COMPUTING CLASSICAL MODULAR FORMS

ALEX J. BEST, JONATHAN BOBER, ANDREW R. BOOKER, EDGAR COSTA, JOHN CREMONA, MAARTEN DERICKX, MIN LEE, DAVID LOWRY-DUDA, DAVID ROE, ANDREW V. SUTHERLAND, AND JOHN VOIGHT

Abstract. We discuss practical and some theoretical aspects of computing a database of classical modular forms in the L-functions and Modular Forms Database (LMFDB).

Contents

1. Introduction

1.1. **Motivation.** Databases of classical modular forms have been used for a variety of mathematical purposes and have almost a 50 year history (see §2). In this article, we report on a recent effort in this direction in the L-functions and Modular Forms Database (LMFDB [62], `https://lmfdb.org`); for more on the LMFDB, see the overview by Cremona [32].

1.2. **Organization.** The paper is organized as follows. In §2, we begin with a short history, and we follow this in §3 with a preliminary discussion of Dirichlet characters. Next, in §4 we make more explicit what we mean by computing (spaces of) modular forms, and then in section §5 we give a short overview of the many existing algorithmic approaches to computing modular forms. We pause in §6 to prove two technical results. In §7, we sample the available implementations and make some comparisons. Next, in §8 we discuss some computational, theoretical, and practical issues that arose in our efforts and in §9 we explain how we (rigorously) computed the L-functions attached to modular newforms. Turning to our main effort, in §10 we provide an overview of the computations we performed, make some remarks on the data obtained, and explain some of the features of our database. Finally, in §11 and §12 we treat twists and issues specific to modular forms of weight 1.

Date: November 12, 2022.

As is clear from this organization, we consider the algorithmic problem of computing modular forms from a variety of perspectives, so this paper need not be read linearly. For the convenience of readers, we draw attention here to a number of highlights:

- In §2, we survey the rather interesting history of computing databases of modular forms.
- In §3.2, we exhibit a labeling scheme for Dirichlet characters, due to Conrey.
- In Theorem 4.3.4, we record formulas for the new, old, and total dimensions of spaces of Eisenstein series of arbitrary integer weight $k \geq 2$, level, and character, obtained from work of Cohen–Oesterlé and Buzzard. (Such formulas are not available for weight $k = 1$.)
- In Corollary 6.1.5, we compute an Eichler–Selberg trace formula restricted to the space of newforms; this was used by Belabas–Cohen [4] in their implementation in Pari/GP.
- In Tables 7.1.1 and 7.1.2, we compare the implementations of Magma and Pari/GP; in Table 7.1.3 we note some computationally challenging newspaces.
- In §8.7, we show that by writing Hecke eigenvalues in terms of an LLL-reduced basis of the Hecke order, we can drastically reduce their total size.
- In §9.4, we certify analytic ranks of L-functions of modular forms and remark on the ranks occurring in our dataset.
- In §9.5, we numerically verify a generalization of Chowla's conjecture for central values of non-self-dual modular form L-functions.
- In §10.2, we present statistics on our data, and in §10.4 we note some interesting and extreme behavior that we observed in our dataset.
- In Theorems 11.2.4 and 11.2.8, we exhibit simple and effectively computable criteria for rigorously certifying that a modular form has an inner twist.
- In section 12.5, we highlight some interesting and extreme behavior found among weight 1 modular forms in our database.

1.3. **Acknowledgments.** The authors would like to thank Eran Assaf, Karim Belabas, Henri Cohen, Alan Lauder, David Loeffler, David Platt, Mark Watkins, and the anonymous referees for their comments. This research was undertaken as part of the *Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation*, with the support of Simons Collaboration Grants: 546235, to Brendan Hassett, supporting Lowry-Duda; 550023, to Jennifer Balakrishnan, supporting Best; 550029, to John Voight; and 550033, to Bjorn Poonen and Andrew V. Sutherland, supporting Costa, Derickx, and Roe. Additional support was provided by a Programme Grant from the UK Engineering and Physical Sciences Research Council (EPSRC) *LMF: L-functions and modular forms*, EPSRC reference EP/K034383/1.

2. History

In this section, we survey the history of computing tables of modular forms; for a broader but still computationally-oriented history, see Kilford [56, Section 7.1].

- Perhaps the first systematic tabulation of modular forms was performed by Wada [101, 102]. As early as 1971, he used the Eichler–Selberg trace formula to compute a factorization of the characteristic polynomial of the Hecke operator T_p on $S_2(\Gamma_0(q), \chi)$ for $q \equiv 1 \pmod 4$ prime where χ was either trivial or the quadratic character of conductor q. The total computation time was reported to be about 300 hours on a TOSBAC-3000.
- The next major step was made in the famous *Antwerp IV* tables [75] (published in 1975), motivated by the study of modularity of elliptic curves. Vélu and Stephens–Vélu computed

all newforms in $S_2(\Gamma_0(N))$ with $N \leq 200$ using modular symbols [75, Table 3] and these forms were matched with isogeny classes of elliptic curves over $\mathbb{Q}$ found by Swinnerton-Dyer. Tingley [99] computed the complete splitting into Hecke eigenspaces of $S_2(\Gamma_0(N))$ for $N \leq 300$, extending an earlier table due to Atkin. In particular he found the dimensions of the Atkin-Lehner eigenspaces, and computed the actual eigenvalues as floating point numbers, numerically matching conjugate newforms. By integrating differentials, he also computed elliptic curves from the newforms with integer eigenvalues. In some cases, this computation revealed the existence of elliptic curves not previously found by search. (According to Birch, this was the case for the elliptic curve with Antwerp label 78A and Cremona label 78a1; the curves in its isogeny class have rather large coefficients.)

- Extending the Antwerp IV tables, Cremona [30] (first edition published in 1992) computed a database of newforms in $S_2(\Gamma_0(N))$ with rational coefficients for $N \leq 1000$, providing also a wealth of data on the corresponding (modular) elliptic curves. In the second edition and in later computations, this data was considerably extended. A more recent report [31] was made on the elliptic curve tables to conductor 130 000, later extended to conductor 500 000 and rank at most 3. By 2016 this database had reached conductor 400 000, and in July 2019 Cremona and Sutherland extended it to conductor 500 000. In this range there are 2 164 260 rational newforms, and the same number of isogeny classes of elliptic curves.
- Miyake [71] published some numerical tables of modular forms as appendices in his book on modular forms; these were computed using the trace formula. These tables included dimensions of $S_k(\Gamma_0(N))$ for $k \geq 2$ even and small values of N, eigenvalues and characteristic polynomials of Hecke operators on $S_2(\Gamma_0(N))$ for small prime values of N, and Fourier coefficients of a primitive form in $S_2(\Gamma_0(N), \chi_N)$ for $N = 29, 37$.
- In the 1990s, Cohen, Skoruppa, and Zagier compiled tables of eigenforms in weights 2 through 12, levels up to 1000 in weight 2 and with a smaller range in higher weight; also some tables of eigenforms with non-trivial character. Their method followed a paper by Skoruppa and Zagier on the trace formula [91], but these tables were not published.
- In the early 2000s, Stein created an online modular forms database [92], computed primarily using a modular symbols package [93] he implemented in Magma [12] starting in the late 1990s. The data was computed using a rack of six custom-built machines and a Sun V480; it was stored in a PostgreSQL database (more than 10 GB), and a (Python-based) web interface to the data was provided. These tables included dimensions, characteristic polynomials, and q-expansions in a variety of weights and levels.
- Using this Magma implementation, Meyer [69, 70] computed a table of newforms for $\Gamma_0(N)$ with rational coefficients: in weight $k = 2$ he went to $N \leq 3000$ and for $k = 4$ to $N \leq 2000$.
- Prior to our work, the LMFDB had a database of classical modular forms computed by Ehlen and Strömberg [43], which used the SageMath [83] implementation of modular symbols. This dataset included partial information on $S_k(\Gamma_0(N))$ for (k, N) in the ranges $[2, 12] \times [1, 100]$ and $[2, 40] \times [1, 25]$, and on $S_k(\Gamma_1(N))$ in the ranges $[2, 10] \times [1, 50]$ and $[2, 20] \times [1, 16]$.

The scope of our modular forms database includes all of the ranges mentioned above (and more), with the exception of Cremona's tables of elliptic curves; see §10.1 for details.

3. Characters

Our database of modular forms is organized into subspaces identified by a level $N \in \mathbb{Z}_{\geq 1}$, a weight $k \in \mathbb{Z}_{\geq 1}$, and a character $\chi\colon \mathbb{Z} \to \mathbb{C}$ taking values in the cyclotomic field $\mathbb{Q}(\zeta_N)$. In order to identify these subspaces and the modular forms they contain, we adopt a standard convention for identifying Dirichlet characters that is well suited to computation, the Conrey labels recalled in §3.2

below. We also introduce a convention for identifying Galois orbits of Dirichlet characters that will be used to identify the newform subspaces and newform orbits defined in §4.

3.1. **Definitions.** For $N \in \mathbb{Z}_{\geq 1}$, a Dirichlet character of modulus N is a pair (χ, N) where $\chi\colon \mathbb{Z} \to \mathbb{C}$ is a periodic function modulo N that is the extension of a group homomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ by zero (defining $\chi(n) = 0$ whenever $\gcd(n, N) \neq 1$)—in particular, χ is totally multiplicative. The degree of a Dirichlet character χ is the degree of the cyclotomic subfield $\mathbb{Q}(\chi) \subseteq \mathbb{C}$ generated by the values of χ.

Given two Dirichlet characters χ, χ' of moduli N, N', we define their product $\chi\chi'$ to be the Dirichlet character of modulus $\operatorname{lcm}(N, N')$ defined by $(\chi\chi')(n) = \chi(n)\chi'(n)$. Under this definition, the set of Dirichlet characters of a fixed modulus N has the structure of a finite abelian group, with identity the principal (or trivial) character with $\chi(n) = 1$ if $\gcd(n, N) = 1$ and $\chi(n) = 0$ otherwise. The order $\operatorname{ord}(\chi)$ of a Dirichlet character χ is its order in this group, i.e., the smallest $m \in \mathbb{Z}_{\geq 1}$ such that χ^m is the principal character.

Let χ be a Dirichlet character of modulus N. Given a multiple N' of N, we may induce χ to a Dirichlet character χ' of modulus N' by $\chi'(n) := \chi(n \bmod N)$ whenever $\gcd(n, N') = 1$ and $\chi'(n) = 0$ otherwise. Consequently, there is a well-defined *minimal* modulus $M := \operatorname{cond}(\chi) \mid N$, called the conductor of χ, such that χ is induced from a Dirichlet character of modulus M. If $\operatorname{cond}(\chi) = N$, i.e., the conductor of χ is equal to its modulus, then we say that χ is a primitive character.

It is sometimes convenient to think about Dirichlet characters *without* a modulus, remembering only a periodic, totally multiplicative arithmetic function χ. In our context, Dirichlet characters arise from modular forms with level structure, so there should be little chance for confusion.

3.2. **Conrey labels.** We briefly describe a scheme, due to Brian Conrey, for labeling and computing with Dirichlet characters. Our labeling scheme can be thought of as a choice of an explicit isomorphism between two finite abelian groups: the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$ and the group of Dirichlet characters modulo N. In particular, our Dirichlet characters by definition take values in the complex numbers, so implicit in our choice of labels is a choice of embedding $\mathbb{Q}^{\mathrm{ab}} \hookrightarrow \mathbb{C}$.

For each $N \in \mathbb{Z}_{\geq 1}$, we will construct a function

$$\chi_N\colon (\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times \tag{3.2.1}$$

satisfying the following three properties:

- χ_N is multiplicative in each variable (separately);
- χ_N is symmetric (i.e., $\chi_N(m, n) = \chi_N(n, m)$ for all $m, n \in (\mathbb{Z}/N\mathbb{Z})^\times$); and
- χ_N is nondegenerate (i.e., if $\chi_N(m, n) = 1$ for all $m \in (\mathbb{Z}/N\mathbb{Z})^\times$, then $n \equiv 1 \pmod{N}$).

Moreover, χ_N will be multiplicative in N, and hence it is sufficient to define it for prime powers p^e and then extend $\chi_N(m, n)$ to general N by multiplicativity:

$$\chi_N(m, n) = \prod_{p^e \| N} \chi_{p^e}(m, n).$$

We use the notation $p^e \| N$ to mean that $p^e \mid N$ but $p^{e+1} \nmid N$. On the left side, m and n denote elements of $(\mathbb{Z}/N\mathbb{Z})^\times$, while on the right they denote the images of these in $(\mathbb{Z}/p^e\mathbb{Z})^\times$. We then extend χ_N to a multiplicative, periodic function on $\mathbb{Z} \times \mathbb{Z}$ by setting $\chi_N(m, n) = 0$ whenever $\gcd(mn, N) > 1$.

Under these conditions, fixing one input to χ_N defines a Dirichlet character modulo N and conversely every Dirichlet character arises in this way. Thus each Dirichlet character is given a unique name of the form $\chi_N(m, \cdot)$ for $m \in (\mathbb{Z}/N\mathbb{Z})^\times$. In particular, by symmetry, we see that $\chi_N(1, \cdot)$ is the trivial character modulo N, and $\chi_N(m, \cdot)$ is a quadratic character when $m \not\equiv$

1 (mod N) but $m^2 \equiv 1 \pmod{N}$. (More generally, the order of the character $\chi_N(m,\cdot)$ is the multiplicative order of m modulo N.)

We now describe the construction of χ_N.

Odd prime powers: Let p be an odd prime. Let g be the smallest positive integer that is a primitive root mod p^e for all $e \geq 1$. (This is almost always the same as the smallest primitive root mod p, but may not be; the only odd prime under one million for which these differ is 40487.) For $m \in (\mathbb{Z}/p^e\mathbb{Z})^\times$, we define $\log_g(m) \in \mathbb{Z}/\phi(p^e)\mathbb{Z}$ by the condition

$$m \equiv g^{\log_g(m)} \pmod{p^e}, \tag{3.2.2}$$

so that $\log_g\colon (\mathbb{Z}/p^e\mathbb{Z})^\times \to \mathbb{Z}/\phi(p^e)\mathbb{Z}$ is an isomorphism of groups.

For $m, n \in (\mathbb{Z}/p^e\mathbb{Z})^\times$, we then define

$$\chi_{p^e}(m,n) := \exp\left(2\pi i \frac{\log_g(m)\log_g(n)}{\varphi(p^e)}\right). \tag{3.2.3}$$

Then χ_{p^e} clearly satisfies the three required conditions (multiplicative, symmetric, and nondegenerate).

Powers of 2: We define χ_2 to be the trivial map (so $\chi_2(1,1) = 1$), and define

$$\chi_4(m,n) = (-1)^{(m-1)(n-1)/2} \tag{3.2.4}$$

for $m, n \in (\mathbb{Z}/4\mathbb{Z})^\times$. Let $e \geq 3$. The group $(\mathbb{Z}/2^e\mathbb{Z})^\times$ is generated by 5 and -1. For $m \in (\mathbb{Z}/2^e\mathbb{Z})^\times$, we define $\epsilon(m) \in \{0,1\}$ and $\log_5(m) \in \mathbb{Z}/2^{e-2}\mathbb{Z}$ by

$$m \equiv (-1)^{\epsilon(m)} 5^{\log_5(m)} \pmod{2^e} \tag{3.2.5}$$

so that now $(\epsilon, \log_5)\colon (\mathbb{Z}/2^e\mathbb{Z})^\times \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}$ is an isomorphism. For $m, n \in (\mathbb{Z}/2^e\mathbb{Z})^\times$, we then define

$$\chi_{2^e}(m,n) := \exp\left(2\pi i \frac{\epsilon(m)\epsilon(n)}{2} + 2\pi i \frac{\log_5(m)\log_5(n)}{2^{e-2}}\right). \tag{3.2.6}$$

As for the case of odd prime power modulus, this function satisfies the required properties.

In this article, as in the LMFDB, the Conrey label of the character $\chi_N(m,\cdot)$ has the form N.m. For example, the Conrey label of $\chi_7(6,\cdot)$, the unique quadratic character of modulus 7, is 7.6.

3.3. **Orbit labels.** There is an action of the absolute Galois group $\mathrm{Gal}_\mathbb{Q} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q})$ of $\mathbb{Q}$ on the set of Dirichlet characters of modulus N, defined by

$$(\sigma\chi)(n) := \sigma(\chi(n)) \tag{3.3.1}$$

for $\sigma \in \mathrm{Gal}_\mathbb{Q}$ and $n \in \mathbb{Z}$.

It is natural to organize characters by Galois orbits, and indeed we will also want to work with modular forms defined without an embedding into the complex numbers, specified up to the action of Galois (see §4.2). So we also assign an orbit label to each Galois orbit of Dirichlet characters, as follows. To choose this label we lexicographically order the sequences

$$\mathrm{ord}(\chi), \mathrm{Tr}\,\chi(1), \mathrm{Tr}\,\chi(2), \mathrm{Tr}\,\chi(3), \mathrm{Tr}\,\chi(4), \ldots$$

of integers, where $\mathrm{Tr}\colon \mathbb{Q}(\chi) \to \mathbb{Q}$ is the absolute trace; we then assign the label written in base 26 using the letters of the alphabet, so

$$\mathsf{a}, \mathsf{b}, \ldots, \mathsf{z}, \mathsf{ba}, \mathsf{bb}, \ldots, \mathsf{bz}, \mathsf{ca}, \ldots, \mathsf{zz}, \mathsf{baa}, \ldots.$$

For every modulus $N \geq 1$, the Dirichlet character orbit N.a is the trivial character, since it is the unique character with (smallest) order 1.

Example 3.3.2. The table below lists the Conrey labels of the eight Dirichlet characters of modulus 20, their values on the generators 11 and 17 of $(\mathbb{Z}/20\mathbb{Z})^\times$, their orders, the absolute traces of their values the first five positive integers coprime to 20 (note $\mathrm{Tr}(\chi(n)) = 0$ if $\gcd(20, n) \neq 1$), and the labels of the six Galois orbits in which they lie.

Conrey label	$\chi(11)$	$\chi(17)$	$\mathrm{ord}(\chi)$	$\mathrm{Tr}(\chi(1))$	$\mathrm{Tr}(\chi(3))$	$\mathrm{Tr}(\chi(7))$	$\mathrm{Tr}(\chi(11))$	$\mathrm{Tr}(\chi(13))$	orbit label
20.1	1	1	1	1	1	1	1	1	20.a
20.11	-1	1	2	1	-1	-1	1	-1	20.b
20.9	1	-1	2	1	-1	-1	1	1	20.c
20.19	-1	-1	2	1	1	1	1	-1	20.d
20.3	-1	$-i$	4	2	0	0	-2	-2	20.e
20.7	-1	i	4	2	0	0	-2	-2	20.e
20.13	1	$-i$	4	2	0	0	-2	2	20.f
20.17	1	i	4	2	0	0	-2	2	20.f

Remark 3.3.3. The field $\mathbb{Q}(\chi)$ is contained in the coefficient field $\mathbb{Q}(f)$ of a newform f with character χ. When the dimension of $\mathbb{Q}(f)$ is large it may be difficult to compute a complex embedding $\mathbb{Q}(f) \to \mathbb{C}$, and we often need to distinguish embeddings that are compatible with the Hecke action, which means we must know the image of $\mathbb{Q}(\chi)$ under embeddings of $\mathbb{Q}(f)$. Matching up roots of unity of large order can be surprisingly nontrivial! So when computing the coefficient field (as an abstract field, not necessarily embedded in the complex numbers), we compute the values of χ on generators for $(\mathbb{Z}/N\mathbb{Z})^\times$ as elements of the coefficient field. In this way, we may organize embeddings of the coefficient field according to a desired embedding of $\mathbb{Q}(\chi)$.

We could instead keep track of the coefficient field as an extension of $\mathbb{Q}(\chi)$, but that approach creates headaches when comparing results across implementations, it shifts the problem to a different place when working with forms in a Galois orbit, and it does not allow us to represent eigenvalues in terms of a nice LLL-reduced basis (see §8.7).

4. Computing modular forms

In this section, we make precise what it means to *compute modular forms*. For background, we refer to the wealth of references available, for example Cohen–Strömberg [26], Diamond–Shurman [39], Serre [86, Chapter VII], and Stein [93].

4.1. **Setup.** The group $\mathrm{SL}_2(\mathbb{R})$ acts (on the left) by linear fractional transformations on the upper half-plane $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}\, z > 0\}$. For $N \in \mathbb{Z}_{\geq 1}$, define the congruence subgroups

$$\begin{aligned} \Gamma_0(N) &:= \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}, \\ \Gamma_1(N) &:= \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}. \end{aligned} \tag{4.1.1}$$

For $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ a congruence subgroup, the quotient $Y(\Gamma) := \Gamma\backslash\mathcal{H}$ can be compactified to $X(\Gamma)$ by adding finitely many cusps, identified with the orbits of Γ on $\mathbb{P}^1(\mathbb{Q})$. As usual, we write $X_0(N), X_1(N)$ for the quotients $X(\Gamma)$ with $\Gamma = \Gamma_0(N), \Gamma_1(N)$.

For $k, N \in \mathbb{Z}_{\geq 1}$, a modular form of weight k and level N is a holomorphic function $f\colon \mathcal{H} \to \mathbb{C}$ that is bounded in vertical strips and satisfies

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \tag{4.1.2}$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$; the $\mathbb{C}$-vector space of such forms is denoted $M_k(\Gamma_1(N))$.

Modular forms are organized by character, as follows. The space $M_k(\Gamma_1(N))$ decomposes according to the action of diamond operators as

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi} M_k(\Gamma_0(N), \chi), \tag{4.1.3}$$

the sum being over all Dirichlet characters $\chi\colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ of modulus N, where $M_k(\Gamma_0(N), \chi)$ is the subspace of modular forms with (Nebentypus) character χ consisting of those forms f satisfying

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z) \tag{4.1.4}$$

for all $\gamma \in \Gamma_0(N)$. Throughout, we will abbreviate $M_k(\Gamma_0(N), \chi)$ to $M_k(N, \chi)$ and when χ is trivial, write simply $M_k(N)$.

In order to handle character values with some finesse (as explained above in §3 and below in §4.2), we work in the absolute situation (relative to $\mathbb{Q}$) and consider the entire Galois orbit $[\chi]$ of χ, and so we write

$$M_k(\Gamma_0(N), [\chi]) := \bigoplus_{\chi' \in [\chi]} M_k(\Gamma_0(N), \chi'), \tag{4.1.5}$$

so that from (4.1.3) we have

$$M_k(\Gamma_1(N)) = \bigoplus_{[\chi]} M_k(\Gamma_0(N), [\chi]),$$

where the direct sum is over Galois orbits of characters $[\chi]$. We similarly abbreviate $M_k(\Gamma_0(N), [\chi])$ to just $M_k(N, [\chi])$.

Every such modular form f has a q-expansion (i.e., Fourier expansion at ∞)

$$f(z) = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{C}[[q]], \tag{4.1.6}$$

where $q = \exp(2\pi i z)$ and $z \in \mathcal{H}$. We call $a_n \in \mathbb{C}$ the coefficients of f, and we write $\mathbb{Z}[\{a_n\}_n]$ for the coefficient ring and $\mathbb{Q}(\{a_n\}_n)$ for the coefficient field of f, the subring and subfield of $\mathbb{C}$ generated by its coefficients, respectively.

A modular form f is a cusp form if f vanishes at the cusps of $X_1(N)$. The subspace of cusp forms is denoted $S_k(\Gamma_1(N)) \subseteq M_k(\Gamma_1(N))$, and similarly $S_k(\Gamma_0(N), \chi) \subseteq M_k(\Gamma_0(N), \chi)$. In particular, a cusp form vanishes at the cusp ∞, so that the coefficient a_0 of its q-expansion is zero.

The Petersson inner product provides an orthogonal decomposition

$$M_k(\Gamma_0(N), \chi) = S_k(\Gamma_0(N), \chi) \oplus E_k(\Gamma_0(N), \chi) \tag{4.1.7}$$

where $E_k(\Gamma_0(N), \chi)$ is the space spanned by Eisenstein series, obtained in an explicit way using characters (see §4.4). Each of the spaces above can further be decomposed into old and new subspaces, and we denote the new subspace by $S_k^{\mathrm{new}}(\Gamma_1(N))$, etc.

The above spaces can be equipped with an action of *Hecke operators* T_n indexed by $n \in \mathbb{Z}_{\geq 1}$. The operators T_n are normal and pairwise commute for $\gcd(n, N) = 1$, so there is a common normalized ($a_1 = 1$) basis for the action of the Hecke operators, called eigenforms; for such forms, $T_n f = a_n f$ for f as in (4.1.6). A new cuspidal eigenform is called an (embedded) newform. The coefficients of a newform are algebraic integers and the coefficient field is a number field. When χ is trivial, this coefficient field is totally real. When χ is trivial, we also have Atkin–Lehner involutions W_p for $p \mid N$, and the Fricke involution $W_N := \prod_{p|N} W_p$. (See subsection 8.3 below.)

For a subring $A \subseteq \mathbb{C}$, we write $M_k(\Gamma_1(N); A) \subseteq M_k(\Gamma_1(N))$ for the A-submodule of modular forms whose q-expansions have coefficients in A, and similarly with the other decorated spaces.

From now on, we suppose we are given the input of a weight $k \in \mathbb{Z}_{\geq 1}$, a level $N \in \mathbb{Z}_{\geq 1}$, and an orbit of Dirichlet characters χ of modulus N and orbit label N.s; we encode this data of a space of modular forms in the label N.k.s.

Example 4.1.8. For $N = 280$, $k = 2$, and trivial character χ having label 280.a, the space $M_2(280) = M_2(\Gamma_0(280))$ has label 280.2.a.

Remark 4.1.9. We restrict ourselves to integral weight forms in this article. For forms of half-integral weight, the algorithms, applications, and issues that arise are quite different.

4.2. **Galois digression.** As is usual in Galois theory, it is convenient to work both with abstract objects as well as embedded objects. To this end, we call the $\mathrm{Aut}(\mathbb{C})$-orbit of an embedded newform f a newform orbit, and write $[f]$ for this orbit. We call a $\mathbb{Q}$-subspace of $S_k^{\mathrm{new}}(\Gamma_0(N), [\chi]; \mathbb{Q})$ that is irreducible under the action of the Hecke operators a newform subspace.

For an eigenform f in a newform subspace, we obtain an embedded newform by a choice of embedding of its coefficient field into $\mathbb{C}$, and all such embeddings are conjugate under $\mathrm{Aut}(\mathbb{C})$. Conversely, given an embedded newform $f \in S_k^{\mathrm{new}}(\Gamma_0(N), \chi)$, the $\mathbb{C}$-subspace of $S_k(\Gamma_0(N), [\chi])$ spanned by $\sigma(f) := \sum_n \sigma(a_n(f))q^n$ for $\sigma \in \mathrm{Aut}(\mathbb{C})$ descends to a newform subspace $V_f \subseteq S_k(\Gamma_0(N), [\chi]; \mathbb{Q})$, visibly depending only on the $\mathrm{Aut}(\mathbb{C})$-orbit of f. In other words, there is a bijection between newform subspaces $V \subseteq S_k^{\mathrm{new}}(\Gamma_1(N))$ and newform orbits $[f]$ of embedded newforms f of weight k and level N.

The coefficient field K of a newform subspace, defined to be the coefficient field of any eigenform in the subspace, is well-defined as an abstract number field. The expansion (4.1.6) considered in K, is similarly well-defined.

4.3. **Dimensions.** The first thing one may ask to compute for a space of modular forms is just dimensions of the subspaces as defined above: the total dimension $\dim_{\mathbb{C}} M_k(\Gamma_0(N), [\chi])$, the dimension of the Eisenstein subspace $\dim_{\mathbb{C}} E_k(\Gamma_0(N), [\chi])$, and the dimension of the cuspidal subspace $\dim_{\mathbb{C}} S_k(\Gamma_0(N), [\chi])$, as well as the old and new subspaces of each of these. Since these subspaces are naturally vector spaces over $\mathbb{Q}$, we have

$$\dim_{\mathbb{C}} M_k(\Gamma_0(N), [\chi]) = \dim_{\mathbb{Q}} M_k(\Gamma_0(N), [\chi]; \mathbb{Q});$$

moreover, an individual space $M_k(\Gamma_0(N), \chi)$ is a vector space over $\mathbb{Q}(\chi)$ and each summand in (4.1.5) has the same dimension, so these absolute dimensions are the product of their relative dimension by the degree $d = [\mathbb{Q}(\chi) : \mathbb{Q}]$ of χ, i.e., we also have

$$\dim_{\mathbb{C}} M_k(\Gamma_0(N), [\chi]) = \dim_{\mathbb{Q}(\chi)} M_k(\Gamma_0(N), \chi; \mathbb{Q}).$$

Remark 4.3.1. To avoid errors, to compare across packages, and to store data conveniently, we found it essential to compute in the absolute setting (over $\mathbb{Q}$) rather than the relative setting (over $\mathbb{Q}(\chi)$).

For weight $k \geq 2$, these dimensions can be computed using the valence formula, the Riemann–Roch theorem, or the trace formula—they are given explicitly e.g. by Cohen–Strömberg [26, Theorem 7.4.1]. Unfortunately, no formula is known for these dimensions when $k = 1$.

Because they can be understood explicitly in terms of Dirichlet characters, there are separately given formulas for the Eisenstein dimension as well as the dimension of the new and old subspaces in all weights $k \geq 1$: see Cohen–Strömberg [26, Propositions 8.5.15 and 8.5.21] for the full dimension, with the new dimension worked out by Buzzard [18] using a formula of Cohen–Oesterlé [25, Theorem 1] as follows. Lacking a reference for these formulas, we record them here.

