# A NOTE ON THE IRREDUCIBILITY OF HECKE POLYNOMIALS 

Kevin James and Ken Ono

To appear in Journal of Number Theory

Let $S_{2 k}$ denote the space of modular cusp forms of weight $2 k$ for $S L_{2}(\mathbb{Z})$. If $f(z):=$ $\sum_{n=1}^{\infty} a_{f}(n) q^{n} \in S_{2 k}$ (here $q:=e^{2 \pi i z}$ throughout), and $p$ is prime, then the Hecke operator $T_{p}^{2 k}$ is the linear transformation on $S_{2 k}$ given by

$$
T_{p}^{2 k} f:=\sum_{n=1}^{\infty}\left(a_{f}(n p)+p^{2 k-1} a_{f}(n / p)\right) q^{n} .
$$

Let $T_{p}^{2 k}(x)$ denote the characteristic polynomial of the action of $T_{p}^{2 k}$ on $S_{2 k}$. It is well known that $T_{p}^{2 k}(x) \in \mathbb{Z}[x]$ and has degree $d_{k}$ where $d_{k}:=\operatorname{dim}\left(S_{2 k}\right)$. However, much more is conjectured to be true. Maeda has conjectured that the Hecke algebra of $S_{2 k}$ over $\mathbb{Q}$ is simple, and that its Galois closure over $\mathbb{Q}$ has Galois group $S_{d_{k}}$. Recently there have been numerous investigations regarding the irreducibility of characteristic polynomials of Hecke operators on $S_{2 k}$. The existence of such polynomials have proven to be useful in proving nonvanishing theorems for central values of level 1 modular $L$-functions, and in constructing base changes to totally real number fields for level 1 eigenforms (see [C-F,H-M,Ko-Z]).

In this note we show that a "positive proportion" of the Hecke polynomials $T_{p}^{2 k}(x)$ are irreducible if there are two distinct primes $\ell$ and $q$ for which $T_{q}^{2 k}(x)$ is irreducible over $\mathbb{F}_{\ell}$, the finite field with $\ell$ elements. Throughout $p$ will denote a prime number.

Theorem 1. If there are distinct primes $\ell$ and $q$ for which the Hecke polynomial $T_{q}^{2 k}(x)$ is irreducible in $\mathbb{F}_{\ell}[x]$, then

$$
\#\left\{p<X \mid T_{p}^{2 k}(x) \text { is irreducible in } \mathbb{Q}[x]\right\}>_{k} \frac{X}{\log X}
$$

This result follows immediately from the following more general result.

[^0]As usual, we will let $S_{k}(N, \chi)$ denote the space of modular cusp forms of weight $k$, level $N$ and character $\chi$. For $f(z)=\sum_{n=1}^{\infty} a_{f}(n) q^{n} \in S_{k}(N, \chi)$ and $p \nmid N$ the Hecke operator $T_{N, p}^{k, \chi}$ is defined by

$$
T_{N, p}^{k, \chi} f=\sum_{n \geq 1}\left(a_{f}(n p)+\chi(p) p^{k-1} a_{f}(n / p)\right) q^{n}
$$

Let $T_{N, p}^{k, \chi}(x)$ denote the characteristic polynomial of $T_{N, p}^{k, \chi}$ on $S_{k}^{\text {new }}(N, \chi)$. Moreover, let $K_{k, \chi, N}$ denote the finite extension of $\mathbb{Q}$ obtained by adjoining the roots of all of the $T_{N, p}^{k, \chi}(x)$ with $p \nmid N$.
Theorem 2. Let $q$ and $\ell$ be distinct primes not dividing $N$, and let $\mathcal{L}$ denote a prime ideal of $\mathbb{K}_{k, \chi, N}$ lying above $\ell$. Then

$$
\#\left\{p<X \quad \mid \quad T_{N, p}^{k, \chi}(x) \equiv T_{N, q}^{k, \chi}(x)(\bmod \mathcal{L})\right\} \ngtr_{N, \chi, k} \frac{X}{\log X}
$$

