THE IRREDUCIBILITY OF SOME LEVEL 1 HECKE POLYNOMIALS

D.W. FARMER
K. JAMES

ABSTRACT. Let $T_{p,k}(x)$ be the characteristic polynomial of the Hecke operator T_p acting on the space of level 1 cusp forms $S_k(1)$. We show that $T_{p,k}(x)$ is irreducible and has full Galois group over $\mathbf{Q}$ for $k \leq 2000$ and $p < 2000$, p prime.

1. INTRODUCTION AND STATEMENT OF RESULTS

Let $S_k(1)$ denote the space of holomorphic cusp forms of even integral weight k for the full modular group $\Gamma(1) = SL_2(\mathbb{Z})$. We will denote by $T_{p,k}(x)$ the characteristic polynomial of the action of the Hecke operator T_p on $S_k(1)$. (For an introductory reference for these terms see Apostol's book [A].)

A conjecture of Maeda asserts that the Hecke algebra of $S_k(1)$ over $\mathbb{Q}$ is simple, and that its Galois closure over $\mathbb{Q}$ has Galois group the full symmetric group. There is even some speculation that $T_{p,k}(x)$ is irreducible in $\mathbb{Q}[x]$ and has full Galois group over $\mathbb{Q}$ for every prime p. This conjecture is related to the nonvanishing of L–functions [KZ][CF], and to constructing base changes to totally real number fields for level 1 eigenforms [HM].

There has been some progress towards this conjecture in recent years. For instance, Maeda's conjecture has been checked for $p = 2$ and $k \leq 540$ [B][CF], and various other small cases. Also, we know the following density result of [JO].

Theorem. *Let $T_{N,q}^{k,\chi}(x)$ denote the characteristic polynomial of the action of the Hecke operator T_q on the space $S_k(N, \chi)$ of cusp forms of weight k, level N and character χ. Let q and ℓ be distinct primes not dividing N, and let $\mathcal{L}$ denote a prime ideal lying above ℓ in $\mathbb{K}_{k,\chi,N}$ (the finite extension of $\mathbb{Q}$ obtained by adjoining all of the Fourier coefficients of the normalized eigenforms of $S_k(N, \chi)$). Then*

$$\#\left\{p < X \quad | \quad T_{N,p}^{k,\chi}(x) \equiv T_{N,q}^{k,\chi}(x) \pmod{\mathcal{L}}\right\} \gg_{N,\chi,k} \frac{X}{\log X}.$$

In particular, if $T_{N,p}^{k,\chi}(x)$ is irreducible mod 4ℓ for some p, then the same holds for a positive proportion of primes p.

If we specialize to $N = 1$, Conrey, Wallace and the first author have obtained a result similar to the last statement of this theorem with the added benefit that they achieve the

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

condition of having full Galois group as well as irreducibility. They also obtained a lower bound of 5/6 for the constant in this case. In this paper we report on calculations which establish:

Theorem 1. *The Hecke polynomial $T_{p,k}(x)$ is irreducible and has full Galois group over $\mathbb{Q}$ for $k \leq 2000$ and $p < 2000$, p prime.*

For the remainder of the paper, p and ℓ will represent distinct rational primes, and we will abbreviate "$T_{p,k}(x)$ is irreducible and has full Galois group over $\mathbb{Q}$" by "$T_{p,k}(x)$ satisfies Maeda's conjecture."

Our calculations have two distinct parts. First we show that if $p < 2000$, then $T_{n,k}(x)$ satisfying Maeda's conjecture for some n implies Maeda's conjecture for $T_{p,k}(x)$. This is described in Section 2. In Section 3 we describe calculations which show that $T_{2,k}(x)$ satisfies Maeda's conjecture for $k \leq 2000$.

$$2. \ T_{p,k}(x) \text{ for fixed } k.$$

We show

Proposition 1. *If $p < 2000$, p prime, and $T_{n,k}(x)$ satisfies Maeda's conjecture for some n, then $T_{p,k}(x)$ satisfies Maeda's conjecture.*

The proof involves exploiting the fact that if $T_{n,k}(x)$ satisfies Maeda's conjecture, then this puts severe restrictions on every other $T_{m,k}(x)$.

Lemma 1. *Suppose $T_{n,k}(x)$ is irreducible and has full Galois group for some n. Then for each m either*

a) $T_{m,k}(x)$ is irreducible and has full Galois group,

or,

b) $T_{m,k}(x) = (x - a)^d$ for some $a \in \mathbb{Z}$.