For $r, s, p \in \mathbb{Z}$ with p prime and $r > 0$ and $s \leq r$, define

$$\lambda(r,s,p) := \begin{cases} p^{r'} + p^{r'-1}, & \text{if } 2s \leq r = 2r'; \\ 2p^{r'}, & \text{if } 2s \leq r = 2r' + 1; \\ 2p^{r-s}, & \text{if } 2s > r; \end{cases} \tag{4.3.2}$$

and

$$\lambda_{\mathrm{new}}(r,s,p) := \begin{cases} \left.\begin{matrix} 2 \\ 2p-4 \\ 2(p-1)^2 p^{r-s-2} \end{matrix}\right\} & \text{if } 2s > r \text{ and } \begin{cases} r = s; \\ r = s+1; \\ r \geq s+2; \end{cases} \\ \left.\begin{matrix} 0 \\ p-3 \\ (p-2)(p-1)p^{s-2} \end{matrix}\right\} & \text{if } 2s = r \text{ and } \begin{cases} p = 2; \\ r = 2 \text{ and } p \geq 3; \\ r \geq 4; \end{cases} \\ \left.\begin{matrix} 0 \\ p-2 \\ (p-1)^2 p^{r/2-2} \end{matrix}\right\} & \text{if } 2s < r \text{ and } \begin{cases} 2 \nmid r; \\ r = 2; \\ r \geq 4 \text{ and } 2 \mid r. \end{cases} \end{cases} \tag{4.3.3}$$

Theorem 4.3.4 (Cohen–Oesterlé, Buzzard)**.** *Let $N, k \in \mathbb{Z}_{\geq 1}$ and let χ be a character of modulus N and conductor $M \mid N$. Then the following statements hold:*

(a) *If $\chi(-1) \neq (-1)^k$, then $\dim_{\mathbb{C}} E_k(N,\chi) = \dim_{\mathbb{C}} E_k^{\mathrm{new}}(N,\chi) = 0$.*

(b) *For $N = 1$, we have*

$$\dim_{\mathbb{C}} E_k(1) = \dim_{\mathbb{C}} E_k^{\mathrm{new}}(1) = \begin{cases} 1, & \text{if } k \geq 4 \text{ and } 2 \mid k; \\ 0, & \text{otherwise.} \end{cases} \tag{4.3.5}$$

Suppose further that $N \geq 2$ and $\chi(-1) = (-1)^k$, and let

$$\begin{aligned} e &:= \prod_{p \mid N} \lambda(\mathrm{ord}_p(N), \mathrm{ord}_p(M), p) \\ e_{\mathrm{new}} &:= \prod_{p \mid N} \lambda_{\mathrm{new}}(\mathrm{ord}_p(N), \mathrm{ord}_p(M), p). \end{aligned} \tag{4.3.6}$$

Then the following hold:

(c) *We have*

$$\dim_{\mathbb{C}} E_k(N,\chi) = \begin{cases} e-1 & \text{if } k = 2 \text{ and } \chi \text{ is trivial;} \\ e/2 & \text{if } k = 1; \\ e & \text{otherwise.} \end{cases} \tag{4.3.7}$$

(d) *We have*

$$\dim_{\mathbb{C}} E_k^{\mathrm{new}}(N,\chi) = \begin{cases} e_{\mathrm{new}}+1 & \text{if } k = 2 \text{ and } \chi \text{ is trivial and } N \text{ is prime;} \\ e_{\mathrm{new}}/2 & \text{if } k = 1; \\ e_{\mathrm{new}} & \text{otherwise.} \end{cases} \tag{4.3.8}$$

(e) *We have*

$$\dim_{\mathbb{C}} E_k(N,[\chi]) = d \dim_{\mathbb{C}} E_k(N,\chi)$$

where $d = [\mathbb{Q}(\chi) : \mathbb{Q}]$ is the degree of χ, and similarly with $\dim_{\mathbb{C}} E_k^{\mathrm{new}}(N,[\chi])$.

Proof. The proof is an elaborate and rather tedious exercise in counting characters using the trace formula. □

We organize this dimension data in a table, as follows.

Example 4.3.9. We consider the space $M_3(560, [\chi])$ with label 560.3.bt; a character χ in this orbit has label 560.bt, order 6, and degree 2. We then compute dimensions as in Table 4.3.10.

	Total	New	Old
Modular forms	408	96	312
Cusp forms	360	96	264
Eisenstein series	48	0	48

Table 4.3.10: Dimensions for subspaces of $M_3(560, [\chi])$

One can also ask for the full trace form

$$\sum_{n=1}^{\infty} \mathrm{Tr}(T_n \mid S_k(N, [\chi]))q^n \in S_k(N, [\chi]; \mathbb{Z}) \tag{4.3.11}$$

on $S_k(N, [\chi])$ to some (q-adic) precision, with analogous definitions for the other subspaces considered above; see also (4.5.3) below.

4.4. **Eisenstein series.** Beyond dimensions, we may next ask for further information about the decomposition of the space $M_k(N, \chi)$. Of course the first step is the decomposition of the Eisenstein subspaces $E_k(N, \chi)$—for this purpose, explicit bases are given by Cohen–Strömberg [26, Theorems 8.5.17, 8.5.22, and 8.5.23].

Remark 4.4.1. We do not currently display an Eisenstein basis in the LMFDB.

4.5. **Decomposition of newspaces into Hecke orbits.** With the Eisenstein subspace described explicitly above, we now turn to the cuspidal subspace. By the newform theory of Atkin–Lehner [1] and Li [60], the multiplicity of the space $S_k^{\mathrm{new}}(M, \chi_M)$ in $S_k(N, \chi)$, is equal to the number of divisors of N/M (so depends only on the conductor and level). While it suffices to study the new subspace, it may be computationally expensive to determine $S_k^{\mathrm{new}}(N, \chi)$ as a subspace of $S_k(N, \chi)$; one way to do this is via projection operators called *degeneracy maps*, one for each prime divisor of N.

At this stage, for each newspace $S_k^{\mathrm{new}}(N, [\chi])$ we may first ask for just the dimensions of its newform subspaces V or Hecke orbits—see §8.5 below for a discussion of decomposition and irreducibility. When χ is trivial, we may also ask for the decomposition of the space under the Atkin–Lehner involutions and the Fricke involution.

Example 4.5.1. The space $S_2^{\mathrm{new}}(3111)$, with trivial character, has dimension 159; it decomposes into newspaces of dimensions $1 + 2 + 3 + 3 + 7 + 13 + 14 + 14 + 21 + 24 + 28 + 29 = 159$, and we have the following decomposition into subspaces under Atkin–Lehner operators:

3	17	61	Fricke	dimension	decomposition
+	+	+	+	13	$1+2+3+7$
+	+	−	−	29	29
+	−	+	−	24	$3+21$
+	−	−	+	14	14
−	+	+	−	24	24
−	+	−	+	14	14
−	−	+	+	13	13
−	−	−	−	28	28

Table 4.5.2: Dimensions for subspaces of $S_2^{\mathrm{new}}(3111)$

In practice, one computes this decomposition as follows. We first compute a $\mathbb{Q}(\chi)$-basis for $S_k^{\mathrm{new}}(N,\chi)$ in some manner, and then we compute the matrix of T_p on this basis for $p \nmid N$ for a few primes p in such a way that a small (finite) $\mathbb{Z}$-linear combination $\sum_p c_p T_p$ has squarefree characteristic polynomial. Therefore, the $\mathbb{Q}$-dimension decomposition is simply the degrees of the irreducible factors each multiplied by $[\mathbb{Q}(\chi):\mathbb{Q}]$. There seems to be no problem in practice finding such a small linear combination, but the best thing that we can say rigorously involves the Sturm bound and appears to be far from optimal. Already at this point engineering concerns enter: for example, the time to compute such a characteristic polynomial may be faster in certain implementations if done over $\mathbb{Q}$ instead.

With this basic decomposition data in hand, we may continue. For each newform orbit $[f] \leftrightarrow V$ (cf. §4.2) we wish to compute the following:

(1) The trace form

$$\mathrm{Tr}(f)(q) := \sum_{n=1}^{\infty} \mathrm{Tr}_{K|\mathbb{Q}}(a_n(f))q^n \in S_k(N,[\chi];\mathbb{Z}) \tag{4.5.3}$$

(well-defined on the Galois orbit $[f]$), where K is the coefficient field of f, to precision n up to the *Sturm bound* (see §8.2). Equivalently, writing $\mathrm{Tr}(f)(q) = \sum_n t_n q^n \in \mathbb{Z}[[q]]$, we have $t_n = \mathrm{Tr}(T_n \,|\, V)$ as the trace of the Hecke operator T_n restricted to V—see §8.6 for further discussion.

(2) A minimal polynomial for the coefficient field K of $[f]$.

(3) A finite set of generators for the Hecke kernel for V, the ideal in the Hecke algebra on $S_k^{\mathrm{new}}(N,\chi)$ that vanishes on V; i.e., a finite set of polynomials in T_n such that the ideal generated by these polynomials cuts out exactly V. (We use the Hecke kernel when computing inner twists: see §11.)

Although it is possible to compute coefficients of the trace form $\mathrm{Tr}(f)$ by computing coefficients of f and taking traces, this is more expensive than other techniques and is not computationally feasible in many cases where it is feasible to compute the trace form (e.g., using the trace formula: see section §5.2). The trace form conveniently records interesting information about the newform orbit, e.g., the coefficient t_1 of the trace form is equal to the dimension of the newform subspace.

Example 4.5.4. Consider the space $S_2(1166,[\chi])$ with label 1166.2.c, the character having order 2 and conductor $53 \mid 1166$. The old subspace decomposes as

$$S_2^{\mathrm{old}}(1166,[\chi]) \simeq S_2^{\mathrm{new}}(53,[\chi])^{\oplus 4} \oplus S_2^{\mathrm{new}}(106,[\chi])^{\oplus 2} \oplus S_2^{\mathrm{new}}(583,[\chi])^{\oplus 2}.$$

The decomposition of the new space $S_2^{\mathrm{new}}(1166, [\chi])$ into irreducibles by $\mathbb{Q}$-dimension is $46 = 2 + 22 + 22$, giving rise to three newform orbits 1166.2.c.a, 1166.2.c.b, 1166.2.c.c with respective trace forms

$$\begin{aligned} \mathrm{Tr}(f_{\mathsf{a}})(q) &= 2q - 2q^4 + 2q^6 - 8q^7 + 4q^9 + O(q^{10}) \\ \mathrm{Tr}(f_{\mathsf{b}})(q) &= 22q - 22q^4 - 6q^6 - 24q^9 + O(q^{10}) \\ \mathrm{Tr}(f_{\mathsf{c}})(q) &= 22q - 22q^4 + 4q^6 + 8q^7 - 34q^9 + O(q^{10}). \end{aligned} \tag{4.5.5}$$

We computed the last two trace forms *without* computing coefficients of a constituent newform (belonging to a number field of degree 22, or even determining what this number field is), which would have been much more time consuming. For the newform orbit $[f_{\mathsf{a}}]$, we determined that its coefficient field is $\mathbb{Q}(\sqrt{-1})$, that it can be constructed as the kernel of the linear operator $T_3^2 + 1$ acting on $S_2^{\mathrm{new}}(1166, [\chi])$, and then computed the first 1000 coefficients a_n of its q-expansion $\sum a_n q^n$ as elements of $\mathbb{Q}(\sqrt{-1})$.

4.6. **Hecke eigenvalues.** Finally, for a newform f, we can ask for the coefficients of f up to (at least) the Sturm bound. These coefficients can be represented either exactly or as complex numbers (approximately, e.g. using interval arithmetic).

- For exact coefficients, there are issues in representing them compactly: see §8.7 for our approaches.
- For the numerical (complex) coefficients a_n, the most useful for computing L-functions (see the next section), we ask for these coefficients for each embedded form in the newspace. These coefficients are of size $O(n^{(k-1)/2+\epsilon})$ for all $\epsilon > 0$, so in large weight we prefer to compute the normalized coefficients $a_n/n^{(k-1)/2}$, which by the Ramanujan–Petersson bounds have absolute value of size $O(n^{\epsilon})$.

For large degree coefficient fields, it is often practical to compute numerical coefficients even when storing exact coefficients would be impractical.

Finally, when the character is trivial, for the signs of the Atkin–Lehner involutions.

Example 4.6.1. Consider the newform orbit 5355.2.a.bf of dimension 3, with coefficient field $\mathbb{Q}(\nu)$ (LMFDB label 3.3.169.1) where ν is a root of the polynomial $x^3 - x^2 - 4x - 1$. The q-expansion of a newform f in this orbit, with coefficients in $\mathbb{Q}(\nu)$, is

$$f(q) = q + (1 - \beta_1)q^2 + (2 - \beta_1 + \beta_2)q^4 + q^5 + q^7 + (2 - \beta_1 + 2\beta_2)q^8 + O(q^{10})$$

where $\beta_1 = \nu$ and $\beta_2 = \nu^2 - \nu - 3$.

The 3 embedded newforms are labeled 5355.2.a.bf.1.m for $m = 1, 2, 3$ encoding the three embeddings $\iota_m \colon \mathbb{Q}(\nu) \hookrightarrow \mathbb{C}$; the embedded coefficients to 6 decimal digits are as follows:

Label	$\iota_m(\nu)$	a_2	a_3	a_4	a_5	a_6	a_7	a_8
1.1	2.65109	−1.65109	0	0.726109	1.00000	0	1.00000	2.10331
1.2	−0.273891	1.27389	0	−0.377203	1.00000	0	1.00000	−3.02830
1.3	−1.37720	2.37720	0	3.65109	1.00000	0	1.00000	3.92498

Table 4.6.2: Embedded newforms for 5355.2.a.bf.

4.7. ***L*-functions.** We can also ask for computations related to (invariants of) L-functions of modular forms, including the sign of the functional equation, the first few zeros, and special values to some precision: see §9 for more detail.

5. Algorithms

In this section, we give a brief overview of different algorithmic methods to compute modular forms and indicate where they are currently implemented. In our computations for the LMFDB, we only used the first two (modular symbols and the trace formula), but here we also survey the others. Our goal is to give a flavor of what each method entails, referring to the references provided for details. Throughout, we keep notation from the previous section.

5.1. **Modular symbols.** The most well-known method to compute modular forms is the method of *modular symbols*, introduced by Birch [6] and developed by Manin [63], Merel [67], Stein [93], and many others. For an extensive history, see Stein [93, 8.10.2], and for a gentle overview see Stein [94]. This method was implemented in Magma [12] by William Stein, with contributions by Steve Donnelly and Mark Watkins, and in SageMath [83] by William Stein, with contributions by David Loeffler, Craig Citro, Peter Bruin, Frédéric Chapoton, Alex Ghitza, and many others.

We now briefly introduce modular symbols. Assume $k \geq 2$. Integration gives a perfect pairing

$$\begin{aligned} S_k(\Gamma_1(N)) \times H_1(X_1(N), \mathbb{R}[x,y]_{k-2}) &\to \mathbb{C} \\ (f, \upsilon \otimes P) &\mapsto \int_\upsilon f(z)\, P(z,1)\, \mathrm{d}z \end{aligned} \tag{5.1.1}$$

where $\mathbb{R}[x,y]_{k-2}$ denotes the $\mathbb{R}$-vector space of homogeneous polynomials of degree $k-2$. In a slogan, (5.1.1) indicates that *the homology of a modular curve is dual to its cusp forms*, and this is formalized as follows. Let $\mathrm{Div}(\mathbb{P}^1(\mathbb{Q}))$ be the free abelian group on symbols $[\alpha]$ for $\alpha \in \mathbb{P}^1(\mathbb{Q})$, and let $\mathrm{Div}^0(\mathbb{P}^1(\mathbb{Q})) \leq \mathrm{Div}(\mathbb{P}^1(\mathbb{Q}))$ be the subgroup of degree zero elements under the natural degree map. Then $\mathrm{Div}^0(\mathbb{P}^1(\mathbb{Q}))$ is generated by elements $\{\alpha, \beta\} := [\alpha] - [\beta]$ for $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, written this way to suggest a path from α to β in $\mathbb{C}$. We define the space of modular symbols of weight k and level N (with $\mathbb{Q}$-coefficients) to be the quotient

$$\mathrm{ModSym}_k(\Gamma_1(N); \mathbb{Q}) := \frac{\mathbb{Q}[x,y]_{k-2} \otimes \mathrm{Div}^0(\mathbb{P}^1(\mathbb{Q}))}{\langle P \otimes \{\alpha,\beta\} - \gamma(P \otimes \{\alpha,\beta\}) \rangle_{\alpha,\beta \in \mathbb{P}^1(\mathbb{Q}), \gamma \in \Gamma_1(N)}}$$

under the natural action of $\Gamma_1(N) \leq \mathrm{SL}_2(\mathbb{Q})$. The space $\mathrm{ModSym}_k(\Gamma_1(N); \mathbb{Q})$ of modular symbols has moreover a natural action of Hecke operators and Atkin-Lehner operators.

Theorem 5.1.2. *There is a Hecke-equivariant isomorphism*

$$\mathrm{ModSym}_k(\Gamma_1(N); \mathbb{Q}) \xrightarrow{\sim} M_k(\Gamma_1(N); \mathbb{Q}) \oplus \overline{S}_k(\Gamma_1(N); \mathbb{Q})$$

where $\overline{S}_k(\Gamma_1(N); \mathbb{Q})$ denotes the space of anti-holomorphic cusp forms, the image of $S_k(\Gamma_1(N); \mathbb{Q})$ under complex conjugation.

Proof. See Manin [63], Merel [67], or Stein [93, §8.5]. □

Theorem 5.1.2 has many variants: one may restrict to $\Gamma_0(N)$, work with the (appropriately defined) space of *cuspidal* modular symbols as the kernel of a certain boundary map, carve out just $M_k(\Gamma_1(N); \mathbb{Q})$ as the $+$-space for a natural action of complex conjugation, and so on.

Example 5.1.3. For $\Gamma_0(N)$, the space of modular symbols has a convenient description in terms of *Manin symbols* as follows: $\mathrm{ModSym}_k(\Gamma_0(N); \mathbb{Q})$ is the $\mathbb{Q}$-vector space generated by the set Δ of elements $\delta = (x^i y^{k-2-i}, (c:d))$ for $i = 0, \ldots, k-2$ and $(c:d) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, modulo the subspace

$$\langle \delta + \delta S, \delta + \delta R + \delta R^2 \rangle_{\delta \in \Delta}$$

where $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $R = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$. The Hecke operators do not preserve Manin symbols, but there is an efficient procedure (arising from the Euclidean algorithm) for reducing an arbitrary element of $\mathrm{ModSym}_k(\Gamma_0(N); \mathbb{Q})$ to a linear combination of Manin symbols.

One feature of modular symbols is that they are especially well-suited for certain applications, including arithmetic invariants of elliptic curve quotients [31] (and more generally modular abelian varieties) as well as L-values of modular forms (see e.g. §9.4 below for an application). Moreover, modular symbols can be employed for arbitrary congruence subgroups (see [3] for an example).

In practice, it is quite efficient to compute the space of modular symbols with its Hecke action. It is a matter of sparse linear algebra to compute a basis of modular symbols, a negligible contribution. The number of field operations to compute the action of the Hecke operator T_n on this basis is $\widetilde{O}(nd)$, where d is the $\mathbb{Q}(\chi)$-dimension of the space under consideration: for each of the d basis elements, we sum the action of $\sigma_1(n) := \sum_{d|n} d = \widetilde{O}(n)$ cosets and reduce to the basis in time polynomial in $\log n$ using continued fractions. In this way, we may compute the q-expansions of a basis to precision $O(q^r)$ using $\widetilde{O}(dr^2)$ field operations, and thereby also the trace form.

The most difficult engineering effort that goes into a working implementation of modular symbols is the careful handling of linear algebra aspects: we apply degeneracy operators to obtain precisely the subspace $S_k^{\mathrm{new}}(N, \chi)$, and once the matrices $[T_n]$ representing the Hecke operators are computed on this space, we compute its decomposition into newform subspaces, etc. Indeed, in the preceding paragraphs, the actual *time* complexity of this method may depend on the output desired and the meaning of "arithmetic operation". If we wish for exact results, which is the approach taken by Magma and Pari/GP, then we need to do exact arithmetic with elements of cyclotomic fields, and the larger the order of the corresponding Dirichlet character, the more expensive the computation. Similarly, the coefficients of the newforms themselves may live in a large extension of the field of character values, and the larger this extension is, the harder the computation.

Remark 5.1.4. As alternatives, we may do all of the computations described using floating point approximations to complex numbers, for example using *complex ball arithmetic* to compute rigorous error bounds for all of the output. In this case, the degree of the field of coefficients of the modular form is irrelevant, and the time complexity matches the estimates above; this is particularly attractive if our application is to the computation of Dirichlet coefficients for input into L-function computations. Similar comments apply by doing computations over a finite field, for example working with coefficients over a finite field with prime cardinality congruent to 1 modulo the order of χ—in this case, we can do all computations over $\mathbb{F}_p$. In both cases, we must do some reconstruction to obtain exact results in characteristic zero.

The above description requires weight $k \geq 2$. For weight 1, there are two approaches that reduce the problem to higher weight. In the approach originated by Buhler [15], further developed by Buzzard [19], and carried out to scale by Buzzard–Lauder [20], we choose nonzero $f \in M_k(\Gamma_1(N))$ and consider $S_1(\Gamma_1(N)) \subseteq f^{-1}M_{k+1}(\Gamma_1(N))$. Intersecting the spaces obtained for many choices of f, we quickly obtain an upper bound for the space $S_1(\Gamma_1(N))$ that can then be matched with a lower bound. Using Buzzard's code, this method was implemented in Magma by Steve Donnelly. (Currently, Magma can provide a basis for the cuspidal subspace, but it does not decompose the space into the old and new subspace and does not provide the action of the Hecke operators; this was implemented by Buzzard–Lauder, but has not yet been incorporated into Magma.) A second related approach is to use the *Hecke stability* method of Schaeffer [84], instead computing the largest subspace of $f^{-1}M_{k+1}(\Gamma_1(N))$ that is stable under the Hecke operators; this has been implemented in SageMath by Schaeffer and Loeffler, and in Pari/GP by Belabas and Cohen [4, §4].

5.2. **Trace formula.** Perhaps the earliest method to compute modular forms used the *trace formula*. The trace formula is an explicit formula for the trace of a Hecke operator acting on a space of modular forms, and it was pioneered by Selberg [85] and later developed by Eichler [41], Hijikata [49], and Cohen–Oesterlé [25]. A comprehensive treatment with references is the book of Knightly–Li [59], and a tidy presentation is given by Schoof–van der Vlugt [89, Theorem 2.2].

Proofs of the trace formula from different vantage points continue to be developed, see e.g. Popa [78]. This method has been implemented in Pari/GP [76] by Belabas–Cohen [4] and in a standalone implementation by Bober, described in §7.2.

We again assume $k \geq 2$. An explicit version of the trace formula for $\mathrm{Tr}(T_n \mid S_k(\Gamma_0(N), \chi)) \in \mathbb{Q}(\chi)$ is too complicated to give here. Aside from easily computed terms, it can be naively understood as a weighted sum of (Hurwitz) class numbers of imaginary quadratic fields: for a precise statement, see e.g. Belabas–Cohen [4, Theorem 4]. We obtain $\mathrm{Tr}(T_n \mid S_k^{\mathrm{new}}(N, \chi))$ from a nontrivial application of the Möbius inversion formula, proven in Corollary 6.1.5 below.

Let $d := \dim_{\mathbb{Q}(\chi)} S_k^{\mathrm{new}}(N, \chi) = O(kN)$. The computation of $\mathrm{Tr}(T_n \mid S_k^{\mathrm{new}}(N, \chi))$ requires computing class numbers of imaginary quadratic fields with absolute discriminant up to $O(n)$, and one can compute all of these at once in time complexity $\widetilde{O}(n^{3/2})$. For the purposes of a large-scale computation, these class numbers are cached and may be assumed to be precomputed (their cost amortized over many computations, thereby negligible). Under this assumption, and given factorizations of n and N, to compute $\mathrm{Tr}(T_n \mid S_k^{\mathrm{new}}(N, \chi))$ we sum $O(\sqrt{n})$ terms giving a complexity of $O(\sqrt{n}N^{\epsilon})$ field operations for any $\epsilon > 0$; computing all traces up to $n > d$ then takes $\widetilde{O}(n^{3/2})$ field operations.

In this manner, we compute the relative trace form on the new cuspidal subspace

$$t(q) := \sum_{n=1}^{\infty} \mathrm{Tr}(T_n \mid S_k^{\mathrm{new}}(N, \chi))q^n \in S_k^{\mathrm{new}}(N, \chi; \mathbb{Z}[\chi]), \tag{5.2.1}$$

and from this we quickly compute the full trace form (4.3.11) in $S_k^{\mathrm{new}}(\Gamma_1(N); \mathbb{Z})$. In particular, using the trace formula method we can compute either trace form to precision $O(q^r)$ using $\widetilde{O}(r^{3/2}N^{\epsilon})$ field operations, which for $r > d$ becomes $\widetilde{O}(r^{3/2})$ as in the previous paragraph.

By multiplicity one theorems, and since the Hecke operators act semisimply on the newspace, the images of t under the Hecke operators span $S_k^{\mathrm{new}}(N, \chi)$. Explicitly, applying T_m to t, we obtain

$$(T_m t)(q) = \sum_{n=1}^{\infty} \mathrm{Tr}(T_m T_n \mid S_k^{\mathrm{new}}(N, \chi))q^n, \tag{5.2.2}$$

and the forms $T_1 t, T_2 t, \ldots$ span $S_k^{\mathrm{new}}(N, \chi)$. (We recall that $T_m T_n = T_{mn}$ when $\gcd(m, n) = 1$, and more generally a recursion for the Hecke operators applies. Therefore, these coefficients can again be expressed in terms of traces of Hecke operators.) Once we have a spanning set, we can extract a basis and apply Hecke operators to that basis.

Typically (in practice) we need $O(d)$ forms to span and $O(d)$ coefficients of each form to get a full rank matrix. Thus writing down a basis typically requires the first $O(d^2)$ values of $\mathrm{Tr}(T_n \mid S_k^{\mathrm{new}}(N, \chi))$, which can be computed using $O(d^3)$ field operations. Finding this basis—and the q-expansion to precision $\widetilde{O}(d)$ for each form—is standard linear algebra, accomplished using $\widetilde{O}(d^3)$ field operations. To compute the matrix of the Hecke operator T_n on this basis requires traces up to $O(nd)$ and so $\widetilde{O}(n^{3/2}d^{3/2})$ operations. Finally and similarly, to compute a basis of q-expansions to precision $O(q^r)$ with $r > d$, we compute traces up to $O(rd)$ and apply a change of basis, for a total of $\widetilde{O}(d^{3/2}r^{3/2})$ arithmetic operations.

We summarize the estimated complexity of these two approaches in Table 5.2.3, where again d is the $\mathbb{Q}(\chi)$-dimension of the space under consideration and we suppose precision $r > d$.

Task	Modular symbols	Trace formula
Full trace form to precision $O(q^r)$, $d = O(r)$	$\widetilde{O}(dr^2)$	$\widetilde{O}(r^{3/2})$
$[T_n]$ on a basis	$\widetilde{O}(dn)$	$\widetilde{O}(d^{3/2}n^{3/2} + d^3)$
Characteristic polynomial of T_n on a basis	$\widetilde{O}(dn + d^3)$	$\widetilde{O}(d^{3/2}n^{3/2} + d^3)$
Basis of q-expansions to precision $O(q^r)$, $d = O(r)$	$\widetilde{O}(dr^2)$	$\widetilde{O}(d^{3/2}r^{3/2})$
Hecke decomposition	$\widetilde{O}(d^3)$	$\widetilde{O}(d^3)$
Minimal polynomials for newspace coefficient fields	$\widetilde{O}(d^3)$	$\widetilde{O}(d^3)$

Table 5.2.3: Heuristic complexity of modular form computations

So although linear algebra eventually dominates both approaches, neither modular symbols nor the trace formula seems to be a winner for all tasks: it seems to be much better to use modular symbols to get information about a small number of Hecke operators, while it is much better to use the trace formula to get a large number of coefficients of a basis of newforms. This heuristic analysis matches our practical experience in the course of our computations.

Similar comments with reference to weight 1 forms apply as in the previous section. The same is true for the issue of time complexity and the coefficient field (see e.g. Remark 5.1.4), with the caveat that the matrices representing Hecke operators using modular symbols tend to be much sparser in comparison to those using the trace formula. In particular, one expects that taking advantage of sparsity will allow a more efficient implementation of the linear algebra aspects for modular symbols.

Remark 5.2.4. In some circumstances, it can be more convenient to work with a basis that is in echelon form with respect to q-expansions (sometimes called a *Victor Miller basis*) in the trace formula method. With such a basis, going back and forth between an action on q-expansions and the matrix form for various linear operators one can see some gains in efficiency.

5.3. **Definite methods.** In both of the previous algorithms, we work (either explicitly or implicitly) on the modular curve. In this section, we indicate another class of algorithms that compute systems of Hecke eigenvalues using a different underlying object.

Going back at least to Jacobi, surely the first modular forms studied were theta series. Let $Q(x) = Q(x_1, \dots, x_d) \in \mathbb{Z}[x_1, \dots, x_d]$ be a positive definite integral quadratic form in $d = 2k \in 2\mathbb{Z}_{\geq 1}$ variables with discriminant N. Let $P(x)$ be a (nonzero) spherical polynomial of degree $m \geq 0$ with respect to Q, for example $P(x) = 1$. We form the generating series for representations of $n \in \mathbb{Z}_{\geq 0}$ by Q weighted by P, a theta series of Q, by

$$\theta_{Q,P}(q) := \sum_{x \in \mathbb{Z}^d} P(x) q^{Q(x)}. \tag{5.3.1}$$

For example, if $P(x) = 1$, then

$$\theta_{Q,1}(q) = \sum_{n=0}^{\infty} r_Q(n) q^n \in \mathbb{Z}[[q]] \tag{5.3.2}$$

where $r_Q(n) = \#\{x \in \mathbb{Z}^d : Q(x) = n\}$ counts the number of representations of n by Q. By letting $q = e^{2\pi i z}$ for $z \in \mathcal{H}$ as usual, we obtain a holomorphic function $\theta_Q \colon \mathcal{H} \to \mathbb{C}$. Further, by an application of the Poisson summation formula (see e.g. Miyake [71, Corollary 4.9.5]), we find that $\theta_{P,Q} \in M_{k+m}(\Gamma_0(2N), \chi_N)$ is a classical modular form of weight $k + m$, level $2N$, and character $\chi_N(a) := \left(\frac{N}{a}\right)$ of order at most 2.

Turning this around, we can use theta series to compute spaces of classical modular forms. Perhaps the most convenient source of such theta series is to work with quaternary ($d = 4$) quadratic forms of square discriminant coming from quaternion algebras—this method goes by the name *Brandt matrices* as it came about from early work of Brandt. Building on work of Eichler [42], Hijikata–Pizer–Shemanske [50] proved that linear combinations of such theta series span the space of cusp forms, up to twists. (See also Martin [64] for a more recent development.) The coefficients of theta series can then be reformulated in terms of classes of right ideals of specified reduced norm in a quaternion order. This method was first developed in an algorithmic context by Pizer [77]; it has been implemented in Magma by David Kohel and in SageMath by Bober, Alia Hamieh, Victoria de Quehen, William Stein, and Gonzalo Tornaría.

