Experimental evidence for Maeda's conjecture on modular forms

Alexandru Ghitza[1], Angus McAndrew[1]

[1] Department of Mathematics and Statistics, University of Melbourne, Parkville, Australia

E-mail: aghitza@alum.mit.edu, mcandrew@student.unimelb.edu.au

Abstract

We describe a computational approach to the verification of Maeda's conjecture for the Hecke operator T_2 on the space of cusp forms of level one. We provide experimental evidence for all weights less than 14 000, as well as some applications of these results. The algorithm was implemented using the mathematical software Sage, and the code and resulting data were made freely available.

2000 Mathematics Subject Classification. **11F25**. 11F11, 11-04.
Keywords. Modular forms, Hecke operators, Sage.

1 Introduction

Modular forms come in many different types. One of the most attractive aspects of the theory is that, despite the apparent variety of definitions and properties, there are some universal guiding principles (such as the Langlands program) that serve to unify and motivate this diversity. On the other hand, there are some special properties that seem to occur in isolation. One such instance is provided by a conjecture formulated by Maeda, which indicates a behavior that seems to be specific[1] to modular forms of level one on GL_2.

Before describing Maeda's conjecture in more detail, we review some basic definitions and properties of modular forms. For a thorough treatment of the background needed in this paper, the reader is invited to consult [22].

Let $k \in \mathbb{Z}$. A *modular form* of level 1 and weight k is a holomorphic function

$$f\colon \mathcal{H} \longrightarrow \mathbb{C}, \quad \text{where } \mathcal{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\},$$

satisfying

- Modularity: for all $z \in \mathcal{H}$ and all $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$,
$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$
- Holomorphicity at $i\infty$: a holomorphic function f satisfying the modularity condition satisfies $f(z+1) = f(z)$ for all $z \in \mathcal{H}$, so it has a Fourier expansion
$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n, \quad \text{where we set } q = e^{2\pi i z}.$$

[1] We must note that recent work of Tsaknias [25] points to a generalisation of Maeda's conjecture to forms of higher level and promises to shed new conceptual light on these questions. We thank Gabor Wiese for bringing Tsaknias' preprint to our attention.

We ask for f to be *holomorphic at* $i\infty$, i.e. that $a_n = 0$ for all $n < 0$.

We say that a modular form f is a *cusp form* if $a_0 = 0$. The cusp forms of weight k form a vector space S_k. These vector spaces are equipped with a family of *Hecke operators* T_m (for $m \in \mathbb{N}$), whose effect on the Fourier expansion $f(q) = \sum a_n q^n$ of $f \in S_k$ is given by

$$(T_m f)(q) = \sum_{n=1}^{\infty} \left(\sum_{d \mid \gcd(m,n)} d^{k-1} a_{mn/d^2} \right) q^n.$$

The complex vector space S_k has dimension

$$d = \begin{cases} \left[\frac{k}{12}\right] - 1 & \text{if } k \equiv 2 \pmod{12}, \\ \left[\frac{k}{12}\right] & \text{if } k \not\equiv 2 \pmod{12}. \end{cases}$$

Let F denote the characteristic polynomial of the operator T_2 acting on S_k, and let $d = \dim S_k$. In the 1970s, Yoshitaka Maeda noticed that F is irreducible over $\mathbb{Q}$ for all k such that $d \leq 12$. In the 1990s, Lee-Hung [17] and Buzzard [5] studied these polynomials further and observed in a number of cases that the Galois group of F is the symmetric group $\mathfrak{S}_d$. Shortly thereafter, Maeda made the following conjectural statement:

Conjecture 1.1 (Maeda [15])**.** Let $m > 1$ and let F be the characteristic polynomial of the Hecke operator T_m acting on S_k. Then

(1) the polynomial F is irreducible over $\mathbb{Q}$;

(2) the Galois group of the splitting field of F is the full symmetric group $\mathfrak{S}_d$, where d is the dimension of S_k.

The conjecture has enjoyed constant attention over the last 15 years, with theoretical as well as computational results. We summarize the computational verifications in Table 1.

Source	weights
Lee-Hung [17]	$k \leq 62$, $k \neq 60$
Buzzard [5]	$k = 12\ell$, ℓ prime, $2 \leq \ell \leq 19$
Maeda [15]	$k \leq 468$
Conrey-Farmer [6]	$k \leq 500$, $k \equiv 0 \pmod 4$
Farmer-James [11]	$k \leq 2\,000$
Buzzard-Stein, Kleinerman [16]	$k \leq 3\,000$
Chu-Wee Lim [18]	$k \leq 6\,000$
present paper	$k \leq 14\,000$

TABLE 1. Summary of known cases of Maeda's conjecture for T_2

The theoretical results focus on whether the validity of the conjecture for a given operator T_m can be used to deduce the conjecture for other operators T_n. We state three such results, each giving a partial answer to this question.

