □

We may use Pontryagin Duality to find that the dual to $T_\mathfrak{a}/2 = M^\vee/2$ is $M[2]$, which is exactly $S_2(\Gamma_0(N), \mathbb{Z}_2)_\mathfrak{a}/(2) = S_2(\Gamma_0(N), \mathbb{F}_2)_\mathfrak{a}$. Thus we obtain a perfect pairing

$$T_\mathfrak{a}/2 \times S_2(\Gamma_0(N), \mathbb{F}_2)_\mathfrak{a} \to \mathbb{F}_2, \qquad (T, f) \to a_1(Tf).$$

We may sum these pairings over all $\mathfrak{a}$, because Hecke operators and forms with incompatible maximal ideals annihilate each other. Therefore we obtain a perfect pairing $\mathbb{T}/2 \times S_2(\Gamma_0(N), \mathbb{F}_2) \to \mathbb{F}_2$.

3.3 $2T_2$ is integral

In this section we prove the following lemma:

Lemma 3.3.1. *For any element $T \in \mathbb{T}$, the element $2T \in \mathbb{T}$ lies inside $\mathbb{T}^{\mathrm{an}}$.*

First we prove a lemma describing the image of the representation corresponding to a non-Eisenstein ideal.

Lemma 3.3.2. *Suppose* $\mathfrak{m}$ *does not contain the Eisenstein ideal. Then there is a representation*

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

that is unramified outside $2N$*, and which satisfies* $\mathrm{Tr}(\rho(\mathrm{Frob}_\ell)) = T_\ell$ *for* $\ell \nmid 2N$*.*

Proof. Let $A = \mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$ and A' is its integral closure over $\mathbb{Z}_2$, which can be written as the product $\prod_i \mathcal{O}_i$ of a collection of integer rings. We know that there exist representations $\rho'_i : G_{\mathbb{Q}} \to \prod_i \mathrm{GL}_2(\mathcal{O}_i)$, by Eichler-Shimura-Deligne-Serre. The image is $\mathrm{GL}_2(\mathcal{O}_i)$, because $G_{\mathbb{Q}}$ is compact, and we may choose an invariant lattice on which it acts. These ρ'_i combine to give a representation

$$\rho' = \prod_i \rho'_i : G_{\mathbb{Q}} \to \prod_i \mathrm{GL}_2(\mathcal{O}_i).$$

We know that the traces of the representations at Frob_ℓ are the images of T_ℓ for all $\ell \nmid pN$, so the trace of ρ' by Chebotarev Density always lands in $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$. We assumed $\mathfrak{m}$ did not contain the Eisenstein ideal, so we know that each ρ'_i, and therefore the full ρ', is residually irreducible. By [10, Theorem 2] we find that ρ' is similar to a representation

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

□

To prove Lemma 3.3.1, we look at the three different possible cases and deduce that the projection of $2T_2$ to $\mathbb{T}_{\mathfrak{a}}$ lies in $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$ for each $\mathfrak{m} \subseteq \mathfrak{a}$. Further, we prove that T_2^2 lies in $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}} \cdot T_2 + \mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$, so that any $T \in \mathbb{T}$, being an element in $\mathbb{T}^{\mathrm{an}}[T_2]$, lies in $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}} \cdot T_2 + \mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$ also, and hence is half of an element in $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$.

3.3.1 $\overline{\rho}$ ordinary irreducible

We first assume that the residual representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}/\mathfrak{m})$ is irreducible but the local residual representation at 2 is reducible. We will show that $2T_2$, as an element of $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}[T_2]$, actually lies in $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$. This will be done by proving it is in the ring generated over $\mathbb{Z}_2$ by the traces of ρ. Equivalently, we will look at the traces of $\rho \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$. This breaks the representation into a direct sum $\bigoplus_i \rho'_i \otimes \mathbb{Q}_2 : G_{\mathbb{Q}} \to \prod_i \mathrm{GL}_2(E_i)$. Each of the ρ'_i themselves have the same residual representation which is reducible when restricted to the decomposition group, so all these representations are ordinary.

Looking at a given ρ'_i, we may apply Theorem 2.1.5 to it to obtain a shape of $\rho'_i|_{D_2}$. In particular, the trace of an element $\rho(g)$ is equal to $\chi(g)\lambda^{-1}(g)+\lambda(g)$ with λ the unramified character whose image of Frobenius is the unit root of $X^2 - T_2X + 2$, and χ is the cyclotomic character. If α denotes the unit root of $x^2 - a_{2,i}x + 2 = 0$, then letting g be an element of $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{ab}}/\mathbb{Q}_2)$ which both is a lift of Frobenius and acts trivially on the 2-power roots of unity (so $\chi(g) = 1$), then we know $\mathrm{Tr}(g) = \alpha + \alpha^{-1}$. If we let h be a lift of Frobenius with $\chi(h) = -1$, we find that $\mathrm{Tr}(h) = \alpha - \alpha^{-1}$. And by definition, we know $\alpha + \frac{2}{\alpha} = a_{2,i}$, so $2a_{2,i} = 2\alpha + 4\alpha^{-1} = 3\,\mathrm{Tr}(g) - \mathrm{Tr}(h)$.