In a little more detail, the method of Brandt matrices runs as follows. Let B be a definite quaternion algebra of discriminant $D := \operatorname{disc} B$, a squarefree product of the primes that ramify in B. Let $\mathcal{O} \subseteq B$ be an Eichler order of level M with $\gcd(D, M) = 1$, and let $N := DM$. Let $\operatorname{Cls}\mathcal{O}$ be the set of locally principal (equivalently, invertible) fractional right $\mathcal{O}$-ideals up to isomorphism (given by left multiplication by an element of $B^\times$). Then $\operatorname{Cls}\mathcal{O}$ is a finite set, so let $\operatorname{Cls}\mathcal{O} = \{[I_1], [I_2], \dots, [I_h]\}$ with $h := \#\operatorname{Cls}\mathcal{O}$. Let $\mathcal{O}_{\mathrm{L}}(I_i)$ be the left order of I_i, and let $\Gamma_i := \mathcal{O}_L(I_i)^\times$ be its unit group with $\#\Gamma_i < \infty$. Let $q_i := \operatorname{nrd}(I_i)$. For $n \in \mathbb{Z}_{\geq 1}$, define

$$\Theta(n)_{i,j} := \Gamma_i \backslash \{\alpha \in I_j I_i^{-1} : \operatorname{nrd}(\alpha) q_i q_j^{-1} = n\}.$$

We have $\alpha \in \Theta(n)_{i,j}$ if and only if $\alpha I_i \subseteq I_j$ with index n^2. To connect this with the previous paragraph, we have

$$\begin{aligned} Q_{ij} &\colon I_j I_i^{-1} \to \mathbb{Z} \\ Q_{ij}(\alpha) &= \operatorname{nrd}(\alpha)\frac{q_i}{q_j} \end{aligned} \tag{5.3.3}$$

is a positive definite integral quaternary quadratic form of discriminant N^2 whose theta series descends to a modular form of level N—in the notation above, we have $r_{Q_{ij}}(n) = \#\Theta(n)_{i,j}$. In this way, we can compute a matrix for the Hecke operator $[T_n]$ acting on $S_k(\Gamma_0(N), \chi)$ by quaternionic arithmetic: for weight $k = 2$, the matrix $[T_n]$ is the adjacency matrix of the directed graph with vertex set $\operatorname{Cls}\mathcal{O}$ and directed edges between $[I_i]$ and $[I_j]$ with multiplicity $\#\Theta(n)_{i,j}$.

The method of Brandt matrices has several advantages. First, the forms computed this way are necessarily new at all primes $p \mid D$, so linear algebra with degeneracy operators can be minimized. Second, the matrices $[T_n]$ of Hecke operators are sparse: for example, in weight $k = 2$ they have nonnegative integer coefficients whose columns sum to $\sigma(n)$. Accordingly, linear algebra steps have an improved complexity both in theory and in practice. Third, Brandt matrices also carry useful arithmetic information about the reduction of modular curves at primes of bad reduction. Fourth, the set $\Theta(n)_{i,j}$ is independent of the weight k and so may be reused. Despite these advantages, the main limitation of Brandt matrices seems to be that it works most simply when there exists a prime p that exactly divides the level N (so that an Eichler order of reduced discriminant N exists); otherwise, we must work with non-Eichler orders. Hence current implementations focus on this case.

The Brandt graph is an expander graph by the Ramanujan–Peterson bound, so with short vector computations one can compute a set of representatives for $\operatorname{Cls}\mathcal{O}$ and a spanning set for $S_k(\Gamma_0(N), \chi)$ using $\widetilde{O}(h^2)$ operations; computing a basis from this is a matter of sparse linear algebra and can be considered to be negligible. To compute a single matrix $[T_n]$, in principle we could use Minkowski reduction (together with some awkward corner cases) on $h\sigma(n)$ right ideals using $\widetilde{O}(hn) = \widetilde{O}(dn)$ operations. To compute a basis of q-expansions to precision $O(q^r)$ with $d = O(r)$, for each of the h classes we can enumerate elements of small reduced norm using the Fincke–Pohst algorithm in time proportional to the volume so $\widetilde{O}(dr^2)$, performing reduction with the same complexity.

These heuristics match the running time of modular symbols with linear algebra again eventually dominating— however, it is here where sparse linear algebra may ultimately in practice give the Brandt matrix method an edge.

A method that shares much in common with Brandt matrices is the *method of graphs* due to Mestre [68] and Oesterlé. We suppose that $p \parallel N$ and work with the quaternion algebra B of discriminant $D = p$. We recall that there is an equivalence of categories between supersingular elliptic curves over an algebraic closure of $\mathbb{F}_p$ under isogenies and invertible right (or left) $\mathcal{O}$-modules under homomorphisms. So to compute a matrix for the Hecke operator, in place of $\operatorname{Cls}\mathcal{O}$ we can compute the set of isomorphism classes of pairs (E, C) where E is a supersingular elliptic curve in characteristic p and C is a cyclic subgroup of order $M = N/p$, and in place of the sets $\Theta(n)_{ij}$ we can enumerate cyclic isogenies between these points up to a natural equivalence.

Finally, a related method of Birch [7] (who sought to generalize the method of graphs beyond discriminant $D = p$) uses *ternary* quadratic forms instead. This method captures all of the advantages above, with an additional feature: work in progress by Hein–Tornaría–Voight shows that one can carve out not just a new subspace but moreover one can specify the Atkin–Lehner eigenvalue, reducing the total dimension and thereby the complexity of linear algebra operations.

5.4. **Other methods.** We conclude by briefly indicating two other methods in addition to the above.

- *Multiplying forms of lower weight.* We compute a presentation for the graded ring of modular forms of level N
$$M(\Gamma_1(N)) := \bigoplus_{k=0}^{\infty} M_k(\Gamma_1(N))$$
(or the same for $\Gamma_0(N)$) in terms of a finite set of generators and a Gröbner basis for the ideal of relations among them; see work of Voight–Zureick-Brown [100] for an explicit description of this graded ring in terms of the genus and number of cusps for $\Gamma_1(N)$ (and more generally in terms of the signature of the uniformizing Fuchsian group) as well as further references and discussion. From this, one can compute for each weight k a set of (leading) monomials in the generators that are a $\mathbb{Q}$-basis for $M_k(\Gamma_1(N))$. Using fast Fourier techniques, the multiplication of these q-expansions allows the computation of a basis for large weights k (and fixed level N) quite efficiently in comparison to any of the approaches above.
- *Polynomial-time algorithms.* By work of Edixhoven–Couveignes [40], Bruin [13], and Mascot [66], one can compute coefficients of modular forms of level 1 in polynomial time: for example, for the modular discriminant $\Delta(q) = \sum_n \tau(n)q^n \in S_{12}(1)$, the value $\tau(p)$ for a prime p can be computed in time bounded by a fixed power of $\log p$.

6. Two technical ingredients

In this section, we consider two technical results that are needed in the above algorithmic description.

6.1. **Eichler–Selberg trace formula for newforms.** We first prove a technical result that is used by Belabas–Cohen [4] in the computation of modular forms in Pari/GP [76], as explained above: we describe the trace of Hecke operators on the new subspace in terms of the trace on the total space.

Let χ be a primitive character of conductor $Q \mid N$ and k a positive integer satisfying $\chi(-1) = (-1)^k$; we take these to be fixed and suppress their dependence from the notation.

For any positive integer n, the nth Hecke operator $T_n\colon S_k(N,\chi)\to S_k(N,\chi)$ may be defined by

$$(T_nf)(z)=\frac{1}{n}\sum_{\substack{ad=n\\ \gcd(a,N)=1}}\chi(a)a^k\sum_{b \bmod d} f\left(\frac{az+b}{d}\right).$$

Then

$$(T_nf)(z)=\sum_{m=1}^{\infty}\left(\sum_{\substack{d\mid(m,n)\\(d,N)=1}}\chi(d)d^{k-1}a_{\frac{mn}{d^2}}\right)e(mz),$$

where $f(z)=\sum_{m=1}^{\infty}a_me(mz)$. This operator stabilizes the subspace $S_k^{\mathrm{new}}(N,\chi)$.

Let $\{f_{N,j}\}_{j=1}^{s_N}$ be a basis of normalized newforms for $S_k^{\mathrm{new}}(N,\chi)$ and write

$$f_{N,j}(z)=\sum_{m=1}^{\infty}a_{N,j}(m)e(mz).$$

We assume that each $f_{N,j}$ is an eigenfunction of T_n of eigenvalue $a_{N,j}(n)$ and define

$$g_n=\sum_{j=1}^{s_N}a_{N,j}(n)f_{N,j}=\sum_{m=1}^{\infty}e(mz)\operatorname{Tr}\left(T_nT_m|_{S_k^{\mathrm{new}}(N,\chi)}\right).$$

We parameterize the basis of $S_k(N,\chi)$: for $M_1,M_2\in\mathbb{Z}_{\geq 1}$ with $Q\mid M_1$ and $M_1M_2\mid N$, let

$$f_{M_1,j}^{M_2}(z):=f_{M_1,j}(M_2z).$$

Then

$$\left\{f_{M_1,j}^{M_2}\ :\ M_1,M_2\in\mathbb{Z}_{\geq 1},\,Q\mid M_1,\,M_1M_2\mid N\right\}$$

is a basis for $S_k(N,\chi)$. Let us extend the definition of $a_{N,j}(n)$ to $\mathbb{Q}_{>0}$ by writing $a_{N,j}(x)=0$ if $x\notin\mathbb{Z}_{\geq 1}$.

If $\gcd(n,N)=1$, then

$$\begin{aligned}T_nf_{M_1,j}^{M_2}&=\sum_{m=1}^{\infty}\sum_{\substack{d\mid(m,n)\\(d,N)=1}}\chi(d)d^{k-1}a_{M_1,j}\left(\frac{mn}{d^2M_2}\right)e(mz)\\&=\sum_{m=1}^{\infty}a_{M_1,j}\left(\frac{m}{M_2}\right)a_{M_1,j}(n)e(mz)=a_{M_1,j}(n)f_{M_1,j}^{M_2},\end{aligned}$$

so each $f_{M_1,j}^{M_2}$ is an eigenfunction of T_n. To compute the action of T_n when $\gcd(n,N)>1$, we need the following theorem.

Theorem 6.1.1. *Let $p\mid N$ be prime, let $\alpha\in\mathbb{Z}_{\geq 0}$, and let $r:=\operatorname{ord}_p M_2$. Let χ_{M_1} be the character modulo M_1 induced from χ. Then*

$$T_{p^\alpha}f_{M_1,j}^{M_2}=\begin{cases}f_{M_1,j}^{M_2p^{-\alpha}}, & \text{if } \alpha-r\leq 0;\\ a_{M_1,j}(p^{\alpha-r})f_{M_1,j}^{M_2p^{-r}}-\chi_{M_1}(p)p^{k-1}a_{M_1,j}(p^{\alpha-r-1})f_{M_1,j}^{M_2p^{-r+1}}, & \text{if } \alpha-r>0.\end{cases}\tag{6.1.2}$$

Proof. By the definition of the Hecke operator, we get

$$T_{p^\alpha}f_{M_1,j}^{M_2}=\sum_{m=1}^{\infty}\sum_{\substack{d\mid(m,p^\alpha),\\(d,N)=1}}\chi(d)d^{k-1}a_{M_1,j}\left(\frac{mp^\alpha}{M_2d^2}\right)e(mz)=\sum_{m=1}^{\infty}a_{M_1,j}\left(\frac{mp^\alpha}{M_2}\right)e(mz).$$

If $\alpha - r \leq 0$, then

$$T_{p^\alpha} f_{M_1,j}^{M_2} = \sum_{m=1}^{\infty} a_{M_1,j}\left(\frac{m}{M_2 p^{-r}\cdot p^{-\alpha+r}}\right) e(mz) = f_{M_1,j}^{M_2 p^{-\alpha}}.$$

Assume that $\alpha - r > 0$. Since $f_{M_1,j}$ is a normalized newform for $\Gamma_0(M_1)$, we get

$$\begin{aligned} (6.1.3)\quad & a_{M_1,j}\left(\frac{m}{M_2 p^{-r}}\right)\cdot a_{M_1,j}\left(p^{\alpha-r}\right) \\ & = \begin{cases} a_{M_1,j}\left(\frac{mp^\alpha}{M_2}\right), & \text{if } p \mid M_1, \\ \sum_{e=0}^{\min\{\mathrm{ord}_p(m),\alpha-r\}} (\chi(p)p^{(k-1)})^e a_{M_1,j}\left(\frac{mp^{\alpha-2e-r}}{M_2 p^{-r}}\right), & \text{if } p \nmid M_1. \end{cases} \end{aligned}$$

Then, if $p \mid M_1$, we have

$$T_{p^\alpha} f_{M_1,j}^{M_2} = a_{M_1,j}(p)^{\alpha-r}\cdot f_{M_1,j}^{M_2 p^{-r}}.$$

We now assume that $\alpha - r > 0$ and $p \nmid M_1$. If $\alpha - r = 1$, we have

$$a_{M_1,j}\left(\frac{mp^\alpha}{M_2}\right) = a_{M_1,j}\left(\frac{m}{M_2 p^{-r}}\right)\cdot a_{M_1,j}\left(p^{\alpha-r}\right) - \delta_{\mathrm{ord}_p(m)\geq 1}\chi(p)p^{(k-1)} a_{M_1,j}\left(\frac{mp^{\alpha-2}}{M_2}\right).$$

By taking the summation over $m \in \mathbb{Z}_{\geq 1}$, we get:

$$\begin{aligned} T_{p^\alpha} f_{M_1,j}^{M_2} &= a_{M_1,j}(p^{\alpha-r}) f_{M_1,j}^{M_2 p^{-r}} - \chi(p)p^{k-1}\sum_{m=1}^{\infty} a_{M_1,j}\left(\frac{mp^{\alpha-1}}{M_2}\right) e(mpz) \\ &= a_{M_1,j}(p^{\alpha-r}) f_{M_1,j}^{M_2 p^{-r}} - \chi(p)p^{k-1} f_{M_1,j}^{M_2 p^{-r+1}}. \end{aligned}$$

Note that when $r = 0$ we have $M_1 M_2 p \mid N$, since $p \mid N$.

If $\alpha - r - 2 \geq 0$, by changing α to $\alpha - 2$, we get

$$\chi(p)p^{k-1} a_{M_1,j}\left(\frac{m}{M_2 p^{-r}}\right)\cdot a_{M_1,j}\left(p^{\alpha-2-r}\right) = \sum_{e=1}^{\min\{\mathrm{ord}_p(m),\alpha-2-r\}+1} (\chi(p)p^{(k-1)})^e a_{M_1,j}\left(\frac{mp^{\alpha-2e-r}}{M_2 p^{-r}}\right).$$

By subtracting from (6.1.3), we get

$$\begin{aligned} &\left\{a_{M_1,j}(p^{\alpha-r}) - \chi(p)p^{k-1} a_{M_1,j}(p^{\alpha-r-2})\right\} a_{M_1,j}\left(\frac{m}{M_2 p^{-r}}\right) = a_{M_1,j}\left(\frac{mp^\alpha}{M_2}\right) \\ &\quad + \begin{cases} -\left(\chi(p)p^{k-1}\right)^{\mathrm{ord}_p(m)+1} a_{M_1,j}\left(\frac{mp^{\alpha-2(\mathrm{ord}_p(m)+1)-r}}{M_2 p^{-r}}\right), & \text{if } 0 \leq \mathrm{ord}_p(m) \leq \alpha-2-r, \\ \left(\chi(p)p^{k-1}\right)^{\alpha-r} a_{M_1,j}\left(\frac{mp^{-(\alpha-r)}}{M_2 p^{-r}}\right), & \text{if } \mathrm{ord}_p(m) \geq \alpha - r, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

After taking the summation over $m \in \mathbb{Z}_{\geq 1}$ on both sides, we get

$$\begin{aligned}\sum_{m=1}^{\infty} a_{M_1,j}\left(\frac{mp^{\alpha}}{M_2}\right) e(mz) &= T_{\alpha} f_{M_1,j}^{M_2}(z) \\ &= \left\{a_{M_1,j}(p^{\alpha-r}) - \chi(p)p^{k-1}a_{M_1,j}(p^{\alpha-2-r})\right\} f_{M_1,j}^{M_2p^{-r}} \\ &\quad + \sum_{\ell=0}^{\alpha-2-r} (\chi(p)p^{k-1})^{\ell+1} \sum_{\substack{m=1,\\ p\nmid m}}^{\infty} a_{M_1,j}\left(\frac{mp^{\alpha-2-r-\ell}}{M_2p^{-r}}\right) e(mp^{\ell}z) \\ &\quad - (\chi(p)p^{k-1})^{\alpha-r} \sum_{m=1}^{\infty} a_{M_1,j}\left(\frac{m}{M_2p^{-r}}\right) e(mp^{\alpha-r}z).\end{aligned}$$

For the last piece, we have

$$\sum_{m=1}^{\infty} a_{M_1,j}\left(\frac{m}{M_2p^{-r}}\right) e(mp^{\alpha-r}z) = f_{M_1,j}^{M_2p^{\alpha-2r}}(z).$$

Now consider

$$\sum_{\substack{m=1,\\ p\nmid m}}^{\infty} a_{M_1,j}\left(\frac{m}{M_2p^{-r}}\right) e(mz) = f_{M_1,j}^{M_2p^{-r}}(z) - \sum_{m=1}^{\infty} a_{M_1,j}\left(\frac{mp}{M_2p^{-r}}\right) e(mpz).$$

Since

$$a_{M_1,j}(p) \cdot f_{M_1,j}^{M_2p^{-r}}(z) = \sum_{m=1}^{\infty} a_{M_1,j}\left(\frac{mp}{M_2p^{-r}}\right) e(mz) + \chi(p)p^{k-1} f_{M_1,j}^{M_2p^{-r+1}}(z),$$

we get

$$\sum_{\substack{m=1,\\ p\nmid m}}^{\infty} a_{M_1,j}\left(\frac{m}{M_2p^{-r}}\right) e(mz) = f_{M_1,j}^{M_2p^{-r}}(z) - a_{M_1,j}(p) \cdot f_{M_1,j}^{M_2p^{-r+1}}(z) + \chi(p)p^{k-1} f_{M_1,j}^{M_2p^{-r+2}}(z).$$

For each $0 \leq \ell \leq \alpha - 2 - r$, we get

$$\begin{aligned}&\sum_{\substack{m=1,\\ p\nmid m}}^{\infty} a_{M_1,j}\left(\frac{mp^{\alpha-2-r-\ell}}{M_2p^{-r}}\right) e(mp^{\ell}z) \\ &\quad = a_{M_1,j}\left(p^{\alpha-2-r-\ell}\right) \cdot \left\{f_{M_1,j}^{M_2p^{-r+\ell}}(z) - a_{M_1,j}(p) \cdot f_{M_1,j}^{M_2p^{-r+1+\ell}}(z) + \chi(p)p^{k-1} f_{M_1,j}^{M_2p^{-r+2+\ell}}(z)\right\}.\end{aligned}$$

So we finally get

$$\begin{aligned}T_{\alpha} f_{M_1,j}^{M_2} &= \left\{a_{M_1,j}(p^{\alpha-r}) - \chi(p)p^{k-1}a_{M_1,j}(p^{\alpha-2-r})\right\} f_{M_1,j}^{M_2p^{-r}} \\ &\quad + \sum_{\ell=0}^{\alpha-2-r} (\chi(p)p^{k-1})^{\ell+1} a_{M_1,j}\left(p^{\alpha-2-r-\ell}\right) \\ &\qquad \cdot \left\{f_{M_1,j}^{M_2p^{-r+\ell}} - a_{M_1,j}(p) \cdot f_{M_1,j}^{M_2p^{-r+1+\ell}} + \chi(p)p^{k-1} f_{M_1,j}^{M_2p^{-r+2+\ell}}\right\} \\ &\quad - (\chi(p)p^{k-1})^{\alpha-r} f_{M_1,j}^{M_2p^{\alpha-2r}}.\end{aligned}$$

For $s \in \mathbb{Z}_{\geq 0}$, we have

$$a_{M_1,j}(p^s) \cdot a_{M_1,j}(p) = a_{M_1,j}(p^{s+1}) + \chi(p)p^{k-1}a_{M_1,j}(p^{s-1}),$$

so we get

$$\begin{aligned}
&\sum_{\ell=0}^{\alpha-2-r}(\chi(p)p^{k-1})^{\ell+1}a_{M_1,j}\left(p^{\alpha-2-r-\ell}\right)a_{M_1,j}(p)\cdot f_{M_1,j}^{M_2p^{-r+1+\ell}}\\
&\quad=\sum_{\ell=0}^{\alpha-2-r}(\chi(p)p^{k-1})^{\ell+1}a_{M_1,j}(p^{\alpha-1-r-\ell})\cdot f_{M_1,j}^{M_2p^{-r+1+\ell}}\\
&\qquad+\sum_{\ell=0}^{\alpha-2-r}(\chi(p)p^{k-1})^{\ell+2}a_{M_1,j}\left(p^{\alpha-3-r-\ell}\right)\cdot f_{M_1,j}^{M_2p^{-r+1+\ell}}\\
&\quad=\sum_{\ell=1}^{\alpha-1-r}(\chi(p)p^{k-1})^{\ell}a_{M_1,j}(p^{\alpha-r-\ell})\cdot f_{M_1,j}^{M_2p^{-r+\ell}}\\
&\qquad+\sum_{\ell=1}^{\alpha-1-r}(\chi(p)p^{k-1})^{\ell+2}a_{M_1,j}\left(p^{\alpha-2-r-\ell}\right)\cdot f_{M_1,j}^{M_2p^{-r+\ell}}.
\end{aligned}$$

Then we have

$$\begin{aligned}
T_\alpha f_{M_1,j}^{M_2}&=\left\{a_{M_1,j}(p^{\alpha-r})-\chi(p)p^{k-1}a_{M_1,j}(p^{\alpha-2-r})\right\}f_{M_1,j}^{M_2p^{-r}}\\
&\quad+\sum_{\ell=0}^{\alpha-2-r}(\chi(p)p^{k-1})^{\ell+1}a_{M_1,j}\left(p^{\alpha-2-r-\ell}\right)f_{M_1,j}^{M_2p^{-r+\ell}}\\
&\quad+\sum_{\ell=2}^{\alpha-r}(\chi(p)p^{k-1})^{\ell}a_{M_1,j}\left(p^{\alpha-r-\ell}\right)f_{M_1,j}^{M_2p^{-r+\ell}}\\
&\quad-\sum_{\ell=1}^{\alpha-1-r}(\chi(p)p^{k-1})^{\ell}a_{M_1,j}(p^{\alpha-r-\ell})\cdot f_{M_1,j}^{M_2p^{-r+\ell}}\\
&\quad-\sum_{\ell=1}^{\alpha-1-r}(\chi(p)p^{k-1})^{\ell+2}a_{M_1,j}\left(p^{\alpha-2-r-\ell}\right)\cdot f_{M_1,j}^{M_2p^{-r+\ell}}\\
&\quad-(\chi(p)p^{k-1})^{\alpha-r}f_{M_1,j}^{M_2p^{\alpha-2r}}\\
&=a_{M_1,j}(p^{\alpha-r})f_{M_1,j}^{M_2p^{-r}}-(\chi(p)p^{k-1})a_{M_1,j}(p^{\alpha-r-1})f_{M_1,j}^{M_2p^{-r+1}}.
\end{aligned}$$

Combining, we obtain (6.1.2). □

For $n, N\in\mathbb{Z}_{>0}$, we write $\gcd(n,N^\infty)$ for the largest positive integer d such that $d\mid n$ and $d\mid N^k$ for some $k\in\mathbb{Z}_{\geq 1}$, i.e.,

$$\gcd(n,N^\infty)=\prod_{p\mid\gcd(n,N)}p^{\mathrm{ord}_p(n)}. \tag{6.1.4}$$

The following corollary is then immediate.

Corollary 6.1.5. *With notation as above, we have*

$$\mathrm{Tr}(T_n\,|\,S_k(N,\chi))=\sum_{\substack{M\in\mathbb{Z}_{\geq 1}\\ M\mid N\\ \mathrm{cond}(\chi)\mid M}}d\left(\frac{N/M}{\gcd(N/M,n^\infty)}\right)\sum_{\substack{b^2\mid\gcd(n,N^\infty)\\ \gcd(b,M)=1}}\mu(b)\chi(b)b^{k-1}\,\mathrm{Tr}(T_{\frac{n}{b^2}}\,|\,S_k^{\mathrm{new}}(M,\chi)).$$

6.2. **Certifying generalized eigenvalues.** Second, we show how to certify generalized eigenvalues. Consider the generalized eigensystem

$$Ax = \lambda Bx, \tag{6.2.1}$$

where A and B are real symmetric $n \times n$ matrices, with B positive definite. Choosing R such that $B = R^T R$ and making the change of variables $x = R^{-1}y$, this becomes

$$A'y = \lambda y, \tag{6.2.2}$$

where $A' = (R^{-1})^T A R^{-1}$. Note that A' is again symmetric, so there is an orthonormal basis $\{y_1, \ldots, y_n\}$ with $A'y_j = \lambda_j y_j$. We set $x_j = R^{-1}y_j$, so that the x_j are orthonormal with respect to the inner product defined by B.

Suppose that we have found approximate eigenvalues $\tilde{\lambda}_j$ and eigenvectors $\tilde{x}_j$, i.e. so that $e_j = (A - \tilde{\lambda}_j B)\tilde{x}_j$ is small. Let

$$\tilde{x}_j = \sum_{k=1}^{n} c_{jk} x_k$$

be the expansion of $\tilde{x}_j$ in terms of the eigenbasis. For any $\varepsilon > 0$, define

$$V_{j,\varepsilon} = \operatorname{span}\{x_k : |\lambda_k - \tilde{\lambda}_j| < \varepsilon\}, \tag{6.2.3}$$

and let

$$v_{j,\varepsilon} = \sum_{\substack{k \\ |\lambda_k - \tilde{\lambda}_j| < \varepsilon}} c_{jk} x_k \tag{6.2.4}$$

be the orthogonal projection (with respect to the inner product defined by B) of $\tilde{x}_j$ onto $V_{j,\varepsilon}$. Then we have

$$\begin{aligned} v_{j,\varepsilon}^T B v_{j,\varepsilon} &= \tilde{x}_j^T B \tilde{x}_j - \sum_{\{k : |\lambda_k - \tilde{\lambda}_j| \geq \varepsilon\}} c_{jk}^2 \geq \tilde{x}_j^T B \tilde{x}_j - \varepsilon^{-2} \sum_{k=1}^{n} c_{jk}^2 (\lambda_k - \tilde{\lambda}_j)^2 \\ &= \tilde{x}_j^T B \tilde{x}_j - \varepsilon^{-2} [(B^{-1}A - \tilde{\lambda}_j)\tilde{x}_j]^T B [(B^{-1}A - \tilde{\lambda}_j)\tilde{x}_j] \\ &= \tilde{x}_j^T B \tilde{x}_j - \varepsilon^{-2} e_j^T B^{-1} e_j \geq \tilde{x}_j^T B \tilde{x}_j - \varepsilon^{-2} b^{-1} |e_j|^2, \end{aligned} \tag{6.2.5}$$

where $b > 0$ is the smallest eigenvalue of B. Note that this is positive if

$$\varepsilon > \varepsilon_j := \frac{|e_j|}{\sqrt{b \tilde{x}_j^T B \tilde{x}_j}},$$

and thus $V_{j,\varepsilon}$ is non-zero. Hence, there is an eigenvalue λ_k in the interval $I_j = [\tilde{\lambda}_j - \varepsilon_j, \tilde{\lambda}_j + \varepsilon_j]$.

Suppose that we are in the favorable situation that the I_j are pairwise disjoint. Then our system has distinct eigenvalues, and we may assume without loss of generality that $\lambda_j \in I_j$. Next, let $\delta_j = \min\{|\lambda - \tilde{\lambda}_j| : \lambda \in \bigcup_{k \neq j} I_k\}$, so that $(\tilde{\lambda}_j - \delta_j, \tilde{\lambda}_j + \delta_j)$ contains λ_j and no other eigenvalues. Put $\Delta_j = \tilde{x}_j - v_{j,\delta_j}$, where $V_{j,\varepsilon}$ and $v_{j,\varepsilon}$ are as above, so that $\tilde{x}_j - \Delta_j$ is an eigenvector with eigenvalue λ_j. To use this in practice, we bound the coordinates of Δ_j from above and add them as small error intervals onto the coordinates of $\tilde{x}_j$. (The resulting vector must then be renormalized in interval arithmetic, according to whatever convention we use, e.g. first Fourier coefficient 1.) To that end, we have

$$\begin{aligned} |R\Delta_j|^2 = \Delta_j^T B \Delta_j &= \sum_{\{k : |\lambda_k - \tilde{\lambda}_j| \geq \delta_j\}} c_{jk}^2 \leq \delta_j^{-2} \sum_{k=1}^{n} c_{jk}^2 (\lambda_k - \tilde{\lambda}_j)^2 \\ &= \delta_j^{-2} [(B^{-1}A - \tilde{\lambda}_j)\tilde{x}_j]^T B [(B^{-1}A - \tilde{\lambda}_j)\tilde{x}_j] = \delta_j^{-2} e_j^T B^{-1} e_j, \end{aligned} \tag{6.2.6}$$

and thus

$$|\Delta_j| \leq \delta_j^{-1}\sqrt{b^{-1}e_j^T B^{-1}e_j} \leq \frac{|e_j|}{b\delta_j}. \tag{6.2.7}$$

Finally, to estimate b we first compute a double-precision approximation $\tilde{P}$ to the orthogonal matrix which diagonalizes B. We then compute in interval arithmetic the matrices

$$S = (s_{jk}) = \tilde{P}^T B\tilde{P} \quad \text{and} \quad T = (t_{jk}) = \tilde{P}^T\tilde{P}.$$

By Sylvester's law of inertia, we have $b > \lambda$ for any λ such that $S - \lambda T$ is positive definite. In turn, by the Gershgorin circle theorem, this holds if the diagonal entries s_{jj} and t_{jj} are strictly positive and

$$\lambda > \lambda^* := \min_j \frac{2s_{jj} - \sum_k |s_{jk}|}{\sum_k |t_{jk}|}. \tag{6.2.8}$$

Hence $b \geq \lambda^*$.

7. A sample of the implementations

7.1. **Comparison of methods.** In the course of our computations we made extensive use of the modular forms functionality included in both Pari/GP [76] and Magma [12]. In this section we compare the performance of the two implementations on a small but representative subset of the modular forms we computed: all newforms of weight k and level N with $Nk^2 \leq 1000$ and $k > 1$. We exclude the case $k = 1$ from this comparison because it is not fully supported in Magma and the algorithms used to compute weight one forms are substantially different. For modular forms of weight $k > 1$ the Magma implementation is based on the modular symbols approach, while the Pari/GP implementation uses the explicit trace formula.

For each level N in our chosen range we fix a representative Dirichlet character χ for each Galois orbit $[\chi]$ of modulus N, and for each newspace $S_k^{\text{new}}(N, \chi)$ with $k > 1$ and $Nk^2 \leq 2000$ we carried out the following computations in both Pari/GP and Magma:

(1) Determine the dimensions of the irreducible subspaces of $S_k^{\text{new}}(N, [\chi])$ (the newform orbits).
(2) For each newform orbit $[f]$, compute the first 1000 integer coefficients t_n of the trace form $\text{Tr}(f) = \sum_{n\geq 1} t_n q^n$.
(3) For each newform orbit $[f]$ of (absolute) dimension $d \leq 20$, compute a (reasonably nice) defining polynomial for its coefficient field K and the first 1000 algebraic integer coefficients $a_n(f) \in K$ for a constituent newform f.
(4) For each newform orbit $[f]$ of dimension $d \leq 20$, compute an LLL-optimized basis for its coefficient ring and express the first 1000 coefficients $a_n(f)$ in this basis.

