Experimental Evidence for Maeda's Conjecture on Modular Forms

Angus McAndrew
The University of Melbourne

(joint with Alex Ghitza)

Australian Mathematical Society 56th Annual Meeting

September 24, 2012

Background

- Modular forms are a prominent area of research in number theory
- The Hecke Operators form a rich theory within the context of Modular forms
- Maeda's conjecture has received attention recently as a new source of insight into this theory
- Our recent work was to provide further numerical evidence for the conjecture, utilizing an improved version of the algorithm of Conrey-Farmer-Wallace, with a view towards the applications of the conjecture

Maeda's Conjecture

Conjecture (Maeda)

Consider the Hecke operator T_n acting on S_k, the space of level 1 cusp forms. Let F be the characteristic polynomial of T_n. 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 Σ_d, where d is the dimension of S_k.*

Motivation (An application)

Definition (L-function)

If a modular form $f(q) = \sum_n a_n q^n$ is a simultaneous eigenvector of all the Hecke Operators, the L-function associated to f is given by

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

Theorem (Non-vanishing of L-functions)

Suppose $k \equiv 0 \pmod 4$ and $k \leq 12000$. Then $L(f, k/2) \neq 0$ for any cuspidal eigenform f of level 1 and weight k.

Previous Results (computational)

Source	weights
Lee-Hung	$k \leq 62,\ k \neq 60$
Buzzard	$k = 12\ell,\ \ell$ prime, $2 \leq \ell \leq 19$
Maeda	$k \leq 468$
Conrey-Farmer	$k \leq 500,\ k \equiv 0 \pmod 4$
Farmer-James	$k \leq 2000$
Buzzard-Stein, Kleinerman	$k \leq 3000$
Chu-Wee Lim	$k \leq 6000$
Our recent work	$k \leq 12000$

Previous Results (theoretical)

Theorem (Conrey-Farmer-Wallace)

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

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

Theorem (Ahlgren)

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 $p \leq 4000000$;*
2. *T_n acting on S_k satisfies Maeda's conjecture for all $n \leq 10000$.*

Basic Lemma

Consider a monic polynomial $F \in \mathbb{Z}[X]$ of degree d. Given a prime p, we denote $F_p \in \mathbb{F}_p[X]$ 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 irrreducible 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.

Basic Lemma

Lemma (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 Σ_d (the symmetric group on d letters).

Basic Lemma (sketch of proof)

We have $F \in \mathbb{Z}[X]$ with splitting field $\mathbb{K}$ and primes of type I, II and III.
Prime of type I $\Rightarrow$ F is irreducible.
Let q, r be the primes of type II and III, respectively. Let $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) < \Sigma_d$ transitive. Let $\mathcal{Q}$ and $\mathcal{R}$ be primes of $\mathbb{K}$ above q and r, respectively. Then consider the Frobenius elements at those primes:

$$\mathrm{Frob}_{\mathcal{Q}}, \mathrm{Frob}_{\mathcal{R}}$$

We now invoke a result of algebraic number theory that the cycle patterns of these elements are identical to the factorization patterns of F mod q and r, respectively. Thus there exists powers of these elements, say τ_1, τ_2, such that $\mathrm{Frob}_{\mathcal{Q}}^{\tau_1}$ and $\mathrm{Frob}_{\mathcal{R}}^{\tau_2}$ are a 2-cycle and an ℓ-cycle (where $\ell > d/2$ is prime), respectively.
Then, by a result of group theory, a transitive subgroup of Σ_d with a 2-cycle and an ℓ-cycle ($\ell > d/2$ prime) must be equal to Σ_d, as required. $\square$

Implementation

1. Compute the Victor Miller basis $\mathcal{B}$ for S_k.
2. Compute the matrix M of the Hecke operator T_2 with respect to the basis $\mathcal{B}$.
3. Pick a random prime $p < 2^{20}$, uniformly over this range.
4. Reduce M modulo p and compute the characteristic polynomial $F_p \in \mathbb{F}_p[X]$.
5. If F_p is irreducible, then p is a prime of type I.
6. Factor F_p over $\mathbb{F}_p$ and use this factorization to decide whether p is a prime of type II or III.
7. Repeat from step (3) until we have found at least one prime of each type.

Theorem (Frobenius)

Let $F \in \mathbb{Z}[X]$ be monic, let $\mathbb{K}/\mathbb{Q}$ be the splitting field of F and let G be the Galois group of $\mathbb{K}/\mathbb{Q}$. 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 and factorization pattern $d_1^{m_1} \ldots d_t^{m_t}$ is equal to

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

Densities of Primes (continued)

- The density of primes of type I is

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

  (This is trivial)

- Let $d > 2$ and let $[d]_e$ be the largest even integer such that $[d]_e \leq d$. The density of primes of type II is

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

  and satisfies the inequality

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

  (This bound comes from an effective version of Stirling's approximation)

Densities of Primes (continued)

- The density of primes of type III is

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

If $d > 10$, then

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

(This bound comes from a bound on sums of reciprocals of primes by Dusart)

Perfomance Comparison with Conrey-Farmer-Wallace

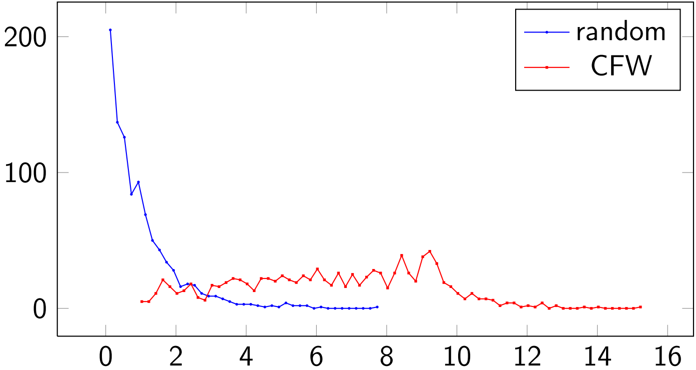

Figure: Histogram illustrating the number of primes tested before finding a prime of type II, in weights up to 2000. The x-axis represents the ratio N/E of the actual number of primes tested over the expected number of primes. The y-axis represents the number of weights featuring that particular ratio.

Main Result

Theorem

Let $k \leq 12000$ and let

$$\begin{aligned} n \in & \{2, \ldots, 10000\} \cup \{p \text{ prime } \mid 2 \leq p \leq 4000000\} \\ & \cup \{p \text{ prime } \mid p \not\equiv \pm 1 \pmod 5\} \\ & \cup \{p \text{ prime } \mid p \not\equiv \pm 1 \pmod 7\}. \end{aligned}$$

Let F be the characteristic polynomial of the Hecke operators 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.

Further Questions

Generalizations of Maeda's Conjecture:

- Higher level (Tsaknias, Chow-Ghitza-Withers)
  "The number of Galois orbits is a bounded function of the weight."
- Siegel Modular Forms
  "The Satake parameters are as irreducible as possible."