We now look at the product of representations. The elements g and h were independent of the coefficient field, so we know that the element of $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}} \otimes \mathbb{Q}_2$ that is $2a_{2,i}$ in each coordinate, namely $2T_2 \otimes 1$, is equal to $3\,\mathrm{Tr}(g) - \mathrm{Tr}(h)$. So $2T_2$ is in the ring generated by the traces of elements, and thus in $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$.

Similarly, we can prove that T_2^2 is in $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}} + T_2 \cdot \mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$: in each coordinate, we can calculate that

$$a_{2,i}^2 = \mathrm{Tr}(g)a_{2,i} + (\mathrm{Tr}(gh) - \mathrm{Tr}(g^2) - 1).$$

So in $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}[T_2]$, we find that $T_2^2 = \mathrm{Tr}(g)T_2 + (\mathrm{Tr}(gh) - \mathrm{Tr}(g^2) - 1)$. So $T_2^2 \subseteq \mathbb{T}_{\mathfrak{m}}^{\mathrm{an}} + T_2 \cdot \mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$, and therefore so is every power of T_2. So we know that $2\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}[T_2] \subseteq \mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$, and the $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$-module quotient $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}[T_2]/\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$ is an $\mathbb{F}_2$ vector space. In section 3.4 we will calculate its dimension.

3.3.2 $\overline{\rho}$ reducible

We now suppose $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$ corresponds to a reducible residual representation, so that $\mathfrak{m}$ is the Eisenstein ideal generated by 2 and T_ℓ for $\ell \nmid N$ (including $\ell = 2$). We claim that T_2 is already in $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$. This is because by [28, Proposition 17.1], the Eisenstein ideal of the full Hecke algebra is generated by $1 + \ell - T_\ell$ for any good prime. So by completeness, $T_2 - 3$ and therefore T_2 can be written as a power series in $T_\ell - \ell - 1$.

3.3.3 $\overline{\rho}$ non-ordinary

We now assume that the residual local representation at 2 is irreducible, or equivalently that in $\mathbb{T}_{\mathfrak{a}}$, T_2 is not a unit, where $\mathfrak{a}$ is some ideal of $\mathbb{T}$ above $\mathfrak{m}$ corresponding to ρ. We claim that T_2 is already in $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$, so that $\mathfrak{a} = \mathfrak{m}$ is actually unique, and the index is 1.

Theorem 3.3.3. *If ρ is non-ordinary with corresponding map $\mathbb{T}^{\mathrm{an}} \to \mathbb{F}$ with maximal ideal $\mathfrak{m}$, then for any $\mathfrak{a} \subseteq \mathbb{T}$ containing $\mathfrak{m}$, $T_2 \in \mathbb{T}_{\mathfrak{a}}$ is already contained in the image of $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$.*

Proof. The $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$-module $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}[T_2]$ requires the same generators as the $\mathbb{T}^{\mathrm{an}}/\mathfrak{m}$-vector space $\mathbb{T}/\mathfrak{m}\mathbb{T}$ by Nakayama's Lemma, so it's enough to prove that $\mathbb{T}/\mathfrak{m}\mathbb{T}$ is one-dimensional over $\mathbb{T}^{\mathrm{an}}/\mathfrak{m}$. If it's not, then all of $\mathbb{T}^{\mathrm{an}}/\mathfrak{m}$ and T_2 are independent over $\mathbb{F}_2$, so there is a homomorphism $\phi \in \mathrm{Hom}(\mathbb{T}/\mathfrak{m}\mathbb{T}, \mathbb{F}_2)$ sending all of $\mathbb{T}^{\mathrm{an}}/\mathfrak{m}$ to 0, and T_2 to 1. Recalling the perfect pairing after Lemma 3.2.2, we find a nonzero modular form $g \in S_2(\Gamma_0(N), \mathbb{F}_2)[\mathfrak{m}]$ with all odd coefficients equal to 0.

By part (3) of the main result of [22], we know that there is some nonzero form $f \in S_1(\Gamma_0(N), \mathbb{F}_2)^{\mathrm{Katz}}$ with $f^2 = g$. (Here, we're considering weight 1 Katz forms, and so the weight 2 forms we construct may be Katz forms as well. So if necessary we enlarge the spaces we're considering, but it doesn't affect the conclusion.) As forms with coefficients in $\mathbb{F}_2$ commute with the Frobenius endomorphism, $f(q^2)$ has the same q-expansion as g. If $\mathbb{T}^1$ and $\mathbb{T}^{1,\mathrm{an}}$ are the weight 1 Hecke algebras, it is quick to check that the corresponding Hecke actions on q-expansions of $\mathbb{T}^{1,\mathrm{an}}$ are identical to those of $\mathbb{T}^{\mathrm{an}}$. Therefore $f \in S_1(\Gamma_0(N), \mathbb{F}_2)^{\mathrm{Katz}}[\mathfrak{m}]$. Further, we know that f is alone in this space, by part (2) of [22]: any other form in $S_1(\Gamma_0(N), \mathbb{F}_2)^{\mathrm{Katz}}[\mathfrak{m}]$ has the same odd coefficients, so the difference between it and f has only even-power coefficients, and hence must be 0 by Katz's theorem. So f is also an eigenform for T_2 in weight 1, say with eigenvalue b_2.