Nk^2	num S	num f	$\sum \dim(S)$	split time (s) Magma	split time (s) Pari/GP	total time (s) Magma	total time (s) Pari/GP
$[1, 200]$	183	214	897	0.4	1.1	73.8	18.2
$[201, 400]$	453	709	7 560	3.5	17.2	302.4	116.6
$[401, 600]$	574	1 050	21 452	22.2	50.2	643.4	220.1
$[601, 800]$	677	1 326	43 515	132.1	70.8	2 444.8	300.6
$[801, 1000]$	764	1 542	71 358	751.3	322.3	9 216.4	728.2
$[1001, 1200]$	879	1 805	109 570	2 653.1	1 253.3	36 940.0	2 347.6
$[1201, 1400]$	905	2 001	152 344	8 889.0	5 517.0	161 327.7	11 855.8
$[1401, 1600]$	995	2 284	203 492	24 841.1	21 256.5	349 656.8	67 233.4
$[1601, 1800]$	1 032	2 420	264 506	63 476.2	59 392.6	952 669.0	194 405.8
$[1801, 2000]$	1 157	2 378	331 348	79 307.2	175 890.1	1 752 685.4	596 779.2
	7 621	15 731	1 206 658	180 089.5	263 771.8	3 266 135.9	874 006.0

Table 7.1.1: Magma 2.24-7 vs. Pari/GP 2.12.1 (Intel Xeon W-2155 3.3GHz); timings for newspaces S of level $N \geq 1$, weight $k > 1$ by Nk^2 range

$\#S$	$\max \dim(f)$	num S	num f	$\sum \dim(S)$	split time (s) Magma	split time (s) Pari/GP	total time (s) Magma	total time (s) Pari/GP
1	$[1, 200]$	2 859	2 859	161 375	423.8	529.9	11 967.2	818.0
1	$[201, 2000]$	1 027	1 027	544 092	26 060.6	55 272.8	701 094.2	53 727.6
1	$[2001, \infty]$	65	65	215 016	146 044.1	170 751.3	2 226 371.4	163 789.9
2	$[1, 200]$	1 703	3 406	100 080	278.7	660.9	4 233.8	30 837.0
2	$[201, 2000]$	145	290	95 704	4 192.1	8 188.7	188 745.7	576 764.6
2	$[2001, \infty]$	4	8	10 870	2 636.5	26 821.1	97 329.8	24 785.1
≥ 3	$[1, 20]$	873	4 785	19 282	46.2	64.1	1 596.2	1 197.9
≥ 3	$[21, 200]$	235	1 155	23 135	160.8	275.7	1 228.8	5 255.3
≥ 3	$[201, \infty]$	3	15	1 024	12.0	347.7	1 364.5	357.4
		7 621	15 731	1 206 658	180 089.5	263 771.8	3 266 135.9	874 006.0

Table 7.1.2: Magma 2.24-7 vs. Pari/GP 2.12.1 (Intel Xeon W-2155 3.3GHz); timings for newspaces S of level $N \geq 1$, weight $k > 1$, $Nk^2 \leq 2000$ by $\#S := \#\{f \in S\}$.

As can be seen in Tables 7.1.1 and 7.1.2, the explicit trace formula approach used by Pari/GP is faster overall than the modular symbol method implemented in Magma, especially for spaces that consists of a single Galois orbit, but for newspaces that split into multiple Galois orbits it is typically slower, and in general Magma is able to decompose newspaces into Galois orbits more quickly than Pari/GP. The large advantage Pari/GP has on irreducible spaces is due to the fact that in this situation we can use `mfsplit` to determine that the space is irreducible without actually computing any eigenforms, and then use `mftraceform` to compute the trace form for the entire space.

In Table 7.1.3 we list the 10 newspaces in our chosen range that were the computationally most difficult for either Magma or Pari/GP. In each case, the 10 most time consuming newspaces

accounted for approximately half of the total time to process the 7621 nonzero newspaces in our test range.

Notably, only two newspaces (467.2.c and 497.2.c) were among the computationally most difficult for both methods (these are the two newspaces of largest dimension in our chosen range). Most of the newspaces listed in Table 7.1.3 were computationally much more difficult for one of the two methods: on the largest irreducible spaces in our test range Pari/GP is typically at least ten times as fast as Magma, but for newspaces that split into two large Galois orbits Magma is faster than Pari/GP by a similar (or even larger) factor. This suggests that the optimal approach is to use the explicit trace formula and modular symbol methods in combination. Indeed, a hybrid approach that uses Magma to decompose the space, and then delegates the computation to Pari/GP whenever the newspace contains a Galois orbit of dimension at least 2/3 the dimension of the newspace, takes a total of 264 726 seconds; this is more than 3 times faster than using Pari/GP alone and more than 10 times faster than using Magma alone.

newspace	$[\mathbb{Q}(\chi):\mathbb{Q}]$	decomposition	Magma(s)	Pari/GP(s)
413.2.i	28	$420+420$	68.91	23 711.71
419.2.g	180	6120	79 654.08	5 175.04
424.2.v	24	1248	60 111.92	150.62
431.2.g	168	5880	82 907.51	5 333.59
435.2.bf	12	$240+240$	39.63	25 272.26
443.2.g	192	6912	180 453.61	8 134.21
454.2.c	112	$1008+1120$	1 197.47	44 216.52
467.2.c	232	8816	370 791.77	22 719.24
472.2.l	28	$56+1568$	103 117.42	562.40
478.2.g	96	$960+960$	861.98	87 147.90
479.2.c	238	9282	363 002.59	26 148.67
486.2.i	54	$702+756$	351.60	139 762.27
487.2.k	162	6480	110 903.14	6 766.85
489.2.q	54	$702+756$	202.91	38 345.59
491.2.k	168	6720	121 405.39	8 558.33
497.2.v	24	$408+456$	99.20	18 438.91
498.2.f	40	$560+560$	269.01	48 844.21
499.2.g	164	6724	119 807.20	12 148.53

Table 7.1.3: Some computationally challenging newspaces

7.2. **A trace formula implementation with complex coefficients.** In this section, we describe an implementation of the trace formula using ball arithmetic over the complex numbers due to Bober [8]. This implementation follows the description given in §5.2. The main focus here is to compute a moderate number of coefficients for all of the newforms in a given space $S_k^{\mathrm{new}}(N,\chi)$ as approximate complex numbers, which enables the computation of modular form L-functions at small height, for example. These computations use Arb [53], a C library which implements arbitrary precision ball arithmetic, so that we can ensure that all of our computations come with rigorous error bounds. There is also some facility for computing with coefficients in a finite field $\mathbb{F}_\ell$, where ℓ is some prime congruent to 1 modulo the order of χ, which is used in the computation of characteristic polynomials of Hecke operators, for example, and in other auxiliary pieces. The

package also contains some limited functionality to compute information about spaces of weight one modular forms, which we do not discuss here.

We describe briefly some details of how this implementation works in practice.

To start a computation we first choose a prime and determine a set of trace forms which will give a full rank basis of the space of newforms modulo this prime, avoiding any issues of computing the rank of a matrix with floating point entries. Specifically, we find some matrix of coefficients $(\mathrm{Tr}(T(m_i)T(n_j) \mid S_k^{\mathrm{new}}(N,\chi)))_{1\le i,j\le d}$ that has full rank, and we also choose our m_i and n_j so that $\gcd(m_i n_j, N) = 1$, which will make later computations easier. Once we know which computation will give us a full rank matrix, we do the computation again over the complex numbers, computing additional coefficients so that we will be able to compute the action of Hecke operators. At this point we find a sum of Hecke operators $T = \sum_n c_n T_n$ such that the characteristic polynomial of T is squarefree (keeping $c_n = 0$ when $\gcd(n, N) \neq 1$).

The diagonalization of T would in general be a computation over the complex numbers, but because we have chosen to only use Hecke operators coprime to the level, we can use knowledge of the arguments of the eigenvalues to turn this into a problem of diagonalizing a real symmetric matrix. This problem is solved by an implementation of Jacobi's algorithm, certifying the result as described in §6.2. Once we have diagonalized, we obtain a change of basis matrix that takes our trace form basis to the newform basis, and we can compute as many coefficients of newforms as we like by evaluation of the trace formula.

Once we have computed all the embeddings of all of our newforms, we may also wish to compute the decomposition of the space into Hecke-irreducible subspaces. To do this we will compute the characteristic polynomial of a linear combination T of Hecke operators (it is sufficient to find one that is squarefree). If we have enough precision in the Hecke eigenvalues we have computed, we can do this simply by forming the product $\prod_\lambda (x - \lambda)$, where λ ranges over the eigenvalues of T. In general we will find that we do not have enough accuracy to uniquely identify a polynomial with coefficients in $\mathbb{Z}[x]$, however, and we refine the computation by computing this polynomial modulo ℓ for enough small primes ℓ to obtain the polynomial exactly.

The factorization of this Hecke polynomial gives the decomposition of $S_k^{\mathrm{new}}(N,\chi)$ into Hecke irreducible subspaces. However, there is still one more problem we may be faced with: namely, identifying which embeddings correspond to which subspaces. In this problem we have a set of polynomials $f_1, f_2, \ldots, f_n$ and a set of approximations of complex numbers $r_1, r_2, \ldots, r_d$, and all we need to do is determine which complex number is a root of which polynomial. This may seem like a relatively trivial problem, but in fact these polynomials may be enormous and obtaining enough precision in the roots to solve this by simple evaluation may not be feasible.

Example 7.2.1. To give a moderately-sized example, we can consider the space 766.2.c. This space is only 32-dimensional over the field of definition of χ, but there are 190 Galois conjugate characters to consider, so the full degree is 6080. The characteristic polynomial of T_3 acting on the space $S_2^{\mathrm{new}}(766, [\chi])$ is squarefree and factors into 2 irreducible factors of degree 3040; each factor contains more than 1.5 million decimal digits.

To make this problem tractable, we again make use of the arguments of the eigenvalues. Let $f(x)$ be one of these irreducible factors. We know that each root of f can be written as ζt for some root of unity ζ and some real number t, and we find that t is a root of the greatest common divisor of $f(\zeta x)$ and $f(\zeta^{-1}x)$ in $\mathbb{Q}(\zeta)[x]$. In fact, as we prefer to work with real numbers, we compute

$$\gcd(f(\zeta x) + f(\zeta^{-1}x), i(f(\zeta x) - f(\zeta^{-1}x))) \in \mathbb{Q}(\zeta + \zeta^{-1})[x].$$

In principle, computing this greatest common divisor when we have only floating point approximations available could be troublesome, but it is possible because we know what its degree is.

8. Issues: computational, theoretical, and practical

8.1. **Analytic conductor.** Earlier efforts to tabulate modular forms have tended to compute all newforms in particular boxes, where the weight and level each vary in a specified range. This approach is easy to describe, but the computational complexity of finding newforms with simultaneously large weight and level ensures that some newforms of interest will be missed (either large weight or large level). Instead of working with boxes, we organized our computation around a single invariant which scales with the complexity of the newform.

Introduced by Iwaniec–Sarnak [52, Eq. (31)] (see also Iwaniec–Kowalski [51, (5.7)]), the analytic conductor of a newform $f \in S_k^{\mathrm{new}}(N,\chi)$ is the positive real number

$$A := N\left(\frac{\exp(\psi(k/2))}{2\pi}\right)^2, \tag{8.1.1}$$

where $\psi(x) := \Gamma'(x)/\Gamma(x)$ is the logarithmic derivative of the Gamma function. The analytic conductor includes a factor that can be thought of as measuring the complexity at infinity. We have $A \sim \dfrac{Nk^2}{16\pi^2}$ as $k \to \infty$, so for simplicity we organized our computations by specifying bounds on the quantity Nk^2.

8.2. **Sturm bound.** In this section, we elaborate upon bounds for truncations of q-expansions of modular forms that determine them uniquely. The most well-known of these bounds is due to Hecke (and more generally to Sturm [95, Theorem 1]).

Theorem 8.2.1 (Hecke, Sturm)**.** *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and let f be a modular form of weight k for Γ. Then $f = 0$ if and only if $a_n(f) = 0$ for all $0 \leq n \leq k[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/12$.*

In fact, for modular forms with character as in our setting, one can apply a sharper bound (as though it was without character) as follows.

Definition 8.2.2. For $k, N \in \mathbb{Z}_{\geq 1}$, define the (Hecke-)Sturm bound

$$\mathrm{Sturm}(k,N) := \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = \frac{Nk}{12}\prod_{p \mid N}\left(1+\frac{1}{p}\right).$$

Proposition 8.2.3 (Hecke, Sturm)**.** *Let $N, k \geq 1$ and let χ be a character of modulus N. Let $\mathcal{T} \subseteq \mathrm{End}_{\mathbb{C}}(S_k(N,\chi))$ be the $\mathbb{Z}$-subalgebra generated by the Hecke operators T_n for all $n \in \mathbb{Z}_{\geq 1}$, and let $\mathbb{Z}[\chi] \subseteq \mathbb{C}$ be the $\mathbb{Z}$-subalgebra generated by the values of χ. Then there is a natural inclusion $\mathbb{Z}[\chi] \hookrightarrow \mathcal{T}$, and the following statements hold.*

(a) *If $f \in S_k(N,\chi)$ has $a_n(f) = 0$ for all $n \leq \mathrm{Sturm}(k,N)$, then $f = 0$.*

(b) *$\mathcal{T}$ is generated as a $\mathbb{Z}[\chi]$-module by T_n for all $n \leq \mathrm{Sturm}(k,N)$.*

(c) *$\mathcal{T}$ is generated as a $\mathbb{Z}[\chi]$-algebra by T_1 and T_p for all primes $p \leq \mathrm{Sturm}(k,N)$.*

Proof. For the inclusion $\mathbb{Z}[\chi] \hookrightarrow \mathcal{T}$, we argue as follows: from the Hecke recursion

$$T_{p^2} - T_p^2 + \chi(p)p^{k-1} = 0 \tag{8.2.4}$$

for $p \nmid N$, we see that $\chi(p)p^{k-1} \in \mathcal{T}$; choosing two distinct primes p congruent modulo N and applying the CRT shows that $\mathbb{Z}[\chi] \subseteq \mathcal{T}$. Consequently, $\mathcal{T}$ is a torsion free $\mathbb{Z}[\chi]$-module. Since $\mathbb{Z}[\chi]$ is a Dedekind domain, $\mathcal{T}$ is locally free.

Abbreviate $S := S_k(N,\chi;\mathbb{Z}[\chi])$. We claim that the pairing

$$\begin{aligned} \mathcal{T} \times S &\to \mathbb{Z}[\chi] \\ (T,f) &\mapsto a_1(Tf) \end{aligned} \tag{8.2.5}$$

is perfect, i.e., the map

$$\begin{aligned} \varphi\colon S &\to \mathrm{Hom}_{\mathbb{Z}[\chi]}(\mathcal{T}, \mathbb{Z}[\chi]) \\ f &\mapsto (T \mapsto a_1(Tf)) \end{aligned} \tag{8.2.6}$$

is an isomorphism. When $\mathbb{Z}[\chi] = \mathbb{Z}$, this is an argument of Ribet [81, Theorem (2.2)], and we only need to make a small modification. The map φ is injective with torsion-free cokernel because $a_1 \circ T_n = a_n$ and the map taking a form to its q-expansion is injective. Since S and $\mathcal{T}$ are locally free $\mathbb{Z}[\chi]$-modules of finite rank, it suffices to show that the rank of $\mathcal{T}$ is at most the rank of S (localizing at primes $\mathfrak{l}$ of $\mathbb{Z}[\chi]$). To this end, consider the other map induced by the pairing, namely,

$$\begin{aligned} \omega\colon \mathcal{T} &\to \mathrm{Hom}_{\mathbb{Z}[\chi]}(S, \mathbb{Z}[\chi]) \\ T &\mapsto (f \mapsto a_1(Tf)). \end{aligned} \tag{8.2.7}$$

We claim that ω is injective. Indeed, if $T \in \ker \omega$, then for all $f \in S$ and all $n \geq 1$ we have

$$0 = \omega(T)(T_n f) = a_1(TT_n f) = a_1(T_n T f) = a_n(Tf)$$

as $\mathcal{T}$ is commutative. Since the q-expansion map is injective, we conclude $Tf = 0$ for all f, so $T = 0$ as an endomorphism, proving the claim. Finally, localizing ω at $\mathfrak{l}$, the injectivity of ω implies the desired rank bound.

We now prove (a) following Buzzard, and suppose that $f \in S_k(N, \chi; \mathbb{Z}[\chi])$ has $a_n(f) = 0$ for all $n \leq \mathrm{Sturm}(k, N)$. Let d be the order of χ, let $s := \mathrm{Sturm}(k, N)$, and consider $f^d \in S_{dk}(\Gamma_0(N); \mathbb{Z}[\chi])$. Since $f = O(q^{s+1})$, we have $f^d = O(q^{d(s+1)})$. Moreover, $\mathrm{Sturm}(kd, N) = ds$, so by the Sturm bound (Theorem 8.2.1) applied to $S_{dk}(\Gamma_0(N); \mathbb{Z}[\chi])$ we conclude $f^d = 0$, which implies $f = 0$.

To prove (b), let $\mathcal{T}_{\leq n} \subseteq \mathcal{T}$ be the $\mathbb{Z}[\chi]$-submodule generated by T_n with $n \leq \mathrm{Sturm}(k, N)$. By the previous paragraph, the pairing (8.2.5) restricted to $\mathcal{T}_{\leq n}$ is still perfect; indeed we can simply argue with $\mathcal{T}_{\leq n}$ in the injectivity of ω in (8.2.7). We conclude that $\mathcal{T}_{\leq n} = \mathcal{T}$.

For part (c), we use multiplicativity to see that T_n for n composite is contained in the algebra generated by the prime power operators T_{p^e}, and then the Hecke recurrence and induction to see that T_{p^e} is contained in the algebra generated by T_1 and T_p. □

8.3. **Atkin–Lehner operators and eigenvalues.** Let χ be a Dirichlet character modulo N. For $M \mid N$ with $\gcd(M, N/M) = 1$, there are unique characters $\chi_M \pmod M$ and $\chi_{N/M} \pmod{N/M}$ such that $\chi = \chi_M \chi_{N/M}$. The Atkin–Lehner–Li operator W_M [2, §1] maps the space $S_k(N, \chi)$ to $S_k(N, \overline{\chi_M}\chi_{N/M})$. In general $\overline{\chi_M}\chi_{N/M}$ is different from χ, so then this operator cannot be used for splitting up spaces. We have $\overline{\chi_M}\chi_{N/M} = \chi$ when the character χ_M is trivial or quadratic, and in these cases, W_M is an involution on the space $S_k(N, \chi)$, which then splits as the direct sum of ± 1-eigenspaces. Magma only implements Atkin-Lehner operators on spaces with trivial character, where they commute with all Hecke operators and hence map every newform f to $\pm f$, and the sign $\pm$ is the *Atkin-Lehner eigenvalue* of f with respect to M. (By a common abuse of notation and terminology, when M is the power of a prime q not dividing N/M, the operator W_M is often denoted W_q.) In our computations we only compute Atkin-Lehner eigenvalues on newforms with trivial character.

In general, the image of a normalized newform f in $S_k(N, \chi_M\chi_{N/M})$ under W_M is a multiple of a normalized newform in $S_k(N, \overline{\chi_M}\chi_{N/M})$, and the multiple, not necessarily ± 1, is called the *pseudo-eigenvalue* of W_M on f. Atkin–Li [2] do not give a general formula for pseudo-eigenvalues, which are not always easy to compute in practice. See also Belabas–Cohen [4, §§5–6].

When $M = 1$ the operator W_M is trivial, while when $M = N$ it is called the *Fricke involution*. The Fricke involution is the product of all W_q for primes $q \mid N$ (using the convention of the previous paragraph.) For a newform of weight k and trivial character, the Fricke eigenvalue ϵ is related to the

sign ε that appears in the functional equation (9.1.3) via $\epsilon = (-1)^{k/2}\varepsilon$, see Miyake [71, Cor. 4.3.7]. Each W_q-eigenvalue is similarly related to the sign of a certain local functional equation.

8.4. **Self-duality.** The coefficient field of a newform $f \in S_k(N, \chi)$ is either totally real or CM [79, Prop 3.2]; we say that f is self-dual in the totally real case. Computing the coefficient field can be time consuming, so we use the following easier criteria when applicable.

Proposition 8.4.1 (Ribet)**.** *Let $f \in S_k(N, \chi)$ have Hecke orbit of dimension d and trace form $\sum_{n=0}^{\infty} t_n q^n$. Then the following statements hold.*

(a) *If χ is trivial or d is odd, then f is self-dual;*

(b) *If χ has order larger than 2, then f is not self-dual;*

(c) *If there exists a prime p so that $t_p \neq 0$ and $\chi(p) \neq 1$, then f is not self-dual.*

Proof. See Ribet [79, Propositions 3.2 and 3.3]. □

8.5. **Efficiently recognizing irreducibility.** Level $N = 2$ is by far the most time-consuming case for Magma (note that this allows for the largest range of k with $N \neq 1$ for any given bound on the analytic conductor). For $k > 400$ with $4 \mid k$, each space takes more than 12 hours of CPU time. However, we observed behavior analogous to the Maeda conjecture in weight 1 up to weight $k \leq 400$. The Atkin–Lehner operator W_2 splits the space as evenly as possible, and the W_2-eigenspaces appear to always be irreducible.

Conjecture 8.5.1. *For all $k \geq 2$, the space $S_k^{\mathrm{new}}(\Gamma_0(2))$ decomposes under the Atkin–Lehner operator W_2 into Hecke irreducible subspaces of dimensions $\lfloor d/2 \rfloor$ and $\lceil d/2 \rceil$, where $d := \dim_{\mathbb{C}} S_k^{\mathrm{new}}(\Gamma_0(2))$.*

The dimensions in the corollary follow from work of Martin [64, Theorem 2.2], which implies that for even weights $k > 2$ we have

$$\dim S_k^{\mathrm{new}}(\Gamma_0(2))^+ - \dim S_k^{\mathrm{new}}(\Gamma_0(2))^- = \begin{cases} 0 & k = 4, 6 \bmod 8, \\ (-1)^{k/2} & k \equiv 0, 2 \bmod 8, \end{cases} \tag{8.5.2}$$

it is only the irreducibility of the eigenspaces that is conjectural. The factor $(-1)^{k/2}$ in (8.5.2) appears as 1 in [65, Theorem 2.2] because there the Atkin-Lehner operator follows the convention of Diamond–Shurman [39, p. 209], which includes a factor of $(-1)^{k/2}$, while we are following the convention of Miyake [71], which does not include this factor.

One can find similar formulas for $\dim S_k^{\mathrm{new}}(\Gamma_0(N))^+ - \dim S_k^{\mathrm{new}}(\Gamma_0(N))^-$ for any squarefree N in Martin [65], in which case they are a linear function of the class number $h(-4N)$. For general $N > 4$ not of the form $M^2, 2M^2, 3M^2, 4M^2$ with M squarefree, we refer the reader to Helfgott [48, pp. 266–267].

Question 8.5.3. Given an $n \times n$ matrix with entries in $\mathbb{Z}[\zeta_m]$ (typically sparse), is there a fast algorithm that with positive probability correctly determines when its characteristic polynomial is irreducible?

In other words, if you expect that a polynomial is irreducible, can you verify this quickly without factoring the polynomial? Under the expectation that the Galois group of the polynomial is transitive and therefore likely to be S_d, one could succeed in some cases by factoring the polynomial modulo primes. This is different than the typical factorization problems solved in computer algebra systems, which compute a factorization p-adically and then reconstruct the factorization over $\mathbb{Z}$. (See Table 7.1.3 for some difficult spaces where this would help.) A natural generalization of this question would be to efficiently determine the degrees of the irreducible factors of its characteristic polynomial (without explicitly computing it).

8.6. **Trace form.** As defined in §4.5, each newform $f \in S_k^{\mathrm{new}}(N, [\chi])$ has an associated trace form $\mathrm{Tr}(f)(q) = \sum_n t_n q^n \in S_k(N, [\chi]; \mathbb{Z})$ equal to the sum of the distinct $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \,|\, \mathbb{Q})$ conjugates of f and thereby well-defined on its Galois orbit $[f]$. More precisely, we have $\mathrm{Tr}(f) \in S_k^{\mathrm{new}}(\Gamma)$ where

$$\Gamma := \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) : \chi(a) = 1 \} \supseteq \Gamma_1(N),$$

(but in general $\mathrm{Tr}(f) \notin S_k(N, \chi)$). One can thus apply the Sturm bound (Theorem 8.2.1) for Γ: trace forms of newforms in $S_k(N, \chi)$ with the same Fourier coefficients a_n for $n \leq k[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/12$ must coincide, but note that this will typically be larger than the Sturm bound $\mathrm{Sturm}(k, N)$. As noted above, we always have $t_1 = [K : \mathbb{Q}]$, where $K = \mathbb{Q}(f)$ is the coefficient field of f.

Trace forms can be efficiently computed using the trace formula. In the common case where $S_k(N, \chi)$ is irreducible, this can be done via the Pari/GP function `mftraceform` [76], which is dramatically faster than computing the coefficients of f as elements of K and taking traces (indeed, it is not even necessary to determine K). More generally, if one knows the decomposition of $S_k(N, [\chi])$ into newform subspaces and has computed trace forms for all but one of them, the remaining trace form can be computed by subtracting corresponding coefficients of the known trace forms from the coefficients given by `mftraceform`, which computes absolute traces of the Hecke operators T_n acting on the entire newspace $S_k(N, [\chi])$. Alternatively, one can sum complex coefficients a_n of the Galois conjugates of f computed to sufficient precision to allow the sum to be identified as a unique integer.

The coefficients t_p of the trace form at primes p are equal to the Dirichlet coefficients of the (typically imprimitive) L-function $L(s) = \sum b_n n^{-s}$ with integer Dirichlet coefficients b_n obtained by taking the product of the L-functions of the Galois conjugates of f. But for nonprime values of n the integer coefficients t_n do not match the integer coefficients b_n unless the newspace has dimension one (in which case $L(s)$ is primitive). Indeed $t_1 = [K : \mathbb{Q}]$ cannot coincide with $b_1 = 1$, and in general the coefficients t_n at nonprime values of n encode different information.

8.7. **Presenting coefficients using LLL-reduction.** One of the most dramatic improvements we saw, both in performance and in display, is in the choice of how to represent coefficient rings. In this section and the next, we explain two such methods.

As explained in section 4.5, one computes a minimal polynomial for the coefficient field by factoring the characteristic polynomial of a Hecke operator. This polynomial may be unwieldy! So we first apply the Pari/GP function `polredbest` which finds an improved minimal polynomial representing the same field by computing an LLL-reduced basis for an order with respect to the Minkowski embedding (whose underlying quadratic form is given by the T_2-norm)—this runs in deterministic polynomial time in the size of the input. When possible, we improve this to `polredabs`, which applies the same technique but to the maximal order (this may require factoring a discriminant, and we frequently encounter situations where this is a bottleneck).

Remark 8.7.1. The function `polredabs` changed in Pari/GP 2.9.5 (Fall 2017); we use the more recent version, described in [33].

We can make significant further improvements by optimizing the $\mathbb{Z}$-basis we use to represent coefficients. Let $f \in S_k^{\mathrm{new}}(N, \chi)$ be a newform. By the Hecke–Sturm bound (Proposition 8.2.3), the coefficient ring of f is generated over $\mathbb{Z}[\chi]$ by the values $a_n(f)$ for $n \leq \mathrm{Sturm}(k, N)$, so by extension we obtain a set of $\mathbb{Z}$-module generators for the ring. We reduce this to an LLL-reduced $\mathbb{Z}$-basis for the coefficient ring, and we rewrite the coefficients in terms of this basis. In our computations, we always use complex precision that is at least as large as the discriminant of the coefficient ring.

We observe the following.

Lemma 8.7.2. *Let F be a number field and let $R \subseteq F$ be a $\mathbb{Z}$-order in F. Then the shortest vectors in R with respect to the T_2-norm are exactly the roots of unity in R.*

Proof. The order R contains 1, and $T_2(1) = n := [F : \mathbb{Q}]$. More generally, for any root of unity $\zeta \in R$, we have $T_2(\zeta) = n$. Conversely, let $\alpha \in R$ have $T_2(\alpha) \leq n$. Then by the arithmetic-geometric mean inequality, we have

$$1 \geq \frac{T_2(\alpha)}{n} = \frac{1}{n}\sum_{i=1}^{n} |\alpha_i|^2 \geq \prod_{i=1}^{n} |\alpha_i|^{2/n} = \left|\mathrm{Nm}_{F|\mathbb{Q}}\, \alpha\right|^{2/n}$$

with equality if and only if $|\alpha_1| = \cdots = |\alpha_n| = 1$. But $\alpha \in R$ is integral, so $\left|\mathrm{Nm}_{F|\mathbb{Q}}\, \alpha\right| \geq 1$, so equality holds. By Kronecker's theorem, we conclude that α is a root of unity. □

In spite of this lemma, because of nonuniqueness, we may not have 1 as an element of an LLL-reduced basis as there may be more roots of unity than the degree, such as in a cyclotomic field. However, using the above lemma we can recognize the roots of unity in the coefficient ring and thereby recognize when the coefficient ring is cyclotomic itself, where we may institute a canonical basis (see also the next section).

The effect of such a representation is dramatic.

Example 8.7.3. Consider the newform 153.2.e.c. Its coefficient field is $\mathbb{Q}(\nu)$ where ν has minimal polynomial

$$x^{20} - x^{19} + 3x^{18} + 2x^{17} + 13x^{16} - 12x^{15} + 54x^{14} + 27x^{13} + 93x^{12} - 54x^{11} + 693x^{10} - 162x^9 + 837x^8 + 729x^7 + 4374x^6 - 2916x^5 + 9477x^4 + 4374x^3 + 19683x^2 - 19683x + 59049.$$

An integral basis written in terms of the powers of ν is too large to record here, and similarly the coefficients of f written in a power basis are enormous!

