Mathematical Research Letters **10**, 709–715 (2003)

IRREDUCIBILITY OF HECKE POLYNOMIALS

Srinath Baba and M. Ram Murty

Abstract. In this note, we show that if the characteristic polynomial of some Hecke operator T_n acting on the space of weight k cusp forms for the group $\mathrm{SL}_2(\mathbb{Z})$ is irreducible, then the same holds for T_p, where p runs through a density one set of primes. This proves that if Maeda's conjecture is true for some T_n, then it is true for T_p for almost all primes p.

1. Introduction

Let V be the d-dimensional space of weight k cusp forms $S_k(\mathrm{SL}_2(\mathbb{Z}))$, and T_n the n^{th} Hecke operator on V. Let $T_n(x)$ denote the characteristic polynomial of T_n. By the theory of eigenforms, it is well known that $T_n(x) \in \mathbb{Z}[x]$ and is monic. Maeda [8] conjectured that for some n, $T_n(x)$ is irreducible with Galois group S_d, where S_d is the symmetric group on d symbols. A popular extension of this conjecture, called **Maeda's conjecture** states that for *every* n, $T_n(x)$ is irreducible with Galois group S_d.

Recent progress related to Maeda's conjecture has been in two different directions. The first is to verify the conjecture for $T_2(x)$ for different weights k ([1], [12]), and the second has been to show irreducibility of $T_p(x)$ assuming the irreducibility of $T_q(x)$ for some q. In [2], it is shown using the trace formula in characteristic p that if some $T_q(x)$ satisfies Maeda's conjecture, then the same holds for $T_p(x)$ for p in a set of primes of density 5/6. Combining this with computer computations, K. James and D. Farmer have shown in [3] that if $T_q(x)$ satisfies Maeda's conjecture for some q, then the same holds for $T_p(x)$ for primes $p \leq 2000$.

The purpose of this note is to extend the work of both [2] and [3]. As opposed to the mod-p versions of the trace formula used by [2], we study Frobenius distributions and Galois representations of Hecke eigenforms to show that

Theorem 1.1. *If $T_q(x)$ is irreducible for some prime q, then*

$$\sharp\{p \leq x; T_p(x) \text{ is reducible}\} \ll x/(\log x)^{1+\delta},$$

for some $\delta > 0$.

In addition, we show the following:

Theorem 1.2. *If $T_q(x)$ is irreducible with Galois group S_d for some prime q, then the same holds for $T_n(x)$ for $n \leq d$.*

Received October 16, 2001.

The argument is based on the existence of a so called Miller basis for V, and uses linear algebra in combination with the Chebotarev density theorem and theorems of Deligne and Serre on the existence of certain ℓ-adic representations attached to Hecke eigenforms.

2. Preliminaries

For any cusp form g, let $g = \sum_{i=1}^{\infty} a_n(g)q^n$ denote its Fourier expansion at the cusp at ∞. Let $K(g) = \mathbb{Q}(\{a_i(g)\}_{i=1}^{\infty})$. Let $f_1, \dots f_d$ denote a basis of normalised Hecke eigenforms for V. For any $i, 1 \leq i \leq d$, it is known that $K(f_i)$ is a number field of finite degree, and that the a_n are all algebraic integers. Since the f_i are simultaneous eigenvectors of all the Hecke operators, we know that $T_n(x) = \prod_{i=1}^{d}(x - a_n(f_i))$.

Lemma 2.1. *Suppose $T_q(x)$ is irreducible, where q is a prime. Then $K(f_i) = \mathbb{Q}(a_q(f_i))$.*

Proof. Let $h_1, \dots h_d$ be the Miller basis for V. This basis is characterised by the property that $K(h_i) = \mathbb{Q}$ for every i, and $a_i(h_j) = \delta_{i,j}$, for $1 \leq i, j \leq d$, where $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise (see [6]). Let f be any of the eigenforms. Expressing f as a linear combination of the h_i, we have

$$f = \sum_{i=1}^{d} a_i(f)h_i = h_1 + \sum_{i=2}^{d} a_i(f)h_i.$$

Since $T_q(x)$ is irreducible, it is immediate that not all of the coefficients $a_q(h_2)$, $\dots$, $a_q(h_d)$ are 0. Without loss of generality, we assume that $a_q(h_2) \neq 0$. By row reducing the Miller basis, we can obtain a basis $g_1 \dots g_d$ so that $a_1(g_1) = 1, a_1(g_j) = 0$ for $j \neq 1$, and $a_q(g_2) = 1, a_q(g_j) = 0$ for $j \neq 2$, and $K(g_j) = \mathbb{Q}$ for every g_j.