So we've discovered that $S_2(\Gamma_0(N), \mathbb{F}_2)^{\mathrm{Katz}}[\mathfrak{m}]$ is at most 2 dimensional, spanned by Vf and Af. Here, V acts as $V\left(\sum_{n=1}^{\infty} a_n q^n\right) = \sum_{n=1}^{\infty} a_n q^{2n}$ on power series, so that $Vf = g$, and can either be a weight-doubling operator, as used in [22], or a level-doubling operator. Additionally, Af is the multiplication of f with the Hasse invariant A, which preserves q-expansions. We can hence calculate the action of T_2 on this space: we know that T_2 acts in weight 2 via $U + 2V$, where $U\left(\sum_{n=1}^{\infty} a_n q^n\right) = \sum_{n=1}^{\infty} a_{2n} q^n$, and in weight 1 as $U + \langle 2\rangle V$ with $\langle 2\rangle$ the diamond operator, which is identically 1 on mod 2 forms. Further, we can compute that $UVf = Af$, as V doubles each exponent and U halves it.

So we find

$$\begin{aligned}
&T_2(Vf) = UVf = Af \\
&T_2(Af) = U(Af) = A(Uf) = A(T_2 f - \langle 2\rangle Vf) = A(b_2 f) - \langle 2\rangle Vf
\end{aligned}$$

and the matrix for the T_2 action is $\begin{pmatrix} b_2 & -\langle 2\rangle \\ 1 & 0 \end{pmatrix}$. (In these computations, the distinction between the level-raising V and the weight-raising V has been blurred, because on q-expansions they are equal; we view both lines as equalities of weight 2 level $\Gamma_0(N)$ forms.) As $\langle 2\rangle$ is trivial, the determinant of this matrix is 1, so T_2 is invertible. This is impossible because the form was non-ordinary. So there cannot be such a form g, and $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}[T_2]$ requires only one generator as a $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$-module, as required. □

3.4 Dimension of $\mathbb{T}/\mathbb{T}^{\mathrm{an}}$

In this section we prove the second half of Theorem 3.1.1. It is enough to look locally, so we will localize at a maximal ideal $\mathfrak{m}$ of $\mathbb{T}^{\mathrm{an}}$. Because completion at only ordinary non-Eisenstein ideals have T_2 not immediately in $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$, we assume that $\mathfrak{m}$ is such an ideal.

3.4.1 Relating $\mathbb{T}/\mathbb{T}^{\mathrm{an}}$ to S_2

We first recall the perfect pairing $S_2(\Gamma_0(N), \mathbb{F}_2) \times \mathbb{T}/2 \to \mathbb{F}_2$, given by $(f, T) \to a_1(Tf)$. While proving this, we proved perfect pairings $S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{a}} \times \mathbb{T}_{\mathfrak{a}}/2 \to \mathbb{F}_2$, and we now combine all $\mathfrak{a}$ that contain $\mathfrak{m}$, to get a perfect pairing $S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}} \times \mathbb{T}_{\mathfrak{m}}/2 \to \mathbb{F}_2$ where we denote $\mathbb{T}_{\mathfrak{m}}$ as the localization of $\mathbb{T}$ at the (not necessarily maximal) ideal $\mathfrak{m}\mathbb{T}$, and $S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}} = e \cdot S_2(\Gamma_0(N), \mathbb{F}_2)$ for e the projection from $\mathbb{T}$ to $\mathbb{T}_{\mathfrak{m}}$. Considering the subspace of forms killed by $A\theta$, the operator defined in [22] which acts as $q\frac{d}{dq}$ on q-expansions and raises the weight by 3, it's clear that the entirety of $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}$ annihilates it under the pairing, and we wish to prove that this is the full annihilator. For ease of notation, let us write $V = \mathbb{T}_{\mathfrak{m}}/2\mathbb{T}_{\mathfrak{m}}$, $W = S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}}$, and $V' = \mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}/2\mathbb{T}_{\mathfrak{m}}$.

Lemma 3.4.1. *$S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}} \cap \operatorname{Ker} A\theta$ and $\mathbb{T}^{\mathrm{an}}_{\mathfrak{m}}/2\mathbb{T}_{\mathfrak{m}}$ are mutual annihilators in this perfect pairing.*

Proof. We've seen that they annihilate each other. Now suppose $f = \sum_{i=1}^{\infty} a_i q^i \in W$ is annihilated by all of V'. By the usual formula for the Hecke action on q-expansions, the coefficient of q^1 in $T_n f$ is a_n, so $a_n = 0$ for all odd n. Therefore $f \in S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}} \cap \operatorname{Ker} A\theta$, and we can call this space $\operatorname{Ann}(V')$. This is enough to show they are mutual annihilators by dimension count, but we'll prove the other direction as well.

The space $W/\operatorname{Ann}(V')$ is represented by sequences of odd-power coefficients that appear in forms in W. We first prove that the map $V' \to \operatorname{Hom}(W/\operatorname{Ann}(V'), \mathbb{F}_2)$ induced by the pairing is surjective. Given a map $\varphi \in \operatorname{Hom}(W/\operatorname{Ann}(V'), \mathbb{F}_2)$ whose input is sequences of odd-power coefficients, we can define a map φ' in the double dual of V' taking maps

$$\chi : V' \to \mathbb{F}_2 \text{ to } \varphi(\chi(T_1), \chi(T_3), \chi(T_5), \ldots).$$

This is the definition of φ' when $(\chi(T_1), \chi(T_3), \ldots)$ appears as the odd-power coefficients of a form. And then if we've not defined φ' on all of the dual of V', we can just extend it any way we want. But because V' is finite dimensional, this φ' determines an element $T_\varphi \in V'$ for which

$$\chi(T_\varphi) = \varphi'(\chi) = \varphi(\chi(T_1), \chi(T_3), \ldots).$$

Then because any sequence of coefficients $(a_1, a_3, \ldots)$ is given by a character $\chi_{(a_i)} : T_n \to a_n$ (the restriction of such a χ from $\mathbb{T}_{\mathfrak{a}}$, for example), the pairing truly does send T_φ to φ.