However, in terms of an LLL-reduced basis $\beta_0 = 1, \cdots, \beta_{19}$, we have coefficients

$$\begin{aligned}
a_2(f) &= \beta_{16} \\
a_3(f) &= -\beta_{10} \\
a_4(f) &= -1 - \beta_3 - \beta_5 \\
&\vdots \\
a_{57}(f) &= \beta_2 - \beta_3 - \beta_4 + \beta_5 - 3\beta_7 + 2\beta_9 - \beta_{10} \\
&\qquad + 2\beta_{13} + \beta_{14} + \beta_{15} - \beta_{16} + 2\beta_{17} - \beta_{18} - \beta_{19} \\
&\vdots
\end{aligned}$$

that are very small integer linear combinations of the basis elements. Moreover, we have

$$\begin{aligned}
1 &= \beta_0 \\
\nu &= \beta_1 \\
\nu^2 &= \beta_8 - \beta_7 - \beta_4 + \beta_2 \\
&\vdots \\
\nu^{19} &= 5114\beta_{19} + 2632\beta_{18} + \cdots - 1807\beta_1 - 6756
\end{aligned}$$

and the powers of ν are reasonably sized $\mathbb{Z}$-linear combinations of our basis elements.

We observe that the matrix that writes the powers of a primitive element in terms of the LLL-reduced basis is noticeably smaller than the other way around. Working with the coefficient ring itself rather than a maximal order containing it is not only more efficient (as it may be prohibitively expensive to compute such a maximal order), but it also seems to give better results.

The intuitive reason that this works is simple: by the Ramanujan–Petersson bounds, the coefficients of a newform are of small size in all complex embeddings, and so it can be expected that writing it in terms of a $\mathbb{Z}$-basis which is LLL-reduced with respect to size provides a small linear combination.

Remark 8.7.4. In the above, we have been concentrating on the case where f is a newform, representing a Galois orbit of newforms, and we write down its q-expansion in terms of a $\mathbb{Z}$-basis for the coefficient ring.

As an alternative, we can consider the $\mathbb{C}$-vector space spanned by f and its conjugates under $\mathrm{Aut}(\mathbb{C})$, making a $\mathbb{C}$-vector space of dimension say d. These conjugates will include conjugates that *do not* preserve the character, so we would either be working implicitly in the direct sum of the spaces over the full Galois orbit of characters, or we need to restrict to quadratic characters, or we only consider conjugates under $\mathrm{Aut}(\mathbb{C} \mid \mathbb{Q}(\chi))$ and get a $\mathbb{Q}(\chi)$-vector space. However, inside this space is a canonical $\mathbb{Q}$-subspace, namely, those forms whose q-expansion belongs to $\mathbb{Q}[[q]]$. So we could instead represent the Galois orbit canonically by an echelonized basis of d individual q-expansions with coefficients in $\mathbb{Q}$. We could then write a representative newform as before as a linear combination of this basis over the coefficient field.

To go from the eigenform to the $\mathbb{Q}$-basis, we apply the operators $\mathrm{Tr}(\beta_i f)$ for β_i any $\mathbb{Q}$-basis for the coefficient field. (To go from the $\mathbb{Q}$-basis to an eigenform one needs to retain sufficiently many eigenvalues to do the linear algebra. In other words, the eigenform contains more information than the $\mathbb{Q}$-basis.) This generalizes the trace form, which is where we take $\beta_i = \beta_0 = 1$.

We could also work integrally and take the $\mathbb{Z}$-module of forms whose q-expansions belong to $\mathbb{Z}$ and then take a LLL-reduced basis which minimizes a (weighted) sum of finitely many coefficients. It is conceivable that in a world where linear algebra over $\mathbb{Q}$ is much faster than linear algebra over number fields that we could succeed in computing a $\mathbb{Q}$-basis in reasonable time but not succeed in computing an eigenform.

8.8. **Presenting coefficients using a sparse cyclotomic representation.** When the coefficient ring of a newform is contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$, writing coefficients in terms of an LLL-optimized basis as described in the previous section does not necessarily give the most compact representation, for two reasons. First, when the coefficient ring is not the maximal order, it may be more compact to express coefficients as elements of the maximal order $\mathbb{Z}[\zeta_m]$. Second, even when the coefficient ring is the maximal order, in which case the LLL-optimized basis will typically be the standard power basis $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\phi(m)-1}$, the eigenvalues a_n can often be written more compactly by expressing them as sparse polynomials in ζ_m rather than integer linear combinations of the power basis. Every integer linear combination of elements of the power basis is of course also a polynomial in ζ_m; the question is whether to allow polynomials of higher degree whose terms involve powers of ζ_m that are not in the power basis (because $m > \phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$), which allows more flexibility and a potentially sparser choice of polynomial.

This added flexibility is particular relevant for weight one newforms, whose coefficients always lie in a cyclotomic field. The correspondence between weight one newforms and (odd irreducible) 2-dimensional Artin representations [37] implies that for weight one newforms the eigenvalues a_p can always be written as a sum of at most two roots of unity. For composite values of n the eigenvalues a_n will not be as sparse, but even if one naïvely expands them as products of polynomials in ζ_m for each a_{p^r}, for most a_n we obtain an expression with $O(2^{\log\log n})$ nonzero coefficients (a typical integer n has $\log\log n$ distinct prime factors p and p-adic valuation 1 at all but $O(1)$ of them), which is exponentially sparser than a generic element of $\mathbb{Z}[\zeta_m]$ written in the power basis. For even values of m we can improve on this naïve approach by using the identity $\zeta_m^{m/2} = -1$ to reduce to polynomials of degree at most $m/2 - 1$ in ζ_m; this never increases the number of terms and may reduce it.

For example, the second Fourier coefficient of the newform 3997.1.cz.a is

$$a_2 = -\zeta_{201}^{570} + \zeta_{570}^{244},$$

but when written in terms of the standard power basis $1, \zeta_{570}, \ldots, \zeta_{570}^{143}$ we instead have

$$\begin{aligned} a_2 = 1 &+ \zeta_{570}^{2} + \zeta_{570}^{5} + \zeta_{570}^{11} - \zeta_{570}^{12} - \zeta_{570}^{15} - \zeta_{570}^{17} + \zeta_{570}^{19} - \zeta_{570}^{20} + \zeta_{570}^{21} + \zeta_{570}^{24} + \zeta_{570}^{27} + \zeta_{570}^{30} - \zeta_{570}^{31} \\ &+ \zeta_{570}^{32} - \zeta_{570}^{34} + \zeta_{570}^{35} - \zeta_{570}^{36} - \zeta_{570}^{39} - \zeta_{570}^{42} - \zeta_{570}^{45} + \zeta_{570}^{46} - \zeta_{570}^{47} + \zeta_{570}^{49} - \zeta_{570}^{50} + \zeta_{570}^{51} - \zeta_{570}^{59} \\ &+ \zeta_{570}^{60} - \zeta_{570}^{61} - \zeta_{570}^{64} + \zeta_{570}^{65} - \zeta_{570}^{66} + \zeta_{570}^{74} - \zeta_{570}^{75} - \zeta_{570}^{78} + \zeta_{570}^{79} - \zeta_{570}^{80} + \zeta_{570}^{88} - \zeta_{570}^{89} + \zeta_{570}^{90} \\ &+ \zeta_{570}^{93} - \zeta_{570}^{94} - \zeta_{570}^{97} - \zeta_{570}^{100} - \zeta_{570}^{103} + \zeta_{570}^{104} - \zeta_{570}^{105} - \zeta_{570}^{106} + \zeta_{570}^{107} - \zeta_{570}^{108} + \zeta_{570}^{109} + \zeta_{570}^{112} + \zeta_{570}^{115} \\ &+ \zeta_{570}^{118} - \zeta_{570}^{119} + \zeta_{570}^{120} - \zeta_{570}^{122} + \zeta_{570}^{123} - \zeta_{570}^{124} - \zeta_{570}^{127} - \zeta_{570}^{130} + \zeta_{570}^{134} + \zeta_{570}^{137} + \zeta_{570}^{139} + \zeta_{570}^{142}. \end{aligned}$$

Among the 585 nonzero a_n with $n \leq 2000$, the average number of terms needed to express a_n as a sparse polynomial in ζ_m is 4.1; by contrast, when written in the power basis the average number of nonzero coefficients of a_n is 42.8. This leads to a more than tenfold reduction in storage and a corresponding reduction in the time to transmit or render the q-expansion.

Remark 8.8.1. For modular forms of weight $k > 1$ with cyclotomic coefficient fields $\mathbb{Q}(\zeta_m)$ there is no *a priori* reason to expect the a_p to be expressible as sparse polynomials in ζ_m, and one can see in examples that this is often not the case. One might instead try to apply a more general approach, which, given $\alpha \in \mathbb{Z}[\zeta_m]$ searches for a sparse polynomial $f(\zeta_m)$ of degree less than m with small coefficients that is equivalent to α. We do not know an efficient solution to this problem, but we note that even if one exists, for generic values of α it is unlikely to result in representations that are significantly more compact than using the power basis for purely information theoretic reasons: the number of $\alpha \in \mathbb{Z}[\zeta_m]$ that can be expressed as r-term polynomials in ζ_m using b bits to represent the coefficients must be approximately the same as the number of integer vectors of length $\phi(m)$ that can be encoded in b bits. For this reason we use sparse cyclotomic coefficient representations only for $k = 1$.

8.9. **Hecke kernels.** Having determined the decomposition of a newspace $S_k^{\mathrm{new}}(N, [\chi])$ into Hecke orbits V_f corresponding to newforms f, we can compute and store information that will allow us to reconstruct a single Hecke orbit, without having to decompose the entire newspace again. This is particularly useful when the dimension of a particular newform f of interest is much smaller than that of $S_k^{\mathrm{new}}(N, [\chi])$. To achieve this we compute a list of pairs $(p, g_p(X))$, where p is a prime and $g \in \mathbb{Z}[X]$ is the minimal polynomial of the Hecke operator T_p acting on V_f (viewed as a $\mathbb{Q}$-subspace of $S_k^{\mathrm{new}}(N, [\chi])$), such that V_f is equal to the intersection of the kernels of the linear operators $g_p(T_p)$ acting on $S_k^{\mathrm{new}}(N, [\chi])$, in other words, the operators $g_p(T_p)$ generate the Hecke kernel of V_f. Such a list of generators can be used to reconstruct the newform f in Magma via the `Kernel` function.

It is computationally convenient to restrict to primes p not dividing the level N, and to use the same list of primes p for all the newforms in $S_k^{\mathrm{new}}(N, [\chi])$. To this end, for a set of primes $\mathcal{S}$, not dividing N, and a newform f, we let $X_f(\mathcal{S})$ denote the set of pairs (p, g_p), where $g_p \in \mathbb{Z}[X]$ is the minimal polynomial of T_p acting on V_f, and say that $\mathcal{S}$ is a set of distinguishing primes for the newspace $S_k^{\mathrm{new}}(N, [\chi])$ if the sets $X_f(\mathcal{S})$ are distinct as f varies over the newforms of $S_k^{\mathrm{new}}(N, [\chi])$.

We construct a set of distinguishing primes as follows. We start by taking $\mathcal{S}$ to be the empty set. If the newspace $S_k^{\mathrm{new}}(N, [\chi])$ consists of a single Hecke orbit, then $\mathcal{S}$ is a set of distinguishing primes, and otherwise we increase the size of $\mathcal{S}$ by adding the least prime $p \nmid N$ not contained in $\mathcal{S}$ for which

$$\{X_f(\mathcal{S}) : f \in S_k^{\mathrm{new}}(N, [\chi])\} \subsetneq \{X_f(\mathcal{S} \cup \{p\}) : f \in S_k^{\mathrm{new}}(N, [\chi])\}.$$

We observe that the cardinality of the set $\mathcal{S}$ constructed in this fashion is at most one less than the number of Hecke orbits in $S_k^{\mathrm{new}}(N, [\chi])$. This greedy approach to constructing $\mathcal{S}$ does not

necessarily minimize its cardinality, but it does minimize the largest p that appears in $\mathcal{S}$, which may be viewed as an invariant of the newspace. For example, we may distinguish the 8 Hecke orbits of the newspace 2608.2.g, where $2608 = 2^4 \cdot 163$, using $p = 3$ and 41. In this case T_3 distinguishes all the forms with the exception of the two CM forms, which both have vanishing a_p for all p split in $\mathbb{Q}(\sqrt{-163})$, hence the smallest prime p such that a_p could possibly distinguish them is 41, and 41 does in fact do so.

Remark 8.9.1. The largest prime p that appears in $\mathcal{S}$ may occasionally exceed the Sturm bound, as in the case of the newforms 66.2.b and 735.2.p, for example. This fact is relevant in the context of Theorem 11.2.8, which we use to determine the group of inner twists of a newform in §11. This is one reason to compute $a_p(f)$ past the Sturm bound.

9. Computing L-functions rigorously

In this section, we describe rigorous methods to compute L-functions of modular forms.

9.1. **Embedded modular forms.** To a newform $f \in S_k^{\mathrm{new}}(N, \chi)$, with q-expansion $\sum a_n q^n$, for each complex embedding of the coefficient field $\iota : \mathbb{Q}(f) \hookrightarrow \mathbb{C}$ we may consider the embedded modular form

$$\iota(f) := \sum \iota(a_n) q^n, \tag{9.1.1}$$

which is a modular form over the complex numbers.

We label such forms by N.k.s.x.c.j, where N.k.s.x is the label of Hecke orbit, N.c is the Conrey label for the character corresponding to the embedding, and j is the index for the embedding within those with the same Dirichlet character; these embeddings are ordered by the vector $\iota(a_n)$, where we order the complex numbers first by their real part and then by their imaginary part.

To such an embedded modular form $\iota(f)$, we may associate a primitive L-function of degree 2

$$\begin{aligned} L(\iota(f), s) &:= \sum \iota(a_n) n^{-s} = \prod_p L_p(\iota(f), p^{-s}) \\ &= \prod_{p \mid N} \left(1 - \iota(a_p) p^{-s}\right)^{-1} \prod_{p \nmid N} \left(1 - \iota(a_p) p^{-s} + \chi(p) p^{-2s}\right)^{-1}. \end{aligned} \tag{9.1.2}$$

Let $\Lambda(\iota(f), s) := N^{s/2} \Gamma_{\mathbb{C}}(s) L(\iota(f), s)$, where $\Gamma_{\mathbb{C}}(s) := 2(2\pi)^{-s}\Gamma(s)$. Then $\Lambda(\iota(f), s)$ continues to an entire function of order 1 and satisfies the functional equation

$$\Lambda(\iota(f), s) = \varepsilon \overline{\Lambda}(\iota(f), k - s), \tag{9.1.3}$$

where ε is the root number of $\Lambda(\iota(f), s)$, a root of unity.

The generalized Riemann hypothesis also predicts that any nontrivial zero of the L-function lies on the line of symmetry of its functional equation $\Re(s) = k/2$, known as the critical line. To study the behavior of $L(\iota(f), s)$ on the critical line, it is natural to introduce the associated Z-function, a smooth real-valued function of a real variable t defined by

$$Z(\iota(f), t) := \bar{\varepsilon}^{1/2} \frac{\gamma(k/2 + it)}{|\gamma(k/2 + it)|} L(\iota(f), k/2 + it), \tag{9.1.4}$$

where $\gamma(s) := N^{s/2}\Gamma_{\mathbb{C}}(s)$ and the square root is chosen so that $Z(t) > 0$ for sufficiently small $t > 0$. By construction, we have $|Z(\iota(f), t)| = |L(\iota(f), k/2 + it)|$, the multiset of zeros of $Z(\iota(f), t)$ matches the multiset of zeros of $L(\iota(f), k/2 + it)$, and $Z(\iota(f), t)$ changes sign at the zeros of $L(\iota(f), k/2 + it)$ of odd multiplicity.

9.2. **Computations.** Given $\iota(f)$ we would like to compute certain invariants of $L(\iota(f), s)$. For example, the root number ε, the imaginary part of the first few zeros on the critical line, an upper bound on the order of vanishing at $s = k/2$, the leading Taylor coefficient at $s = k/2$, and the plot $Z(\iota(f), t)$ on some interval. Given that a majority of these items cannot be represented exactly, we instead aim to determine a small interval in $\mathbb{R}$ or rectangle in $\mathbb{C}$. Precisely, let b denote the number of bits of target accuracy. We would like to compute the following:

- the root number: $x_\varepsilon, y_\varepsilon \in \mathbb{Z}$ such that $2^{b+1}\Re(z) \in [x_\varepsilon - 1, x_\varepsilon + 1]$ and $2^{b+1}\Im(z) \in [y-1, y+1]$;
- the imaginary part of the first few zeros on the critical line: $t_1, \ldots, t_n \in \mathbb{Z}$ such that $\bigcup_i [t_i - 1, t_i + 1]2^{-b-1}$ covers the first n zeros of $L(\iota(f), k/2 + it)$;
- an upper bound on the order of vanishing at $s = k/2$: $r := \max_i\{i : |L^{(i)}(\iota(f), k/2)/i!| < 2^{-b-1}\}$;
- the leading Taylor coefficient at $s = k/2$: $0 \neq s \in \mathbb{Z}$ such that $2^{p+1}L^{(r)}(\iota(f), k/2)/r! \in [s + 1, s - 1]$;
- an approximation to the plot of $Z(\iota(f), t)$: approximations as doubles of $Z(\iota(f), i\delta)$ for some chosen δ and $i = 0, \ldots, n$.

In order to rigorously compute the items above, we follow an approach that builds on several improvements and extensions of the algorithm from [11] specialized to the motivic case, the details of which will appear in future work [9]. In practice, given the first $C_k\sqrt{N}$ embedded Dirichlet coefficients, with sufficient precision, and while carrying out all floating-point calculations using rigorous error bounds and interval arithmetic [53], one may compute all the items above to the desired bit accuracy. A generic library to carry out such computations, due originally to Dave Platt [28], has been developed.

Example 9.2.1. For an explicit example, we encourage the reader to peruse the source file `examples/cmf_23.1.b.a.cpp` in [28], where the authors show how to use the library to compute all of the items above for the modular form 23.1.b.a, which matches its unique embedding. By running this example, one can compute that

$$\epsilon = (1 \pm 10^{-117}) + (0 \pm 4.7 \times 10^{-59})\, i,$$

(since f is self dual, we must actually have $\epsilon = 1$), and

$$L(f, 1/2) = 0.17403632698793418349950459 2018 \pm 8.2317 \times 10^{-59},$$

as well as approximate values for the imaginary part of the first ten zeros. Using the notation above, we can represent an approximation to the imaginary part of the first zero

$$5.11568332881511759855335642038 \pm 3.9443 \times 10^{-31}$$

by the interval $[t_1 - 1, t_1 + 1]2^{-101}$, where

$$t_1 = 12969798084700060914517716069360.$$

The imaginary part of the following nine zeros are approximately 7.15926, 8.88140, 10.2820, 11.4300, 12.9344, 14.6625, 16.4982, 17.1013, and 18.0807.

We carried out this computation with 100 bits of target accuracy for the 14 398 359 embedded newforms in our database with $k \leq 200$. In our computation we observed that it was sufficient to work with 200 bits of precision and $C_k \leq 0.08k\log(k) + 24$. While we did not keep track of CPU time used along the way, by rerunning some of the computations, we extrapolate that we spent at least 11 CPU years on these computations.

9.3. **Imprimitive L-function.** Associated to a newform f with coefficient field $\mathbb{Q}(f)$ of degree d, we may also consider the L-function of degree $2d$ associated to its Galois orbit:

$$L(f,s) := \prod_{\iota:\mathbb{Q}(f)\hookrightarrow\mathbb{C}} L(\iota(f),s) \quad = \prod_p L_p(f,p^{-s}). \tag{9.3.1}$$

This gives rise to a $\mathbb{Q}$-primitive L-function with $L_p(f,T) \in 1+T\mathbb{Z}[T]$, which satisfies the functional equation

$$\Lambda(f,s) := N^{sd/2}\Gamma_{\mathbb{C}}(s)^d L(f,s) = \varepsilon\overline{\Lambda}(f,k-s), \tag{9.3.2}$$

where now we have $\varepsilon = \pm 1$. Using the invariants for each $L(\iota(f),s)$ mentioned above, one can easily deduce the respective invariants for $L(f,s)$.

For these L-functions we would also like to compute the local factors for small p. This is straightforward if one has access to an exact representation of a_p in $\mathbb{Q}(f)$. Otherwise, we relied on Newton identities to compute $L_p(f,T) \in \mathbb{Z}[T]$ from the roots of $L_p(\iota(f),T) \in \mathbb{C}[T]$, while working with interval arithmetic [53]: see $L(500.2.e.c)$ for an example. In some cases, for example when $[\mathbb{Q}(f):\mathbb{Q}]$ or the weight is large, we were only able to compute the initial coefficients for some local factors—this occurred for $L(20.10.e.b)$, for example.

9.4. **Verifying the analytic rank.** In this section, we discuss methods for rigorously verifying the analytic rank of a modular form L-function. Throughout, let N and k be positive integers and let $f \in S_k(\Gamma_1(N);\mathbb{C})$ be a newform of weight k and level N (with coefficient field embedded in the complex numbers).

Definition 9.4.1. Suppose k is *even*. We define the analytic rank of f to be the order of vanishing of $L(f,s)$ at $k/2$.

When $L^{(n)}(f,k/2) \neq 0$ one can certify such a statement using ball arithmetic by working with enough precision. However, if $L^{(n)}(f,k/2) = 0$, this approach does not work, as there is no known bound ε such that $|L^{(n)}(f,k/2)| < \varepsilon$ implies $L^{(n)}(f,k/2) = 0$. Nonetheless, if the order of vanishing is small, then there are other methods to computationally verify the order of vanishing. Using these methods we were able to provably verify the analytic rank of all modular forms for which the L-functions were computed. The way the analytic computations were verified is detailed below. The strategy used depends on the order of vanishing, and whether the modular form is self-dual or not. The analytic rank zero case is skipped because this can just be done by computing $L(f,k/2)$ to enough precision using interval arithmetic until 0 is no longer in the computed interval.

	Analytic rank				
	0	1	2	3	≥ 4
Self-dual	83 338	85 254	2 565	1	0
Not self-dual	63 804	1 798	1	0	0
Total	147 142	87 052	2 566	1	0

Table 9.4.2: Number of even weight newforms in the database by analytic rank

Self-dual and analytic rank 1. We begin by considering self-dual newforms f whose analytic rank numerically appears to be 1. All such forms in the range of our computation have trivial character. In this case the functional equation takes the form

$$\Lambda(f,s) = \varepsilon' i^k \Lambda(f,k-s), \tag{9.4.3}$$

where $\varepsilon' = \pm 1$ is the eigenvalue of the Atkin Lehner involution W_N. For such forms in the database, we verified that $\varepsilon' i^k = -1$, forcing $\Lambda(f,k/2) = 0$, and the non-vanishing of $N^{s/2}\Gamma_{\mathbb{C}}(k/2)$

then implies that $L(f, k/2) = 0$. The upper bound of 1 on the analytic rank was obtained using interval arithmetic.

Non-self-dual and analytic rank 1. Following Stein [93, §8.5], we define a pairing between modular forms and modular symbols

$$S_k(\Gamma_1(N)) \oplus \overline{S}_k(\Gamma_1(N)) \times \mathrm{ModSym}_k(\Gamma_1(N)) \to \mathbb{C}$$

by defining

$$\langle (f, g), P\{a, b\}\rangle := \int_a^b f(z)P(z, 1)dz + \int_a^b g(z)P(\overline{z}, 1)d\overline{z}.$$

This pairing allows one to determine the vanishing of L-functions, because for every integer $1 \leq j \leq k-1$ we have

$$L(f, j) = \frac{(-2\pi i)^j}{(j-1)!}\langle (f, 0), X^{j-1}Y^{k-2-(j-1)}\{0, \infty\}\rangle.$$

The pairing is Hecke-equivariant, meaning that $\langle (T_n f, T_n g), x\rangle = \langle (f, g), T_n x\rangle$ for all integers n.

Let $f \in S_k^{\mathrm{new}}(\Gamma_1(N))$ be a newform and $V_f \subseteq S_k^{\mathrm{new}}(\Gamma_1(N))$ the subspace generated by its Galois conjugates. Then by Atkin–Lehner–Li theory, V_f is a simple module over the Hecke algebra $\mathcal{T}$, and there exists a Hecke operator $t_f \in \mathcal{T}$ such that $t_f \colon M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$ is a projection onto V_f. Because t_f is a projection we have $\langle (f, 0), x\rangle = \langle (t_f f, t_f 0), x\rangle = \langle (f, 0), t_f x\rangle$ for all $x \in \mathrm{ModSym}_k(\Gamma_1(N))$, and hence in particular this means that if

$$t_f(X^{j-1}Y^{k-2-(j-1)}\{0, \infty\}) = 0$$

then $L(f, j) = 0$.

A map t'_f with the same kernel as t_f can be obtained from $t_f(\mathrm{ModSym}_k(\Gamma_1(N), \mathbb{Q}))$ in Magma using the command `PeriodMapping`. Furthermore, this Magma command only uses exact arithmetic over $\mathbb{Q}$. For all non-self-dual modular forms whose analytic rank numerically seemed to be 1, it was verified that indeed $t'_f(X^{k/2-1}Y^{k/2-1}\{0, \infty\}) = 0$, implying that $L(f, k/2) = 0$. The upper bound of 1 on the analytic rank was again obtained using interval arithmetic.

Self-dual and analytic rank 2. As in the preceding subsection, all newforms in the database whose analytic rank numerically seemed to be 2 have trivial character. This time it was verified that $\varepsilon' \iota^k = 1$ for all these modular forms. In particular, the functional equation then forces all odd derivatives of $\Lambda(f, s)$ to vanish at $k/2$. This forces the order of vanishing of $\Lambda(f, s)$ at $k/2$ to be even, and hence the analytic rank of $L(f, s)$ to be even as well. The techniques of the preceding paragraph were used to prove that for all these modular forms one has that $L(f, k/2) = 0$, which together with the parity argument gives a lower bound of 2 on the analytic rank. The upper bound of 2 was again obtained using interval arithmetic.

Non-self-dual analytic rank 2. There is exactly one Galois orbit of non-self-dual newforms in the database whose analytic rank numerically seems to be 2. Let f denote the newform of weight 2 and level 1154 with LMFDB label 1154.2.e.a with coefficient field $\mathbb{Q}(\zeta_3)$. This pair corresponds to an isogeny class of abelian surfaces, and our first goal is to find a representative of this isogeny class. By searching for hyperelliptic curves over $\mathbb{F}_p$ that match the local factors of $L(f, s)$ for small p, and then by lifting their Weierstrass equations to $\mathbb{Z}$ we found the following genus 2 curve:

$$C \colon y^2 = x^6 - 12x^5 + 34x^4 - 18x^3 - 11x^2 + 6x + 1. \tag{9.4.4}$$

Letting J denote its Jacobian, we find it is of conductor 1154^2 as desired. Our goal is first to show that J really is in the isogeny class of abelian surfaces corresponding to the newform 1154.2.e.a. Using [27] we were able to compute the endomorphism ring of J, and verify that J is of GL_2-type and hence is modular [82, 58]. Thus, J is a good candidate to be a representative of the isogeny

class of abelian surfaces corresponding to the newform 1154.2.e.a. Alternatively, one can also verify that J is of GL_2-type by noting that C has an automorphism of order 3 given by $x \mapsto 1 - 1/x$, $y \mapsto -y/x^3$ and thus showing that its Jacobian is of GL_2-type. Additionally, the Euler factor at 5 of its L-function is

$$1 + 6T + 17T^2 + 30T^3 + 25T^4$$

which is irreducible. Hence its Jacobian is simple, showing that its Jacobian corresponds to a pair of Galois conjugate newforms of level 1154. There is one other pair of Galois conjugate newforms whose coefficient field is $\mathbb{Q}(\zeta_3)$, namely that with LMFDB label 1154.2.c.a. So it remains to show that J does not come from the newform with label 1154.2.c.a. However the Euler factor of the L-function at 5 for that newform is $1 - 3T + 4T^2 - 15T^3 + 25T^4$ which does not match that of J. This means that Jacobian of C really is in the isogeny class of abelian surfaces corresponding to the newform 1154.2.e.a.

Using the Magma function `RankBounds` one readily computes that J has Mordell-Weil rank 4. In particular, it has rank 2 as a module over $\mathbb{Z}[\zeta_3]$. The generalization by Kato of the work of Kolyvagin and Logachev on the Birch–Swinnerton-Dyer conjecture in the analytic rank 0 and 1 cases to all isogeny factors of $J_1(N)$ (see Kato [55, Corollary 14.3]) shows that the order of vanishing of $L(f, s)$ at 1 cannot be 0 or 1 since this would give J rank 0 or 1 as a $\mathbb{Z}[\zeta_3]$-module. So the order of vanishing is at least 2. An upper bound was again obtained using interval arithmetic.

Self-dual analytic rank 3. The approach here is similar to that in §9.4 and the result was already briefly mentioned in [31, Section 3.4] where the analytic rank is determined for all elliptic curves of conductor $N < 130\,000$. There is only one newform that numerically seems to be of analytic rank 3 in the database, namely 5077.2.a.a of weight 2, level 5077 and trivial character. This modular form corresponds to the elliptic curve $y^2 + y = x^3 - 7x + 6$ which has rank 3 and is the only one in its isogeny class. The verification that its L-function has analytic rank 3 is a famous calculation of Buhler–Gross–Zagier [16], used by Gross–Zagier [46] in their solution to the Gauss class number 1 problem. We confirm it quickly as follows: by known cases of the Birch–Swinnerton-Dyer conjecture, the analytic rank cannot be 0 or 1; by parity of the root number, the analytic rank cannot be 2, so it must be at least 3; and an upper bound on the analytic rank of 3 is obtained by interval arithmetic.

9.5. **Chowla's conjecture.** The definition of analytic rank (Definition 9.4.1) as an order of vanishing also makes sense for k odd, and by analogy one might also find it natural to study the central values of $L(f, s)$ at $k/2$ and their derivatives. However, for k odd the central value $s = k/2$ is not a *special* value in the sense of Deligne [38] and thus there is no abelian group whose rank (as a module over an appropriate coefficient ring) is conjecturally related to its leading Taylor coefficient. It would therefore be a stretch to call the order of vanishing at the central point an *analytic rank*. Moreover, one does not expect $L(f, k/2)$ to ever vanish, and this is a generalization of Chowla's conjecture for Dirichlet L-functions [22], as follows.

Let χ be a non-trivial Dirichlet character, then the functional equation associated to $L(\chi, s) := \sum \chi(n) n^{-s}$, similar to equation 9.1.3, relates $L(\chi, s)$ to $L(\overline{\chi}, 1 - s)$. The value of $L(\chi, 1)$ is quite well understood. For example, the fact that $L(1, \chi) \neq 0$ gives us Dirichlet's theorem on arithmetic progressions, and for primitive real characters the value $L(\chi, 1)$ gives us Dirichlet's class number formula. As mentioned above, inspired by Definition 9.4.1, one might also find it natural to study the order of vanishing of $L(\chi, s)$ at $s = 1/2$ and its derivatives. However, it is believed that $L(\chi, 1/2) \neq 0$; this was first conjectured by Chowla [22] for primitive real characters and later generalized to other characters. One of the reasons behind such a belief is that for primitive real characters the root number of such L-functions is always 1 [45], and thus there is no simple reason for $L(\chi, 1/2)$ to vanish. Although Chowla's conjecture remains open, it has been numerically verified

for all real characters χ of modulus less than 10^{10} [74], and substantial progress towards showing the non-vanishing of $L(\chi, 1/2)$ has also been made, see [45] for a short overview.

