Generating the Hecke algebra

Amod Agashe, William A. Stein

November 11, 2004

Abstract

Let $\mathbf{T}$ be the Hecke algebra associate to weight k modular forms for $X_0(N)$. We give a bound for the number of Hecke operators T_n needed to generate $\mathbf{T}$ as a $\mathbf{Z}$-module.

Introduction

In this note we apply a theorem of Sturm [S] to prove a bound on the number of Hecke operators needed to generate the Hecke algebra as a $\mathbf{Z}$-module. This bound was observed by to Ken Ribet, but has not been written down. In section 2 we record our notation and some standard theorems. In section 3 we state Sturm's theorem and use it to deduce a bound on the number of generators of the Hecke algebra.

1 Modular forms and Hecke operators

Let N and k be positive integers and let $M_k(N) = M_k(\Gamma_0(N))$ be the $\mathbf{C}$-vector space of weight k modular forms on $X_0(N)$. This space can be viewed as the set of functions $f(z)$, holomorphic on the upper half-plane, such that

$$f(z) = f|[\gamma]_k(z) := (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

for all $\gamma \in \Gamma_0(N)$, and such that f satisfies a certain holomorphic condition at the cusps.

Any $f \in M_k(N)$ has a Fourier expansion

$$f = a_0(f) + a_1(f)q + a_2(f)q^2 + \cdots = \sum a_n q^n \in \mathbf{C}[[q]]$$

where $q = e^{2\pi i z}$. The map sending f to its q-expansion is an injective map $M_k(N) \hookrightarrow \mathbf{C}[[q]]$ called the q-expansion map. Define $M_k(N;\mathbf{Z})$ to be the inverse image of $\mathbf{Z}[[q]]$ under this map. It is known (see §12.3, [DI]) that

$$M_k(N) = M_k(N;\mathbf{Z}) \otimes \mathbf{C}.$$

For any ring R, define $M_k(N;R) := M_k(N;\mathbf{Z}) \otimes_{\mathbf{Z}} R$.

Let p be a prime. Define two operators on $\mathbf{C}[[q]]$:

$$V_p(\sum a_n q^n) = \sum a_n q^{np}$$

and

$$U_p(\sum a_n q^n) = \sum a_{np} q^n.$$

The Hecke operator T_p acts on q-expansions by

$$T_p = U_p + \varepsilon(p) p^{k-1} V_p$$

where $\varepsilon(p) = 1$, unless $p|N$ in which case $\varepsilon(p) = 0$. If m and n are coprime, the Hecke operators satisfy $T_{nm} = T_n T_m = T_m T_n$. If p is a prime and $r \geq 2$,

$$T_{p^r} = T_{p^{r-1}} T_p - \varepsilon(p) p^{k-1} T_{p^{r-2}}.$$

The T_n are linear maps which preserves $M_k(N;\mathbf{Z})$. The Hecke algebra $\mathbf{T} = \mathbf{T}(N) = \mathbf{Z}[T_1, T_2, T_3, \ldots]$, which is viewed as a subring of the ring of linear endomorphisms of $M_k(N)$, is a finite commutative $\mathbf{Z}$-algebra.

Proposition 1.1. *Let $\sum a_n q^n$ be the q-expansion of $f \in M_k(N)$ and let $\sum b_n q^n$ be the q-expansion of $T_m f$. Then the coefficients b_n are given by*

$$b_n = \sum_{d|(m,n)} \varepsilon(d) d^{k-1} a_{mn/d^2}.$$

Note in particular that $a_1(T_m f) = a_m(f)$.

Proof. Proposition 3.4.3, [DI]. ☐

Proposition 1.2. *For any ring R, there is a perfect pairing*

$$\mathbf{T}_R \otimes_R M_k(N;R) \to R, \qquad (T, f) \mapsto a_1(Tf),$$

where $\mathbf{T}_R = \mathbf{T} \otimes_{\mathbf{Z}} R$.

Proof. Proposition 12.4.13, [DI]. ☐

2 Bounding the number of generators

Let $\mu(N) = N \prod_{p|N}(1 + \frac{1}{p})$ be the index of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbf{Z})$.

