MATHEMATICS OF COMPUTATION
Volume 77, Number 263, July 2008, Pages 1725–1731
S 0025-5718(08)02078-4
Article electronically published on February 1, 2008

ON THE IRREDUCIBILITY OF HECKE POLYNOMIALS

SCOTT AHLGREN

Abstract. Let $T_{n,k}(X)$ be the characteristic polynomial of the nth Hecke operator acting on the space of cusp forms of weight k for the full modular group. We record a simple criterion which can be used to check the irreducibility of the polynomials $T_{n,k}(X)$. Using this criterion with some machine computation, we show that if there exists $n \geq 2$ such that $T_{n,k}(X)$ is irreducible and has the full symmetric group as Galois group, then the same is true of $T_{p,k}(X)$ for each prime $p \leq 4,000,000$.

1. Introduction and statement of results

Let k be a positive even integer, and let S_k denote the space of cusp forms of weight k for the modular group $\mathrm{SL}_2(\mathbb{Z})$. With $q := e^{2\pi i z}$, we may identify a cusp form $f(z) \in S_k$ with its Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a_n(f) q^n.$$

For each prime p, the Hecke operator $T_{p,k}$ is an endomorphism of S_k whose action is described via the formula

$$T_{p,k}\left(\sum_{n=1}^{\infty} a_n q^n\right) = \sum_{n=1}^{\infty} (a_{np} + p^{k-1} a_{n/p}) q^n. \tag{1.1}$$

More generally, for $n \geq 1$, the operators T_n are defined via the Euler product

$$\sum T_{n,k} n^{-s} = \prod_p (1 - T_{p,k} p^{-s} + p^{k-1-2s})^{-1}. \tag{1.2}$$

For complete background one may consult [7], for example.

We let $T_{n,k}(X)$ be the characteristic polynomial of the operator $T_{n,k}$ on the space S_k. Since S_k has a basis of forms with rational integer coefficients, we see from (1.1) and (1.2) that $T_{n,k}(X) \in \mathbb{Z}[X]$. Let d_k denote the dimension of the complex vector space S_k, and let Ω_d denote the symmetric group on d letters. Maeda ([5], Conjecture 1.2) made the conjecture that the Hecke algebra of each S_k over $\mathbb{Q}$ is simple (i.e. it is a single number field) and that the Galois closure has Galois group Ω_{d_k}. This would be implied by the existence of an n for which $T_{n,k}(X)$ is irreducible with group Ω_{d_k}. The conjecture implies that there is a single Galois

Received by the editor February 21, 2007 and, in revised form, May 31, 2007.

2000 *Mathematics Subject Classification.* Primary 11F11.

The author thanks the National Science Foundation for its support through grant DMS 01-34577. He also thanks the Department of Computing at Macquarie University for its hospitality during part of the time when this research was conducted.

orbit of Hecke eigenforms in S_k, which has implications for the work of Maeda and Hida [5] on base change for totally real fields.

In recent years a number of authors have investigated the irreducibility of the polynomials $T_{n,k}(X)$. James and Ono [6] studied the reductions of Hecke polynomials (of arbitrary level) modulo primes ℓ. Buzzard [2] proved that if $\ell \leq 19$ is prime and $k = 12\ell$, then the polynomial $T_{2,k}$ is irreducible and has Galois group Ω_{d_k}. Exploiting some periodicities in the factorization of $T_{p,k}(X)$ modulo 5 and 7, Conrey, Farmer, and Wallace proved the following result.

Theorem 1.1 ([3], Theorem 1). *Let k be a positive even integer, and suppose that there exists an n for which $T_{n,k}(X)$ is irreducible and has Galois group Ω_{d_k}. Then the same is true of the polynomial $T_{p,k}(X)$ for each prime p such that*

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

Farmer and James [4] proved that for each $p \leq 2000$ and each $k \leq 2000$, the polynomial $T_{p,k}(X)$ is irreducible and has Galois group Ω_{d_k}. More recently, Baba and Murty, using Frobenius distributions and an effective form of the Chebotarev Density Theorem, have proved the following.