A generalization of Chowla's conjecture is that $L(f, k/2) \neq 0$ for k odd. As in the case of Dirichlet L-functions for primitive real characters, we also have that the root number of $L(f, k/2)$ can never be -1 when f is self-dual. This is in stark contrast to the case of self dual even weight modular forms, where the root numbers are split approximately 50-50 between -1 and 1. We verified this generalization of Chowla's conjecture, as we computed $L(f, k/2)$ for every newform in our database with $k \leq 200$, and found that this was nonzero for all the odd weight newforms.

10. An overview of the computation

In this section, we provide an overview of the computations we performed, the results of which are now available in the LMFDB [62]. These were accomplished using a combination of Magma, Pari/GP, and SageMath scripts, as well as hand written C code for some of the more computationally-intensive tasks. In aggregate, these computations consumed more than 100 years of CPU time.

10.1. **Data extent.** Our database consists of four overlapping sets of newforms described in Table 10.1.1. These datasets were chosen both for reasons of mathematical interest, and to ensure that the database included all modular forms contained in existing datasets such as the Stein tables of modular forms [92], the Buzzard-Lauder tables of weight one newforms [20], and the previous database of modular forms contained in the LMFDB. More detailed statistics on the newforms in the database can be found at the statistics page.

Constraints on $S_k^{\text{new}}(N, \chi)$	Newspaces	Newforms	Embeddings
(1) $Nk^2 \leq 4\,000$	30 738	67 180	9 966 498
(2) $Nk^2 \leq 40\,000$, $\lvert\chi\rvert = 1$	16 277	170 611	3 092 301
(3) $Nk^2 \leq 40\,000$, $k > 1$, $\dim S_k^{\text{new}}(N, \chi) \leq 100$	30 345	131 540	1 648 617
(4) $Nk^2 \leq 40\,000, N \leq 24$ or $Nk^2 \leq 100\,000, N \leq 10$ or $N \leq 100, k \leq 12$	7 627	12 237	676 574
Union of sets above	62 142	281 219	14 398 359

Table 10.1.1: Extent of the newform database (only nonzero newspaces are included)

For the first dataset (1), we used three independent sources of newform data:

- Complex eigenvalue data for each embedded newform of weight $k > 1$ computed by the `mflib` software package [8], which uses Arb [53] to rigorously implement the trace formula (as described in [89], for example) to obtain approximate complex values to a precision of 200 decimal digits.
- Exact algebraic eigenvalue data for each newform of weight $k > 1$ and dimension $d \leq 20$ computed using Magma's [12] modular symbols package (originally written by William Stein);
- Exact algebraic eigenvalue data for each newform of weight $k > 1$ and dimension $d \leq 20$ were computed using the modular forms implementation in Pari/GP [76] described in [4], which was also applied to all newforms of weight $k = 1$.

For $k > 1$ and $Nk^2 \leq 4000$ the decomposition of every newspace $S_k^{\text{new}}(N, \chi)$ was computed in all three cases and compared for consistency. Exact algebraic data was computed only for newforms of dimension $d \leq 20$, except for $k = 1$ where exact algebraic data was computed in every case.

For newforms of weight $k > 1$ and dimension $d \leq 20$, the algebraic data independently computed by Magma and Pari/GP were checked for consistency (this was not a completely trivial task, as it generally required determining an appropriate automorphism of the coefficient field in order to compare sequences of Fourier coefficients). We also compared the trace forms using all three methods and compared the results for consistency, and for newforms of weight $k = 1$ and level $N \leq 1500$ we compared the Pari/GP computations with the Buzzard-Lauder database [20].

Datasets (2) and (3) were computed entirely in Magma, as was dataset (4), except for 12 spaces of high dimension where complex analytic methods were used. For the portions of these datasets that overlap with the Stein database of modular forms [92], we compared the results for consistency.

For newforms $f = \sum a_n q^n$ of level $N \leq 1000$ we computed 1000 coefficients a_n, while for newforms of level $1001 \leq N \leq 4000$ we computed 2000 coefficients, and for newforms of level $4001 \leq N \leq 10\,000$ we computed 3000 coefficients. This substantially exceeds the Sturm bound in every case, and also exceeds the bound $30\sqrt{N}$ required for the L-function calculations described in §9. For every newform in the database we computed complex coefficients to a precision of at least 200 bits. In cases where we compute algebraic coefficient data we computed an optimized representation using an LLL-basis as described in §8.7, along with a set of generators for the coefficient ring.

For each newform we determined any non-trivial self-twists admitted by the newform (CM, RM, or both), and for newforms with algebraic eigenvalue data available, we computed all inner twists as described in §11. We also computed the analytic rank of every newform, as described in §9.4, and for weight one newforms we computed the image of the associated projective Artin representation and a defining polynomial for its kernel, as described in §12. These computations have now all been rigorously verified.

In addition to the newform database, we computed dimension tables for all newspaces in the range $Nk^2 \leq 40\,000$ with $k > 1$, and we computed trace forms for all newspaces of level $N \leq 4000$ in this range using the `mftraceform` function in Pari/GP.

10.2. **Statistics.** In addition to the ability to browse and to search for examples with specific properties, the modular forms database allows for an investigation of arithmetic statistics. The LMFDB [62] includes precomputed tables displaying how various quantities vary across the database, some of which we have duplicated here in Tables 10.2.2, 10.2.3, 10.2.4, and 10.2.5.

In addition to these static tables, we have added *dynamic statistics*

`http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/dynamic_stats`

which allow users to customize which variables to view and any constraints to impose. For example, a researcher might create a table displaying how the weight and level vary among forms with complex multiplication. We hope that this new feature will enable examination of large-scale patterns, both in the modular form data and elsewhere in the LMFDB.

Remark 10.2.1. The statistics and examples presented in this article reflect the dataset defined in §10.1, which represents the state of the LMFDB as of January 2020. As new data is added to the LMFDB these statistics may no longer match those displayed in the LMFDB, and the number of newforms returned by some of the example queries listed below may increase.

analytic rank	0	1	2	3
count	191 520	87 052	2 566	1
proportion	68.12%	30.96%	0.91%	0.00%
example	23.1.b.a	37.2.a.a	389.2.a.a	5077.2.a.a

Table 10.2.2: Distribution of analytic ranks

projective image	A_4	S_4	A_5	D_2	D_n
count	458	1 033	202	1 311	17 613
proportion	2.37%	5.35%	1.05%	6.79%	91.23%
example	124.1.i.a	148.1.f.a	1763.1.p.b	3600.1.e.a	3997.1.cz.a

Table 10.2.3: Distribution of projective images

Inner twists	Unknown	1	2	4	6	8	10	12
count	73 993	129 197	47 492	25 803	24	4 295	6	51
proportion	26.31%	45.94%	16.89%	9.18%	0.01%	1.53%	0.00%	0.02%

Inner twists	16	20	24	32	40	44	56
count	311	3	14	20	7	1	2
proportion	0.11%	0.00%	0.00%	0.01%	0.00%	0.00%	0.00%

Table 10.2.4: Distribution of inner twists

	weight					
	1	2	3	4	5-316	total
neither	1 693	174 853	11 117	27 877	40 278	255 818
	8.77%	98.27%	87.85%	98.02%	93.91%	90.97%
CM only	15 841	3 074	1 538	563	2 613	23 629
	82.05%	1.73%	12.15%	1.98%	6.09%	8.40%
RM only	461					461
	2.39%					0.16%
both	1 311					1 311
	6.79%					0.47%

Table 10.2.5: Distribution of self twist types by weight

10.3. **Data reliability.** All of our modular form data was computed or verified using rigorous algorithms that do not depend on any unproved assumptions or conjectures.

- Self-twists were either verified via Theorem 11.2.4 and Proposition 11.1.7 using exact algebraic Fourier coefficients a_n or ruled out using complex approximations of sufficient precision to rigorously distinguish zero and nonzero values of a_n and checking for self-twists by all primitive quadratic characters ψ of conductor dividing the level (a newform that admits a self-twist by ψ must have $a_n = 0$ whenever $\psi(a_n) \neq 1$).
- We computed and verified inner twists for all newforms in our dataset that are either of weight one or have dimension at most 20 by computing sufficiently many algebraic Fourier coefficients and applying Theorem 11.2.4 and Proposition 11.1.7.
- Analytic ranks were computed using complex approximations as described in §9 and then rigorously verified using the symbolic methods described in §9.4.
- For weight one newforms the classification of projective images as D_n, A_4, S_4, A_5 was rigorously verified by explicitly computing the number field fixed by the kernel of the associated

projective Galois representation. As described in §12, this was accomplished using a combination of the ray class field functionality provided by Pari/GP and Magma, the rigorous tabulation of all A_4, S_4, and A_5 number fields with compatible ramification, and the explicit computation of quotients of ring class fields of orders in imaginary quadratic fields via the theory of complex multiplication.

In addition to using mathematically rigorous algorithms, we performed a variety of consistency checks intended to catch any errors in the software packages used to compute modular forms data, or any errors that might have been introduced during post-processing. The following checks have been performed:

- All newforms of weight $k > 1$ and level N satisfying $Nk^2 \leq 2000$ have been independently computed using Magma and Pari/GP. By comparing the results of these computations we have verified that the decompositions of each newspace $S_k^{\mathrm{new}}(N, \chi)$ into Galois orbits agree (with matching coefficient fields), that the first 1000 coefficients of the trace forms for each Galois orbit agree, and for newforms of dimension $d \leq 20$, that there is an automorphism of the coefficient field that relates the sequences of algebraic eigenvalues $(a_1, \ldots, a_{1000})$ computed by Pari/GP and Magma.
- For all newforms of weight $k > 1$ and level N satisfying $Nk^2 \leq 4000$ we have verified that the trace forms computed by Magma (using modular symbols) agree with the trace forms obtained from complex analytic data computed using the explicit trace formula. This also verifies the dimensions of the coefficient fields.
- For newforms of weight $k = 1$ and level $N \leq 1000$ we have matched the data computed using Pari/GP with the tables computed by Buzzard and Lauder [20].
- For all dihedral newforms of weight $k = 1$ and level $N \leq 4000$ we have matched trace forms with data computed using the explicit trace formula in Pari/GP with data independently computed using the ray class field functionality implemented in Pari/GP and Magma.

As a consistency check for our L-function computations, after computing a provisional list of all non-trivial zeros on the critical line up to a chosen height bound b we confirmed that no zeros are missing, in other words, that the Riemann Hypothesis holds for each L-function up to height b. We use the method described in [17] based on the Weil–Barner explicit formula. If an L-function also arises from another object in the LMFDB for which we already had computed its L-function we verified that these computations match.

10.4. **Interesting, extreme behavior and examples from the literature.** When putting modular forms in a database it is easy to view them as an aggregate, but of course each modular form is distinct and many have unique interesting properties.

We take this opportunity to recall the rich history and special properties of several forms in this database. We also provide links between these forms and the literature and note several forms that have naturally arisen in previous work. We focus on weight $k \geq 2$ in this section; see §12.5 for interesting behavior in weight $k = 1$.

- The most well known, and the prototypical, example of a modular form is the Ramanujan Δ function, of weight 12 and level 1; its label is 1.12.a.a. This is the lowest weight in which a cusp form appears for the full modular group, so many properties of more general newforms were first noticed for Δ. Similarly, Δ has served as a testing ground for techniques and results before they were known more generally. For instance, the Ramanujan–Petersson conjecture was first made by Ramanujan for Δ but later extended to all newforms. Additionally, computation of the q-expansion coefficients of Δ, traditionally denoted by $\tau(n)$ and known as Ramanujan's τ function, is the subject of the monograph [40].

- By the modularity theorem, newforms of weight 2 with rational coefficients correspond to isogeny classes of elliptic curves over $\mathbb{Q}$. The smallest level in which a weight 2 form appears is 11, corresponding to the smallest conductor of an elliptic curve over $\mathbb{Q}$. Here we necessarily have trivial character and the label is 11.2.a.a; this form has q-expansion

$$q\prod_{k\geq 1}(1-q^k)^2(1-q^{11k})^2.$$

- The weight 2 newforms with CM by fields with the largest absolute discriminants in the database are 2169.2.d.a with CM by $\mathbb{Q}(\sqrt{-723})$, 8388.2.e.c and 2097.2.d.a with CM by $\mathbb{Q}(\sqrt{-699})$, 2061.2.c.c with CM by $\mathbb{Q}(\sqrt{-687})$, and 7524.2.l.b with CM by $\mathbb{Q}(\sqrt{-627})$—the last of these has 8 inner twists.
- The weight 2 newform 867.2.i.a with CM by $\mathbb{Q}(\sqrt{-51})$ has 32 inner twists, and the weight 1 newform 3481.1.d.a with CM by $\mathbb{Q}(\sqrt{-59})$ has 56 inner twists.
- The weight 3 newform 7.3.b.a has CM by $\mathbb{Q}(\sqrt{-7})$, making it the first (by analytic conductor) newform of weight ≥ 3 with CM.
- Watkins [103, §9.1.3] discusses several examples of modular forms of analytic rank 2. The query `http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/?weight=4-&analytic_rank=2-` returns 130 forms of weight at least 4 and analytic rank at least 2, many of which are mentioned by Watkins, including 2 of weight 8.
- Watkins also discusses modular forms of weight 2 with which are non-self-dual yet have positive analytic rank, particularly examples with quadratic character, such as 122.2.b.a. The query `http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/?weight=2&char_order=2&is_self_dual=no&analytic_rank=1-` produces 567 such examples. In larger weight we have 8.14.b.a which is non-self-dual and has analytic rank 1, as does 162.12.c.i.
- The index of the coefficient ring in the ring of integers of the coefficient field can get quite large, as in the case of the newform 8.21.d.b where the index is at least $2^{153}\cdot 3^{15}\cdot 5^4\cdot 7^2$. In weight 2, the largest index we computed was $2^{26}\cdot 3^4$ for 2016.2.k.b and 4032.2.k.h.
- Many newforms in our database have very large Hecke orbits. For example, the newform 983.2.c.a has relative dimension 81 over its character field $\mathbb{Q}(\zeta_{491})$ and $\mathbb{Q}$-dimension 39 690.

10.5. **Pictures.** For every newform f, every nonempty newspace $S_k^{\mathrm{new}}(N,\chi)$, and $S_k^{\mathrm{new}}(\Gamma_1(N))$ for which we have all the newforms, we have created a portrait based on their trace forms, a total of 641 562 portraits. The picture is generated by plotting the absolute value of the trace form in the Poincaré disk, obtained as the image of $(1-iz)/(z-i)$ in $\mathcal{H}$, where the color hue represents the absolute value modulo 1 (with blue being zero, and increasing through purple, red, orange, yellow, ...). For example, as the trace form is always zero at ∞, the top center is always blue, see Figure

10.5.1.

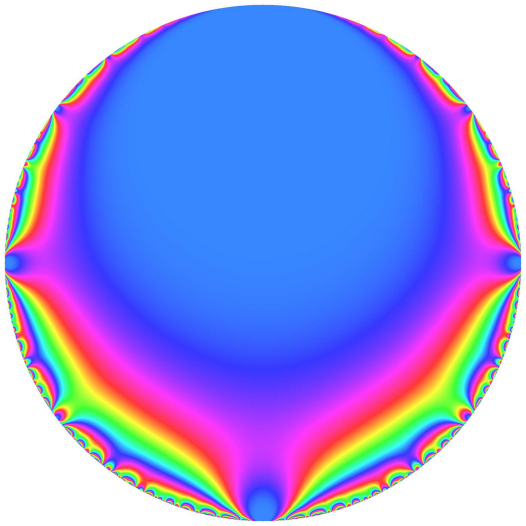

Figure 10.5.1: Portrait of 23.1.b.a

We deviated from the normal approach, used by `complex_plot` in SageMath, of representing magnitude by brightness (with zero being black and infinity being white) and the argument by hue, as this often leads to an overexposed or underexposed picture, see Figure 10.5.2.

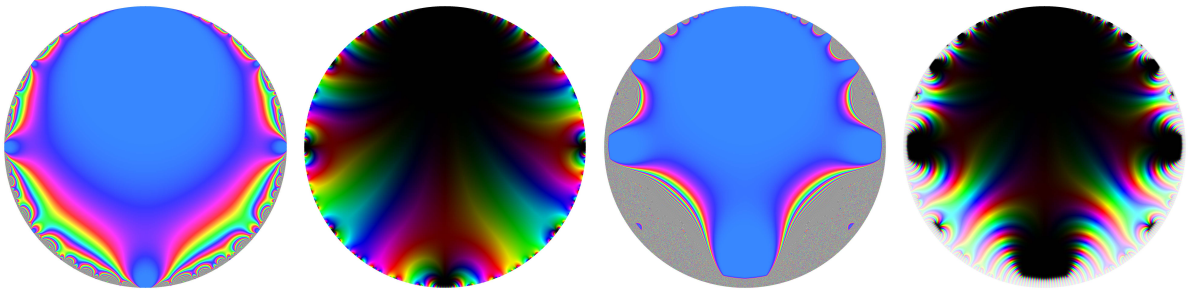

Figure 10.5.2: Portraits of 11.2.a.a and 1.12.a.a and their plots using `complex_plot` in SageMath

Given the number of portraits needed, we limited ourselves to the first 100 Dirichlet coefficients of the trace form, working with 200 bits of precision, evaluating it in a 300×300 grid in $[-1, 1]^2$, and storing the picture as a 184×184 PNG. Overall this consumed about 100 CPU days, and their disk footprint is 45 GB. For aesthetic reasons, the portraits presented here were computed to a higher quality, which creates some discrepancies with the online version, especially in higher weight newforms.

Even though we opted for a plot with less information, it still captures some mathematically interesting features. For example, the behavior on the edge of the disk is a good indicator for level

and weight, see Figures 10.5.3 and 10.5.4.

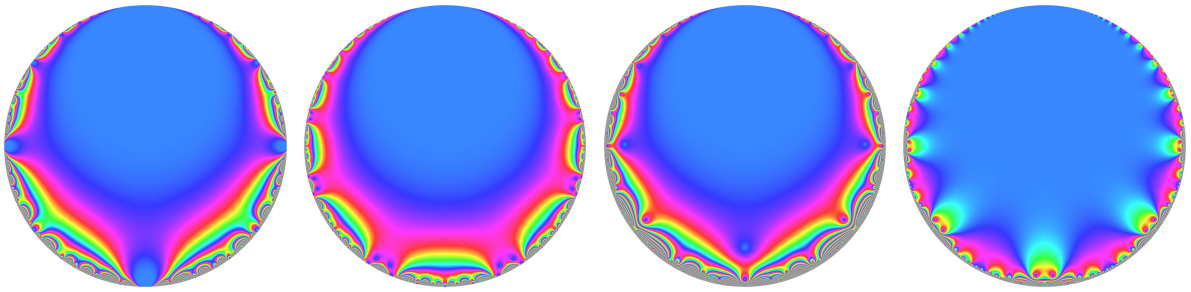

Figure 10.5.3: The portraits for 11.2.a.a, 100.2.a.a, 1001.2.a.a, and 9996.2.a.a

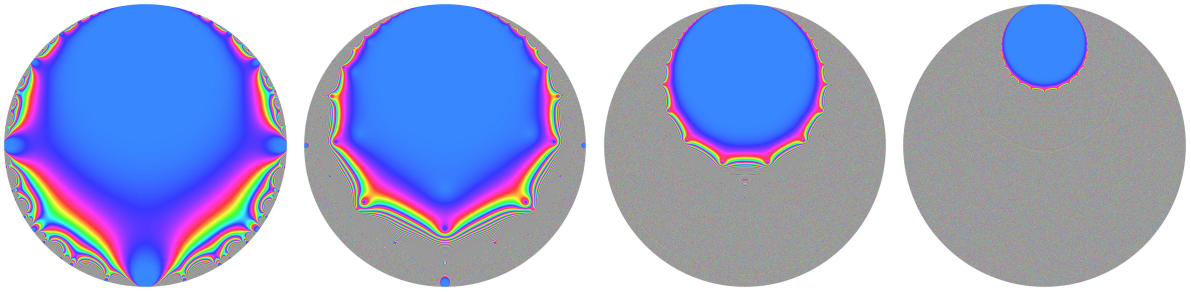

Figure 10.5.4: The portraits for 7.3.b.a, 7.9.b.a, 7.27.b.a, and 7.81.b.a

The size of the blue spot on top center is inversely correlated with the growth of the trace form away from ∞, thus for fixed weight this is a good indicator for the dimension, see Figures 10.5.5: their dimensions are 1, 4, 33, and 120, respectively.

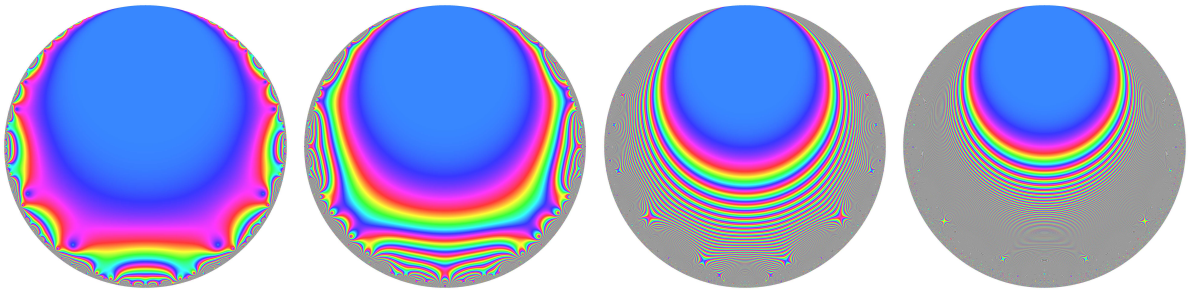

Figure 10.5.5: The portraits for 9359.2.a.a, 9359.2.a.e, 9359.2.a.k, and 9359.2.a.r

Finally, one could also be tempted to infer the self-twists of a newform by comparing it with other forms in $S_k^{\mathrm{new}}(\Gamma_1(N))$, see Figures 10.5.6 for $S_1^{\mathrm{new}}(\Gamma_1(164))$.

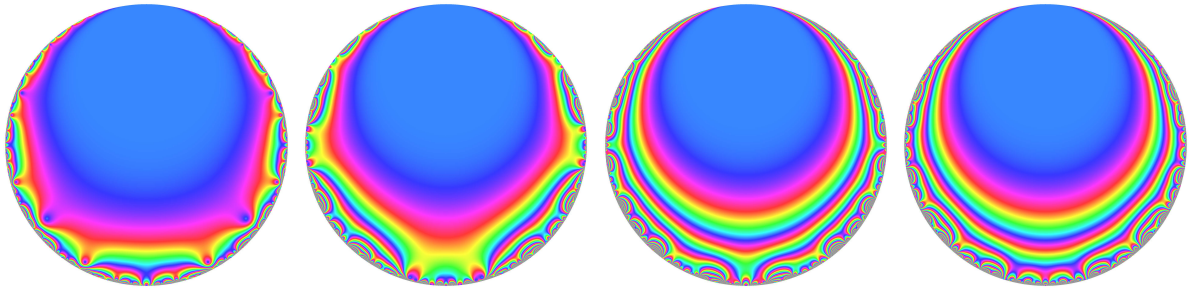

Figure 10.5.6: The portraits for 164.1.d.a, 164.1.d.b, 164.1.j.a, and 164.1.l.a

Remark 10.5.7. These portraits differ from those now used in the LMFDB. Between writing and publishing this article we chose to instead use the pure phase portraits describe in §2.2.5 of [61].

10.6. **Features.** In parallel to carrying out the computations described elsewhere in this paper, we rewrote the user interface to the database. We highlight some of the more prominent new features in this section, some of which are being extended to other sections of the LMFDB.

The search interface includes multiple modes for viewing results. After entering constraints such as weight, level and dimension, there are four different search buttons available. In addition to the standard list of results, a user can choose to go straight to a randomly chosen newform. Alternatively, there are dimension tables available which display the dimension of the spaces of newforms as a function of weight and level. Finally, a table of traces allows for searching on specific Fourier coefficients, including specifying a particular class modulo an arbitrary integer. This feature can be used to find modular forms matching geometric objects via point-counting.

All of these search modes are also available for newspaces. For newspaces, the list mode shows the dimensions of the corresponding newforms as well as the Atkin-Lehner dimensions in the case of trivial character. For both newforms and newspaces, users can customize the order of the search results.

The homepage for an individual newform has also been completely restructured. Newforms can be downloaded and reconstructed in Magma, allowing for further computations if desired. We include complex eigenvalues for embedded modular forms even when exact Fourier coefficients are not feasible to compute.

One of the key motivations for our extensive computations of (exact or inexact) Fourier coefficients of newforms is to allow their L-functions to be computed. In addition to providing additional mathematical information about the newform, such as its analytic rank and special values, this allows us to automatically connect newforms to other objects in the LMFDB. Examples include:

- The L-function L(256.2.a.e) lists both the Bianchi modular form 2.0.4.1-4096.1-b and the Hilbert modular form 2.2.8.1-1024.1-m as origins (both arise as base changes of 256.2.a.e), as well as the corresponding elliptic curve isogeny classes 2.0.4.1-4096.1-b over $\mathbb{Q}(i)$ and 2.2.8.1-1024.1-m over $\mathbb{Q}(\sqrt{2})$.
- The L-function L(72.2.d.a) has (at least) three additional origins: the Hilbert modular form 2.2.8.1-81.1-b, the elliptic curve isogeny class 2.2.8.1-81.1-b, and the isogeny class 5184.a of the Jacobian of the genus 2 curve 5184.a.46656.1.
- The L-function L(1948.1.b.a) also arises as the L-function of (the Galois orbit of) the icosahedral Artin representation 2.1948.24T576.1. The L-functions home page also lists

the four conjugate Artin representations (and four embedded weight one newforms) whose L-functions are primitive factors of this imprimitive L-function of degree 8.

11. Twisting

In this section, we discuss twists of modular forms and related computational issues. For background and further reading, we refer the reader to the foundational articles by Ribet [79, 80].

11.1. **Definitions.** We begin with definitions, followed by some examples. Throughout this section, let $f \in S_k^{\mathrm{new}}(N,\chi)$ be a newform of weight $k \in \mathbb{Z}_{\geq 1}$, level $N \in \mathbb{Z}_{\geq 1}$, and character χ, and let $K_f := \mathbb{Q}(\{a_n(f)\}_n) \subseteq \mathbb{C}$ be its coefficient field. Let ψ be a Dirichlet character of conductor $\mathrm{cond}(\psi)$, and let ψ_0 be the primitive Dirichlet character inducing ψ (with $\mathrm{cond}(\psi_0) = \mathrm{cond}(\psi)$). Then there is a unique newform $g := f \otimes \psi$ characterized by the property that

$$a_n(g) = \psi_0(n)a_n(f) \quad \text{for all } n \text{ coprime to } N\,\mathrm{cond}(\psi); \tag{11.1.1}$$

we call g the twist of f by ψ. However, more is true: in fact, we have

$$a_n(g) = \psi_0(n)a_n(f) \quad \text{for all } n \text{ coprime to } \mathrm{cond}(\psi) \tag{11.1.2}$$

including those n that are not necessarily coprime to $N\,\mathrm{cond}(\psi)$: see Atkin–Li [2, Theorem 3.2]. By the recurrence satisfied by the Hecke operators, (11.1.2) is equivalent to the condition

$$a_p(g) = \psi(p)a_p(f) \quad \text{for all } p \nmid \mathrm{cond}(\psi). \tag{11.1.3}$$

The newform g has character $\chi\psi^2$ (by (11.1.8) below) and level dividing $\mathrm{lcm}(N, \mathrm{cond}(\psi)\,\mathrm{cond}(\chi\psi))$ (by Lemma 11.2.1 below). We call the newform g the twist of f by ψ and say that g is a twist of f.

As above, the group $\mathrm{Aut}(\mathbb{C})$ acts on the set of newforms in $S_k^{\mathrm{new}}(N,\chi)$, with $a_n(\sigma(f)) = \sigma(a_n(f))$ for all $n \geq 1$. We have $\sigma(f) \in S_k^{\mathrm{new}}(N, \sigma(\chi))$, where $\sigma(\chi)(n) = \sigma(\chi(n))$ for all $n \geq 1$. If $g = f \otimes \psi$, then $\sigma(g) = \sigma(f) \otimes \sigma(\psi)$ for all $\sigma \in \mathrm{Aut}(\mathbb{C})$. Accordingly, the set

$$[f] \otimes [\psi] := \{f' \otimes \psi' : f' \in [f], \psi' \in [\psi]\} \tag{11.1.4}$$

has an action of $\mathrm{Aut}(\mathbb{C})$ and so consists of finitely many $\mathrm{Aut}(\mathbb{C})$-orbits (possibly more than one). Accordingly, we say that $[g]$ is a twist of $[f]$ by $[\psi]$ if there exist $f' \in [f]$, $\psi' \in [\psi]$, $g' \in [g]$ such that $g' = f' \otimes \psi'$, or equivalently, $[g] \subseteq [f] \otimes [\psi]$.

Example 11.1.5. The newform orbits 3380.1.v.e and 3380.1.v.g are both twists of 3380.1.g.c by 13.f (and by 260.bc).

With this Galois digression out of the way, we return to the treatment of twists of (embedded) newforms.

Definition 11.1.6. Let ψ be a Dirichlet character and $\sigma\colon K_f \hookrightarrow \mathbb{C}$ be a field embedding. We say that f admits an inner twist by the pair (ψ, σ) if $f \otimes \psi = \sigma(f)$. In the special case that $\sigma = \mathrm{id}\,|_{K_f}$, we say that f admits a self-twist by ψ.

Let $\mathrm{InnTw}(f)$ denote the set of inner twists of f and $\mathrm{SelfTw}(f) \subseteq \mathrm{InnTw}(f)$ the subset of self-twists. Then projection onto the first component identifies $\mathrm{SelfTw}(f)$ with a subgroup of Dirichlet characters. By (11.1.2), the form f has an inner twist by (ψ, σ) if and only if $\sigma(a_n) = \psi(n)a_n$ for almost all n. The twist is said to be inner because such twists stay "within" the Galois orbit of f (a nontrivial inner twist is sometimes also referred to as an "extra twist"). Every newform has a trivial self-twist by $(\mathsf{1.a}, \mathrm{id}\,|_{K_f})$.

Proposition 11.1.7 (Ribet [80], Momose [72])**.** *The following statements hold.*

(a) *If $(\psi, \sigma) \in \mathrm{InnTw}(f)$, then*

$$\sigma(\chi) = \chi\psi^2;$$

so if $\psi \in \mathrm{SelfTw}(f)$ then ψ is quadratic.

(b) *If* $(\psi, \sigma) \in \mathrm{InnTw}(f)$ *then* $\sigma \in \mathrm{Aut}(K_f)$.

