ON MOD p MODULAR REPRESENTATIONS WHICH ARE DEFINED OVER $\mathbf{F}_p$

L. J. P. Kilford

University of Bristol, United Kingdom

ABSTRACT. In this paper, we will use techniques of Conrey, Farmer and Wallace to find spaces of modular forms $S_k(\Gamma_0(N))$ where all of the eigenspaces have Hecke eigenvalues defined over $\mathbf{F}_p$, and give a heuristic that these are all such spaces.

1. INTRODUCTION

Let N and k be positive integers and let l and p be primes. We will let $S_k(\Gamma_0(N), \chi)$ be the space of holomorphic cusp forms of integer weight k for the congruence subgroup $\Gamma_0(N)$, and we will define $T_{l,k}^{N,\chi}$ to be the characteristic polynomial of the Hecke operator T_l acting on $S_k(\Gamma_0(N), \chi)$. We will call this polynomial the *Hecke polynomial*.

For modular forms in characteristic 0, there is a well-known conjecture (Maeda's conjecture) that says that the characteristic polynomials of the Hecke operators acting on modular forms for $SL_2(\mathbf{Z})$ are irreducible:

CONJECTURE 1.1 (Maeda's Conjecture). *Let k be a positive integer, and let l be a prime number. The Hecke polynomial of $T_{l,k}^{1,1}$ is irreducible, with Galois group S_n, where n is the dimension of $S_k(SL_2(\mathbf{Z}))$ as a complex vector space.*

Some progress has been made towards this conjecture; methods introduced in [4] prove that certain Hecke polynomials are irreducible and have full Galois group, and results such as those in [6], [2] and [1] show that if a certain T_l is irreducible then other T_r must be irreducible also.

In the paper [6], a method for showing that certain of the $T_{l,k}^{1,1}$ are irreducible over $\mathbf{Q}$ is given; this involves a careful study of how level 1 Hecke polynomials factor modulo certain primes which uses the fact that the factorizations of the Hecke polynomials are periodic. In [7] and [2], the authors first show that certain of the $T_{2,k}^{1,1}$ are irreducible and then using effective versions of the Chebotarev density theorem to show that a positive proportion of the $T_{l,k}^{1,1}$ are irreducible, and in [1], plausible hypotheses on the non-vanishing of certain coefficients of modular forms are used to prove irreducibility of the Hecke polynomials (when the weight is 12, for instance, these hypotheses are exactly Lehmer's conjecture on the Ramanujan τ-function).

The situation in characteristic p is rather different. We see from Table 1 that the Hecke polynomials $T_{l,k}^{1,1}$ factor into linear factors for all the primes less than 19. In this paper we will investigate such examples where a "mod p version of Maeda's conjecture" fail so completely.

We quote some results from [6], which will show that the factorization of the Hecke polynomials $T_{l,k}^{N,\chi}$ modulo p is periodic. Firstly, we will show that certain mod p reductions of Hecke polynomials divide one another. Let $B_k(N, \chi)$ be a basis of $S_k(\Gamma_0(N), \chi)$.

LEMMA 1.2 ([6, Lemma 1]). *Let $[T_n]_{k,N,\chi}$ be the matrix of the Hecke operator T_n with respect to the basis $B_k(N, \chi)$, and let $q = p - 1$ if $p \neq 2$ and 2 if $p = 2$. Then $[T_n]_{k,N,\chi}$ is block upper-triangular and*

$$[T_n]_{k,N,\chi} \subset [T_n]_{k+q,N,\chi},$$

where the smaller matrix appears as a block in the upper left corner of the larger matrix. In particular, we have

$$T_{n+q}^{N,\chi} \equiv g(x) \cdot T_{n,k}^{N,\chi} \mod p$$

for some polynomial $g(x)$.