Theorem 1.2 ([1], Theorem 1.1). *Let k be a positive even integer, and suppose that there exists a prime p for which $T_{p,k}(X)$ is irreducible. Then for some $\delta > 0$ we have*

$$\#\{p \leq N \ : \ T_{p,k}(X) \textit{ is reducible}\} \ll \frac{N}{(\log N)^{1+\delta}}.$$

Baba and Murty also obtain

Theorem 1.3 ([1], Theorem 1.2). *Let k be a positive even integer, and suppose that there exists a prime p for which $T_{p,k}(X)$ is irreducible with Galois group Ω_{d_k}. Then the same holds for $T_{n,k}(X)$ for all $n \leq d_k$.*

Our aim here is to record a simple criterion which is equivalent to the irreducibility of $T_{n,k}(X)$ under the hypotheses in Theorems 1.1, 1.2, and 1.3. This criterion is quite amenable to computation (cf. Theorem 1.5 below). To simplify the exposition, we introduce "Hypothesis O" for the space S_k:

> **Hypothesis O for S_k:** There exists an n for which $T_{n,k}(X)$ is irreducible and has Galois group Ω_{d_k}.

We define the space S'_k by

$$S'_k := \{f \in S_k \ : \ \operatorname{ord}_\infty(f) \geq 2\}. \tag{1.3}$$

When $\dim S_k \geq 1$ we have

$$\dim S'_k = \dim S_k - 1.$$

With this notation, we have the following result.

Theorem 1.4. *Let k be such that $\dim S_k \geq 2$, and suppose that S_k satisfies Hypothesis O. Then for every $n \geq 2$, the following are equivalent:*

1. *$T_{n,k}(X)$ is irreducible with Galois group Ω_{d_k}.*
2. *There exists a modular form $f \in S'_k$ such that $a_n(f) \neq 0$.*

Remark. It is known that the polynomial $T_{2,24}(X)$ is irreducible. Let $\Delta(z)$ be the unique normalized cusp form of weight 12 (defined explicitly in (1.6) below), and write

$$\Delta^2(z) = \sum_{n=2}^{\infty} a(n)q^n. \tag{1.4}$$

Since $d_{24} = 2$, it follows from Theorem 1.4 that

$$T_{n,24}(X) \text{ is irreducible } \iff a(n) \neq 0.$$

One might speculate that the coefficients $a(n)$ in (1.4) are never zero (or more generally that the second condition in Theorem 1.4 is always satisfied). To prove this seems to be a very difficult problem; the same speculation for the coefficients of $\Delta(z)$ is a famous unsolved problem of Lehmer.

It is typically easy to check the second condition in Theorem 1.4 numerically. Via some machine computation, we obtain the following result.

Theorem 1.5. *Let k be such that $\dim S_k \geq 2$, and suppose that S_k satisfies Hypothesis O. Then the following are true:*

(1) *$T_{p,k}(X)$ is irreducible with Galois group Ω_{d_k} for each prime $p \leq 4,000,000$.*
(2) *$T_{n,k}(X)$ is irreducible with Galois group Ω_{d_k} for each $n \in \{2, 3, \ldots, 10,000\}$.*

Remark. This may be compared with Theorem 1.3 when k is large. The bounds in Theorem 1.5 could easily be increased if necessary with more computation.

We briefly indicate the connection between Theorem 1.1 and Theorem 1.4. To this end, we recall the definition of the Eisenstein series

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

where $k \geq 4$ is even, B_k is the kth Bernoulli number, and $\sigma_{k-1}(n)$ is the sum of the $(k-1)$st powers of the divisors of n. Each E_k is a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$. For primes $p \geq 5$, the von Staudt-Claussen theorem on the p-adic valuation of Bernoulli numbers implies the congruence

$$E_{p-1}(z) \equiv 1 \pmod{p}. \tag{1.5}$$

We have the relation

$$\Delta(z) := \frac{E_4^3(z) - E_6^2(z)}{1728}. \tag{1.6}$$

We have the following congruences, which can be verified using standard techniques from the theory of modular forms modulo ℓ (see, for example, [8] or [7]):