(c) $\mathrm{InnTw}(f)$ *naturally forms a group under*

$$(\psi, \sigma) \cdot (\psi', \sigma') := (\psi\, \sigma(\psi'), \sigma\sigma').$$

(d) *There is an exact sequence of groups*

$$1 \to \mathrm{SelfTw}(f) \to \mathrm{InnTw}(f) \xrightarrow{\pi} \mathrm{Aut}(K_f)$$
$$(\psi, \sigma) \mapsto \sigma.$$

Let $A := \pi(\mathrm{InnTw}(f))$. *Then* $\mathrm{InnTw}(f) \simeq \mathrm{SelfTw}(f) \times A$ *is a* direct *product.*

(e) *The projection* $(\psi, \sigma) \mapsto \psi$ *from* $\mathrm{InnTw}(f)$ *to the set of Dirichlet characters is an injective map of sets.*

(f) *The group* A *is abelian.*

(g) *Suppose* $\mathrm{SelfTw}(f)$ *is trivial. Then* π *is an isomorphism and the assignment* $\sigma \mapsto \psi_\sigma$ *if and only if* $(\psi_\sigma, \sigma) \in \mathrm{InnTw}(f)$ *is a well-defined* 1*-cocycle, i.e.,*

$$\psi_{\sigma\sigma'} = \psi_\sigma \sigma(\psi_{\sigma'}).$$

Proof. These results originate with Ribet [80, §3] and Momose [72, Lemma (1.5)], but they work under the hypothesis that f has no self-twists. For clarity, we repeat these arguments to show this hypothesis is unnecessary. Let $f(q) = \sum_n a_n q^n$.

Part (a) follows by looking at (Nebentypus) characters using the Hecke recurrence (or the determinant of the associated Galois representations). Explicitly, on the one hand, the character of $\sigma(f)$ is $\sigma(\chi)$; on the other, if ϵ is the character of $f \otimes \psi$ then for all good primes p the Hecke recurrence reads

$$\varepsilon(p)p^{k-1} = a_p(f \otimes \psi)^2 - a_{p^2}(f \otimes \psi)^2 = \psi(p)^2(a_p(f)^2 - a_{p^2}(f)) = \psi(p)^2\chi(p)p^{k-1} \tag{11.1.8}$$

so $\varepsilon = \chi\psi^2$. Consequently, a self-twist by ψ gives $\chi = \chi\psi^2$, so ψ^2 is the trivial character.

For part (b), by (a) we have $\psi^2 = \sigma(\chi)\chi^{-1}$, and we claim ψ takes values in $\mathbb{Q}(\chi)$: indeed, if $\chi(n) = \zeta$ is a primitive dth root of unity, then checking cases based on the parity of d reveals that $\sigma(\zeta)/\zeta \in \langle\zeta^2\rangle$. Since $\mathbb{Q}(\psi) \subseteq K_f$, we conclude $\sigma(a_n) = \psi(n)a_n \in K_f$ for almost all n, so $\sigma(K_f) \subseteq K_f$ as desired.

For part (c), we start with $\sigma'(a_n) = \psi'(n)a_n$ and apply σ to get

$$(\sigma\sigma')(a_n) = \sigma(\psi')(n)\sigma(a_n) = \sigma(\psi')(n)\psi(n)a_n$$

for almost all n, so $(\psi\sigma(\psi'), \sigma\sigma') \in \mathrm{InnTw}(f)$. This product is associative: the identity element in $\mathrm{InnTw}(f)$ is $(1.\mathsf{a}, \mathrm{id}\,|_{K_f})$, and inverses are given by $(\psi, \sigma)^{-1} = (\sigma^{-1}(\psi), \sigma^{-1})$.

In part (d), the exact sequence is evident from (c). The group $\mathrm{InnTw}(f)$ visibly has the structure of a semidirect product $\mathrm{InnTw}(f) \simeq \mathrm{SelfTw}(f) \rtimes A$ via $A \to \mathrm{Aut}(\mathrm{SelfTw}(f))$ by $\sigma \mapsto (\psi \mapsto \sigma(\psi))$. However, by (b) $\mathrm{SelfTw}(f)$ consists only of quadratic characters, so $\sigma(\psi) = \psi$ for all σ so the product is direct.

Part (e) follows from the fact that ψ uniquely determines σ.

Part (f) is claimed by Ribet [80, Proposition (3.3)]: we prove it as follows. As in (a), let $\chi(n) = \zeta$ and $\sigma(\chi)(n) = \zeta^k$. Then again $\psi(n) = \zeta^{(k-1)/2}$ (for some choice of square root of ζ). Write similarly $\sigma'(\chi)(n) = \zeta^{k'}$. Then

$$\frac{\sigma'(\psi)}{\psi}(n) = \frac{\zeta^{k'(k-1)/2}}{\zeta^{(k-1)/2}} = \zeta^{(k-1)(k'-1)/2}$$

is well-defined, and by symmetry this is equal to $(\sigma(\psi)/\psi)(n)$, giving $\psi\,\sigma(\psi') = \psi'\,\sigma'(\psi)$, and similarly $\sigma'(\chi)(n) = \zeta^{k'}$. This calculation shows the projection of the products $(\psi, \sigma)(\psi', \sigma') =$

$(\psi\sigma(\psi'), \sigma\sigma')$ and $(\psi', \sigma')(\psi, \sigma) = (\psi'\sigma'(\psi), \sigma\sigma')$ agree. By part (e), it follows that $\sigma\sigma' = \sigma'\sigma$ and A is abelian.

Finally, part (g) is immediate from (c). □

Example 11.1.9. Consider the (embedded) newform 180.1.m.a.107.2; it represents the unique newform orbit in the space 180.1.m of weight 1 and level 180 with character orbit 180.m, whose q-expansion begins

$$f(q) = q - \zeta_8^3 q^2 - \zeta_8^2 q^4 + \zeta_8^3 q^5 - \zeta_8 q^8 + O(q^{10}),$$

where $\zeta_8 = \exp(2\pi i/8) = (1+i)/\sqrt{2}$ is the primitive eighth root of unity in the upper quadrant and $K_f = \mathbb{Q}(\zeta_8)$.

The group $\mathrm{SelfTw}(f)$ of self-twists is of order 2 with nontrivial character 4.3, the quadratic character of conductor 4 associated to the field $\mathbb{Q}(\sqrt{-1})$. The group of inner twists has order $\#\,\mathrm{InnTw}(f) = 8$, and we compute $\mathrm{InnTw}(f) \simeq (\mathbb{Z}/2\mathbb{Z})^3$, generated by the elements

$$(4.3, \mathrm{id}), (3.2, \zeta_8 \mapsto -\zeta_8), (5.3, \zeta_8 \mapsto \zeta_8^3).$$

The character ψ_5 with label 5.3 has order 4, so letting $\sigma_3 \in \mathrm{Aut}(\mathbb{Q}(\zeta_8))$ by $\sigma_3(\zeta_8) = \zeta_8^3$, we have

$$(\psi_5, \sigma_3)^2 = (\psi_5\, \sigma_3(\psi_5), \sigma_3^2) = (\psi_5\psi_5^{-1}, \mathrm{id}) = 1.$$

The projection of $\mathrm{InnTw}(f)$ onto the set of characters yields characters with conductors 1, 3, 4, 5, 12, 15, 20, 60.

Example 11.1.10. For f with label 361.2.e.d and $K_f = \mathbb{Q}(\zeta_{18})$, we have no nontrivial self-twists and $\pi\colon \mathrm{InnTw}(f) \to \mathrm{Aut}(K_f)$ is an isomorphism onto its image. In fact, we compute that π is surjective, so $\mathrm{InnTw}(f) \simeq \mathbb{Z}/6\mathbb{Z}$. More precisely, the elements of order 3 in $\mathrm{InnTw}(f)$ correspond to the characters 19.7 and 19.11 of order 3, and in the character orbit 19.e there are three characters whose elements match with automorphisms of order 2 and two of order 6.

Example 11.1.11. Among the forms of weight $k = 2$, trivial character, and dimension 2, we can search for forms with inner twist, and we should see a table that matches Cremona [29, Table 3] up to level $N \le 300$. The lists match with one exception: we found one form 169.2.a.a that was missed by Cremona.

Newforms of weight $k \ge 2$ that admit nontrivial self-twists are commonly said to have *complex multiplication*, for reasons we now explain.

Proposition 11.1.12 (Ribet)**.** *The following statements hold.*

(a) *If $k \ge 2$ and f has nontrivial self-twist by ψ, then ψ is associated to an imaginary quadratic field and is unique, i.e.,* $\mathrm{SelfTw}(f) \simeq \mathbb{Z}/2\mathbb{Z}$.

(b) *If $k = 1$, then f has nontrivial self-twist by ψ if and only if f has dihedral projective image. If so, then ψ may be real or imaginary and* $\mathrm{SelfTw}(f)$ *is a subgroup of* $(\mathbb{Z}/2\mathbb{Z})^2$.

Proof. For part (a), see Ribet [79, Theorem (4.5)], a consequence of the theory of complex multiplication.

For part (b), we recall §12 and observe that f has self-twist by ψ if and only if $a_p(f) = 0$ for all p inert in $\mathbb{Q}(\psi)$ and by classification this happens if and only if the image of the projective Galois representation is dihedral. In this case, let L be the fixed field of the kernel of the projective Galois representation associated to f, so $\mathrm{Gal}(L \,|\, \mathbb{Q}) \simeq D_n$, the dihedral group of order $2n$. Then for each quadratic subfield $F \subseteq L$, the form f has self-twist by the character associated to F. Accordingly, when $n > 2$ the subfield F and associated self-twist character are unique, and when $n = 2$ (so K is biquadratic) there are three distinct subfields and corresponding characters and there is a real quadratic subfield. □

Example 12.5.1 shows that forms in Proposition 11.1.12(b) indeed occur. In light of Proposition 11.1.12, we make the following definition.

Definition 11.1.13. We say f has real multiplication (RM) if f has self-twist by a character attached to a real quadratic field and complex multiplication (CM) if f has self-twist by a character attached to an imaginary quadratic field.

Remark 11.1.14. It is common in the literature to just replace the term *self-twist* by *complex multiplication*. By Proposition 11.1.12(a), there is no harm in this for weight $k \geq 2$, but for weight $k = 1$ we think this is potentially confusing, and we want to avoid saying "f has complex multiplication by $\mathbb{Q}(\sqrt{5})$."

Example 11.1.15. As in the proof of Proposition 11.1.12(b), weight 1 forms can have RM or CM or both. Forms with RM correspond precisely to ray class characters of real quadratic fields that are of mixed signature (i.e., even at one real place and odd at another).

Example 11.1.16. CM modular forms may also have an inner twist that is not a self-twist: the smallest example by analytic conductor is 52.1.j.a, having CM by $\mathbb{Q}(\sqrt{-1})$ and two inner twists that are not self-twists. This phenomenon is not restricted to weight 1, for example the same is true of the form with label 20.2.e.a.

Continuing with the theme of working with newforms that have not yet been embedded, we conclude this section by showing that the inner twist group is well-defined on the Galois orbit.

Lemma 11.1.17. *For all $\tau \in \mathrm{Aut}(\mathbb{C})$, we have an isomorphism of groups*

$$\begin{aligned} \mathrm{InnTw}(f) &\xrightarrow{\sim} \mathrm{InnTw}(\tau(f)) \\ (\psi, \sigma) &\mapsto (\tau\psi, \tau\sigma\tau^{-1}). \end{aligned} \tag{11.1.18}$$

Proof. From $\sigma(a_n) = a_n\psi(n)$ for almost all n we conclude

$$(\tau\sigma\tau^{-1})(\tau(a_n)) = \tau(a_n)(\tau\psi)(n)$$

for almost all n, and conversely. □

11.2. **Detecting inner twists.** With definitions out of the way, we now drill down to precisely understand the level of twists. We keep notation from the previous section, in particular $f(q) = \sum_n a_n(f)q^n \in S_k^{\mathrm{new}}(N, \chi)$ is a newform and ψ is a Dirichlet character of conductor $\mathrm{cond}(\psi)$.

Lemma 11.2.1. *Let M be the level of $f \otimes \psi$, so $f \otimes \psi \in S_k^{\mathrm{new}}(M, \chi\psi^2)$. Then the following statements hold:*

(a) *For all primes p, we have the inequality*

$$\mathrm{ord}_p(M) \leq \max\big(\mathrm{ord}_p(N), \mathrm{ord}_p(\mathrm{cond}(\psi)\,\mathrm{cond}(\chi\psi))\big),$$

with equality if $\mathrm{ord}_p(N) \neq \mathrm{ord}_p(\mathrm{cond}(\psi)\,\mathrm{cond}(\chi\psi))$. In particular, the level M divides $\mathrm{lcm}(N, \mathrm{cond}(\psi)\,\mathrm{cond}(\chi\psi))$.

(b) *For all primes p we have*

$$\mathrm{ord}_p(\mathrm{cond}(\psi)) \leq \mathrm{ord}_p(\mathrm{cond}(\psi)\,\mathrm{cond}(\chi\psi)) \leq \max(\mathrm{ord}_p(N), \mathrm{ord}_p(M)).$$

In particular, $\mathrm{cond}(\psi)\,\mathrm{cond}(\chi\psi) \mid \mathrm{lcm}(M, N)$, and if $M \mid N$, then $\mathrm{cond}(\psi)\,\mathrm{cond}(\chi\psi) \mid N$.

Proof. Statement (a) can be found in Booker–Lee–Strömbergsson [10, Lemma 1.4]: this improves the upper bound of Shimura [90, Proposition 3.64] and Atkin–Li [2, Proposition 3.1] that

$$M \mid \mathrm{lcm}(N, \mathrm{cond}(\psi)^2, \mathrm{cond}(\chi)\,\mathrm{cond}(\psi)), \tag{11.2.2}$$

which can be proven directly.

For statement (b), we prove the contrapositive. Let $p \mid \operatorname{cond}(\psi)\operatorname{cond}(\chi\psi)$ and suppose that $\operatorname{ord}_p(\operatorname{cond}(\psi)\operatorname{cond}(\chi\psi)) > \operatorname{ord}_p(N)$. Then by (b) we have

$$\operatorname{ord}_p(M) = \operatorname{ord}_p(\operatorname{cond}(\psi)\operatorname{cond}(\chi\psi)) > \operatorname{ord}_p(N). \qquad \square$$

Lemma 11.2.3. *If $a_p(f) \neq 0$ for some prime number p, then $\operatorname{ord}_p(N) \in \{1, \operatorname{ord}_p \operatorname{cond}(\chi)\}$.*

Proof. If $\operatorname{ord}_p(N) = 0$, then $\operatorname{ord}_p(\operatorname{cond}(\chi)) = 0$; if $\operatorname{ord}_p(N) = 1$, also done (without using any hypothesis). Finally, if $\operatorname{ord}_p \operatorname{cond}(\chi) \neq \operatorname{ord}_p(N)$, i.e., χ is a character modulo N/p, then $a_p(f) \neq 0$ implies $\operatorname{ord}_p(N) = 1$ by a result of Li [60, Theorem 3]. $\square$

We recall by Proposition 11.1.7(b) that if $(\psi, \sigma) \in \operatorname{InnTw}(f)$, then $\sigma \in \operatorname{Aut}(K_f)$. But since we do not need this in the proof, we state the following theorem more generally.

Theorem 11.2.4. *Let $f(q) = \sum_n a_n(f)q^n \in S_k^{\mathrm{new}}(N, \chi)$, and let $\sigma \in \operatorname{Gal}(\widetilde{K}_f \mid \mathbb{Q})$ where $\widetilde{K}_f \subseteq \mathbb{C}$ is the Galois closure of K_f. Let ψ be a primitive Dirichlet character, and let ψ' be the primitive character that induces $\chi\psi$. Then $f \otimes \psi = \sigma(f)$ if and only if all of the following conditions hold:*

(i) $\operatorname{cond}(\psi)\operatorname{cond}(\psi') \mid N$;

(ii) $\chi\psi^2 = \sigma(\chi)$; *and*

(iii) $\sigma(a_p(f)) \in \{a_p(f)\psi(p), \overline{a_p(f)}\psi'(p)\}$ *for all primes $p \leq \operatorname{Sturm}(k, N)$.*

Proof. Let $\bar{f} \in S_k^{\mathrm{new}}(N, \overline{\chi})$ denote the dual of f, with coefficients $a_n(\bar{f}) = \overline{a_n(f)}$. Thus $\bar{f} = f \otimes \overline{\chi}$ (cf. Atkin–Li [2, Proposition 1.5] or Ribet [79, §1, p. 21]) and consequently $f \otimes \psi = \bar{f} \otimes \psi'$ as

$$a_n(\bar{f})\psi'(n) = a_n(f)\bar{\chi}(n)(\chi\psi)(n) = a_n(f)\psi(n)$$

whenever $\gcd(n, N) = 1$.

First we prove ($\Rightarrow$), and suppose that $f \otimes \psi = \sigma(f)$. By Proposition 11.1.7 we have $\chi\psi^2 = \sigma(\chi)$. Since $\operatorname{cond}(\sigma(f)) = \operatorname{cond}(f) = N$, we have $\operatorname{cond}(\psi)\operatorname{cond}(\psi') \mid N$ by Lemma 11.2.1(c). Let $D := \gcd(\operatorname{cond}(\psi), \operatorname{cond}(\psi'))$. Then

$$\operatorname{cond}(\chi) = \operatorname{cond}(\psi'\overline{\psi}) \mid \operatorname{lcm}(\operatorname{cond}(\psi), \operatorname{cond}(\psi')) = (\operatorname{cond}(\psi)\operatorname{cond}(\psi')/D) \mid (N/D). \tag{11.2.5}$$

Let p be prime. If $p \nmid \operatorname{cond}(\psi)$ then $\sigma(a_p(f)) = a_p(f \otimes \psi) = a_p(f)\psi(p)$. Similarly, if $p \nmid \operatorname{cond}(\psi')$ then $\sigma(a_p(f)) = a_p(\bar{f} \otimes \psi') = \overline{a_p(f)}\psi'(p)$. Hence we may suppose that $p \mid D$, so by (11.2.5) we have $\operatorname{ord}_p(N) > \max\{1, \operatorname{ord}_p \operatorname{cond}(\chi)\}$. By Lemma 11.2.3, it follows that $a_p(f) = 0$, and thus $\sigma(a_p(f)) = a_p(f)\psi(p)$.

Now we prove the converse ($\Leftarrow$), and suppose that conditions (i)–(iii) hold. Let M be the level of $f \otimes \psi$. Let Q denote the product of primes $p \mid N$ such that either

- $p \nmid M$, or
- $a_p(f) = 0$ and $a_p(f \otimes \psi) \neq 0$.

Let ξ denote the trivial character modulo Q, and define

$$g(q) := \sum_{n=1}^{\infty} a_n(f \otimes \psi)\xi(n)q^n. \tag{11.2.6}$$

We claim that conditions (i)–(ii) imply that $g \in S_k(N, \chi\psi^2)$. By Atkin–Li [2, Proposition 3.1] it suffices to show that

$$\operatorname{lcm}\big(M, \operatorname{cond}(\psi\psi')Q, Q^2\big) \mid N. \tag{11.2.7}$$

By Lemma 11.2.1(a) and the fact that $\operatorname{cond}(\psi)\operatorname{cond}(\psi') \mid N$, we have

$$\operatorname{cond}(\psi\psi') \mid M \mid \operatorname{lcm}\{N, \operatorname{cond}(\psi)\operatorname{cond}(\psi')\} = N,$$

so to prove (11.2.7) it suffices to show that $\mathrm{ord}_p(N) \geq 1 + \max\{1, \mathrm{ord}_p \mathrm{cond}(\psi\psi')\}$ for all primes $p \mid Q$.

Let p be such a prime. Then either $p \nmid M$ or $a_p(f) = \overline{a_p(f)} = 0$ and $a_p(f \otimes \psi) = a_p(\bar{f} \otimes \psi') \neq 0$. In either case we must have $p \mid \gcd(\mathrm{cond}(\psi), \mathrm{cond}(\psi'))$ and, by Lemma 11.2.3, $\mathrm{ord}_p(M) \in \{1, \mathrm{ord}_p \mathrm{cond}(\psi\psi')\}$. It follows that

$$\max\{1, \mathrm{ord}_p \mathrm{cond}(\psi\psi'), \mathrm{ord}_p(M)\} \leq \max\{\mathrm{ord}_p \mathrm{cond}(\psi), \mathrm{ord}_p \mathrm{cond}(\psi')\}.$$

Since $p \mid \gcd(\mathrm{cond}(\psi), \mathrm{cond}(\psi'))$, we have $\min\{\mathrm{ord}_p \mathrm{cond}(\psi), \mathrm{ord}_p \mathrm{cond}(\psi')\} \geq 1$, and hence

$$\mathrm{ord}_p(\mathrm{cond}(\psi)\,\mathrm{cond}(\psi')) \geq 1 + \max\{1, \mathrm{ord}_p \mathrm{cond}(\psi\psi'), \mathrm{ord}_p(M)\}.$$

By Lemma 11.2.1(b) we have

$$\mathrm{ord}_p(N) = \mathrm{ord}_p(\mathrm{cond}(\psi)\,\mathrm{cond}(\psi')) \geq 1 + \max\{1, \mathrm{ord}_p \mathrm{cond}(\psi\psi')\}.$$

This concludes the proof that $g \in S_k(N, \chi\psi^2)$.

Next, we claim that $a_n(g) = \sigma(a_n(f))$ for all $n \leq \mathrm{Sturm}(k, N)$. Since both sequences are multiplicative and $\chi\psi^2 = \sigma(\chi)$, it suffices to verify this equality at primes, p. There are three cases to consider:

- If $p \nmid N$ then $a_p(f)\psi(p) = \overline{a_p(f)}\psi'(p)$, so that $\sigma(a_p(f)) = a_p(g)$.
- If $p \mid N$ and $a_p(f) = 0$ then $a_p(g) = 0$ by construction, and $\sigma(a_p(f)) = 0$.
- If $p \mid N$ and $a_p(f) \neq 0$ then $0 \neq \sigma(a_p(f)) \in \{a_p(f)\psi(p), \overline{a_p(f)}\psi'(p)\}$.
  - If $\sigma(a_p(f)) = a_p(f)\psi(p)$ then $p \nmid \mathrm{cond}(\psi)$, so $a_p(f)\psi(p) = a_p(f \otimes \psi)$.
  - If $\sigma(a_p(f)) = \overline{a_p(f)}\psi'(p)$ then $p \nmid \mathrm{cond}(\psi')$, so
  $$\overline{a_p(f)}\psi'(p) = a_p(\bar{f} \otimes \psi') = a_p(f \otimes \psi).$$
  In either case, we conclude that $\sigma(a_p(f)) = a_p(f \otimes \psi) = a_p(g)$.

By the Hecke–Sturm bound (Proposition 8.2.3), it follows that $g = \sigma(f)$. Finally, since f is a newform, $\sigma(f)$ is as well, and thus $\sigma(f) = g = f \otimes \psi$, by strong multiplicity one. □

We conclude with a variant, similarly useful for algorithmic purposes. We recall the notion of *distinguishing primes* from §8.9.

Theorem 11.2.8. *With the same hypotheses as in Theorem 11.2.4, we have $f \otimes \psi = \sigma(f)$ if and only if conditions hold:*

(i) $\mathrm{cond}(\psi)\,\mathrm{cond}(\chi\psi) \mid N$;

(ii) $\chi\psi^2 = \sigma(\chi)$;

(iii) $\sigma(a_p(f)) = a_p(f)\psi(p)$ *for all primes* $p \leq \mathrm{Sturm}(k, N)$ *with* $p \nmid N$; *and*

(iv) $\sigma(a_p(f)) = a_p(f)\psi(p)$ *for p in a set of distinguishing primes for f.*

Proof. The implication ($\Rightarrow$) is clear, so we prove ($\Leftarrow$).

As in the proof of ($\Leftarrow$) of Theorem 11.2.4, we again consider the form g as in (11.2.6) with ξ the trivial character modulo Q. Let N_g be the level of g. Then in the proof we showed that $N_g \mid N$ and $h := g - \sigma(f) \in S_k(N, \sigma(\chi))$. By (iii) and Hecke recursion, we have $a_n(h) = 0$ for all $n \leq \mathrm{Sturm}(k, N)$ coprime to N.

If $N_g = N$, then by (iv), we have $\sigma(f) = f \otimes \psi$. So we may assume that N_g is a proper divisor of N. We now employ degeneracy operators to upgrade (iii). It is convenient to switch from lower-triangular to upper-triangular matrices. Let

$$\Gamma^1(N) := \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \pmod N\right\}$$

and similarly $\Gamma^0(N)$, and define spaces of modular forms on these groups similarly. We refer to Diamond–Shurman [39, §5.7] for the results we need. The groups $\Gamma_1(N)$ and $\Gamma^1(N)$ are conjugate by the matrix $\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$, giving an isomorphism $\iota_N := S_k(\Gamma_1(N)) \to S_k(\Gamma^1(N))$ whose effect on Fourier expansions is $\sum_n b_n q^n \mapsto \sum_n b_n q_N^n$ where $q_N := \exp(2\pi i z/N)$. Moreover, this map preserves the Nebentypus character. For any $d \mid N$, the trace operator defines a map

$$\pi_d \colon S_k(\Gamma^1(N)) \to S_k(\Gamma_d) \subseteq S_k(\Gamma^1(N))$$

where $\Gamma_d := \Gamma_1(N) \cap \Gamma^0(N/d)$: its effect on Fourier expansions is

$$\sum_{n=1}^{\infty} b_n q_N^n \mapsto \sum_{\substack{n=1 \\ d \mid n}}^{\infty} b_n q_N^n.$$

The operator π_d is a projection operator, and for $d, d' \mid N$ with $\gcd(d, d') = 1$ we have $\pi_d \pi_{d'} = \pi_{d'} \pi_d$.

Consider

$$h' := \prod_{p \mid N} (1 - \pi_p) \iota_N(h) \in S_k(\Gamma^0(N), \chi).$$

By construction, multiplicativity, and (iii), we have $a_n(h') = 0$ for all $n \leq \mathrm{Sturm}(k, N)$. Then by the Hecke–Sturm bound (Proposition 8.2.3), we conclude $h' = 0$. Thus

$$h(q) = \sum_{\substack{n=1 \\ \gcd(n,N) \neq 1}}^{\infty} a_n(h) q^n. \tag{11.2.9}$$

We have realized h as a sum of oldforms. Turning this back to $\Gamma_1(N)$, we conclude that

$$h(q) = \sum_{p \mid N} h_p(q^p) \tag{11.2.10}$$

with $h_p(q) \in S_k(\Gamma_p, \sigma(\chi)_p)$, as in the oldform theory of Atkin–Lehner [1, Theorem 1] and Li [60, Corollary 1]; moreover, $h_p = 0$ if and only if h is new at p.

We now show that $h = 0$. Let $p \mid N$. If χ is not a character modulo N/p, then $S_k(\Gamma_p, \sigma(\chi)_p) = 0$ so $h_p = 0$. So suppose χ is a character modulo N/p.

- Suppose that $a_p(f) \neq 0$. Then by Lemma 11.2.3, we have $p \parallel N$. Thus $\mathrm{ord}_p(\mathrm{cond}(\chi)) = 0$, so by (i) we have $\mathrm{ord}_p(N) \geq 2\,\mathrm{ord}_p(\mathrm{cond}(\psi))$. If $\mathrm{ord}_p(\mathrm{cond}(\psi)) = 0$, then we have twisted by a character trivial at p, so $\mathrm{ord}_p(M) = \mathrm{ord}_p(N)$ by Lemma 11.2.1(b). Therefore $f \otimes \psi$ is new at p, so g is new at p and $a_p(g) = a_p(f \otimes \psi)$ so $h_p = 0$. If instead $\mathrm{ord}_p(\mathrm{cond}(\psi)) \geq 1$, then $p^2 \mid N$, a contradiction.
- Suppose $a_p(f) = 0$. If $a_p(f \otimes \psi) \neq 0$, then by construction, $a_p(g) = 0$ so by multiplicativity $a_n(f) = a_n(g)$ for all $p \mid n$; therefore $h_p = 0$.

We have shown that $\sigma(f) = g$. We then conclude as in the end of the proof of Theorem 11.2.4. □

Example 11.2.11. Consider the space 24.2.f.a. There are two Galois-conjugate newforms with the same Nebentypus character. The Sturm bound is 8, but the smallest $p \nmid N$ where the Fourier coefficients differ is 11. In particular, this shows that in the Hecke–Sturm bound (Proposition 8.2.3) we cannot ignore the primes $p \mid N$.

The virtue of Theorems 11.2.4 and 11.2.8 is that they give explicit criteria to certify inner twists, with care taken concerning primes dividing the level.

11.3. **Computing inner twists.** We used Theorem 11.2.8 to compute the complete group of inner twists for all the modular forms in our dataset. Specifically, we enumerate the finite set X of Dirichlet characters ψ satisfying condition (i) of Theorem 11.2.8 for which $\chi\psi^2$ is conjugate to χ. Note that the set X does not depend on f or its coefficient field, only the character χ and level N. We then determine the subset of X that satisfy conditions (iii) and (iv) for some $\sigma \in \mathrm{Gal}(\widetilde{K}_f)$ as follows:

(1) We first remove from X all characters ψ for which there is a prime $p \le \mathrm{Sturm}(k, N)$ not dividing N such that $a_p(f)\psi(p)$ is not conjugate to $a_p(f)$; this is accomplished by comparing the minimal polynomials of $a_p(f)\psi(p)$ and $a_p(f)$.

(2) For all remaining $\psi \in X$, set $T := \mathrm{Gal}(\widetilde{K}_f)$ and for successive primes $p \le \mathrm{Sturm}(k, N)$ with $p \nmid N$, replace T with $\{\sigma \in T : \sigma(a_p(f)) = a_p(f)\psi(p)\}$, stopping if T becomes empty. This yields a list of candidate inner twists (ψ, σ) containing $\mathrm{InnTw}(f)$.

(3) Finally, for each candidate (ψ, σ) we check whether (iv) holds; if so then Theorem 11.2.8 implies that (ψ, σ) is an inner twist of f.

As shown by Example 11.2.11, the third step above is potentially necessary, but in our computation we never encountered a case where a candidate inner twist that survived step (2) was discarded in step (3).