Expressing f in terms of the new basis, we realise that one of the Fourier coefficients $a_{q^2}(g_3), \dots , a_{q^2}(g_d)$ must be non-zero. By repeating the row reduction argument and producing a new basis each time, we construct a basis $F_1, \dots F_d$ with the property that $a_{q^{i-1}}(F_j) = \delta_{i,j}$. In addition, $K(F_i) = \mathbb{Q}$ for every F_i. Expressing f in terms of this basis, and observing that $a_{q^l}(f) \in \mathbb{Q}(a_q(f))$ for every $l \in \mathbb{Z}$, we have

$$f = \sum_{i=1}^{d} a_{q^{i-1}}(f)F_i = \sum_{i=1}^{d} b_i F_i \text{ where } b_i \in \mathbb{Q}(a_q).$$

Thus, for any n, $a_n(f) \in \mathbb{Q}(a_q(f))$, and so the lemma follows. □

Lemma 2.2. *If $T_q(x)$ is irreducible for some prime q with Galois group G, then for any other n, $T_n(x)$ has exactly one irreducible factor. In addition, if $G = S_d$, then the irreducible factor of T_n has degree d or 1.*

Proof. Suppose $T_q(x)$ is irreducible with Galois group G. Then G acts transitively on the roots of $T_q(x)$. Since the roots of $T_n(x)$ by Lemma 2.1, are rational linear combinations of the roots of $T_q(x)$, they form a Galois orbit with a G action. Thus, they are all roots of the same irreducible polynomial. If, in addition, $G = S_d$, then the roots of $T_n(x)$ must form an orbit for a transitive S_d action, and thus must all be equal, or all distinct. This proves the lemma. □

Consider a Galois extension $L/\mathbb{Q}$ with Galois group G discriminant d_L and degree n_L. Suppose S is the set of primes in K ramified in L. Let C be a collection of conjugacy classes in G. Let

$$\pi_C(x) = \text{ the number of primes } v \in \mathcal{O}_L; N_{L/\mathbb{Q}}(v) \le x \text{ and } \mathrm{Frob}_v \in C.$$

The Chebotarev density theorem states that

$$\pi_C(x) \sim \frac{|C|}{|G|}\pi(x)$$

where $\pi(x) =$ the number of primes $p \in \mathbb{Z}; p \le x$.

The following unconditional effective version of this theorem was provided by Lagarias, Montgomery and Odlyzko in [7], we state a version due to Serre (see [11], Theorem 3, page 132).

Proposition 2.3. (Effective version of the Chebotarev density theorem) *If* $x \ge 3$ *and* $\log x \ge c(\log d_L)(\log\log d_L)(\log\log\log 6d_L))$, *then* $\pi_C(x) \ll \frac{|C|}{|G|}\pi(x)$, *where* c *is an absolute constant.*

We can bound the discriminant d_L of L by the following (see [11] Page 129, Proposition 4′ for a general statement)

Proposition 2.4. (Hensel) $\log d_L \le (n_L - 1)\sum_{l \in S} \log l + n_L \log n_L$.

3. Fourier coefficients of Hecke eigenforms

Let f be a normalised Hecke eigenform, and suppose that for some q,

$$[\mathbb{Q}(a_q(f)) : \mathbb{Q}] = d.$$

This is the same as saying $T_q(x)$ is irreducible. From Lemma 2.1, we know that $K(f) = \mathbb{Q}(a_q(f))$.

Theorem 3.1. *Let* $L \subset K(f)$ *be any proper subfield. Then,*

$$\sharp\{p \le x; a_p(f) \in L\} \ll \frac{x}{(\log x)^{1+\delta}} \ ,$$

for some $\delta > 0$.

Proof. Let $K(f) = K$, and let $L \subset K(f)$ be a proper subfield. Let $\lambda \in \mathcal{O}_K$ be a prime of degree $f \ge 2$ lying above $l \in \mathcal{O}_L$. By a well-known construction of Deligne and Serre (see [10], pages 260-261), there exists a continuous representation

$$\rho_{f,\lambda} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathcal{O}_K/\lambda)$$

satisfying the following conditions for $p \ne l$:

(i) $\rho_{f,\lambda}$ is unramified at p
(ii) $\operatorname{trace}(\rho_{f,\lambda}(\operatorname{Frob}_\pi)) = a_p(f)$, for any prime ideal π lying above p.