Proof. Let $\left\{f_{1}, \ldots, f_{d}\right\}$ be a basis of $S_{k}^{\text {new }}(N, \chi)$ such that each $f_{i}$ is an eigenform for all of the $T_{N, p}^{k, \chi}$ where $p \nmid N$. Let $\lambda_{f_{i}}(p)$ be the eigenvalue of $T_{N, p}^{k, \chi}$ corresponding to the eigenform $f_{i}$ (i.e. $T_{N, p}^{k, \chi} f_{i}=\lambda_{f_{i}}(p) f_{i}$ ). By the work of Deligne, Serre and Shimura [D,D-S,Sh], there exist continuous representations

$$
\rho_{f_{i}, \mathcal{L}}: \operatorname{Gal}(\overline{\mathbb{Q}} / \mathbb{Q}) \rightarrow \operatorname{GL}_{2}\left(\mathcal{O}_{\mathcal{L}}\right)
$$

satisfying the following conditions:
(i) $\rho_{f_{i}, \mathcal{L}}$ is unramified for $p \nmid N \ell$,
(ii) $\operatorname{trace}\left(\rho_{f_{i}, \mathcal{L}}\left(\operatorname{Frob}_{p}\right)\right)=\lambda_{f_{i}}(p)$ for $p \nmid N \ell$,
(iii) $\operatorname{det}\left(\rho_{f_{i}, \mathcal{L}}\left(\operatorname{Frob}_{p}\right)\right)=\chi(p) p^{k-1}$ for $p \nmid N \ell$.

Here $\mathcal{O}$ denotes the ring of integers of $K_{k, \chi, N}, \mathcal{O}_{\mathcal{L}}$ denotes its completion at $\mathcal{L}$ and $\operatorname{Frob}_{p}$ denotes any Frobenius element for $p$. Let $\mathfrak{l}$ denote a uniformizer for $\mathcal{O}_{\mathcal{L}}$. By reducing the representations $\rho_{f_{i}, \mathcal{L}}$ modulo $\mathfrak{l}$, we obtain representations from $\operatorname{Gal}(\overline{\mathbb{Q}} / \mathbb{Q})$ to $\mathrm{GL}_{2}\left(\mathcal{O}_{\mathcal{L}} /\langle\mathfrak{l}\rangle\right)$. These representations have finite image and therefore factor to yield representations:

$$
\bar{\rho}_{f_{i}, \mathcal{L}}: \operatorname{Gal}(K / \mathbb{Q}) \rightarrow \operatorname{GL}_{2}\left(\mathcal{O}_{\mathcal{L}} /\langle\mathfrak{l}\rangle\right),
$$

where $K$ is a finite extension of $\mathbb{Q}$.
By the Chebotarev density theorem, there is a set $S$ of rational primes having positive Dirichlet density and having the property that for each $p \in S$, Frob $\mathfrak{P}$ is conjugate to $\mathrm{Frob}_{\mathfrak{Q}}$, where $\mathfrak{P}$ and $\mathfrak{Q}$ are prime ideals of $K$ lying above $p$ and $q$ respectively, and therefore have the property that for each $1 \leq i \leq d$

$$
\operatorname{trace}\left(\bar{\rho}_{f_{i}, \mathcal{L}}\left(\operatorname{Frob}_{\mathfrak{P}}\right)\right) \equiv \lambda_{f_{i}}(p) \quad(\bmod \mathfrak{l}) \quad \text { if } p \nmid N \ell
$$