The proof involves considering the action of $G = Gal(\mathbb{K}_k/\mathbb{Q})$ on the Hecke basis for $S_k(1)$, where $\mathbb{K}_k$ is the field generated by the Fourier coefficients of the Hecke basis. Since G acts on both the individual coefficients and the Hecke basis, if one $T_{m,k}(x)$ is irreducible then all of the eigenforms are in one Galois orbit. And if $T_{m,k}(x)$ also has full Galois group then there are no intermediate subfields between $\mathbb{K}_k$ and $\mathbb{Q}$.

Thus, if $T_{n,k}(x)$ satisfies Maeda's conjecture, then we need only check that $T_{p,k}(x)$ has at least two distinct roots in order to verify Maeda's conjecture for $T_{p,k}(x)$. Our approach is to show that $T_{p,k}(x)$ has at least two distinct roots mod ℓ for some ℓ. The following result from [CFW] verifies this for 5/6 of all primes p.

Lemma 2. *Suppose $\dim(S_k(1)) \geq 2$. If $p \not\equiv -1, 0, 1 \bmod 5$ then $T_{p,k}(x)$ has at least two distinct roots mod 5, and if $p \not\equiv -1, 0, 1 \bmod 7$ then $T_{p,k}(x)$ has at least two distinct roots mod 7.*

The proof is by inspection of the factorization of $T_{p,k}(x)$ mod 5 and mod 7, which is given in [CFW].

By Lemmas 1 and 2, we have Proposition 1 for all p except those in four congruence classes mod 35. That is a total of 45 primes $p < 2000$. For those primes we must do some explicit calculations. However, the need for calculation can be further reduced by the following, which is part of Lemma 1 of [CFW].

Lemma 3. *If $\ell \geq 5$ then $T_{p,k}(x)$ divides $T_{p,k+\ell-1}(x)$ mod ℓ.*

The proof is to consider the inclusion $S_k(1) \subset S_{k+\ell-1}(1)$ mod ℓ, given by multiplication by the level 1 Eisenstein series $E_{\ell-1}(z)$.

Thus, if $T_{p,k}(x)$ has at at least two distinct roots mod ℓ, then so does $T_{p,k'}(x)$ for all $k' \geq k$ with $k' \equiv k$ mod $(\ell - 1)$.

We will let $\ell = 11$ for the remainder of this section. For each of the 45 primes p described above, and for each of the 5 possible values of k mod 10, we will determine the smallest k such that $T_{p,k}(x)$ has at least two distinct roots mod 11. The most favorable situation (for our purposes) is when $T_{p,k}(x)$ has at least two distinct roots mod 11 for $k = 24$ and $28 \leq k \leq 36$. By Lemma 3 this would imply that $T_{p,k}(x)$ has at least two distinct roots for all k, so conclusion b) of Lemma 1 never holds for $T_{p,k}(x)$.

It turns out that this "favorable situation" holds for 35 out of the 45 primes $p < 2000$ not covered by Lemma 2. For the remaining 10 cases we find larger values of k for which $T_{p,k}(x)$ has at least two distinct roots mod 11. This will leave a small number of exceptional cases to check.

We first summarize the results of our calculations, and then describe the method used for the calculations.

Proposition 2. *Table 1 shows all pairs (p, k) with p prime, $p < 2000$, such that Lemma 2 does not apply, $\dim S_k(1) \geq 2$, and $T_{p,k}(x)$ has only one root mod 11.*

p	k
251	24, 34
379	24, 34
419	28, 30, 38, 40, 50
461	28, 30, 38, 40, 50
601	32
659	28, 30, 38, 40, 50
769	28, 30, 38, 40, 50
881	28, 30, 38, 40, 50
1231	28, 30, 38, 40, 50
1429	28, 30, 38, 40, 50

Table 1: All pairs p, k with $p < 2000$, p prime, such that Proposition 1 cannot be established by a calculation mod 5, 7, or 11.

Thus, Proposition 1 is established except for the 40 cases given in Table 1. Those remaining cases were checked by explicitly verifying that the polynomial was irreducible. This completes the proof of Proposition 1.

We briefly review the methods required to generate the Hecke polynomials. For details, see [A]. The Hecke operator T_p acts on $S_k(1)$ by

$$(T_p f)(z) = p^{k-1} f(pz) + p^{-1} \sum_{b=0}^{p-1} f\left(\frac{z+b}{p}\right).$$

In terms of Fourier expansions, if $f(z) = \sum a(n)q^n$ and $(T_p f)(z) = \sum b(n)q^n$, then it is easy to check that

$$b(n) = \begin{cases} a(pn) & if \;\; p \nmid n \\ a(pn) + p^{k-1}a(n/p) & if \;\; p|n. \end{cases}$$

Thus, given a (partial) Fourier expansion of a basis for $S_k(1)$, it is straightforward to find the matrix of T_p with respect to that basis.