Let $S \subset \operatorname{GL}_2(\mathcal{O}_K/\lambda)$ be the set of elements whose trace lies in the subfield $\mathcal{O}_L/l \subset O_K/\lambda$. By a simple counting argument, we see that

$$\sharp(S) \ll l^{3f+1} \text{ and } \sharp(\operatorname{GL}_2(\mathcal{O}_K/\lambda)) \sim l^{4f}.$$

Let M be the fixed field of the kernel of the representation $\rho_{f,\lambda}$. By the effective version of the Chebotarev density theorem in M, if $l \sim (\log x)^\delta$, then

$$\sharp\{p \leq x; \operatorname{trace}(\rho_{f,\lambda}(\operatorname{Frob}_p)) \in \mathcal{O}_L/l \subset O_K/\lambda\} \ll \frac{\sharp(S)}{\sharp(\operatorname{GL}_2(\mathcal{O}_K/\lambda))} x/\log x.$$

By the bounds on $\sharp(S)$ and $\sharp(\operatorname{GL}_2(\mathcal{O}_K/\lambda))$ and on l, we see that

$$\sharp\{p \leq x; \operatorname{trace}(\rho_{f,\lambda}(\operatorname{Frob}_p)) \in \mathcal{O}_L/l \subset O_K/\lambda\} \ll \frac{x}{l^{f-1}\log x} \ll \frac{x}{(\log x)^{1+\delta}}.$$

This proves the theorem. □

Proof of Theorem 1.1. By Lemma 2.2, if $T_q(x)$ is irreducible, then $T_p(x)$ is reducible if and only if it has a repeated root. Thus, $K(f_1)$ contains $\mathbb{Q}(a_p(f_1))$ as a proper subfield. Since there are only finitely many proper subields of $K(f_1)$, we can apply Theorem 3.1 to each subfield. Thus, we see that

$$\sharp\{p \leq x; T_p(x) \text{ is reducible }\} \ll \frac{x}{(\log x)^{1+\delta}}.$$

This proves the theorem. □

4. Initial Fourier coefficients

Proof of Theorem 1.2. By Lemma 2.2, we know that $T_n(x)$ is reducible only if it has a single repeated root, i.e., $a_n(f_1) = \cdots a_n(f_d) = a \in \mathbb{Z}$. Suppose this holds for some $i, 2 \leq i \leq d$. Let h_i be as in Lemma 2.1. Let h_i be written as a linear combination of the eigenforms as

$$h_i = \sum_{i=1}^{d} c_{i,j} f_j\,.$$

Since $a_1(h_i) = 0$ and $a_1(f_j) = 1$ for every f_j, we conclude that $\sum_{i=i}^{d} c_{i,j} = 0$. Thus,

$$1 = a_i(h_i) = \sum_{i=1}^{d} c_{i,j} a_i(f_j) = \sum_{i=1}^{d} c_{i,j} a = 0\,,$$

which shows us that our assumption is false. This proves the theorem. □

5. Comparison Theorems for Fourier coefficients of two eigenforms

Let f and g be two distinct Hecke eigenforms for $\mathrm{SL}_2(\mathbb{Z})$ of weights k_1 and k_2 respectively. If $k_1 = k_2$, then Theorem 1.1 implies the following:

Theorem 5.1. *If $T_q(x)$ is irreducible for some prime q, then*

$$\sharp\{p \leq x; a_p(f) = a_p(g)\} \ll \frac{x}{(\log x)^{1+\delta}}$$

for some $\delta > 0$

In the case $k_1 \neq k_2$, we can prove a similar result unconditionally.

Theorem 5.2. *If $k_1 \neq k_2$, then*

$$\sharp\{p \leq x; a_p(f) = a_p(g)\} \ll \frac{x}{(\log x)^{1+\delta}}$$

for some $\delta > 0$

In [10], section 5, Ribet studied pairs of Galois representations and showed that if l is sufficiently large, the two Galois representations $\rho_{f,\lambda}$ and $\rho_{g,\lambda}$ are "as independent as possible", i.e., the image of the product representation is as large as possible. In the case f and g are as in Theorem 5.2, we state Ribet's theorem as follows:

Lemma 5.3. $\mathrm{Im}(\rho_{f,\lambda}, \rho_{g,\lambda}) =$
$\{(u, u') \in GL_2(\mathcal{O}_\lambda) \times GL_2(\mathcal{O}_\lambda);\ det(u) = v^{k_1-1}; det(u') = v^{k_2-1}, v \in \mathcal{O}_\lambda\}$

Let $\mathbf{F}_\lambda = \mathcal{O}_\lambda/\lambda$. If we let $\bar{\rho}_{f,\lambda} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{F}_\lambda)$ denote the residual representation of $\rho_{f,\lambda}$, we see that

$$\mathrm{Im}\,(\bar{\rho}_{f,\lambda}, \bar{\rho}_{g,\lambda}) =$$
$$\{(u, u') \in \mathrm{GL}_2(\mathbf{F}_\lambda) \times \mathrm{GL}_2(\mathbf{F}_\lambda); \det(u) = v^{k_1-1}; \det(u') = v^{k_2-1}, v \in \mathbf{F}_\lambda\}.$$