Since the trace is conjugation invariant, it follows that for $p \in S$,

$$
\lambda_{f_{i}}(p) \equiv \lambda_{f_{i}}(q) \quad(\bmod \mathfrak{l})
$$

Since the $\lambda_{f_{i}}(p)(1 \leq i \leq d)$ are precisely the roots of $T_{N, p}^{k, \chi}(x)$, the theorem follows.
Example. Here we shall give a simple example that illustrates Theorem 2. We consider the Hecke polynomials on the three dimensional space $S_{5}^{\text {new }}\left(11, \chi_{-11}\right)$. For convenience, let $T_{p}(x)$ denote the characteristic polynomial for the Hecke operator $T_{11, p}^{5, \chi-11}$. The first few terms of the Fourier expansions of the three newforms are

$$
\begin{aligned}
& N_{1}(z)=\sum_{n=1}^{\infty} a_{1}(n) q^{n}=q+7 q^{3}+16 q^{4}-49 q^{5}-32 q^{9}+\cdots, \\
& N_{2}(z)=\sum_{n=1}^{\infty} a_{2}(n) q^{n}=q+\sqrt{-30} q^{2}-3 q^{3}-14 q^{4}+31 q^{5}-3 \sqrt{-30} q^{6}-10 \sqrt{-30} q^{7}+\cdots, \\
& N_{3}(z)=\sum_{n=1}^{\infty} a_{3}(n) q^{n}=q-\sqrt{-30} q^{2}-3 q^{3}-14 q^{4}+31 q^{5}+3 \sqrt{-30} q^{6}+10 \sqrt{-30} q^{7}-\cdots .
\end{aligned}
$$

It is easy to verify that if $p \neq 11$ is prime, then

$$
\begin{equation*}
a_{2}(p)=a_{3}(p) \in \mathbb{Z} \quad \text { if }\left(\frac{p}{11}\right)=1 \tag{1}
\end{equation*}
$$

and

$$
\begin{equation*}
a_{2}(p)=-a_{3}(p) \quad \text { if }\left(\frac{p}{11}\right)=-1 \tag{2}
\end{equation*}
$$

Moreover, if $\left(\frac{p}{11}\right)=-1$, then

$$
\begin{equation*}
\frac{a_{2}(p)}{\sqrt{-30}} \in \mathbb{Z} \tag{3}
\end{equation*}
$$

These all follow from standard facts about eigenvalues of Hecke operators (e.g. [Kob]).
The form $N_{1}(z)$ has complex multiplication by $\mathbb{Q}(\sqrt{-11})$ in the sense of Ribet (see $\left.[\mathrm{R}]\right)$. By construction, there is exactly one such form in this space. In particular if $p \neq 11$ is prime, then

$$
a_{1}(p)= \begin{cases}0 & \text { if }\left(\frac{p}{11}\right)=-1 \\ \frac{2 x^{4}-132 x^{2} y^{2}+242 y^{4}}{16} & \text { if }\left(\frac{p}{11}\right)=1 \text { and } 4 p=x^{2}+11 y^{2}\end{cases}
$$

This implies that if $p \neq 11$ is prime, then

$$
a_{1}(p) \equiv\left\{\begin{array}{lc}
0(\bmod 11) & \text { if }\left(\frac{p}{11}\right)=-1  \tag{4}\\
2 p^{2}(\bmod 11) & \text { if }\left(\frac{p}{11}\right)=1
\end{array}\right.
$$

Now if $B(z)=\sum_{n=1}^{\infty} b(n) q^{n}$ is defined by

$$
B(z):=\frac{15+\sqrt{-30}}{30} \cdot N_{2}(z)+\frac{15-\sqrt{-30}}{30} \cdot N_{3}(z)=q-2 q^{2}-3 q^{3}-\cdots,
$$

then the methods of Swinnerton-Dyer [S-D] suggest that $B(z)$ may satisfy a congruence with a linear combination of twisted Eisenstein series. Using a theorem of Sturm [St], we verify indeed that there is such a congruence modulo 11, and it turns out that

$$
\begin{equation*}
b(n) \equiv\left(8 n+4 n\left(\frac{n}{11}\right)\right) \sum_{d \mid n} d^{7} \quad(\bmod 11) \tag{5}
\end{equation*}
$$