A basis for $S_k(1)$ is given by

$$B_k = \{\Delta^a E_4^b E_6^c \mid a \geq 1, \; b \geq 0, \; c = 0 \; or \; 1, \; 12a + 4b + 6c = k\}.$$

Here $E_k(z)$ is the weight k Eisenstein series, which has Fourier expansion

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n,$$

and $\Delta(z)$ is the weight 12 cusp form given by

$$\Delta(z) = \frac{E_4(z)^3 - E_6(z)^2}{1728}$$
$$= \sum_{n=1}^{\infty} \tau(n)q^n.$$

Thus, finding a partial Fourier expansion of a basis for $S_k(1)$ is straightforward.

For the cases required in this section, the dimension of $S_k(1)$ was at most 5, a total of 2000 Fourier coefficients were required, and the calculation took less than one day using Mathematica on a personal computer. This is a reflection of the fact that we were able to assume that $T_{p,k}(x)$ was irreducible and had full Galois group for some p, and this is an extremely strong assumption. The verification that this assumption holds takes a considerable amount of additional work, and this is described in the next section.

3. $T_{2,k}(x)$ FOR LARGE k

Since the size of the coefficients of $T_{2,k}(x)$ explodes as k grows, it is advantageous to work modulo a suitable prime ℓ. Thus our strategy for verifying that $T_{2,k}(x)$ satisfies Maeda's conjecture is to find appropriate factorizations of $T_{2,k}(x) \bmod \ell$ for various ℓ as described in the following lemma from [CF], which is an elaboration of the corresponding lemma of [B].

Lemma 4. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree d, with splitting field $\mathbb{K}/\mathbb{Q}$. Suppose there are primes q, r and s such that*

    i) *$f \equiv g_0 g_1 \cdots g_j \pmod{q}$ for distinct irreducible $g_i \in \mathbb{F}_q[x]$ with $\deg(g_0) = 2$ and $\deg(g_i)$ odd for $i \geq 1$.*

    ii) *$f \equiv h_0 h_1 \cdots h_l \pmod{r}$ for distinct irreducible $h_i \in \mathbb{F}_r[x]$ with $\deg(h_0) = p$, where $p > d/2$ is prime.*

    iii) *f is irreducible modulo s.*

Then f is irreducible and $Gal(\mathbb{K}/\mathbb{Q})$ is the full symmetric group S_d.

In the remainder of this section we will first briefly recall some facts about fast multiplication of polynomials modulo a prime ℓ using the discrete fast Fourier transform. We then review how the Berlekamp-Massey algorithm can be used to compute a factor of the characteristic polynomial of a matrix. Finally, we will use these algorithms in conjunction with Lemma 4 to obtain an algorithm for verifying Maeda's conjecture for $T_{2,k}(x)$ for $k = 542, \ldots, 2000$.

First, we recall (see Prop. III.2.9 in [Ko]) that we only need the first $k/12$ coefficients in order to distinguish the cuspforms in $S_k(1)$. Thus for computational purposes we will treat these cuspforms as polynomials modulo x^N for some $N > k/12$. Now if N is a power of 2, then we will let ℓ be a prime which is 1 modulo $2N$, and let ω be a primitive $2N$-th root of unity modulo ℓ. Recall the discrete fast Fourier transform (FFT) allows us to evaluate any polynomial f of degree less than $2N$ simultaneously at all of the $2N$-th roots of unity modulo ℓ in time proportional to $N \log N$. For a detailed account of the fast Fourier transform, we refer the reader to [Ch]. If we wish to multiply two polynomials f and g each of degree less than N, then we can use FFT to evaluate each of these at all of the $2N$-th roots of unity. Note that $h = fg$ is the unique polynomial of degree less than $2N$ with $h(\omega^i) = f(\omega^i)g(\omega^i)$ for $i = 1, 2, \ldots, 2N$. Thus, to determine the coefficients of h all we need to do is solve the linear system:

$$
\begin{pmatrix}
1 & \omega & \omega^2 & \ldots & \omega^{2N-1} \\
1 & \omega^2 & \omega^4 & \ldots & (\omega^2)^{2N-1} \\
 & & \ddots & & \\
1 & \omega^N & (\omega^N)^2 & \ldots & (\omega^N)^{2N-1}
\end{pmatrix}
\begin{pmatrix}
h_0 \\
h_1 \\
\vdots \\
h_{2N-1}
\end{pmatrix}
=
\begin{pmatrix}
h(\omega) \\
h(\omega^2) \\
\vdots \\
h(\omega^{2N-1})
\end{pmatrix}.
$$