$$\begin{aligned} \Delta^2 &\equiv 2\sum n(n^2-1)\sigma(n)q^n \pmod{5},\\ \Delta^2 E_6 &\equiv \sum n^2(n^2-1)\sigma(n)q^n \pmod{5}, \end{aligned} \tag{1.7}$$

and

$$\begin{aligned} \Delta^2 &\equiv \sum(n^2\sigma(n) - n\sigma_3(n))q^n \pmod{7},\\ \Delta^2 E_4 &\equiv 2\sum(n\sigma(n) - n^3\sigma_3(n))q^n \pmod{7},\\ \Delta^2 E_4^2 &\equiv 3\sum(n^2\sigma_3(n) - n^3\sigma(n))q^n \pmod{7}. \end{aligned} \tag{1.8}$$

In view of (1.5), we see that if $\dim S_k \geq 2$, then the space S'_k contains a modular form with integer coefficients which is congruent to one of the two forms in (1.7) modulo 5, and a form which is congruent to one of the three forms in (1.8) modulo 7. Therefore we obtain the following as corollaries to Theorem 1.4.

Corollary 1.6. *Suppose that* $\dim S_k \geq 2$ *and that* S_k *has Hypothesis O. Suppose that*

$$n(n^2-1)\sigma(n) \not\equiv 0 \pmod 5.$$

Then $T_{n,k}(X)$ *is irreducible and has Galois group* Ω_{d_k}.

Corollary 1.7. *Suppose that* $\dim S_k \geq 2$ *and that* S_k *has Hypothesis O. Suppose that*

$$n^2\sigma(n) - n\sigma_3(n) \not\equiv 0 \pmod 7 \quad \text{if } k \equiv 0, 2 \pmod 6,$$
$$n\sigma(n) - n^3\sigma_3(n) \not\equiv 0 \pmod 7 \quad \text{if } k \equiv 4 \pmod 6.$$

Then $T_{n,k}(X)$ *is irreducible and has Galois group* Ω_{d_k}.

Specializing to the case when $n = p$ is prime, we see that Theorem 1.1 follows from these corollaries.

2. Proof of Theorem 1.4

The proof is similar to that of Theorem 1.3. We begin with a lemma which has been recorded in various forms in [3], [4], and [1]. We give a proof here for completeness.

Lemma 2.1. *Suppose that* $k \geq 2$ *is an even integer and that there exists* $n_0 \geq 2$ *with the property that* $T_{n_0,k}(X)$ *is irreducible with Galois group* Ω_{d_k}. *Then for each* $n \geq 2$, *one of the following is true:*

(1) $T_{n,k}(X)$ *is irreducible.*
(2) $T_{n,k}(X) = (X-a)^{d_k}$ *for some constant* a.

In the first case, $T_{n,k}(X)$ *has Galois group* Ω_{d_k}.

Proof. Set $d = d_k$ and let

$$\{f_1, \dots, f_d\} \tag{2.1}$$

be a basis of normalized eigenforms for the space S_k. Let the Fourier expansions of these forms be given by

$$\begin{aligned} f_1 &= q + \dots + \quad a_{n_0}(f_1)q^{n_0} + \dots + a_n(f_1)q^n + \dots \\ &\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ f_d &= q + \dots + \quad a_{n_0}(f_d)q^{n_0} + \dots + a_n(f_d)q^n + \dots . \end{aligned} \tag{2.2}$$

Then for each n we have

$$T_{n,k}(X) = (X - a_n(f_1)) \dots (X - a_n(f_d)). \tag{2.3}$$

By hypothesis, the roots $a_{n_0}(f_i)$ are distinct and the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts as the full permutation group Ω_d on the set $\{a_{n_0}(f_i)\}$. It follows that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts as the full permutation group Ω_d on $\{f_i\}$ and therefore that it acts transitively on $\{a_n(f_i)\}$. From this we see that $T_{n,k}(X) = f(X)^r$ for some r, where $f(X)$ is an irreducible polynomial of degree $e := d/r$. If it were the case that both $e > 1$ and $r > 1$, then we could select distinct indices i, j, and k for which $a_n(f_i) = a_n(f_j)$ and