Proof of Theorem 5.2. Let $E/\mathbb{Q}$ be an extension containing both E_f and E_g, and λ a degree one prime in E of norm l (by the prime number theorem in number fields, we know that degree 1 primes are of full density, see [6], Theorem 4, Page 350). Let

$$S = \{(u, u') \in \mathrm{GL}_2(\mathbf{F}_\lambda) \times \mathrm{GL}_2(\mathbf{F}_\lambda);\ \det(u) = v^{k_1-1}, \det(u') = v^{k_2-1}, v \in \mathbf{F}_\lambda\},$$
$$S' = \{(u, u') \in S;\ \mathrm{trace}(u) = \mathrm{trace}(u')\},$$
$$|S| \leq l^7 \text{ and } |S'|/|S| \leq 1/l. \tag{1}$$

By the above, we know that the image of the product representation $\bar{\rho}_{f,\lambda} \times \bar{\rho}_{g,\lambda}$ is exactly the group S. Let K be the fixed field of the kernel of the representation, i.e., $\mathrm{Gal}(K/\mathbb{Q}) = S$. Then, by the calculation in (a) above, the proportion of elements of $\mathrm{Gal}(K/\mathbb{Q})$ whose image lies in S' is approximately $1/l$.

Let C denote the set $\{\mathrm{Frob}_\pi\}$ for primes $\pi \in K$ with $\bar{\rho}_{f,\lambda} \times \bar{\rho}_{g,\lambda}(\mathrm{Frob}_\pi) \in S'$. Then C is clearly invariant under conjugation, and thus we can apply the effective version of the Chebotarev density theorem, Proposition 2.3. We see that $|C|/|\mathrm{Gal}(K/\mathbb{Q})| = |S'|/|S|$ and thus,

$$\pi_C(x) \ll \frac{|S'|}{|S|}\pi(x).$$

By property (ii) of the Galois representations $\rho_{f,\lambda}$ and $\rho_{g,\lambda}$, we see that

$$\sharp\{p \leq x; a_p(f) = a_p(g)\} \ll \sharp\{p \leq x; \mathrm{Frob}_\pi \in C\},$$

for some π dividing p. Thus, we see that

$$\sharp\{p \leq x; a_p(f) = a_p(g)\} \ll \frac{|S'|}{|S|}\pi(x)$$

if x is sufficiently large. By property (i) of the representations, we know that K is ramified only at l, and so we can apply Proposition 2.4. Using equation 1, we see that

$$\log d_L \leq 8l^7 \log l.$$

Thus, for large x, if we choose $l \sim (\log x)^{1/8}$, we see that the conditions of Proposition 2.3 are satisfied, and so we have, by all of the above,

$$\sharp\{p \leq x; \mathrm{Frob}_\pi \in C\} \ll \frac{1}{l}\pi(x) \ll x/(\log x)^{9/8}.$$

This proves the theorem. □

6. Conditional estimates

The estimates in Theorem 1.1 and Theorem 5.2 can be improved considerably if we assume the generalised Riemann hypothesis for Dedeking Zeta functions of number fields (GRH) (see [9]). By the methods of [9], it follows that we have the following results.

Theorem 6.1. *Assume GRH for Dedekind zeta functions of number fields. If $T_q(x)$ is irreducible for some prime q, then*

$$\sharp\{p \leq x; T_p(x) \text{ is reducible}\} \ll x^{1-\delta}$$

for some $\delta > 0$.

Theorem 6.2. *Assume GRH for Dedekind Zeta functions of number fields. If $k_1 \neq k_2$, then*

$$\sharp\{p \leq x; a_p(f) = a_p(g)\} \ll x^{1-\delta}$$

for some $\delta > 0$.

References

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

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

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

[4] K. James, K. Ono, *A note on the irreducibility of Hecke polynomials*, J. Number Theory **73** (1998), 527–532.

[5] S. Lang, *Introduction to modular forms*, Grundlehren der mathematischen Wissenschaften, No. **222**. Springer-Verlag, Berlin-New York, 1976.

[6] ———, *Algebraic number theory*, Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

[7] J. C. Lagarias, H. L. Montgomery, A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), 271–296.

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

[9] M. R. Murty, V. K. Murty, N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), 253–281.

[10] K. Ribet, *On l-adic representations attached to modular forms*, Invent. Math. **28** (1975), 245–275.

[11] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, (French) [Some applications of the Chebotarev density theorem] Inst. Hautes Études Sci. Publ. Math. No. **54**, (1981), 323–401.

[12] W. Stein, www.modular.fas.harvard.edu/∼stein

Max Planck Institut für Mathematik, Vivatsgasse 7, D-53111, Bonn, Germany.
E-mail address: `sbaba@mpim-bonn.mpg.de`

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, K7L 3N6, Canada.
E-mail address: `murty@mast.queensu.ca`