Theorem 1.2 (Conrey-Farmer-Wallace [7])**.** Let k be a positive even integer. Suppose there exists $n \geq 2$ such that the operator T_n acting on S_k satisfies Maeda's conjecture. Then so does T_p acting on S_k, for every prime p in the set of density $5/6$ defined by the conditions

$$p \not\equiv \pm 1 \pmod 5 \qquad \text{or} \qquad p \not\equiv \pm 1 \pmod 7.$$

Stated differently, this says that if Maeda's conjecture in weight k holds for one index n, then the density of primes for which the conjecture fails is at most $1/6$. The next result considers only the irreducibility part of the conjecture, but it is stronger since it says that the density of primes for which the conjecture fails is zero.

Theorem 1.3 (Baba-Murty [2])**.** Let k be a positive even integer. Suppose there exists a prime p such that the characteristic polynomial of T_p acting on S_k is irreducible over $\mathbb{Q}$. Then there exists $\delta > 0$ such that

$$\#\{\ell \leq N \text{ prime} \mid \operatorname{charpoly}(T_\ell | S_k) \text{ is reducible}\} \ll \frac{N}{(\log N)^{1+\delta}}.$$

Finally, Ahlgren gave a simple criterion for extending the validity of Maeda's conjecture from one index to another, and used it together with some computer work to prove the following result.

Theorem 1.4 (Ahlgren [1])**.** Let k be such that $d := \dim S_k \geq 2$. Suppose there exists $n \geq 2$ such that the operator T_n acting on S_k satisfies Maeda's conjecture. Then

(1) T_p acting on S_k satisfies Maeda's conjecture for all primes $p \leq 4\,000\,000$;

(2) T_n acting on S_k satisfies Maeda's conjecture for all $n \leq 10\,000$.

We can now state our main result.

Theorem 1.5. Let $k \leq 14\,000$ and let

$$\begin{aligned} n \in &\{2, \ldots, 10\,000\} \cup \{p \text{ prime} \mid 2 \leq p \leq 4\,000\,000\} \\ &\cup \{p \text{ prime} \mid p \not\equiv \pm 1 \pmod 5\} \cup \{p \text{ prime} \mid p \not\equiv \pm 1 \pmod 7\}. \end{aligned}$$

Let F be the characteristic polynomial of the Hecke operator T_n acting on the space S_k of cusp forms of weight k and level 1. Then F is irreducible over $\mathbb{Q}$ and the Galois group of its splitting field is the full symmetric group $\mathfrak{S}_d$, where d is the dimension of the space S_k.

Proof. The statement for T_2 is the result of the computations described below. Given this, we deduce the result for the other T_n by applying the results of Conrey-Farmer-Wallace and Ahlgren, as stated above. Q.E.D.

Our computational approach follows the "multimodular" method introduced by Buzzard in [5] and refined by Conrey-Farmer in [6]. The main improvement is the use of random primes of moderate size, instead of going through primes consecutively until suitable ones are found. In Section 3 we describe the theoretical foundation of this approach, and we estimate the densities of the different types of primes we are looking for. This provides us with expected running times for our randomized algorithm, the Sage implementation of which we discuss in detail in Section 4. Finally, Section 5 gives some direct corollaries of Theorem 1.5 to some questions about modular forms of level one.

We have made the code and data used to verify Theorem 1.5 available at

`http://bitbucket.org/aghitza/maeda_data`

Acknowledgements

We thank David Harvey for asking a question that lead us to drastically improve our Sage implementation, and David Farmer, Gabor Wiese and the referees for very useful comments.

Research of the first author was supported by a Discovery Grant from the Australian Research Council. Some of the computations described in this paper were performed on the Sage cluster at the University of Washington, partly supported by National Science Foundation Grant No. DMS-0821725, held by William Stein.

2 Polynomial factorization and Frobenius elements

Our algorithm is based on a correspondence between the factorization of polynomials over finite fields and the cycle decomposition of Frobenius elements in Galois groups. We give a short review of these results, which go back all the way to the beginnings of algebraic number theory, appearing for instance in the work of Frobenius. A fascinating exposition of the mathematics and history of these ideas is given by Stevenhagen and Lenstra in [24].

We start with a bit of terminology. If τ is a permutation on d letters, it can be decomposed into a product of disjoint cycles, uniquely up to permutation of the cycles. We say that τ has *cycle pattern* $d_1^{m_1}d_2^{m_2}\dots d_t^{m_t}$ if its decomposition contains exactly m_j cycles of length d_j, for $j = 1, \dots, t$. (Note: $m_1d_1+m_2d_2+\dots+m_td_t = d$.) If H is a polynomial in $\mathbb{F}_p[X]$, we say that H has *factorization pattern* $d_1^{m_1}d_2^{m_2}\dots d_t^{m_t}$ if H has exactly m_j irreducible factors of degree d_j over $\mathbb{F}_p$. We recall that H is said to be *separable* if it has distinct roots over $\overline{\mathbb{F}}_p$.

Lemma 2.1. Let $F \in \mathbb{Z}[X]$ be monic, let p be a prime and let $F_p \in \mathbb{F}_p[X]$ be the reduction of F modulo p. If F_p is separable, then there exists an element τ of the Galois group of F such that the cycle pattern of τ is the same as the factorization pattern of F_p.

We sketch a proof of this classical result.