$a_n(f_i) \neq a_n(f_k)$. However, this would contradict the fact that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ contains an element σ whose action on $\{f_i\}$ is described by the cycle (i, j, k). Therefore either $T_{n,k}(X)$ is irreducible or has the form $(X-a)^d$. In the former case it is clear that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts as the full permutation group on the set of roots. □

Proof of Theorem 1.4. Let k be as in the hypotheses. Suppose first that $n \geq 2$ is an integer for which $T_{n,k}(X)$ is reducible; by Lemma 2.1 it follows that there is a constant a with the property that $a_n(f_i) = a$ for each eigenform f_i in the basis (2.1). Let f be a form in S'_k, and write

$$f = \sum_{i=1}^{d} c_i f_i \tag{2.4}$$

as a linear combination of this basis. Since each f_i has the form $f_i = q + \dots$, and f vanishes to order ≥ 2 at infinity, it follows that $\sum c_i = 0$. But then $a_n(f) = \sum c_i a = 0$.

Conversely, suppose that $n \geq 2$ is such that each form $f \in S'_k$ has $a_n(f) = 0$. Writing f as in (2.4), and with notation as in (2.2), we conclude that

$$\sum_{i=1}^{d} c_i = 0 \quad \Longrightarrow \quad \sum_{i=1}^{d} c_i a_n(f_i) = 0. \tag{2.5}$$

Therefore there exists a constant a with $a_n(f_i) = a$ for all i, and so $T_{n,k}(X) = (X-a)^d$. □

3. Proof of Theorem 1.5

To prove Theorem 1.5, we use Theorem 1.4 together with some machine computation. Write $S'_k(\mathbb{Z})$ for the $\mathbb{Z}$-module of forms in S'_k with rational integer coefficients. Recall the congruence (1.5). To prove Theorem 1.5, it will suffice, for each prime $p < 4,000,000$ and for each k with $\dim S_k \geq 2$, to produce the following:

(1) A prime $\ell \geq 5$ and an integer $k_0 \leq k$ with $k_0 \equiv k \pmod{\ell - 1}$.
(2) A form $f \in S'_{k_0}(\mathbb{Z})$ with the property that $a_p(f) \not\equiv 0 \pmod{\ell}$.

Define the Eisenstein series $\widetilde{E}_k$ via the formulas

$$\widetilde{E}_k := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12}, \\ E_{14} & \text{if } k \equiv 2 \pmod{12}, \\ E_4 & \text{if } k \equiv 4 \pmod{12}, \\ E_6 & \text{if } k \equiv 6 \pmod{12}, \\ E_8 & \text{if } k \equiv 8 \pmod{12}, \\ E_{10} & \text{if } k \equiv 10 \pmod{12}. \end{cases} \tag{3.1}$$

Suppose first that $k \geq 240$ and $k \neq 242$; in this case the computations can be done using the primes $\ell = 5$ and $\ell = 7$. We fix a class $\overline{k} \pmod{12}$ of weights and compute, for each $d \in \{2, 3, \dots, 20\}$, the first $4,000,000$ coefficients of each of the modular forms

$$f_{d,5} := \Delta^d \widetilde{E}_{\overline{k}} \pmod{5} \quad \text{and} \quad f_{d,7} := \Delta^d \widetilde{E}_{\overline{k}} \pmod{7}. \tag{3.2}$$

To simplify computations, we use the formulas

$$\Delta \equiv \sum_{n=1}^{\infty} n\sigma_1(n) \pmod 5, \qquad \Delta \equiv \sum_{n=1}^{\infty} n\sigma_3(n) \pmod 7.$$

We find, for each $p \leq 4,000,000$, that at least one of the forms $f_{d,\ell}$ in (3.2) has the property that

$$a_p(f_{d,\ell}) \not\equiv 0 \pmod \ell. \tag{3.3}$$

This establishes the result when $k \geq 240$, $k \neq 242$. We note that this step required a little more than one hour of computation (using MAGMA) on a desktop computer.