Now, we note that the matrix on the left is a Vandermonde and its inverse is:

$$
\frac{1}{N}
\begin{pmatrix}
1 & \omega^{-1} & \omega^{-2} & \ldots & (\omega^{-1})^{2N-1} \\
1 & \omega^{-2} & \omega^{-4} & \ldots & (\omega^{-2})^{2N-1} \\
 & & \ddots & & \\
1 & \omega^{-N} & \omega^{-2N} & \ldots & (\omega^{-N})^{2N-1}
\end{pmatrix}.
$$

Therefore, in order to determine the coefficients $h_0, \ldots h_{2N-1}$ we simply need to evaluate the polynomial $\sum_{i=0}^{2N-1} h(\omega^i)x^i$ at all of the $2N$-th roots of unity and we can once again rely on FFT for this. Thus we can multiply any two polynomials each having degree less than N over $\mathbb{F}_\ell$ in $O(N \log N)$ time.

Another algorithm which proved useful for our purposes was the Berlekamp-Massey algorithm (see [M]). This algorithm takes as input a sequence of integers $a_0, a_1, \ldots, a_n$ and gives as its output the coefficients $c_1, c_2, \ldots, c_L$ of the shortest linear recurrence which generates the input sequence, that is the shortest sequence of numbers $c_1, c_2, \ldots, c_L$ such that

$$
a_j = -\sum_{i=1}^{L} c_i a_{j-i} \qquad j = L, L+1, \ldots.
$$

It can be shown (see [M Theorem 3]) that if $L \leq n/2$ then $c_1, c_2, \ldots, c_L$ is the unique minimal length sequence that generates $a_0, a_1, \ldots, a_n$. The running time of this algorithm is $O(n)$.

Now, let A be a non-singular square matrix of dimension d and let $f(x) = x^m + \sum_{m=0}^{d-1} b_{d-m} x^m$ be its characteristic polynomial. Following [W], we note that if for any fixed vector $\vec{V}$, we define a sequence of integers $\{v_m\}_{m \in \mathbb{N}}$ by

$$v_m = (A^m \vec{V}) \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

then for all $j \geq d$ we have $f(A)A^{j-d}\vec{V} = 0$, which implies

$$v_j = -\sum_{i=1}^{d} b_i v_{j-i}.$$

Thus, our sequence is generated by the linear recurrence with coefficients $b_1, \ldots, b_d$. Therefore, given the first $2d$ terms of this sequence, the Berlekamp-Massey algorithm will return the coefficients $c_1, \ldots, c_L$ of the unique shortest linear recurrence which generates the v_i's. Let $g(x) = x^L + \sum_{i=0}^{L-1} c_{L-i} x^i$. Since, the coefficients of f and g generate the same sequence and since g is the minimal such polynomial, one can show that $g|f$. Thus, given the first $2d$ terms of the above sequence, the Berlekamp-Massey algorithm will produce for us a factor of the characteristic polynomial of A in time proportional to d. Unfortunately, the time needed to produce the first $2d$ terms of this sequence is proportional to d^3. Thus we can find a factor of the characteristic polynomial of A in $O(d^3)$ time, which is a bit better than computing the characteristic polynomial in the straight forward manner which is $O(d^4)$. It is noteworthy that in practice it seems that the Berlekamp-Massey algorithm quite often produces the entire characteristic polynomial of our matrix. In any case, the most difficult aspect of our task proved to be producing primes for which $T_{2,k}(X)$ was irreducible and for this it is sufficient to produce any factor of $T_{2,k}(X)$.

The computation for checking that $T_{2,k}(X)$ satisfied Maeda's conjecture for $540 \leq k \leq 2000$ proceeded as follows. We set $N = 512$, the first power of 2 greater than $2 \times 2000/12$. We need the extra factor of 2 because we wish to distinguish modular forms in $S_k(1)$ for $k \leq 2000$ which are in the image of T_2. Next, we generated a list of primes which were 1 modulo $2N$ and a list of corresponding primitive $2N$-th roots of unity modulo those primes for use with FFT. For each of the primes p on our list, we performed the following calculations. For each weight $540 \leq k \leq 2000$, we first generated $N - 1$ coefficients of the rational basis forms for $S_k(1)$ and then constructed the matrix giving the action of T_2 on $S_k(1)$ with respect to our choice of basis. The Berlekamp-Massey algorithm was then employed to compute a factor of the characteristic polynomial of $T_{2,k}(X)$ modulo p. If the entire polynomial was not computed then we discarded it and proceeded to the next weight. If we were able to obtain the entire characteristic polynomial of T_2, then by analyzing the degrees of $\gcd(T_{2,k}(X), x^{p^i} - x)$ for $i = 1, 2, \ldots, \deg(T_{2,k}(X))$ we attempted