Remark 11.3.1. The Magma function `InnerTwists` implements a weaker form of Theorem 11.2.4. It requires checking eigenvalues up to the Sturm bound for level $\mathrm{lcm}(N, \mathrm{cond}(\psi)^2, \mathrm{cond}(\psi)\,\mathrm{cond}(\chi))$, and it performs eigenvalue comparisons using complex approximations that do not guarantee a rigorous result. Indeed, even when the optional parameter `Proof` is set to `True`, Magma version 2.24-7 displays the following message:

```
WARNING: Even if Proof is True, the program does not prove that every twist
returned is in fact an inner twist (though they are up to precision 0.00001).
```

12. Weight one

Modular forms of weight one are of particular interest due to the connection with Artin representations, provided by a theorem of Deligne and Serre [37]: one can associate to each weight one newform f an odd irreducible 2-dimensional Galois representations $\rho_f \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ for which $L(f, s) = L(\rho_f, s)$ (recall that a Galois representation is odd if complex conjugation has determinant -1). Following the proof of Serre's conjecture by Khare and Wintenberger [58], we now know that the map $f \mapsto \rho_f$ is in fact a bijection. This connection allows one to attach several additional arithmetic invariants to weight one newforms that we would like to compute, including:

- The projective image of ρ_f in $\mathrm{PGL}_2(\mathbb{C})$, which by Klein's classification is isomorphic to either D_n (dihedral of order $2n$, including $D_2 := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), or one of the exceptional groups A_4 (tetrahedral), S_4 (octahedral), or A_5 (icosahedral).
- The projective field of ρ_f: the fixed field of the kernel of $G_{\mathbb{Q}} \xrightarrow{\rho_f} \mathrm{GL}_2(\mathbb{C}) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{C})$.
- The Artin image of ρ_f: the finite group $\rho_f(G_{\mathbb{Q}}) \le \mathrm{GL}_2(\mathbb{C})$.
- The Artin field of ρ_f: the fixed field of $\ker \rho_f$, with Galois group isomorphic to $\rho_f(G_{\mathbb{Q}})$.

One can also consider the projective representation $\bar{\rho}_f \colon G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$ induced by ρ_f as an invariant in its own right: it uniquely determines the twist class of f. Two newforms f and g are said to be twist equivalent if $g = f \otimes \psi$ for some Dirichlet character ψ, and in weight 1 this occurs if and only if $\bar{\rho}_f = \bar{\rho}_g$.

12.1. **Computational observations.** The Deligne–Serre theorem also has important computational implications. In the typical case where ρ_f is a dihedral representation (meaning that its projective image is dihedral), the Artin L-function $L(\rho_f, s)$ is also the Weber L-function $L(\omega, s)$ of a ray class character ω of the quadratic field K fixed by the preimage of $C_n \subseteq D_n \simeq \bar{\rho}_f(G_{\mathbb{Q}})$. (For $n = 2$ there are three choices for $C_2 \subseteq D_2$; we can use any one of the three.) The quadratic field K and the ray class character ω necessarily satisfy

$$|d_K| \operatorname{Nm}(\operatorname{cond}(\omega)) = \operatorname{cond}(\rho_f) = N, \tag{12.1.1}$$

where d_K is the discriminant of K and N is the level of f. In order to obtain an odd representation ρ_f we also require that if K is a real quadratic field then the modulus for ω should include exactly one of the real places of K.

For any given level N, it is straightforward to enumerate all quadratic fields K of discriminant $d_K \mid N$, all $\mathcal{O}_K$-ideals of absolute norm dividing $N/|d_K|$, and all ray class characters ω of K for the modulus with finite part I and infinite part compatible with an odd representation. This makes it feasible to explicitly compute Fourier expansions of all dihedral newforms of level N to any desired precision; to compute $a_p(f)$ for $p \nmid N$ this simply amounts to evaluating the corresponding ray class character ω at the prime ideals of $\mathcal{O}_K$ above p.

Pari/GP contains extensive support for computing with ray class characters that are particularly efficient in the case of quadratic fields. We used this to compute all dihedral newforms of level $N \leq 40\,000$ with Fourier coefficients $a_n(f)$ computed for $n \leq 6000$ (well past the Sturm bound). This yielded a total of 572 462 dihedral newforms, corresponding to 14 634 052 embedded newforms. The largest dimension we found was 2818, which arises for a dihedral newform of level 39473, and the largest projective image we found was D_{2846} for a newform of level 39 851.

These computations go far beyond the extent of our database described in §10.1, which only covers levels $N \leq 4000$ in weight one. For comparison, the largest dimension arising for $N \leq 4000$ is 232 and the largest projective image is D_{285}. The reason for this discrepancy is that while it is computationally very easy to compute dihedral newforms, to obtain a complete enumeration of all the newforms in a given weight one newspace, one must also enumerate the tetrahedral, octahedral, and icosahedral newforms, which is more difficult—particularly in the icosahedral case. Interestingly, the main difficulty often lies not in enumerating these exceptional newforms, but in verifying that one has actually found them all. In contrast to the case $k > 1$ where there are well known dimension formulas, while there are computational tricks that work well in special cases, to our knowledge no efficient method for computing $\dim S_1^{\text{new}}(N)$ for general N is currently known.

12.2. **Classifying the projective image.** The Pari/GP function `mfgaloistype` can be used to classify the projective image, but given that we actually computed the projective field in every case (which of course determines the projective image), we did not exploit this feature.

Remark 12.2.1. Buzzard–Lauder [20] describe an approach to classifying the projective image by computing projective orders of elements that they applied to all weight one newforms of level up to 1500. They note in their paper that their approach relies on the convenient fact that there are no weight one newforms of level $N \leq 1500$ with projective image A_4 whose coefficient field contains $\mathbb{Q}(\sqrt{5})$. Five such examples arise in our dataset, the first of which is 2299.1.w.a.

12.3. **Computing the projective field.** Our strategy for computing the projective field is to exhaustively compute a complete set of candidates and then rule out all but one. As noted in §12.1, we can effectively determine all the dihedral forms at each level, so we know in advance exactly which forms are dihedral (and the exact order of the projective image in each of these cases). In cases where a dihedral image has moderate degree—less than 100, say—it is feasible to use the ray class field functionality in Pari/GP to compute the projective field. This notably includes

all of the dihedral projective fields whose distinguished quadratic subfield is real: the largest such example in our database is 2605.1.bd.a with projective image D_{40}.

The dihedral fields in which the distinguished subfield is imaginary quadratic can be much larger: the largest example 3997.1.cz.a has projective image D_{285}. In these cases, we exploit the fact that every dihedral field whose distinguished quadratic subfield is imaginary can be realized as a subfield of a ring class field that can be explicitly computed using the theory of complex multiplication. There is a well-developed theory for efficiently computing these ring class fields, even in cases where the degree may be in the millions, motivated by applications to cryptography and elliptic curve primality proving (the CM method for constructing elliptic curves over finite fields).

Given a dihedral weight one newform $f \in S_1^{\mathrm{new}}(N, \chi)$ with dihedral image D_n and distinguished imaginary quadratic field K, there is a finite set of possible suborders $\mathcal{O}$ of $\mathcal{O}_K$ and conductors c such that the projective field of f arises as a cyclic degree-n extension of K of conductor c contained in the ring class field K of $\mathcal{O}$. The enumeration of these dihedral fields was achieved using an algorithm based on the techniques developed by Enge-Sutherland [44] and Sutherland [96, 97] that will be described in a forthcoming paper.

Having enumerated a complete list of candidate fields $L := \mathbb{Q}[x]/(g_L(x))$, for successive primes $p \nmid N$ we can compute the order of $\rho_f(\mathrm{Frob}_p)$ in $\mathrm{PGL}_s(\mathbb{C})$ by determining the positive integer n for which $a_p(f)^2/\chi(p) = \zeta_n + \zeta_n^{-1} + 2$ and compare this to the inertia degree of the primes above p in $\mathcal{O}_L$. This will eventually eliminate all but one candidate field, since the sequence of inertia degrees uniquely determines a Galois number field, and in practice this happens very quickly. To accelerate the computation we precompute defining polynomials for the real cyclotomic fields we may encounter and use p coprime to the discriminants of the defining polynomials g_L so that we can compute the inertia degree as the degree of the irreducible factors of $g_L(x)$ in $\mathbb{F}_p[x]$.

For the non-dihedral projective images we used the methods of Cohen–Diaz y Diaz–Olivier [23, 24] to enumerate all A_4 and S_4 fields unramified outside a given set of primes, and for the A_5 fields we used existing tables of fields in the Jones–Roberts database and the LMFDB combined with a targeted Hunter search for some missing cases, as described by Jones–Roberts [54]. This allowed us to construct complete lists of candidate fields for each non-dihedral weight one form from which we then ruled out all but one candidate by comparing orders of Frobenius elements with inertia degrees as described above.

12.4. **Computing the Artin image, the Artin field, and the associated Artin representation.** As of January 2020 the LMFDB contained 5116 odd 2-dimensional Artin representations of conductor $N \leq 4000$, all of which we were able to uniquely match to a corresponding newform of weight one. For each of these Artin representations the LMFDB provides the Artin image, the Artin field, and a complete description of the Artin representation given values on each conjugacy class of Frobenius elements. We were also able to compute the Artin image and Artin field for 833 additional weight one newforms that are twists of a weight one newform for which we know the corresponding Artin representation by taking the compositum of the known Artin field with an appropriate cyclotomic field.

There is work in progress to add as many of the Artin representations corresponding to the remaining 14 190 weight one newforms as possible; these will be linked to the corresponding weight 1 newforms as they become available.

12.5. **Interesting and extreme behavior.** Weight one modular forms behave rather differently than those of higher weight. As seen in §12, one important invariant of weight one forms is the projective image of the associated Galois representation. We will discuss some forms with dihedral projective image first.

Hecke also constructed weight one modular forms starting from imaginary quadratic fields with odd class number at least 3. The first examples of such fields come from $\mathbb{Q}(\sqrt{-23})$, $\mathbb{Q}(\sqrt{-31})$,

$\mathbb{Q}(\sqrt{-39})$, and the corresponding modular forms are the three smallest level weight one newforms; these have labels 23.1.b.a, 31.1.b.a and 39.1.d.a, respectively. [47]

Example 12.5.1. The last of these, 39.1.d.a, is the D_2 form of lowest level and has CM by both $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-39})$, and RM by $\mathbb{Q}(\sqrt{13})$. This form appears in work of Darmon–Lauder–Rotger [35, Example 2.5].

The first examples of newforms with RM but no CM occur in level 145 with 145.1.f.a (RM by $\mathbb{Q}(\sqrt{5})$, [35, Example 3.3], [34, Example 4.1]) and 145.1.h.a (RM by $\mathbb{Q}(\sqrt{29})$, [36, Example 1.2]).

The problem of constructing weight one forms whose projective image is not dihedral was considered by Tate and Serre in the 1970s. These forms are sometimes called *non-banal* or *exotic*. Such forms divide up into 3 cases based on their projective image, which can be one of A_4, S_4, A_5: the forms are then known as tetrahedral, octahedral and icosahedral, respectively.

Tate together with his students, Flath, Kottwitz, Tunnell, and Weisinger, and additionally Atkin, exhibited a form of level 133, with projective image A_4 described in a letter to Atkin [98, p. 713]; this form is 133.1.m.a in our database. The smallest level example is actually in level 124, given by 124.1.i.a.

In the octahedral case, the smallest level example is in level $4 \cdot 37 = 148$ with label 148.1.f.a; this newform is discussed by Buzzard [19, §2.3] and Darmon–Lauder–Rotger [34, Example 5.6].

Many modular forms previously considered in the literature with interesting Galois representations can now be found in our database. Ogasawara [73] takes the mod-3 Galois representations attached to certain elliptic curves and constructs a $\mathrm{GL}_2(\mathbb{F}_3)$ Artin representation: for example, the elliptic curve of conductor 11 with label 11.a3 is used and the corresponding octahedral modular form of weight one over $\mathbb{Q}(\sqrt{-2})$ is constructed. Using the q-expansion coefficients given there, we can use the trace search functionality to locate a (unique) matching form in our database: 3267.1.b.d. We then verify that it has the right Artin field: a degree 8 extension over which 11.a3 gains 3-torsion.

Buhler [14, 15] constructs the icosahedral Galois representation of level 800, labeled 800.1.bh.a. Kiming–Wang [57] gave several more instances of icosahedral newforms of weight one with characters of order 2, showing their existence in order to verify the Artin conjecture in these cases. The new database now contains all but one of these: 2083.1.b.b, 1948.1.b.a, 3004.1.b.a, 3548.1.d.a, 3676.1.c.a, 2336.1.c (two newforms). The only newspace discussed in loc. cit. with level outside our range would have label 6176.1.b. The database also contains the icosahedral newforms 1376.1.r.a, 2416.1.p.a, 3184.1.t.a, 3556.1.ba.a and 3756.1.q.b which were all shown to satisfy Artin's conjecture by Buzzard–Stein [21]. The proof of Serre's conjecture [58] established Artin's conjecture for all odd irreducible 2-dimensional representations, including all of the icosahedral cases. The smallest level example of an icosahedral newform is 633.1.m.b.

Constructing exotic forms of prime level with specific projective image is also a much studied problem. Such forms do not exist in the tetrahedral case [87, Theorem 7, p. 245], leaving only octahedral and icosahedral forms with the possibility of prime level.

In the octahedral case the smallest prime level is 229, and the space of newforms 229.1.d splits into two Galois orbits, (see Serre [87, p. 265]). The second smallest level is 283, where we have the newform 283.1.b.b that appears also in work of Serre [88].

In the icosahedral case, we have seen above the first example of such a form: the one with level 2083 of Kiming–Wang. In fact the query for forms with projective image A_5 shows that there are 4 such forms with prime level ≤ 4000: 2083.1.b.b, 2707.1.b.b, 3203.1.b.a, 3547.1.b.c. It is conjectured that these forms are rare.

Conjecture 12.5.2. *For any $\epsilon > 0$, the number of exotic newforms of prime level N is $O_\epsilon(N^\epsilon)$.*

Bhargava–Ghate [5] have shown an averaged version of this conjecture in the octahedral case.

References

[1] A. O. L. Atkin and Joseph Lehner, *Hecke operators on $\Gamma_0(m)$*, Math. Ann. **185** (1970), 134–160.

[2] A. O. L. Atkin and Wen-Ch'ing Winnie Li, *Twists of newforms and pseudo-eigenvalues of W-operators*, Invent. Math. **48** (1978), no. 3, 221–243.

[3] B. Banwait and J. Cremona, *Tetrahedral elliptic curves and the local-to-global principle for isogenies*, Algebra & Number Theory **8** (2014), no. 5, 1201–1229.

[4] Karim Belabas and Henri Cohen, *Modular forms in Pari/GP*, Res. Math. Sci. **5** (2018), no. 3, Paper No. 37, 19 pp.

[5] Manjul Bhargava and Eknath Ghate, *On the average number of octahedral newforms of prime level*, Math. Ann. **344** (2009), no. 4, 749–768.

[6] B. J. Birch, *Elliptic curves over $\mathbb{Q}$: A progress report*, 1969 Number Theory Institute (State Univ. New York, Stony Brook, N.Y., 1969), Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, 1971, 396–400.

[7] B. J. Birch, *Hecke actions on classes of ternary quadratic forms*, Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, 191–212.

[8] Jonathan Bober, `mflib` software library, available at `https://github.com/jwbober/mflib`, 2019.

[9] Jonathan W. Bober, Andrew R. Booker, Edgar Costa, Min Lee, David J. Platt, and Andrew Sutherland, *Computing motivic L-functions*, in preparation.

[10] Andrew R. Booker, Min Lee, and Andreas Strömbergsson, *Twist-minimal trace formulas and the Selberg eigenvalue conjecture*, J. Lond. Math. Soc. **102** (2020) no. 3, 1067–1134.

[11] Andrew R. Booker, *Artin's conjecture, Turing's method, and the Riemann hypothesis*, Exp. Math. **15** (2006), no. 4, 385–408.

[12] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997) no. 3–4, 235–265.

[13] Peter Bruin, *Computing coefficients of modular forms*, Actes de la Conférence "Théorie des Nombres et Applications", 19–36, Publ. Math. Besançon Algèbre Théorie Nr., 2011, Presses Univ. Franche-Comté, Besançon, 2011.

[14] Joe Buhler, *An icosahedral modular form of weight one*, Modular functions of one variable V, eds. Jean-Pierre Serre and Don Bernard Zagier, Lecture Notes in Math., vol. 601, Springer, Berlin-Heidelberg, 1977, 289–294.

[15] Joe P. Buhler, *Icosahedral Galois representations*, Lecture Notes in Math., vol. 654, Springer-Verlag, Berlin-New York, 1978.

[16] Joe P. Buhler, Benedict H. Gross, and Don B. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3*, Math. Comp. **44** (1985), 473–481.

[17] Jan Büthe, *A method for proving the completeness of a list of zeros of certain L-functions*, Math. Comp. **84** (2015), no. 295, 2413–2431.

[18] Kevin Buzzard, *Dimension of spaces of Eisenstein series*, preprint available at `http://wwwf.imperial.ac.uk/~buzzard/maths/research/notes/dimension_of_spaces_of_eisenstein_series.pdf`, 2012.

[19] Kevin Buzzard, *Computing weight one modular forms over $\mathbb{C}$ and $\overline{\mathbb{F}}_p$*, Computations with modular forms, Contrib. Math. Comput. Sci., vol. 6, Springer, Cham, 2014, 129–146.

[20] Kevin Buzzard and Alan Lauder, *A computation of modular forms of weight one and small level*, Ann. Math. Qué. **41** (2017), no. 2, 213–219.

[21] Kevin Buzzard and William A. Stein, *A mod five approach to modularity of icosahedral Galois representations*, Pacific J. Math. **203** (2002), no. 2, 265–282.

[22] Sarvadaman Chowla, *The Riemann hypothesis and Hilbert's tenth problem*, Mathematics and Its Applications, vol. 4, Gordon and Breach, New York, 1965.

[23] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *Construction of tables of quartic fields*, Construction of tables of quartic number fields, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, 257-268.

[24] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *Constructing complete tables of quartic fields using Kummer theory*, Math. Comp. **72** (2003), no. 242, 941–951.

[25] H. Cohen and J. Oesterlé, *Dimensions des espaces de formes modulaires*, Modular functions of one variable VI, eds. Jean-Pierre Serre and Don Zagier, Lecture Notes in Math., vol. 627, Springer, Berlin, 1977, 69–78.

[26] Henri Cohen and Fredrik Strömberg, *Modular forms: a classical approach*, Grad. Studies in Math., vol. 179, Amer. Math. Soc., Providence, 2017.

[27] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comp. **88** (2019), 1303–1339.

[28] Edgar Costa and David Platt, *A generic L-function calculator for motivic L-functions*, available at `https://github.com/edgarcosta/lfunctions`, 2019.

[29] John E. Cremona, *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. (2) **45** (1992), no. 3, 404–416.
[30] John E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997.
[31] John E. Cremona, *The elliptic curve database for conductors to 130000*, Algorithmic number theory, eds. Florian Hess, Sebastian Pauli, and Michael Pohst, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, 11–29.
[32] John E. Cremona, *The L-functions and modular forms database project*, Found. Comput. Math. **16** (2016), no. 6, 1541–1553.
[33] John E. Cremona, Aurel Page, Andrew V. Sutherland, *Sorting and labeling integral ideals in a number field*, arXiv:2005.09491v1.
[34] Henri Darmon, Alan Lauder, and Victor Rotger, *Stark points and p-adic iterated integrals attached to modular forms of weight one*, Forum Math. Pi **3** (2015), e8, 95 pp.
[35] Henri Darmon, Alan Lauder, and Victor Rotger, *First order p-adic deformations of weight one newforms*, L-functions and automorphic forms, Contrib. Math. Comput. Sci., vol. 10, Springer, Cham, 2017, 39–80.
[36] Henri Darmon, Alan Lauder, and Victor Rotger, *Overconvergent generalised eigenforms of weight one and class fields of real quadratic fields*, Adv. Math. **283** (2015), 130–142.
[37] Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids 1*, Ann. Sci. Éc. Norm. Sup. (4) **7** (1974), no. 4, 507–530.
[38] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, appendix by N. Koblitz and A. Ogus, Automorphic forms, representations and L-functions (Oregon State Univ., Corvallis, Ore., 1977), Part 2, eds. A. Borel, W. Casselman, Proc. Sympos. Pure Math., vol. 33, Amer. Math. Soc., Providence, 1979, 313–346.
[39] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Grad. Texts in Math., vol. 228, Springer-Verlag, New York, 2005.
[40] Bas Edixhoven and Jean-Marc Couveignes, *Computational aspects of modular forms and Galois representations: how one can compute in polynomial time the value of Ramanujan's tau at a prime*, Annals of Math. Studies, vol. 176, Princeton University Press, Princeton, NJ, 2011.
[41] M. Eichler, *Einige Anwendungen der Spurformel im Bereich der Modularkorrespondenzen*, Math. Ann. **168** (1967), 128–137.
[42] M. Eichler, *The basis problem for modular forms and the traces of the Hecke operators*, Modular functions of one variable I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), ed. W. Kuijk, Lecture Notes in Math., vol. 320, Springer, Berlin, 1973, 75–151.
[43] Stephan Ehlen and Fredrik Strömberg, `modforms-db` software package, available at `https://github.com/sehlen/modforms-db/tree/refactor`, 2014.
[44] Andreas Enge and Andrew V. Sutherland, *Class invariants by the CRT method*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, 142–156.
[45] Daniel Fiorilli, *On the non-vanishing of Dirichlet L-functions at the central point*, Q. J. Math. **66** (2015), no. 2, 517–528.
[46] B.H. Gross and D.B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.
[47] Erich Hecke, *Mathematische Werke*, Göttingen, Vandenhoeck & Ruprecht, 1959.
[48] Harald A. Helfgott, *Root numbers and the parity problem*, Ph.D. Thesis, Princeton University, 2003.
[49] Hiroaki Hijikata, *Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$*, J. Math. Soc. Japan **26** (1974), 56–82.
[50] Hiroaki Hijikata, Arnold K. Pizer, and Thomas R. Shemanske, *The basis problem for modular forms on $\Gamma_0(N)$*, Mem. Amer. Math. Soc. **82** (1989), no. 418.
[51] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, Amer. Math. Soc. Colloquium Publications, vol. 53, Amer. Math. Soc., Providence, 2004.
[52] H. Iwaniec and P. Sarnak, *Perspectives on the analytic theory of L-functions*, GAFA 2000 (Tel Aviv, 1999), Geom. Funct. Anal. 2000, Special Volume, Part II, 705–741.
[53] Fredrik Johansson, *Arb: a C library for ball arithmetic*, ACM Communications in Computer Algebra **47** (2013), no. 4, 166–169.
[54] John W. Jones and David P. Roberts, *Timing analysis of targeted Hunter searches*, Algorithmic number theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, 412–423.
[55] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290.
[56] Lloyd J. P. Kilford, *Modular forms: A classical and computational introduction*, 2nd ed., Imperial College Press, London, 2015.

[57] Ian Kiming and Xiang Dong Wang, *Examples of 2-dimensional, odd Galois representations of A_5-type over $\mathbb{Q}$ satisfying the Artin conjecture*, On Artin's conjecture for odd 2-dimensional representations, Lecture Notes in Math., vol. 1585, Springer, Berlin, 1994, 109–121.

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

[59] Andrew Knightly and Charles Li, *Traces of Hecke operators*, Math. Surveys Monogr., vol. 133, Amer. Math. Soc., Providence, 2006.

[60] Wen-Ch'ing Winnie Li, *Newforms and functional equations*, Math. Ann. **212** (1975), no. 4, 285–315.

[61] David Lowry-Duda, *Visualizing modular forms*, arXiv:2002.05234v2, 2020.

[62] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, `http://www.lmfdb.org`, 2019.

[63] Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat., **36** (1972), 19–66, translated in Math.-USSR Izvestija, **6** (1972), no. 1, 19–64.

[64] Kimball Martin, *The basis problem revisited*, arXiv:1804.04234v2, 2019.

[65] Kimball Martin, *Refined dimensions of cusp forms, and equidistribution and bias of signs*, J. Number Theory **188** (2018), 1–17.

[66] Nicolas Mascot, *Certification of modular Galois representations*, Math. Comp. **87** (2018), 381–423.

[67] Loïc Merel, *Universal Fourier expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations, Lecture Notes in Math., vol. 1585, Springer, Berlin, 1994, 59–94.

[68] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), Nagoya Univ., Nagoya, 1986, 217–242.

[69] Christian Meyer, *Newforms of weight two for $\Gamma_0(N)$ with rational coefficients*, `http://meyer-idstein.de/weight2.pdf`, 2005.

[70] Christian Meyer, *Newforms of weight four for $\Gamma_0(N)$ with rational coefficients*, `http://meyer-idstein.de/weight4.pdf`, 2005.

[71] Toshitsune Miyake, *Modular forms*, Springer Monographs in Math., Springer-Verlag, Berlin, 2006.

[72] Fumiyuki Momose, *On the l-adic representations attached to modular forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 1, 89–109.

[73] Takeshi Ogasawara, *Octahedral newforms of weight one associated to three-division points of elliptic curves*, Funct. Approx. Comment. Math. **49** (2013), no. 1, 103–109.

[74] Sami Omar, *Non-vanishing of Dirichlet L-functions at the central point*, Algorithmic Number Theory (ANTS 2008), Lecture Notes in Comp. Sci. **5011** (2008) 443–453.

[75] *Modular functions of one variable IV*, Proceedings of the International Summer School on Modular Functions of One Variable and Arithmetical Applications, RUCA, University of Antwerp, Antwerp, July 17–August 3, 1972, eds. Bryan J. Birch and Willem Kuyk, Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin, 1975.

[76] The PARI-group, *Pari/GP* (versions 2.11 and 2.12), Univ. Bordeaux, available at `http://pari.math.u-bordeaux.fr`, 2019.

[77] Arnold Pizer, *An algorithm for computing modular forms on $\Gamma_0(N)$*, J. Algebra **64** (1980), no. 2, 340–390.

[78] Alexandru Popa, *On the trace formula for Hecke operators on congruence subgroups, II*, Res. Math. Sci. **5** (2018), no. 1, Paper No. 3, 24 pp.

[79] Kenneth A. Ribet, *Galois representations attached to eigenforms with Nebentypus*, Modular functions of one variable V, eds. Jean-Pierre Serre and Don Bernard Zagier, Lecture Notes in Math., vol. 601, Springer, Berlin-Heidelberg, 1977, 17–51.

[80] Kenneth A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. **253** (1980), no. 1, 43–62.

[81] Kenneth A. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), no. 1, 193–205.

[82] Kenneth A. Ribet, *Abelian varieties over $\mathbb{Q}$ and modular forms*, Modular curves and abelian varieties, eds. John E. Cremona, Joan-C. Lario, Jordi Quer, and Kenneth A. Ribet, Progress in Math. **224**, Birkhäuser, Basel, 2004, 241–261.

[83] The Sage Developers, *SageMath* (version `8.8`), available at `https://www.sagemath.org`, 2019.

[84] George J. Schaeffer, *Hecke stability and weight 1 modular forms*, Math. Z. **281** (2015), no. 1–2, 159–191.

[85] A. Selberg, *Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series*, J. Indian Math. Soc. (N.S.) **20** (1956), 47–87.

[86] Jean-Pierre Serre, *A course in arithmetic*, Grad. Texts in Math. **7**, Springer-Verlag, New York, 1973.

[87] J. P. Serre, *Modular forms of weight one and Galois representations*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), ed. A. Fröhlich, Academic Press, London, 1977, 193–268.

[88] Jean-Pierre Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. **40** (2003), no. 4, 429–440.
[89] Rene Schoof and Marcel van der Vlugt, *Hecke operators and the weight distribution of certain codes*, J. Combin. Ser. A. **57** (1991) no. 2, 163–186.
[90] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kano Memorial Lectures, No. 1, Publications of the Mathematical Society of Japan, no. 1, Princeton Univ. Press, Princeton, N.J., 1971.
[91] Nils-Peter Skoruppa and Don Zagier, *Jacobi forms and a certain space of modular forms*, Invent. Math. **94** (1988), no. 1, 113–146.
[92] William Stein, *The Modular Forms Database*, available at `http://wstein.org/Tables/`.
[93] William A. Stein, *Modular forms, a computational approach*, with an appendix by Paul E. Gunnells, Graduate Studies in Math., vol. 79, Amer. Math. Soc., Providence, 2007.
[94] William A. Stein, *An introduction to computing modular forms using modular symbols*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, 641–652.
[95] Jacob Sturm, *On the congruence of modular forms*, Number theory (New York, 1984-1985), Lecture Notes in Math., vol. 1240, Springer, Berlin, 1987, 275–280.
[96] Andrew V. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. **80** (2011), no. 273, 501–538.
[97] Andrew V. Sutherland, *Accelerating the CM method*, LMS J. Comput. Math. **15** (2012), 172–204.
[98] John Tate, *Collected works of John Tate, Part I (1951-1975)*, eds. Barry Mazur and Jean-Pierre Serre, Amer. Math. Soc., Providence, 2016.
[99] Dave J. Tingley, *Elliptic curves uniformized by modular functions*, Ph.D. thesis, University of Oxford, 1975.
[100] John Voight and David Zureick-Brown, *The canonical ring of a stacky curve*, accepted to Mem. Amer. Math. Soc., preprint available at `https://arxiv.org/abs/1501.04657v3`, 2019.
[101] Hideo Wada, *Tables of Hecke operators. I*, Seminar on Modern Methods in Number Theory (Inst. Statist. Math., Tokyo, 1971), Paper No. 39, Inst. Statist. Math., Tokyo, 1971, 1–10.
[102] Hideo Wada, *A table of Hecke operators. II*, Proc. Japan Acad. **49** (1973), no. 6, 380–384.
[103] Mark Watkins, *A discursus on 21 as a bound for ranks of elliptic curves over $\mathbb{Q}$, and sundry related topics*, available at `https://magma.maths.usyd.edu.au/~watkins/papers/DISCURSUS.pdf`, 2015.

Department of Mathematics & Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA
Email address: alexjbest@gmail.com
URL: https://alexjbest.github.io/

School of Mathematics, University of Bristol, Bristol, BS8 1TW, UK, and the Heilbronn Institute for Mathematical Research, Bristol, UK
Email address: j.bober@bristol.ac.uk
URL: https://people.maths.bris.ac.uk/~jb12407/

School of Mathematics, University of Bristol, Woodland Road, Bristol, BS8 1UG, UK
Email address: andrew.booker@bristol.ac.uk
URL: http://people.maths.bris.ac.uk/~maarb/

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
Email address: edgarc@mit.edu
URL: https://edgarcosta.org

Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
Email address: j.e.cremona@warwick.ac.uk

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
Email address: maarten@mderickx.nl
URL: http://www.maartenderickx.nl/

School of Mathematics, University of Bristol, Woodland Road, Bristol, BS8 1UG, UK
Email address: min.lee@bristol.ac.uk
URL: https://people.maths.bris.ac.uk/~ml14850/

Institute of Computational and Experimental Research in Mathematics, 121 South Main Street, Box E, 11th Floor, Providence, RI 02903, USA
Email address: david@lowryduda.com
URL: https://davidlowryduda.com

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
Email address: roed@mit.edu
URL: http://math.mit.edu/~roed/

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
Email address: drew@math.mit.edu
URL: http://math.mit.edu/~drew/

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
Email address: jvoight@gmail.com
URL: http://www.math.dartmouth.edu/~jvoight/