The weights $k < 240$ and $k = 242$ can be dealt with individually (in several hours of computation). In view of congruences like (1.7) and (1.8), small primes ℓ are less suitable for this purpose. To proceed, we compute, for each $2 \leq d \leq 19$, and for each residue class $\overline{k}$ (mod 12) of weights, the first $4,000,000$ coefficients of each of the modular forms

$$g_{(d,\overline{k}),691} := \Delta^d \widetilde{E_{\overline{k}}} \pmod{691} \quad \text{and} \quad g_{(d,\overline{k}),701} := \Delta^d \widetilde{E}_{\overline{k}} \pmod{701} \tag{3.4}$$

(these particular primes are used for the sole reason that their size is suited to the purpose). For each pair $(d, \overline{k})$, we see from this computation that for almost every prime p with $d \leq p < 4,000,000$, at least one of the following is true:

1. The *pth* coefficient of $g_{(d,\overline{k}),691}$ is non-zero modulo 691.
2. The *pth* coefficient of $g_{(d,\overline{k}),701}$ is non-zero modulo 701.

The exceptional primes $p_1, \ldots, p_e$ are those for which neither of the two conditions hold (for none of the pairs $(d, \overline{k})$ in our range are there more than 3 exceptional primes). Most of these can be eliminated using Theorem 1.1. The few remaining exceptional primes p can be eliminated by exhibiting another modular form $h \in S'_k$ with the property that $a_p(h) \not\equiv 0 \pmod 7$. To illustrate, we record the result of this computation for those weights $k < 240$ with $k \equiv 10 \pmod{12}$.

Exceptional primes when $\overline{k} = 10$, $2 \leq d \leq 19$.

d	Exceptional primes p	Reason for elimination
3	1337363	$p \equiv 3 \pmod 5$
4	3906883	$p \equiv 3 \pmod 5$
9	3911	$p \equiv 5 \pmod 7$
11	718411 3565921	pth coeff. of $\Delta^4 E_4 E_6^{15}$ is $3 \pmod 7$ $p \equiv 2 \pmod 7$
13	189671	pth coeff. of $\Delta^4 E_4 E_6^{19}$ is $2 \pmod 7$
14	80777	$p \equiv 2 \pmod 5$
15	902263	$p \equiv 3 \pmod 5$
18	3019571	$p \equiv 2 \pmod 7$

Similar methods can be used to establish the second assertion in Theorem 1.5; for brevity we do not include the details here.

References

[1] S. Baba and M. R. Murty, Irreducibility of Hecke polynomials, Math. Res. Lett. **10** (2003), no. 5-6, 709–715. MR2024727 (2005g:11064)

[2] K. Buzzard, On the eigenvalues of the Hecke operator T_2, J. Number Theory **57** (1996), no. 1, 130–132. MR1378578 (96m:11033)

[3] J. B. Conrey, D. W. Farmer and P. J. Wallace, Factoring Hecke polynomials modulo a prime, Pacific J. Math. **196** (2000), no. 1, 123–130. MR1797238 (2001k:11072)

[4] D. W. Farmer and K. James, The irreducibility of some level 1 Hecke polynomials, Math. Comp. **71** (2002), no. 239, 1263–1270. MR1898755 (2003e:11046)

[5] H. Hida and Y. Maeda, Non-abelian base change for totally real fields, Pacific J. Math. **1997**, Special Issue, 189–217. MR1610859 (99f:11068)

[6] K. James and K. Ono, A note on the irreducibility of Hecke polynomials, J. Number Theory **73** (1998), no. 2, 527–532. MR1658012 (2000a:11063)

[7] S. Lang, *Introduction to modular forms*, Corrected reprint of the 1976 original, Springer, Berlin, 1995. MR1363488 (96g:11037)

[8] H. P. F. Swinnerton-Dyer, On l-adic representations and congruences for coefficients of modular forms, in *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, 1–55. Lecture Notes in Math., 350, Springer, Berlin. MR0406931 (53:10717a)

Department of Mathematics, University of Illinois, Urbana, Illinois 61801
E-mail address: ahlgren@math.uiuc.edu