to verify the conditions of Lemma 4 for $T_{2,k}(X)$ modulo p. We made note of any successes and then moved up to the next weight. We then selected another prime from our list and carried out the above computation again. We repeated this process until the conditions of Lemma 4 were verified for $T_{2,k}(X)$ for all weights $540 \leq k \leq 2000$. Since all computations were carried out modulo p, the growth of the coefficients of the basis forms for $S_k(1)$ and $T_{2,k}(X)$ became irrelevant. Also, our selection of primes allowed us to use FFT to quickly multiply forms together, which made construction of the basis much faster.

For the sake of brevity we include the following table containing the last 40 weights and the corresponding primes q, r and s as in Lemma 4. All computations were coded in C and performed on Penn State's IBM SP (a 32 processor machine devoted solely to parallel applications) which allowed us to check for the conditions of Lemma 4 modulo 32 primes simultaneously. The computer time necessary for these computations was roughly 12 weeks.

k	q	r	s
1922	319489	974849	16465921
1924	1720321	1720321	11591681
1926	1130497	188417	20635649
1928	1032193	319489	37306369
1930	1843201	286721	13344769
1932	1990657	114689	1130497
1934	1097729	65537	3194881
1936	1810433	1662977	14663681
1938	3194881	163841	35880961
1940	270337	286721	3383297
1942	417793	417793	1146881
1944	319489	65537	35045377
1946	7667713	925697	12042241
1948	286721	737281	3022849
1950	6684673	925697	20914177
1952	114689	417793	737281
1954	5767169	557057	1097729
1956	1769473	286721	13631489
1958	1769473	147457	1810433
1960	925697	925697	26214401
1962	974849	163841	20316161
1964	557057	270337	18128897
1966	417793	147457	21594113
1968	1196033	147457	2424833
1970	925697	925697	17440769
1972	4866049	270337	13631489
1974	3383297	638977	1843201
1976	2482177	417793	925697
1978	737281	319489	15228929
1980	6725633	319489	22552577
1982	319489	786433	3604481
1984	147457	1196033	48906241
1986	1179649	147457	22454273
1988	2277377	417793	40058881
1990	778241	163841	17440769
1992	778241	188417	38256641
1994	1318913	114689	33005569
1996	4882433	1032193	26238977
1998	4620289	286721	53370881
2000	2424833	974849	17522689

References

[A] *T. Apostol*, Modular functions and Dirichlet series in number theory, GTM 41, Springer–Verlag, (1990).

[B] *K. Buzzard*, On the eigenvalues of the Hecke operator T_2, J. Number Theory **57** (1996), no. 1, 130–132.

[Ch] *P. Chiu*, Transforms, finite fields, and fast multiplication, Math. Mag. **63** (1990), no. 5, 330–336.

[Co] *H. Cohen*, A course in computational algebraic number theory, Springer–Verlag. (1996).

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

[CFW] *J.B. Conrey*, *D.W. Farmer*, and *P.J. Wallace*, Factoring Hecke polynomials modulo a prime, to appear in Pacific J. of Math.

[HM] *H. Hida* and *Y. Maeda*, Non–abelian base change for totally real fields, Pac. J. Math (to appear).

[JO] *K. James* and *K. Ono*, A note on the irreducibility of Hecke polynomials. J. Number Theory 73 (1998), no. 2, 527–532.

[Ko] *N. Koblitz*, Introduction to elliptic curves and modular forms, second edition, GTM 97, Springer–Verlag, (1984).

[KZ] *W. Kohnen* and *D. Zagier*, Values of L-series of modular forms at the center of the critical strip, Invent. Math. **64** (1981), no. 2, 175–198.

[M] *J. L. Massey*, Shift-register synthesis and BCH decoding, IEEE Trans. Inform. Theory. **vol IT-15** (1969), no. 1, 122–127.

[W] *D. H. Wiedemann*, Solving sparse linear equations over finite fields, IEEE Trans. Inform. Theory. **vol IT-32** (1986), no. 1, 54–62.