Now given T that sends all of $\operatorname{Ann}(V')$ to 0, Tf must only depend on the odd coefficients of f. But then $\varphi : f \to a_1(Tf)$ is an element of $\operatorname{Hom}(W/\operatorname{Ann}(V'), \mathbb{F}_2)$. So by surjectivity there is some element T' of V' with $a_1(Tf) = \varphi(f) = a_1(T'f)$ for all $f \in W/\operatorname{Ann}(V')$. Then $a_1((T - T')f)$ is 0 for all f either in $\operatorname{Ann}(V')$ or a lift of an element of $W/\operatorname{Ann}(V')$, and so in all of W. Because the pairing is perfect, $T = T' \in V'$ as we needed. □

Now that we know these are mutual annihilators, we obtain an isomorphism

$$V/V' \to \mathrm{Hom}(\mathrm{Ann}(V'), \mathbb{F}_2),$$

and taking dimensions and reinterpreting, we've proven that

$$\dim \mathbb{T}_{\mathfrak{m}}/\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}} = \dim S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}} \cap \operatorname{Ker} A\theta.$$

So we have proven the following.

Lemma 3.4.2. *The index of* $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$ *in* $\mathbb{T}_{\mathfrak{m}}$ *equals the order of* $S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}} \cap \operatorname{Ker} A\theta$.

3.4.2 Lifting from weight 1 to weight 2

Now we use the main theorem of [22] to find a subspace of $S_1(\Gamma_0(N), \mathbb{F}_2)^{\mathrm{Katz}}$ that maps under V to $S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}} \cap \operatorname{Ker} A\theta$. As in Section 3.3.3, we have $\mathbb{T}^{\mathrm{an}}$-equivariance, and so the maximal ideal $\mathfrak{m}$ has an exact analogue in $\mathbb{T}^{1,\mathrm{an}}$ and we land in the subspace $S_1(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}}^{\mathrm{Katz}}$. We may not obtain the whole subspace because, while Vf is in the kernel of $A\theta$ for all $f \in S_1(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}}^{\mathrm{Katz}}$, we don't know that it's a form that is the reduction of a $\mathbb{Z}_2$ form, which is what $\mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$ parametrizes. In this section we will prove that the space of Katz forms of weight 2 actually are all standard forms.

The first case is $N \equiv 3 \mod 4$, which was taken care of Edixhoven:

Theorem 3.4.3 ([14, Theorem 5.6])**.** *Let* $N \geq 5$ *be odd and divisible by a prime number* $q \equiv -1$ *modulo* 4 *(hence the stabilizers of the group* $\Gamma_0(N)/\{1, -1\}$ *acting on* *the upper half plane have odd order). Then $S_2(\Gamma_0(N), \mathbb{F}_2)^{\text{Katz}}$ and $\mathbb{F}_2 \otimes S_2(\Gamma_0(N), \mathbb{Z})$ are equal, and the localizations at non-Eisenstein maximal ideals of the algebras of endomorphisms of $S_2(\Gamma_0(N), \mathbb{F}_2)^{\text{Katz}}$ and $H^1_{\text{par}}(\Gamma_0(N), \mathbb{F}_2)$ generated by all T_n ($n \geq 1$) coincide: both are equal to that of $S_2(\Gamma_0(N), \mathbb{Z})$ tensored with $\mathbb{F}_2$.*

So for primes $N \equiv 3 \mod 4$, we've proven the equality in Theorem 3.1.1. For the remainder of this section we therefore assume $N \equiv 1 \mod 4$. Further, up until this point we've only worked with $\mathbb{F}_2$-forms, but we change coefficients to $\overline{\mathbb{F}}_2$ so that we can find eigenforms associated to each maximal ideal. Theorem 3.4.3 still applies as its proof in [14] can be extended to all finite extensions of $\mathbb{F}_2$.

Theorem 3.4.4. *There are no Katz forms that are not the reduction of a form in $S_2(\Gamma_0(N), \overline{\mathbb{Z}}_2)$. That is,*

$$S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)^{\text{Katz}} = S_2(\Gamma_0(N), \overline{\mathbb{F}}_2).$$

Proof. Let ℓ be an arbitrary prime that is 3 mod 4, and we will look at the space $S_2(\Gamma_0(N\ell), \overline{\mathbb{F}}_2)^{\text{Katz}}$. We can apply Theorem 3.4.3 to it and conclude that this space is exactly the characteristic 0 forms tensored with $\overline{\mathbb{F}}_2$, so we may drop the Katz superscript. Further, we know that all Katz forms of level $\Gamma_0(N)$ lie in this space. So we just need to know there are no extra level $\Gamma_0(N)$ forms within this space.