Fix a prime p and consider the field automorphism $\sigma\colon \overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p$ given by $\sigma(a) = a^p$. Since σ fixes the subfield $\mathbb{F}_p$, it permutes the roots of any polynomial $H \in \mathbb{F}_p[X]$. Moreover, Galois theory tells us that the cycle pattern of σ (viewed as a permutation) is the same as the factorization pattern of H over $\mathbb{F}_p$.

We now take a monic polynomial $F \in \mathbb{Z}[X]$ and we let $K/\mathbb{Q}$ be its splitting field, $\mathcal{O}_K$ the ring of integers of K, and G the Galois group of $K/\mathbb{Q}$. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$ over p. Suppose the reduction F_p of F modulo p is a separable polynomial (in this case, we say that p is unramified in $K/\mathbb{Q}$). Then there is a *Frobenius element* $\mathrm{Frob}_\mathfrak{p} \in G$ determined uniquely by the property

$$\mathrm{Frob}_\mathfrak{p}(\alpha) \equiv \sigma(\alpha) \pmod{\mathfrak{p}} \qquad \text{for all } \alpha \in \mathcal{O}_K.$$

This implies that $\mathrm{Frob}_\mathfrak{p}$ permutes the roots $\alpha_1, \dots, \alpha_d \in \mathcal{O}_K$ of F in the exact same way as σ permutes the roots in $\overline{\mathbb{F}}_p$ of F_p. We conclude that the cycle pattern of $\mathrm{Frob}_\mathfrak{p}$ is the same as the factorization pattern of F_p over $\mathbb{F}_p$. Therefore we can take τ in the conclusion of Lemma 2.1 to be $\mathrm{Frob}_\mathfrak{p}$.

Note that τ is not uniquely determined by F and p, as the choice of a prime $\mathfrak{p}$ of $\mathcal{O}_K$ above p matters. However, any two such τ are conjugate in the Galois group.

The following result follows easily from Lemma 2.1 and the fact that for any $F \in \mathbb{Z}[X]$ there are only finitely many primes p (namely the ones dividing the discriminant of F) for which F_p is not separable.

Theorem 2.2 (Frobenius)**.** Let $F \in \mathbb{Z}[X]$ be monic, let $K/\mathbb{Q}$ be the splitting field of F and let G be the Galois group of $K/\mathbb{Q}$. Let $\deg F = m_1 d_1 + \ldots + m_t d_t$ be a partition of $\deg F$. The density of primes p for which F_p has factorization pattern $d_1^{m_1} \ldots d_t^{m_t}$ is equal to

$$\frac{\#\{\sigma \in G \mid \text{the cycle pattern of } \sigma \text{ is } d_1^{m_1} \ldots d_t^{m_t}\}}{\#G}.$$

3 The basic lemma and density estimates

Consider a monic polynomial $F \in \mathbb{Z}[X]$ of degree d. Given a prime p, we denote by $F_p \in \mathbb{F}_p[X]$ the reduction modulo p of F. We say that the prime p is

(1) *of type I* if F_p is irreducible over $\mathbb{F}_p$;

(2) *of type II* if F_p factors over $\mathbb{F}_p$ into a product of distinct irreducible factors

$$F_p = f_0 f_1 \cdots f_s$$

with

$$\begin{aligned} &\deg f_0 = 2 \\ &\deg f_j \text{ odd for } j = 1, \ldots, s; \end{aligned}$$

(3) *of type III* if F_p factors over $\mathbb{F}_p$ into a product of distinct irreducible factors

$$F_p = f_0 f_1 \cdots f_s$$

with $\deg f_0 > d/2$ and prime.

Remark 3.1. Hida and Maeda use a similar approach in Section 5 of [15], but replace primes of type III with *primes of type IV*, i.e. p such that $F_p = f_0 f_1$ with f_0, f_1 distinct and irreducible, and $\deg f_0 = 1$. We will see below that primes of type III are significantly more common (and therefore better suited for our algorithm) than those of type IV.

Remark 3.2. These types are not necessarily mutually exclusive: if d itself is prime, then a prime p of type I is clearly also of type III.

Remark 3.3. In either of the three types, the conditions imply that the reduced polynomial F_p is separable:

- If p is a prime of type I, then F_p is irreducible, hence separable.
- If p is a prime of type II or III, F_p is a product of distinct irreducible factors. Each of the factors is then separable, and they cannot have any common roots, since otherwise they would have a nonconstant common factor and would therefore be reducible. Hence F_p has distinct roots.

Our computational approach to Maeda's conjecture is based on the following result, first proved in a special case in [5] and then generalized in [6].

Lemma 3.4 (Buzzard, Conrey-Farmer)**.** Let $F \in \mathbb{Z}[X]$ be a monic polynomial of degree d. Suppose that F has primes of respective types I, II and III. Then F is irreducible over $\mathbb{Q}$ and its splitting field over $\mathbb{Q}$ has full Galois group $\mathfrak{S}_d$.

Proof. The fact that F is irreducible is immediate from the existence of a prime of type I.

Let $K/\mathbb{Q}$ be the splitting field of F and let G be the Galois group of $K/\mathbb{Q}$. Since F is irreducible, G is a transitive subgroup of $\mathfrak{S}_d$.