By combining (1-5), if $p \neq 11$ is prime, then

$$
T_{p}(x) \equiv \begin{cases}x^{3}+5 x^{2}+x+3(\bmod 11) & \text { if } p \equiv 1(\bmod 11), \\ x^{3}+8 x(\bmod 11) & \text { if } p \equiv 2(\bmod 11) \\ x^{3}+10 x^{2}+3(\bmod 11) & \text { if } p \equiv 3(\bmod 11), \\ x^{3}+8 x^{2}+4(\bmod 11) & \text { if } p \equiv 4(\bmod 11), \\ x^{3}+9 x^{2}+2 x+9(\bmod 11) & \text { if } p \equiv 5(\bmod 11) \\ x^{3}+10 x(\bmod 11) & \text { if } p \equiv 6(\bmod 11) \\ x^{3}+8 x(\bmod 11) & \text { if } p \equiv 7(\bmod 11) \\ x^{3}+7 x(\bmod 11) & \text { if } p \equiv 8(\bmod 11) \\ x^{3}+x^{2}+6 x+3(\bmod 11) & \text { if } p \equiv 9(\bmod 11) \\ x^{3}(\bmod 11) & \text { if } p \equiv 10(\bmod 11)\end{cases}
$$

If $p$ is a prime for which $\left(\frac{p}{11}\right)=1$, then by (1) and (4) we see that $T_{p}(x)$ factors into three linear factors in $\mathbb{Z}[x]$. If $p$ is a prime for which $\left(\frac{p}{11}\right)=-1$ and $a_{2}(p) \neq 0$, then by (2) and (3) it follows that $T_{p}(x)$ factors into irreducibles in $\mathbb{Z}[x]$ as

$$
T_{p}(x)=x\left(x^{2}+a_{2}(p)^{2}\right) .
$$

By (5) one easily finds that $a_{2}(p) \neq 0$ for every such $p \equiv 2,6,7,8(\bmod 11)$.

## References

[B] K. Buzzard, On the eigenvalues of the Hecke operator $T_{2}$, J. Numb. Th. 57 (1996), 130-132.
[C-F] B. Conrey and D. Farmer, Hecke operators and the nonvanishing of L-functions, (preprint).
[D] P. Deligne, Formes modulaires et ré́resentations $\ell$-adiques, Seminaire Bourbaki 355 (1969).
[D-S] P. Deligne and J.-P. Serre, Formes modulaires de poids 1, Ann. Sci. École Normale Sup. $4^{e}$ sér. 7 (1974).
[H-M] H. Hida and Y. Maeda, Non-abelian base change for totally real fields, Pac. J. Math. (to appear).
[Kob] N. Koblitz, Elliptic curves and modular forms, Springer Verlag, Berlin, 1984.
[Ko-Z] W. Kohnen and D. Zagier, Values of L-series of modular forms at the center of the critical strip, Invent. Math. 64 (1981), 175-198.
[R] K. Ribet, Galois representations attached to eigenforms with Nebentypus, Modular functions of one variable, V, Springer Lect. Notes 601 (1977), 17-51.
[Sh] G. Shimura, Introduction to the arithmetic theory of automrphic functions, Iwanami Shoten and Princeton Univ. Press, 1971.
[St] J. Sturm, On the congruence of modular forms, Springer Lect. Notes 1240 (1987), 275-280.
[S-D] H. P. F. Swinnerton Dyer, On $\ell$-adic representations and congruences for coefficients of modular forms, Modular functions of one variable, III, Springer Lect. Notes 350 (1973), 1-55.

Department of Mathematics, Penn State University, University Park, Pa. 16802
E-mail address: klj@math.psu.edu

Department of Mathematics, Penn State University, University Park, Pa. 16802
E-mail address: ono@math.psu.edu


[^0]:    The second author supported by NSF grant DMS-9508976 and NSA grant MSPR-97Y012.