As $\mathbb{T}^{\text{Katz}} \otimes \overline{\mathbb{F}}_2$ can be broken into a direct sum of $\overline{\mathbb{F}}_2$-vector spaces on which the semi-simple action of each operator is by multiplication by a constant, we know $S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)^{\text{Katz}}$ can be written as a direct sum of generalized eigenspaces. If we show every generalized eigenform in $S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)^{\text{Katz}}$ is the reduction of a modular form from $S_2(\Gamma_0(N), \overline{\mathbb{Z}}_2)$, then we're done. So suppose f is a generalized Katz eigenform for all T_n, including T_2. Let the eigenvalue corresponding to T_ℓ equal a_ℓ; we will prove that if $f \notin S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)$, then $a_\ell = 0$.

There are two maps from $S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)^{\mathrm{Katz}}$ to $S_2(\Gamma_0(N\ell), \overline{\mathbb{F}}_2)$: the plain embedding with equality on q-expansions, and the map V_ℓ sending $f(q)$ to $f(q^\ell)$. We know $T_\ell = U_\ell + \ell V_\ell$ on q-expansions, so we find that

$$U_\ell(T_\ell - a_\ell) = U_\ell(U_\ell + \ell V_\ell - a_\ell) = U_\ell^2 - a_\ell U_\ell + \ell U_\ell V_\ell = U_\ell^2 - a_\ell U_\ell + \ell$$

as operators from $S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)^{\mathrm{Katz}}$ to $S_2(\Gamma_0(N\ell), \overline{\mathbb{F}}_2)$. Then because f is a generalized eigenform, we find

$$0 = (U_\ell^k(T_\ell - a_\ell)^k)f = U_\ell^{k-1}(U_\ell^2 - a_\ell U_\ell + \ell)(T_\ell - a_\ell)^{k-1} f = \ldots = (U_\ell^2 - a_\ell U_\ell + \ell)^k f.$$

If we factor $X^2 - a_\ell X + \ell$ as $(X - \alpha)(X - \beta)$ for some lift of a_ℓ, we've proven that $(U_\ell - \alpha)(U_\ell - \beta)$ acts topologically nilpotently on any lift of f (which exists by Theorem 3.4.4). This will eventually be used to prove that one of α or β, and hence both, reduce to 1 mod the maximal ideal of $\overline{\mathbb{Z}}_2$.

Lemma 3.4.5. *For any characteristic* 0 *newform* g *of level* $N\ell$*,* $U_\ell - 1$ *acts topologically nilpotently.*

Proof. The eigenform g gives us a representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_2)$. The shape of this representation at the decomposition group at ℓ is given by [12, Theorem 3.1(e)], as we recalled in the proof of Theorem 3.2.1, which says that

$$\rho|_{D_\ell} = \begin{pmatrix} \chi\varepsilon & * \\ 0 & \chi \end{pmatrix}$$

where χ is the unramified representation that sends Frob_ℓ to the U_ℓ-eigenvalue of g, and ε is the 2-adic cyclotomic character. Because the determinant is the 2-adic cyclotomic character as well, we know that $\chi^2 = 1$, so the U_ℓ-eigenvalue of g is ± 1. So $U_\ell - 1$ is either 0 or -2, which both act nilpotently. □

If $\alpha - 1$ and $\beta - 1$ have valuation 0, then $(U_\ell - \alpha)(U_\ell - \beta)$ will not act nilpotently on any linear combination of eigenforms which includes at least one newform, by Lemma 3.4.5. As $(U_\ell - \alpha)(U_\ell - \beta)$ acts nilpotently on a lift of f, we know that this lift is a linear combinaton of only oldforms, and hence f lifts to $S_2(\Gamma_0(N), \overline{\mathbb{Z}}_2)$. Otherwise, one of α and β, and hence both, are 1 mod the maximal ideal of $\overline{\mathbb{Z}}_2$, and so $\alpha + \beta \equiv 0 \equiv a_\ell$.

Therefore, we have proven that if f is a generalized eigenform in $S_2(\Gamma_0(N), \overline{\mathbb{F}}_2)^{\mathrm{Katz}}$ that has no lift to characteristic 0, then $a_\ell = 0$ for any prime $\ell \equiv 3 \mod 4$, as our choice of ℓ was arbitrary. Letting g be a true eigenform in the same eigenspace as f, we obtain a representation $\overline{\rho}_g : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ with $\mathrm{Tr}(\rho_g(\mathrm{Frob}_p)) = a_p$. We showed that $\overline{\rho}_g$ has trace 0 on all Frob_ℓ, so it must be the induction of a character from $G_{\mathbb{Q}(i)}$ to $G_{\mathbb{Q}}$. But such a representation is dihedral in the terminology of [23], and [23, Theorem 12(1)] proves that it's impossible for a dihedral representation on $G_{\mathbb{Q}(i)}$ to give rise to a form of level $\Gamma_0(N)$. So there can be no Katz eigenforms of level $\Gamma_0(N)$ that don't lift, and hence no generalized eigenforms and therefore no forms at all. □

From this, we conclude that all the forms $V_2 f$, where f is a weight 1 form of level N, are classical forms, and so the dimension of the space $S_2(\Gamma_0(N), \mathbb{F}_2)_\mathfrak{m} \cap \operatorname{Ker} A\theta$ is exactly the dimension $S_1(\Gamma_0(N), \mathbb{F}_2)_\mathfrak{m}^{\mathrm{Katz}}$. And so from Lemma 3.4.2, taking a direct sum over all $\mathfrak{m}$, we obtain Theorem 3.1.1.