Theorem 2.1. *Let λ be a prime ideal in the ring of integers $\mathcal{O}$ of some number field. Suppose $f \in M_k(N;\mathcal{O})$ is such that $a_n(f) \equiv 0 \pmod{\lambda}$ for $n \leq \frac{k}{12}\mu(N)$. Then $f \equiv 0 \pmod{\lambda}$.*

Proof. Theorem 1, [S]. ☐

Denote by $\lceil x \rceil$ the smallest integer $\geq x$.

Proposition 2.2. *Suppose* $f \in M_k(N)$ *and*

$$a_n(f) = 0 \quad \textit{for} \quad n \le r = \left\lceil \frac{k}{12}\mu(N) \right\rceil .$$

Then $f = 0$.

Proof. We must show that the composite map

$$M_k(N) \hookrightarrow \mathbf{C}[[q]] \to \mathbf{C}[[q]]/(q^{r+1})$$

is injective. Because $\mathbf{C}$ is a flat $\mathbf{Z}$-module, it suffices to show that the map $\Phi : M_k(N;\mathbf{Z}) \to \mathbf{Z}[[q]]/(q^{r+1})$ is injective. Suppose $\Phi(f) = 0$, and let p be a prime number. Then $a_n(f) = 0$ for $n \le r$, hence plainly $a_n(f) \equiv 0 \pmod p$ for any such n. By Theorem 2.1, it follows that $f \equiv 0 \pmod p$. Repeating this argument shows that the coefficients of f are divisible by all primes p, i.e., they are 0. □

Theorem 2.3. *The Hecke algebra is generated as a* $\mathbf{Z}$*-module by* $T_1, \ldots, T_r$ *where* $r = \lceil \frac{k}{12}\mu(N) \rceil$.

Proof. Let A be the submodule of $\mathbf{T}$ generated by $T_1, T_2, \ldots, T_r$. Consider the exact sequence of additive abelian groups

$$0 \to A \xrightarrow{i} \mathbf{T} \to \mathbf{T}/A \to 0.$$

Let p be a prime and tensor with $\mathbf{F}_p$ to obtain

$$A \otimes \mathbf{F}_p \xrightarrow{\bar{i}} \mathbf{T} \otimes \mathbf{F}_p \to (\mathbf{T}/A) \otimes \mathbf{F}_p \to 0$$

(tensor product is right exact). Put $R = \mathbf{F}_p$ in Proposition 1.2, and suppose $f \in M_k(N, \mathbf{F}_p)$ pairs to 0 with each of $T_1, \ldots, T_r$. Then by Proposition 1.1, $a_m(f) = a_1(T_m f) = 0$ in $\mathbf{F}_p$ for each m, $1 \le m \le r$. By Theorem 2.1 it follows that $f = 0$. Thus the pairing, when restricted to the image of $A \otimes \mathbf{F}_p$ in $\mathbf{T} \otimes \mathbf{F}_p$, is also perfect and so

$$\dim_{\mathbf{F}_p} \bar{i}(A \otimes \mathbf{F}_p) = \dim_{\mathbf{F}_p} M_k(N, \mathbf{F}_p) = \dim_{\mathbf{F}_p} \mathbf{T} \otimes \mathbf{F}_p.$$

We see that $(\mathbf{T}/A) \otimes \mathbf{F}_p = 0$; repeating the argument for all p shows that the finitely generated abelian group $\mathbf{T}/A$ must be trivial. □

References

[DI] F. Diamond, J. Im, *Modular forms and modular curves.* Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), 39–133, CMS Conf. Proc., 17, Amer. Math. Soc., Providence, RI, 1995.

[L] S. Lang, *Introduction to modular forms.* Grundlehren der Mathematischen Wissenschaften, 222. Springer-Verlag, Berlin, 1995.

[S] J. Sturm, *On the Congruence of Modular Forms*. Number theory (New York, 1984–1985), 275–280, Lecture Notes in Math., 1240, Springer, Berlin-New York, 1987.