PROOF. If $p \geq 5$, we can follow the argument of [6]; recall that the classical Eisenstein series E_{p-1} has Fourier expansion at ∞ which is congruent to 1 modulo p, so there is a an inclusion

$$S_k(\Gamma_0(N), \chi) \subset S_{k+p-1}(\Gamma_0(N), \chi)$$

given by multiplication by E_{p-1}. We can choose $B_k(N, \chi)$ to respect this inclusion, and we also note that the Hecke operator T_n mod p respects this inclusion map because using the definition of the Hecke operators we have

$$(T_n f)(z) = \frac{1}{n} \sum_{ad=n} \chi(a) a^k \sum_{0 \leq b < d} f\left(\frac{az+b}{d}\right)$$

and $a^k \equiv a^{k+p-1} \mod p$.

We note that if $p = 2$ or $p = 3$, then the argument involving E_{p-1}, which is the argument at the bottom of page 124 of [6] is not applicable, as there

is no level 1 modular form of weight 1 or 2. The solution here is to consider the spaces of modular forms as being mod p modular forms in the sense of Katz [8]; this then means that the Hasse invariant A is a nonzero weight $p-1$ mod p modular form, and then there is a map from weight k to weight $k+q$ given by multiplication by A (if $p=3$) or A^2 (if $p=2$). The rest of the proof does not depend on $p \geq 5$.   □

Using Lemma 1.2, we see that there is a sequence of polynomials $f_j \in (\mathbf{Z}/p\mathbf{Z})[x]$ depending only on N, χ, p, l and $(k \mod p-1)$ such that

$$(1.1) \qquad T_{l,k}^{N,\chi}(x) \equiv \prod_{j=1}^{J} f_j(x) \mod p.$$

It is in fact the case that a finite amount of computation suffices to compute any of the $T_{l,k}^{N,\chi}(x)$, by the following proposition:

PROPOSITION 1.3 ([6, Proposition 1]). *The sequence of polynomials f_i in (1.1) is periodic.*

PROOF. See [6].   □

One elementary observation which follows from (1.1) is that the degrees of the f_j are bounded above by

$$(1.2) \qquad M := \max_k \left(\dim S_{k+p-1}(\Gamma_0(N), \chi) - \dim S_k(\Gamma_0(N), \chi) \right);$$

if we have that $p=2$, then this formula is still true, but we see that this formula is not optimal, because one of these two spaces is zero. We can obtain a better bound by considering

$$(1.3) \qquad M := \max_k \left(\dim S_{k+2}(\Gamma_0(N), \chi) - \dim S_k(\Gamma_0(N), \chi) \right)$$

or (if one is willing to consider mod 2 modular forms)

$$(1.4) \qquad M := \max_k \left(\dim S_{k+1}(\Gamma_0(N), \chi; \mathbf{F}_2) - \dim S_k(\Gamma_0(N), \chi; \mathbf{F}_2) \right)$$

instead.

In Section 3 of [6], it is shown that the $T_{l,k}^{1,1}$ factor completely for $l \leq 7$ and $l = 13$; this follows from (1.2), because $M = 1$ in these particular cases. In Section 2, we will extend their results to higher levels.

A natural question that arises is:

QUESTION 1.1. Are there finitely many prime levels N and primes p such that the polynomials $T_{l,k}^{N,1} \mod p$ split completely? If there are only finitely many, is the table in Section 2 complete?

In Section 3, we will give a heuristic argument suggesting that there should indeed be only finitely many levels N and primes p such that $T_{l,k}^{N,1} \mod p$ splits completely.

A natural extension to this question is to consider the situation for other finite fields $\mathbf{F}_{p^r}$; it is clear that if we enlarge the field of definition, then we will find more Hecke polynomials which split completely, so we have to specify a fixed $\mathbf{F}_q$ for the question to be meaningful.

2. TABLES OF RESULTS

In Table 1, we see a list of all prime levels N (with $p \nmid N$), together with $N = 1$, less than 1000 where all of the $T_{l,k}^{N,1}$ factor completely modulo p, for p less than 41.

N	primes p where the $T_{l,k}^{N,1}$ factor completely
1	2, 3, 5, 7, 11, 13, 17, 19
2	2, 3, 5, 7
3	2, 5, 7, 11
5	2, 3
7	2, 3
11	2, 3
13	2
17	2
19	2, 3
29	2
41	2
53	2
89	2

TABLE 1. Levels N where all of the $T_{l,k}^{N,1}$ factor completely

This table was computed using MAGMA [3].