3.5 Examples

In this section we use Theorem 3.1.1 to make nontrivial observations about the index of $\mathbb{T}^{\mathrm{an}}$ inside $\mathbb{T}$.

3.5.1 $N \equiv 3 \bmod 4$

Lemma 3.5.1. *If $N \equiv 3 \bmod 4$ is prime, the anemic Hecke algebra $\mathbb{T}^{\mathrm{an}}$ is equal to the full algebra $\mathbb{T}$ if and only if the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-N}))$ is trivial.*

Proof. If $K = \mathbb{Q}(\sqrt{-N})$ has class number greater than 1, by Proposition 2.2.3(a), since the discriminant of K is $-N$ which is divisible by only a single prime, the 2-part of the class group of K is trivial, so $\mathrm{Cl}(K)$ has a nontrivial mod 2 multiplicative character which translates to an unramified mod 2 character χ of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Inducing this to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we get a dihedral representation with Artin conductor equal to N. Wiese proves in [42] that all dihedral representations give rise to Katz modular forms, and so the space $S_1(\Gamma_0(N), \mathbb{F}_2)^{\mathrm{Katz}}$ is nontrivial, and hence $\mathbb{T}^{\mathrm{an}} \subsetneq \mathbb{T}$.

This shows that if N is not $3, 7, 11, 19, 43, 67$ or 163 (and is still a 3 mod 4 prime), $\mathbb{T}^{\mathrm{an}}(N) \subsetneq \mathbb{T}(N)$. On the other hand, for $N = 3$ and $N = 7$ there are no modular forms of weight 2, and for the other N, computer verification using the techniques of modular symbols, such as described in [35], provides the following table:

N	T_2
11	$-2T_1$
19	0
43	$-2T_1 - 2T_3 + T_5$
67	$T_3 - T_{11}$
163	$30T_1 - 16T_3 - 23T_5 - 9T_7 + 18T_9 + 3T_{11} - 24T_{13}$ $+12T_{15} + 40T_{17} - 16T_{19} - 14T_{21} - 9T_{23} + 2T_{25} + 32T_{27}$

Table 3.1: T_2 values in $\mathbb{T}^{\text{an}}$ for remaining N

These each prove that there are no Katz eigenforms of weight 1 and level N for any of these N, and in turn that there are no Galois representations that could provide such forms. Of course, we knew *a priori* there were no dihedral representations, as they would need to arise from the class group, but we now know that there are no larger-image representations. □

3.5.2 $N \equiv 1 \bmod 4$

Question 3.5.2. Is it true that for a positive proportion of prime $N \equiv 1 \bmod 4$, the anemic Hecke algebra $\mathbb{T}^{\text{an}}$ is not equal to the full algebra $\mathbb{T}$, and for a positive proportion of N, $\mathbb{T}^{\text{an}}$ is equal to $\mathbb{T}$?

We cannot immediately claim anything about the class group, because the Cohen-

Lenstra heuristics [11, C11] claim that approximately 75.446% of positive prime-discriminant quadratic extensions have trivial class group, so that there can be no dihedral modular forms.

The strong form of Serre's conjecture due to Edixhoven [13, Conjecture 1.8] is not known, where the strong form differs from the form proven by Khare and Wintenberger in [24] in this weight 1 case. A result of Wiese for dihedral representations [42] is known, and a converse (that the corresponding representation $\overline{\rho}$ is unramified at 2) has been proven [44, Corollary 1.3]. We may also use Theorem 3.1.1 to construct weight 1 forms in the case that the eigenvalues of Frob_2 in the characteristic 2 representation are distinct, because there are two possible values for a_2, implying that $\mathbb{T}_{\mathfrak{m}} \neq \mathbb{T}_{\mathfrak{m}}^{\mathrm{an}}$.

We also know the subgroups of $\mathrm{SL}_2(\overline{\mathbb{F}}_2)$, by Dickson, of four types: cyclic, upper-triangular, dihedral, and full-image (see [36, Chapter 3, Theorem 6.17]). We know a modular representation must be absolutely irreducible: if not, say f is a weight 1 form for which $\overline{\rho}_f$ is reducible. Then Af is a weight 2 form with the same representation, along with Vf in the same generalized eigenspace. But in Section 3.3.2 we proved that T_2 is already contained in the Hecke algebra corresponding to any eigenform with reducible representation, meaning that the dimension of $S_2(\Gamma_0(N), \mathbb{F}_2)_{\mathfrak{m}}$ is dimension 1, not 2. Therefore only absolutely irreducible representations can be modular, so only dihedral and full-image representations can exist. So assuming the strong version of Serre's conjecture, we know that for any weight 1 forms to exist at level N, we need either a dihedral extension of $\mathbb{Q}$, which must arise from inducing from the class group of $\mathbb{Q}(\sqrt{N})$, or we need an extension of $\mathbb{Q}$ unramified outside N with

Galois group isomorphic to $\mathrm{SL}_2(\mathbb{F}_{2^k})$ for some k.