We also have a prime of type II. By Lemma 2.1, there exists $\tau_1 \in G$ whose decomposition into disjoint cycles contains exactly one even cycle (of length 2). Let a be the least common multiple of the lengths of the other cycles in τ_1, then $\tau_1^a \in G$ is a transposition.

Finally, there is a prime of type III. By Lemma 2.1, there exists $\tau_2 \in G$ whose decomposition into disjoint cycles contains one cycle of prime length $p > d/2$. Therefore the other cycles have lengths that are coprime to p; letting b denote the least common multiple of these lengths, we find that $\tau_2^b \in G$ is a p-cycle.

We now use the existence of these elements of G to conclude that $G = \mathfrak{S}_d$. For $i, j \in S = \{1, \dots, d\}$, write $i \sim j$ if $i = j$ or if the transposition $(i\ j)$ is in G. This is an equivalence relation on S. Since G is transitive, each equivalence class has the same number n of elements and it follows that $n \mid d = \#S$. Note that $n > 1$ since G contains at least one transposition, namely τ_1^a. Let T be the subset of S permuted by τ_2^b, and let G_T be the subgroup of G fixing $S \setminus T$. Define an equivalence relation on T by $i \simeq j$ if $i = j$ or if the transposition $(i\ j) \in G_T$. As before, each equivalence class has the same number m of elements and $m \mid p = \#T$. Since $n > 1$, we have $m > 1$, so $m = p$ since p is prime. But $n \geq m$ because $G_T \subset G$. Thus $n > d/2$, so $n = d$. This implies $G = \mathfrak{S}_d$. Q.E.D.

Our algorithm will consist of picking random primes and checking whether they are of type I, II or III for the characteristic polynomial of the Hecke operator T_2. According to Theorem 2.2, it is therefore important to estimate the number of permutations having certain types of cycle patterns. For a fixed pattern, the following well-known result (see, for instance, Proposition 1.3.2 of [21]) gives an exact expression for the number of permutations.

Lemma 3.5. Let an element σ of $\mathfrak{S}_d$ have cycle pattern $d_1^{m_1} d_2^{m_2} \dots d_t^{m_t}$, where m_i is the number of times a cycle of length d_i appears in the cycle decomposition of σ. The number of elements of $\mathfrak{S}_d$ of cycle pattern $d_1^{m_1} d_2^{m_2} \dots d_t^{m_t}$ is equal to

$$C(d_1^{m_1} d_2^{m_2} \dots d_t^{m_t}) = \frac{d!}{\prod_{j=1}^{t} \left(d_j^{m_j} m_j!\right)}.$$

Proposition 3.6. The density of primes of type I is

$$D_I(d) = \frac{1}{d}.$$

Proof. Primes of type I correspond to d-cycles in $\mathfrak{S}_d$. Each such cycle can be written uniquely as a sequence $1, a_1, \dots, a_{d-1}$, where $a_1, \dots, a_{d-1} \in \{2, \dots, d\}$ can appear in any order. Therefore there are $(d-1)!$ d-cycles, and by Theorem 2.2, the density of primes of type I is

$$\frac{(d-1)!}{d!} = \frac{1}{d}.$$

Q.E.D.

In order to state our result on primes of type II, recall that for $n \in \mathbb{Z}_{>0}$ odd, the *double factorial* $n!!$ of n is the product of all the odd positive integers less than or equal to n.

Proposition 3.7. Let $d > 2$ and let $\tilde{d}$ be the largest even integer such that $\tilde{d} \leq d$. The density of primes of type II is given by

$$D_{II}(d) = \frac{[(\tilde{d}-3)!!]^2}{2(\tilde{d}-2)!}$$

and satisfies the inequality

$$D_{II}(d) > \frac{1}{4\sqrt{d}}.$$

Proof. Primes of type II correspond to elements in $\mathfrak{S}_d$ containing a 2-cycle and no other even cycles. There are $\binom{d}{2}$ 2-cycles in $\mathfrak{S}_d$; fixing a 2-cycle, we need the number $\mathscr{O}(d-2)$ of elements of odd order in $\mathfrak{S}_{d-2}$. We have

$$D_{II}(d) = \frac{1}{d!}\binom{d}{2}\mathscr{O}(d-2) = \frac{\mathscr{O}(d-2)}{2(d-2)!}.$$

The sequence $(\mathscr{O}(n) \mid n \in \mathbb{N})$ appears in nature in several guises, see [10]. The recurrence formulas that appear there and in Chapter IV of [19] easily give the exact expression

$$\mathscr{O}(n) = \begin{cases} (n-1)!!, & \text{if } n \text{ is even} \\ (n-2)!!n, & \text{if } n \text{ is odd,} \end{cases}$$

which immediately provides us with the exact expression for $D_{II}(d)$ in the statement.

