# CONGRUENCES FOR NEWFORMS AND THE INDEX OF THE HECKE ALGEBRA

SCOTT AHLGREN AND JEREMY ROUSE

ABSTRACT. We study congruences between newforms in the spaces $S_4(\Gamma_0(p), \overline{\mathbb{Z}}_p)$ for primes $p$. Under a suitable hypothesis (which is true for all $p < 5000$ with the exception of 139 and 389) we provide a complete description of the congruences between these forms, which leads to a formula (conjectured by Calegari and Stein [6]) for the index of the Hecke algebra $\mathbb{T}_{\mathbb{Z}_p}$ in its normalization. Since the hypothesis is amenable to computation we are able to verify the conjectured formula for $p < 5000$. In [6] Calegari and Stein gave a number of conjectures which provide an outline for the proof of this formula, and the results here clarify the dependencies between the various conjectures. Finally, we discuss similar results for the spaces $S_6(\Gamma_0(p), \overline{\mathbb{Z}}_p)$.

## 1. INTRODUCTION

Suppose that $k$ is an even positive integer. If $N$ is a positive integer, denote by $S_k(N, \mathbb{Z})$ the free $\mathbb{Z}$-module of cusp forms of weight $k$ on $\Gamma_0(N)$ whose Fourier expansions at infinity have integer coefficients. For any ring $A$ we may define

$$S_k(N, A) := S_k(N, \mathbb{Z}) \otimes A.$$

Let $p \geq 5$ be prime. Fixing once and for all an algebraic closure $\overline{\mathbb{Q}}_p$ of the field $\mathbb{Q}_p$ of $p$-adic numbers, we define

$$S_k(p) := S_k(p, \overline{\mathbb{Q}}_p), \quad S_k = S_k(1, \overline{\mathbb{Q}}_p).$$

For a form $f = \sum a(n)q^n$, let

$$f|U_p := \sum a(pn)q^n.$$

The Fricke involution on $S_k(p)$ is then given by

$$f|w_p := -p^{1-\frac{k}{2}} f|U_p.$$

For each such space we have the canonical decomposition

$$S_k(p) = S_k^+(p) \oplus S_k^-(p) \tag{1.1}$$

into the plus and minus eigenspaces for the Fricke involution $w_p$.

Let $\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[\dots, T_n, \dots]$ (where $T_n$ is the usual Hecke operator) be the full Hecke algebra associated to $S_k(p, \mathbb{Z})$. For any ring $A$ we may define $\mathbb{T}_A := \mathbb{T} \otimes A$. Here we will be primarily concerned with

$$\mathbb{T} := \mathbb{T}_{\mathbb{Z}_p} = \mathbb{T} \otimes \mathbb{Z}_p = \mathbb{Z}_p[\dots, T_n, \dots].$$

*Date*: July 15, 2010.

2000 *Mathematics Subject Classification.* Primary 11F33; Secondary 11F30.

The second author was supported by NSF grant DMS-0901090.

We restrict our attention to those values of $k$ for which there are no oldforms. In this case we have

$$T_p = U_p = -p^{\frac{k}{2}-1} w_p,$$

from which we see that $\mathbb{T}$ acts both on the plus and minus spaces. We define the two quotients

$$\mathbb{T}^+ = \mathbb{T}/(T_p + p^{\frac{k}{2}-1}), \quad \mathbb{T}^- = \mathbb{T}/(T_p - p^{\frac{k}{2}-1}).$$

A newform in $S_k(p)$ is a normalized eigenform of all of the Hecke operators. Its coefficients lie in $\overline{\mathbb{Z}}_p$, and generate an extension of finite degree over $\mathbb{Q}_p$. Therefore it makes sense to speak of a congruence between newforms.

Roughly speaking, congruences between newforms arise in two ways: from the failure of the Hecke ring $\mathbb{T}$ to be integrally closed, or from ramification in the coefficient fields of the newforms. In [6], Calegari and Stein conjecture that for any prime $p$, the Hecke algebra $\mathbb{T}$ of $S_2(p)$ is integrally closed. They also show that the only prime $p < 50923$ for which there is a congruence between two weight two newforms is $p = 389$.

Questions about congruences between newforms have a surprising number of applications to the arithmetic of elliptic curves. If Calegari and Stein's conjecture is true for the prime $p$, then it follows (see [17, 1, 7]) that if $E/\mathbb{Q}$ is an elliptic curve of conductor $p$, then $p$ does not divide the degree of the modular parametrization $\Phi : X_0(p) \to E$. A result of Shimura relates the modular degree to the special value of $L(\mathrm{Sym}^2 E, s)$ at $s = 2$ (the edge of the critical strip). Hence the statement that $p$ does not divide the modular degree of $E$ can be thought of as an elliptic curve analogue of the classical conjecture of Vandiver that $p$ does not divide the class number of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Watkins [16] has verified this conjecture for about 54000 elliptic curves of prime conductor.