Work has been done by Lipnowski [27] to interpret Bhargava's heuristics for the Galois group $\mathrm{GL}_2(\mathbb{F}_p)$ for p a prime, in order to count elliptic curves by their conductors through their p-adic representations. Although not done in this thesis, it appears tractable to similarly analyze the groups $\mathrm{SL}_2(\mathbb{F}_{2^k})$ and obtain a heuristic, explicit or not, on how many primes p have an elsewhere-unramified extension with each of these as their Galois groups. Because of the Cohen-Lenstra heuristics, it appears likely that infinitely many, even a positive proportion, of primes 1 mod 4 have no weight 1 forms, so $\mathbb{T} = \mathbb{T}^{\mathrm{an}}$, and a positive proportion of primes have some weight 1 form so $\mathbb{T}^{\mathrm{an}} \subsetneq \mathbb{T}$.

Explicit example: $N = 653$

An instructive example is that of $N = 653$. Of course this is 1 mod 4, and so any dihedral representation that would give a weight 1 form would have to come from an induction of the class group of $\mathbb{Q}(\sqrt{653})$, but the Minkowski bound is $\frac{1}{2}\sqrt{653} \approx 12.77$, and $2, 3, 5$ are inert and $7 = 230^2 - 653 \cdot 9^2$ and $-11 = 51^2 - 653 \cdot 2^2$ are norms of principal ideals. So $\mathbb{Q}(\sqrt{653})$ has class number 1. But the Galois closure L of the field $\mathbb{Q}[x]/(x^5 + 3x^3 - 6x^2 + 2x - 1)$ has Galois group $A_5 = \mathrm{SL}_2(\mathbb{F}_4)$, and is ramified only at 653 with ramification degree 2 and inertial degree 2. Therefore, Edixhoven predicts that the tautological Galois representation gives rise to a weight 1 level $\Gamma_0(653)$ modular form. This is not a classical form, as $\mathrm{SL}_2(\mathbb{F}_4)$ does not embed into $\mathrm{GL}_2(\mathbb{C})$, where all weight 1 characteristic 0 eigenforms must arise from.

On the other hand, $\mathrm{SL}_2(\mathbb{F}_4)$ does embed into $\mathrm{PGL}_2(\mathbb{C})$, and by a theorem of Tate, all projective Galois representations lift. We can follow the proof given by Serre in [31] to obtain a lift, unramified away from 653, and with Artin conductor 653^2. The fixed field of the kernel of this representation is a quadratic extension of $L[x]/(x^4 - x^3 + 82x^2 - 1102x + 13537)$, which is itself the compositum of L and the quartic subfield of the 653rd roots of unity. Locally at 653 it is a faithful representation of $\mathrm{Gal}(\mathbb{Q}_{653}(\sqrt[8]{653}, \sqrt{2})/\mathbb{Q}_{653})$, a Galois group isomorphic to $\langle x, y | x^8 = y^2 = e, yx = x^5 y\rangle$.

We therefore find that, as the Artin conjecture for odd representations has been proven in [24], an eigenform of weight 1 and level 653^2 that reduces to the characteristic 2 form of level 653 we found above. We can additionally twist by the nontrivial character of $\mathbb{Q}(\sqrt{653})/\mathbb{Q}$, not changing the determinant or level, to get a second Artin representation, and hence a second modular form of the same weight and nebentypus. These two eigenforms are congruent mod 2, so their average is also an integral form, and there is therefore a nilpotent element of the weight 1 mod 2 Hecke algebra, in a similar sense to [9, Lemma 3.8]. And conjugating the $\mathbb{F}_4$-forms, we obtain 2 more weight 1 forms of level 653. So the index of $\mathbb{T}^{\mathrm{an}}$ in $\mathbb{T}$ must be at least 16.

Indeed, we can find the following four (non-eigen)forms of weight 2 and level 653:

$$\begin{array}{rlllllll}
f_1 = 0q^1 & +1q^2 & +2q^3 & -4q^4 & +0q^5 & +2q^6 & +0q^7 \\
+4q^8 & +0q^9 & +4q^{10} & +0q^{11} & +1q^{12} & -6q^{13} & +\dots \\
f_2 = 0q^1 & +0q^2 & +2q^3 & -3q^4 & +0q^5 & +2q^6 & +2q^7 \\
+2q^8 & +4q^9 & -3q^{10} & +4q^{11} & -6q^{12} & +0q^{13} & +\dots \\
f_3 = 0q^1 & +0q^2 & +0q^3 & +4q^4 & +0q^5 & +1q^6 & +2q^7 \\
+2q^8 & +4q^9 & +5q^{10} & +2q^{11} & +0q^{12} & +4q^{13} & +\dots \\
f_4 = 0q^1 & -2q^2 & -6q^3 & +2q^4 & +0q^5 & +2q^6 & +2q^7 \\
-5q^8 & +0q^9 & +0q^{10} & -2q^{11} & -6q^{12} & -2q^{13} & +\dots
\end{array}$$

each of whose odd-power coefficients are all even, proving that none of T_2, T_4, T_6 or T_8 are in $\mathbb{T}^{\text{an}}$ plus the other 3. But a calculation up to the Sturm bound of 109 proves that there are no other modular forms with all odd-power coefficients and coefficients of q^2, q^4, q^6, q^8 all even but some other coefficient is odd. Therefore $\mathbb{T} = \mathbb{T}^{\text{an}} + 2\mathbb{T} + \langle T_2, T_4, T_6, T_8 \rangle$, so $\mathbb{T}/(2\mathbb{T} + \mathbb{T}^{\text{an}})$ is generated as an $\mathbb{F}_2$-vector space by T_2, T_4, T_6, T_8. By Lemma 3.3.1, $\mathbb{T}^{\text{an}}$ contains $2\mathbb{T}$, but from the above forms T_2, T_4, T_6, T_8 are independent in $\mathbb{T}/\mathbb{T}^{\text{an}}$ so the index of $\mathbb{T}^{\text{an}}$ in $\mathbb{T}$ must be exactly $2^4 = 16$.