It remains to establish the lower bound. Write $\tilde{d} = 2c$ for some $c \in \mathbb{Z}$ (recall that $\tilde{d}$ is the largest even integer less than or equal to d). Then

$$\mathscr{O}(d-2) = \frac{[(2c-3)!!]^2}{2(2c-2)!} = \frac{(2c-3)!}{2^{2c-3}(2c-2)[(c-2)!]^2}. \tag{1.1}$$

We use the following bounds on the factorial, which can be thought of as an effective version of Stirling's approximation and were obtained by Robbins (see [20] and Section II.9 in [12]):

$$\sqrt{2\pi}n^{n+\frac{1}{2}}e^{-n+\frac{1}{12n+1}} < n! < \sqrt{2\pi}n^{n+\frac{1}{2}}e^{-n+\frac{1}{12n}}.$$

Then by using the lower bound for the numerator and the upper bound for the denominator on the right hand side of Equation (1.1), we obtain

$$D_{II}(d) > \frac{2c-3}{2c-2}\,\frac{1}{2\sqrt{\pi(c-2)}}\,e^{\frac{1}{24(c-2)+1}-\frac{1}{6(c-2)}} > \left(\frac{9}{10}\right)^2 \frac{\sqrt{2}}{\sqrt{\pi}}\frac{1}{\sqrt{d}},$$

where we use the elementary inequalities (valid for $c > 6$):

$$e^{\frac{1}{24(c-2)+1}-\frac{1}{6(c-2)}} > e^{-\frac{5}{24c}} > \frac{9}{10},$$
$$\frac{2c-3}{2c-2} \geq \frac{9}{10}.$$

Since

$$\left(\frac{9}{10}\right)^2 \frac{\sqrt{2}}{\sqrt{\pi}} > \frac{1}{4},$$

this gives us the desired lower bound for $d > 12$, and the remaining cases $2 < d \leq 12$ are easily checked. Q.E.D.

Proposition 3.8. The density of primes of type III is

$$D_{III}(d) = \sum_{d/2<\ell\leq d,\, \ell \text{ prime}} \frac{1}{\ell}.$$

If $d > 2$, then

$$D_{III}(d) > \frac{1}{d}.$$

Proof. Fix a prime ℓ such that $d/2 < \ell \leq d$. According to Theorem 2.2, we need to count the number of elements of $\mathfrak{S}_d$ that contain an ℓ-cycle. Choosing the ℓ-cycle itself involves the $\binom{d}{\ell}$ ways of picking its constituents, which can then be rearranged within the cycle in $(\ell-1)!$ ways. It remains to take into account the number of permutations of the remaining $d-\ell$ symbols, so overall we have

$$\binom{d}{\ell}(\ell-1)!(d-\ell)! = \frac{d!}{\ell}$$

elements of $\mathfrak{S}_d$ containing an ℓ-cycle, which gives the stated density.

The inequality given in the statement follows from Bertrand's postulate (proved by Chebyshev), which says that for any integer $n > 1$ there is at least one prime ℓ such that $n < \ell < 2n$. Q.E.D.

We can get a much better lower bound on the density D_{III} by using some recent results of Dusart on explicit estimates for sums over primes.

Theorem 3.9 (Dusart, Theorem 6.10 in [9])**.** Let $B \approx 0.26149$ denote the Meissel-Mertens constant. For all $x > 1$ we have

$$\log\log x + B - \left(\frac{1}{10\log^2 x} + \frac{4}{15\log^3 x}\right) \leq \sum_{p\leq x} \frac{1}{p}. \tag{1.2}$$

We will also need an upper bound on the sum of the reciprocals of primes up to x, but Dusart's upper bound only holds for $x \geq 10\,372$. For our purposes, the following weaker result is sufficient: for all $x > 1$ we have

$$\sum_{p\leq x} \frac{1}{p} \leq \log\log x + B + \frac{1}{\log^2 x}. \tag{1.3}$$

(This inequality can be found in Theorem 8.8.5 of [3].)

Proposition 3.10. If $d > 10$, then

$$D_{III}(d) > \frac{1}{3\log d}.$$

Proof. We put together inequalities (1.2) and (1.3) to get

$$D_{III}(d) > \log\log d - \log\log\frac{d}{2} - \frac{1}{10\log^2 d} - \frac{4}{15\log^3 d} - \frac{1}{\log^2\frac{d}{2}}.$$

We write

$$\log\log d - \log\log\frac{d}{2} = \log\left(1 + \frac{\log 2}{\log d - \log 2}\right)$$

and use the inequality

$$\log(1+x) \geq x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} \qquad \text{for all } 1 < x \leq 1$$

to get that for all $d \geq 4$

$$\begin{aligned} D_{III}(d) >& \frac{1}{\log d - \log 2}\left[\log 2 - \left(\frac{\log^2 2}{2} + \frac{11}{10}\right)\frac{1}{\log d - \log 2}\right. \\ & \left. - \left(\frac{4}{15} - \frac{\log^3 2}{3}\right)\frac{1}{(\log d - \log 2)^2} - \frac{\log^4 2}{4}\frac{1}{(\log d - \log 2)^3}\right] \\ >& \frac{1}{\log d}\left[0.693 - 1.341\frac{1}{\log d - \log 2} - 0.156\frac{1}{(\log d - \log 2)^2}\right. \\ & \left. - 0.058\frac{1}{(\log d - \log 2)^3}\right]. \end{aligned}$$

If $d > 94$, then the expression in the brackets is bigger than $1/3$, and we get the desired inequality. We check that it holds for the remaining cases $10 < d \leq 94$ by computation. Q.E.D.