In [6], it is shown that if the level is 1 and $p \in \{2, 3, 5, 7, 11\}$ then the $T_{l,k}^{1,1}$ will factor completely modulo p, because each of the f_i will have degree 1. We notice that for our largest example, level 89 and $p = 2$, the dimension of $S_2(\Gamma_0(89))$ is 7, so therefore it is possible that quite large degree Hecke polynomials can still split modulo p; this, again, differs sharply from the characteristic 0 case, where it is believed that the only eigenforms for $SL_2(\mathbf{Z})$ which have coefficients in $\mathbf{Q}$ are those which are forced to be defined over $\mathbf{Q}$ by dimension considerations, such as the Δ-function.

Table 2 is the corresponding table showing those prime levels N less than 1000, together with $N = 4$, where all of the $T_{l,k}^{N,\chi}$ split completely modulo p for $\chi = \left(\frac{\cdot}{N}\right)$. We note that for the largest of these levels, the dimension

N	primes p where all the $T_{l,k}^{N,\chi}$ factor completely
3	2,5,7
4	3,5
5	2,3
7	2,3,5
11	2,3,5
13	2,3
17	2
19	2
23	3
29	2
31	3
41	2
53	2

TABLE 2. Levels N where all of the $T_{l,k}^{N,\chi}$ factor completely

of the space of modular forms $S_2(\Gamma_0(53), \left(\frac{\cdot}{N}\right))$ is 8, which is very close to the largest dimension, 7, that we found above. We also note that there are two levels, 23 and 31, where the Hecke polynomials factor completely modulo 3 but not modulo 2.

3. Heuristics

We will briefly outline elementary arguments for why there should be only finitely many spaces of modular forms $S_k(\Gamma_0(N))$ where all the Hecke polynomials factor completely over $\mathbf{F}_p$, for N prime. Let us choose such an N.

It is well-known (see [5], for instance) that the dimension of these spaces of modular forms tends to ∞ as N tends to ∞ (in a rather irregular way; see [9, Remark 6.3]), and that all but finitely many spaces $S_k(\Gamma_0(N))$ are greater than any given integer. This means that the quantity M in (1.2) is increasing, so the spaces which have Hecke polynomials which factor automatically by dimension considerations are finite in number.

However, we noted in the previous section that there are examples where the Hecke polynomials factor completely when $M \neq 1$; we note that in our tables these become rarer and rarer as the dimension becomes higher.

Let us assume that the Hecke polynomials $T_{2,k}^{N,1}$ mod p are randomly distributed amongst polynomials of their degree d. There are p^d monic polynomials of degree d, and the number of polynomials of degree d which split completely is polynomial in d; for instance, if $p = 2$, it is $d + 1$, and if $p = 3$,

it is $(d+1)(d+2)/2$. Therefore, as N increases, the degree of the first polynomial f_1 in the expansion (1.1) increases, and this makes it more likely that the polynomial f_1 does not factor completely.

REFERENCES

[1] S. Ahlgren, *On the irreducibility of Hecke polynomials*, Mathematics of Computation, 2008, to appear.

[2] Srinath Baba and M. Ram Murty, *Irreducibility of Hecke polynomials*, Math. Res. Lett. **10** (2003), 709-715.

[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), 235-265. See `http://magma.maths.usyd.edu.au`.

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

[5] H. Cohen and J. Oesterlé, *Dimensions des espaces de formes modulaires*, Lecture Notes in Mathematics **627** (1977), 69-78.

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

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

[8] N. M. Katz, *p-adic properties of modular schemes and modular forms*, in Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pages 69-190. Lecture Notes in Mathematics **350**, Springer, Berlin, 1973.

[9] W. A. Stein, Modular forms, a computational approach. With an appendix by Paul E. Gunnells., Graduate Studies in Mathematics, American Mathematical Society, Providence, 2007.

L. J. P. Kilford
Department of Mathematics
University of Bristol
University Walk
Bristol, BS8 1TW
United Kingdom