REFERENCES

[1] Patrick Allen, Frank Calegari, Ana Caraiani, Toby Gee, David Helm, Bao Le Hung, James Newton, Peter Scholze, Richard Taylor, and Jack Thorne. Potential automorphy over CM fields. Preprint, 2018.

[2] James Arthur and Laurent Clozel. *Simple algebras, base change, and the advanced theory of the trace formula*, volume 120 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1989.

[3] Mahdi Asgari and A. Raghuram. A cuspidality criterion for the exterior square transfer of cusp forms on GL(4). In *On certain L-functions*, volume 13 of *Clay Math. Proc.*, pages 33–53. Amer. Math. Soc., Providence, RI, 2011.

[4] Thomas Barnet-Lamb, Toby Gee, David Geraghty, and Richard Taylor. Potential automorphy and change of weight. *Ann. of Math. (2)*, 179(2):501–609, 2014.

[5] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy II. *Publ. Res. Inst. Math. Sci.*, 47(1):29–98, 2011.

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

[7] George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni. Abelian surfaces over totally real fields are potentially modular. Preprint, 2018.

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

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

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

[11] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[12] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[13] Bas Edixhoven. Serre's conjecture. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 209–242. Springer, New York, 1997.

[14] Bas 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(1):1–34, 2006. With appendix A (in French) by Jean-François Mestre and appendix B by Gabor Wiese.

[15] Francesc Fité, Kiran S. Kedlaya, Ví ctor Rotger, and Andrew V. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.*, 148(5):1390–1442, 2012.

[16] Toby Gee and Olivier Taïbi. Arthur's multiplicity formula for GSp_4. preprint, 2018.

[17] Neven Grbac and Freydoon Shahidi. Endoscopic transfer for unitary groups and holomorphy of Asai L-functions. *Pacific J. Math.*, 276(1):185–211, 2015.

[18] Michael Harris. Potential automorphy of odd-dimensional symmetric powers of elliptic curves and applications. In *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. II*, volume 270 of *Progr. Math.*, pages 1–21. Birkhäuser Boston, Inc., Boston, MA, 2009.

[19] Michael Harris, Nick Shepherd-Barron, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy. *Ann. of Math. (2)*, 171(2):779–813, 2010.

[20] Christian Johansson. On the Sato-Tate conjecture for non-generic abelian surfaces. *Trans. Amer. Math. Soc.*, 369(9):6303–6325, 2017. With an appendix by Francesc Fité.

[21] Nicholas M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350, 1973.

[22] Nicholas M. Katz. A result on modular forms in characteristic p. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 53–61. Lecture Notes in Math., Vol. 601, 1977.

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

[24] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[25] Henry H. Kim. Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2. *J. Amer. Math. Soc.*, 16(1):139–183, 2003. With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak.

[26] Henry H. Kim and Freydoon Shahidi. Cuspidality of symmetric powers with applications. *Duke Math. J.*, 112(1):177–197, 2002.

[27] Michael Lipnowski. On bhargava's heuristics for $\mathbf{GL}_2(\mathbf{F}_p)$-number fields and the number of elliptic curves of bounded conductor. *arXiv preprint arXiv:1610.09467*, 2016.

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

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

[30] Kenneth A. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Algebra and topology 1992 (Taejŏn)*, pages 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.

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

[32] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[33] Jean-Pierre Serre. *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL, 2012.

[34] Freydoon Shahidi. On non-vanishing of twisted symmetric and exterior square L-functions for $\mathrm{GL}(n)$. *Pacific J. Math.*, (Special Issue):311–322, 1997. Olga Taussky-Todd: in memoriam.

[35] William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[36] Michio Suzuki. *Gun ron. Vol. 1*, volume 18 of *Gendai Sūgaku [Modern Mathematics]*. Iwanami Shoten, Tokyo, 1977.

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

[38] Noah Taylor. On Seven Conjectures of Kedlaya and Medvedovsky. Preprint, 2020.

[39] Noah Taylor. Sato-Tate distributions on Abelian surfaces. *Trans. Amer. Math. Soc.*, 373(5):3541–3559, 2020.

[40] Noah Taylor. The index of $\mathbb{T}^{\mathrm{an}}$ in $\mathbb{T}$, 2021.

[41] Richard Taylor. Remarks on a conjecture of Fontaine and Mazur. *J. Inst. Math. Jussieu*, 1(1):125–143, 2002.

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

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

[44] Gabor Wiese. On Galois representations of weight one. *Doc. Math.*, 19:689–707, 2014.

[45] A. Wiles. On ordinary λ-adic representations associated to modular forms. *Inventiones mathematicae*, 94(3):529–574, 1988.