For completeness, we treat the case of primes of type IV, as defined in Remark 3.1.

Proposition 3.11. Let $d > 1$. The density of primes of type IV is

$$D_{IV}(d) = \frac{1}{d-1}.$$

Proof. We need to count the number of $(d-1)$-cycles in $\mathfrak{S}_d$. There are d choices for the letter that is fixed, and $(d-2)!$ choices for permuting the other letters appropriately, therefore the density of primes of type IV is

$$\frac{d(d-2)!}{d!} = \frac{1}{d-1}.$$

Q.E.D.

4 Implementation and results

Our approach is a randomized version of the algorithm from [6], based on the results introduced in the previous section. We implemented this algorithm using the mathematical software Sage, see [23].

Here is a description of the main steps used to verify Maeda's conjecture for a fixed weight k; in those cases where a major step is delegated to a component of Sage (rather than using native Sage code), we mention the relevant component.

(1) Compute the Victor Miller basis $\mathcal{B}$ for S_k up to precision $2(d+2)$, where d is the dimension of S_k. The Sage implementation of this basis uses [14] polynomials as the internal data structure.

(2) Compute the matrix M of the Hecke operator T_2 with respect to the basis $\mathcal{B}$ – this is very efficient since the basis $\mathcal{B}$ is echelonized.

(3) Pick a random prime $p < 2^{20}$, uniformly over this range. (This choice of upper bound gives a large enough range so that it is likely to contain primes of type we are looking for, but not so large that the arithmetic over $\mathbb{F}_p$ gets too expensive.)

(4) Reduce M modulo p and compute the characteristic polynomial $F_p \in \mathbb{F}_p[X]$. The characteristic polynomial is computed by the [8] library.

(5) Is F_p irreducible? If so, p is a prime of type I. The irreducibility test uses [14].

(6) Factor F_p over $\mathbb{F}_p$ and use this factorization to decide whether p is a prime of type II or III. The factorization is done by [14].

(7) Repeat from step (3) until we have found at least one prime of each type.

According to Propositions 3.6, 3.7 and 3.10, we expect to look on average at d primes before we find one of type I, at $4\sqrt{d}$ primes to find one of type II, and at $3\log d$ primes to find one of type III.

The actual performance of this algorithm (as well as a comparison to the consecutive version of the algorithm, used in [6]) is illustrated in Figure 1. Some care needs to be taken in interpreting the graphs:

- There is no difference in running times for Steps (1) and (2), which are common between the two algorithms.
- As the weight increases, the major component of the running time is finding a prime of type I. Therefore, even though the randomized algorithm does much better at finding primes of types II and III, this advantage has only a minor impact on the overall running time.
- In the range illustrated in the graphs (i.e. weights less than 2 000), the randomized algorithm required on average one third of the number of primes needed by the consecutive algorithm. However, some of this is counteracted by the fact that the consecutive algorithm works with much smaller primes, which are faster to test.
- Overall, for weights less than 2 000, the randomized algorithm was about twice as fast as the consecutive one.

It would be very interesting to understand why small primes are ill-suited for the purposes of this multimodular algorithm. We can only offer a heuristic reason: we observed that the discriminant of the Hecke operator T_2 tends to be highly divisible by a lot of small primes; this means that the characteristic polynomial of T_2 is not squarefree at these primes, which disqualifies them from being primes of types I, II or III.

For weight $k = 14\,000$, the entire verification took about 14 hours. The majority (59%) of the time was spent looking for a prime of type I; this required testing 655 primes, and each test took about 47 seconds. The computation of the Victor Miller basis took about 4.9 hours, and the computation of the characteristic polynomial of T_2 took about 1 hour.

	consec	random
min	1.85	0.01
max	10.00	6.50
med	2.93	0.69
mean	3.21	0.96

	consec	random
min	0.93	0.03
max	15.15	7.65
med	6.64	0.70
mean	6.47	0.99

	consec	random
min	4.00	0.12
max	40.46	8.47
med	23.03	0.68
mean	22.13	0.94

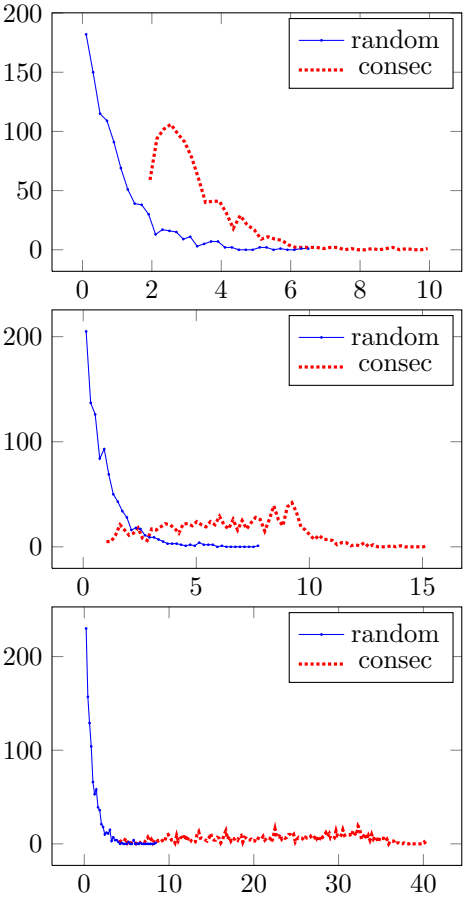

FIGURE 1. Histograms illustrating the number of primes tested before finding a prime of type I, II, respectively III, in weights up to 2 000. In each graph, the numbers on the x-axis represent the ratio N/E of the actual number of primes tested over the expected number of primes (coming from the densities described in Section 3). The y-value represents the number of weights featuring (a small neighborhood of) that particular ratio N/E. The blue continuous line corresponds to our randomized algorithm, while the red dotted line corresponds to the consecutive algorithm from [6]. As an example: in the top graph, the global maximum on the continuous line is at $(0.1, 182)$, meaning that for 182 weights, the number of candidates for a prime of type I tested in the randomized algorithm was about $1/10$ of the expected number of primes.

5 Some applications

We record some immediate consequences of Theorem 1.5.

5.1 Non-vanishing of L-functions

A modular form is called an *eigenform* if it is an eigenvector for all the Hecke operators T_n. The *L-function* associated to an eigenform $f = \sum_{n=1}^{\infty} a_n q^n$ of weight k is given by

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

If $k \equiv 2 \pmod 4$, the functional equation of L implies that $L(f,k/2) = 0$. It is believed that if $k \equiv 0 \pmod 4$, then $L(f,k/2) \neq 0$. The following result follows immediately from work of Conrey-Farmer:

Corollary 5.1 (see Theorem 1 in [6])**.** Suppose $k \equiv 0 \pmod 4$ and $k \leq 14\,000$. Then $L(f,k/2) \neq 0$ for any cuspidal eigenform f of level 1 and weight k.

5.2 Base change for totally real fields

It is in the context of this work of Hida and Maeda that Maeda's conjecture was formulated. We content ourselves with giving a general description of this application, and we refer the interested reader to [15] for details.

Let $f \in S_k$ be a Hecke eigenform. For each prime p, there is a p-adic Galois representation

$$\rho\colon \operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \operatorname{GL}_2\left(\overline{\mathbb{Q}}_p\right).$$

There is an Artin L-function $L(\rho,s)$ attached to ρ, and the relation between ρ and f can be summarized by

$$L(\rho,s) = L(f,s).$$

Now let E be a number field. There is a purely algebraic notion of a cohomological eigenform $\hat{f}$ on $\operatorname{GL}_2(\mathbb{A}_E)$, where $\mathbb{A}_E$ is the ring of adeles of E. We say that $\hat{f}$ is a *base change of f to E* if

$$L(\hat{f},s) = L(\rho_E,s),$$

where $\rho_E\colon \operatorname{Gal}(\overline{\mathbb{Q}}/E) \longrightarrow \operatorname{GL}_2(\overline{\mathbb{Q}}_p)$ is the restriction of ρ to E.

The work of Hida and Maeda, together with Theorem 1.5, implies that for $k \leq 14\,000$ and a totally real field E satisfying some ramification conditions, any eigenform $f \in S_k$ has a base change to E.

5.3 Eigenforms divisible by eigenforms

It is easy to see from the definition of a modular form that if f_1 and f_2 are modular forms of respective weights k_1 and k_2, then the product $f_1 f_2$ is a modular form of weight $k_1 + k_2$. In other words, modular forms of all weights put together form a graded algebra

$$M = \bigoplus_{k \in \mathbb{Z}} M_k.$$

A natural question is whether the product of eigenforms can be an eigenform. This will clearly happen for small weights (for instance, when the product lives in a one-dimensional space of cusp forms). Since the Hecke operators do not act on the entire algebra M of modular forms (they act differently on the graded pieces M_k), it seems reasonable that the one-dimensional coincidences are the only situation in which a product of eigenforms is an eigenform. Such questions have been studied by several authors, with the latest results appearing in a recent paper by Beyerl-James-Xue [4]. They consider the more general question of divisibility of an eigenform by another eigenform, i.e. relations of the form $h = fg$ where f, g, h are modular forms and f, h are eigenforms. The relation with Maeda's conjecture is discussed in Section 6 of [4], and Theorem 1.5 implies the following result.

Corollary 5.2. Let h be a cuspidal eigenform of weight $\leq 14\,000$, and let f be an eigenform (which could be cuspidal or Eisenstein). Then $h = fg$ for some modular form $g \in M_k$ with $k > 2$ if and only if we are in one of the cases listed in Table 2.

weight of f	weight of g modulo 12	nature of f
4	$0, 4, 6, 10$	Eisenstein
6	$0, 4, 8$	Eisenstein
8	$0, 6$	Eisenstein
10	$0, 4$	Eisenstein
12	$0, 2, 4, 6, 8, 10$	cuspidal
14	0	Eisenstein
16	$0, 4, 6, 10$	cuspidal
18	$0, 4, 8$	cuspidal
20	$0, 6$	cuspidal
22	$0, 4$	cuspidal
26	0	cuspidal

TABLE 2. The only cases in which a cuspidal eigenform of weight $\leq 14\,000$ can be factored into $h = fg$ with f an eigenform, see Corollary 5.2.

5.4 Distinguishing Hecke eigenforms

How many initial Fourier coefficients are necessary to completely determine a Hecke eigenform? Theorem 1 in [13] says that a_2, a_3 and a_4 are sufficient, but our computational verification of Maeda's conjecture gives a stronger result[2]:

Corollary 5.3 (see Theorem 6 in [13])**.** Let f and g be cuspidal eigenforms of level 1 and (possibly distinct) weights $\leq 10\,000$. Then $a_2(f) = a_2(g)$ if and only if $f = g$.

[2]Corollary 5.3 relies on Theorem 1.5, which holds for $k \leq 14\,000$, but also needs another computation from [13], which has only been done for weights up to $10\,000$.

References

[1] Scott Ahlgren, *On the irreducibility of Hecke polynomials*, Math. Comp., 77(263) (2008), 1725–1731.

[2] Srinath Baba and M. Ram Murty, *Irreducibility of Hecke polynomials*, Math. Res. Lett., 10(5-6) (2003), 709–715.

[3] Eric Bach and Jeffrey Shallit, *Algorithmic number theory. Vol. 1.* Foundations of Computing Series. MIT Press, Cambridge, MA, 1996. Efficient algorithms.

[4] Jeffrey Beyerl, Kevin James and Hui Xue, *Divisibility of an eigenform by another eigenform*, 2011.

[5] Kevin Buzzard, *On the eigenvalues of the Hecke operator T_2*, J. Number Theory, 57(1) (1996), 130–132.

[6] J. B. Conrey and D. W. Farmer, *Hecke operators and the nonvanishing of L-functions*, In m Topics in number theory (University Park, PA, 1997), volume 467 of Math. Appl., pages 143–150. Kluwer Acad. Publ., Dordrecht, 1999.

[7] J. B. Conrey, D. W. Farmer and P. J. Wallace, *Factoring Hecke polynomials modulo a prime*, Pacific J. Math., 196(1) (2000), 123–130.

[8] Dumas, Gautier, Giesbrecht, Giorgi, Hovinen, Kaltofen, Saunders, Turner and Villard, *Linbox: a generic library for exact linear algebra*, In A. Cohen, X-S Gao, and N. Takayama, editors, Mathematical software: ICMS 2002, pages 40–50, Beijing, 2002. World Scientific.

[9] Pierre Dusart, *Estimates of some functions over primes without R.H*, available as arXiv:1002.0442v1, 2010.

[10] N. J. A. Sloane et al, *The on-line encyclopedia of integer sequences, sequence A000246*, 2012.

[11] D. W. Farmer and K. James, *The irreducibility of some level 1 Hecke polynomials*, Math. Comp., 71(239):1263–1270 (electronic), 2002.

[12] William Feller, *An Introduction to Probability Theory and Its Applications*, volume 1. Wiley, New York, 1968.

[13] Alexandru Ghitza, *Distinguishing Hecke eigenforms*, Int. J. Number Theory, 7(5) (2011), 1247–1253.

[14] William Hart, *Fast library for number theory: an introduction*, In Mathematical Software – ICMS 2010, volume 6327 of Lecture notes in computer science, pages 88–91. Springer, Heidelberg, 2010.

[15] Haruzo Hida and Yoshitaka Maeda, *Non-abelian base change for totally real fields*, Pacific J. Math., (Special Issue):189–217, 1997. Olga Taussky-Todd: in memoriam.

[16] Seth Kleinerman, *Some computations in support of Maeda's conjecture*, 2004.

[17] Hong-Chang Lee and Wan-Hui Hung, *alois groups of Hecke eigenforms*, Chinese J. Math. 23(4) (1995), 329–342.

[18] Chu-Wee Lim, *Decomposition of spaces of cusp forms over Q, and variants of partial Nim*, ProQuest LLC, Ann Arbor, MI, 2005. Thesis (Ph.D.)–University of California, Berkeley.

[19] John Riordan, *An introduction to combinatorial analysis*, Wiley Publications in Mathematical Statistics. John Wiley & Sons Inc., New York, 1958.

[20] Herbert Robbins, *A remark on Stirling's formula*, Amer. Math. Monthly, 62 (1955), 26–29.

[21] Richard P. Stanley, *Enumerative combinatorics. Vol. 1*, volume 49 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

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

[23] W. A. Stein et al, *Sage Mathematics Software (Version 5.0)*, The Sage Development Team, 2012.

[24] P. Stevenhagen and H. W. Lenstra, *Chebotarëv and his density theorem*, Math. Intelligencer, 18(2) (1996), 26–37.

[25] Panagiotis Tsaknias, *A possible generalization of Maeda's conjecture*, available as arXiv:1205.3420, 2012.