The conjecture of Calegari and Stein is also related to the following question. If $p$ is a fixed prime, is there an elliptic curve $E/\mathbb{Q}(\zeta_p)$ for which all of the $p$-torsion points are defined over $\mathbb{Q}(\zeta_p)$? There are infinitely many such curves $E/\mathbb{Q}$ with this property when $p = 2, 3$ and 5. In [12], Merel and Stein prove that there are no such curves if $7 \leq p \leq 1000$ and $p \neq 13$. They show, under suitable technical hypotheses, that each order $p$ subgroup $C$ of $E[p]$ gives rise to a point on $X_0(p)$ defined over $\mathbb{Q}(\sqrt{p})$. This is shown to be impossible, and so it suffices to verify the technical hypotheses. One of these hypotheses is verified by checking that there are no congruences between newforms in $S_2(p)$ (a little more care is needed in the case $p = 389$). Subsequently, Rebolledo [13] proved there are no such curves for $p = 13$ using a different method.

In this paper, we are concerned with weights $k \geq 4$, in which case there are congruences between newforms. In [6], Calegari and Stein provide a conjectural picture of the situation. Their main conjecture (Conjecture 1) is a formula for the index of the Hecke algebra in its normalization. In addition, an outline for the proof of this conjecture is given. Calegari and Stein conjecture that $\mathbb{T}^+$ and $\mathbb{T}^-$ are integrally closed (Conjecture 3), and in the case that $k = 4$, they predict (Conjecture 5) that the existence of a congruence for a particular newform is determined by whether or not the newform lies in the image of the $\Theta$ operator.

The goal in this paper is to clarify the dependencies among these conjectures, and to prove the main conjecture in the case $k = 4$ subject to the hypothesis which we introduce next.

**Hypothesis 1.** *There is no congruence between two newforms which lie in $S_k^+(p)$, nor any congruence between two newforms which lie in $S_k^-(p)$.*

Hypothesis 1 is slightly stronger than Conjecture 3 of [6]. Namely, if $K$ is the finite extension of $\mathbb{Q}_p$ generated by the coefficients of all of the newforms in $S_k(p)$, then Hypothesis 1 is equivalent to this conjecture with the extra assumption that the extension $K/\mathbb{Q}_p$ is unramified. (These connections may not be immediately obvious to the non-expert–see the next section for a discussion.)

Hypothesis 1 is amenable to computation, and we have verified its truth for $S_4(p)$ for all $p < 5000$ with the exception of 139 and 389. (In these cases the fields in question are ramified, so that Conjecture 3 of [6] is indeed true for all primes in this range.) These computations extend those of Calegari and Stein, who computed the discriminant of the Hecke algebra of each $S_4(p)$ for $p < 500$. See Section 5 for a description of the algorithm.

Here we will prove the following result, the conclusion of which is the $k = 4$ case of Conjecture 1 of [6].

**Theorem 1.** *Suppose that $p \geq 5$ is prime and that Hypothesis 1 is true for $S_4(p)$. Then the index of $\mathbb{T}$ in its normalization is $p^{\lfloor \frac{p}{12} \rfloor}$.*

**Corollary 2.** *The conclusion of Theorem 1 is true for all $p < 5000$.*

This theorem will follow from the next result, which gives a precise description of the congruences between cusp forms of weight four. Before we state the result, we require some definitions. If $N \geq 1$ is an integer, let $M_k(N, \mathbb{Z})$ denote the free $\mathbb{Z}$-module of holomorphic modular forms of weight $k$ on $\Gamma_0(N)$ whose Fourier expansions at infinity have integer coefficients. For any ring $A$, let $M_k(N, A) := M_k(N, \mathbb{Z}) \otimes A$ (we will only be concerned with the cases $N = 1$ and $N = p$). Next, if $f \in M_k(N, \overline{\mathbb{Z}}_p)$, we let $\overline{f} \in M_k(N, \overline{\mathbb{F}}_p)$ be the form obtained by reducing the coefficients of $f$ mod $p$. We say that two forms $f$ and $g$ are congruent if $\overline{f} = \overline{g}$. Now, we define the Ramanujan $\Theta$ operator: If

$$f = \sum_{n=0}^{\infty} a(n) q^n,$$

then

$$\Theta f := \sum_{n=1}^{\infty} n a(n) q^n.$$

If $f \in M_k(p, \overline{\mathbb{Z}}_p)$, then $\Theta f$ is congruent modulo $p$ to a modular form in $S_{k+2}(p, \overline{\mathbb{Z}}_p)$.

We recall (see for example Theorem 4.1 of [3]) that if $f \in S_4(p)$ is a newform, then $f$ is congruent modulo $p$ to a form of level 1 and weight $2p + 2$; therefore the filtration of $f$ (see the next section for the definition) is either $2p + 2$ or $p + 3$.

**Theorem 3.** *Suppose that $p \geq 5$ is prime and that Hypothesis 1 is true for $S_4(p)$. Suppose that $h \in S_4(p)$ is a newform. Then the following conditions are equivalent.*

1. *$h$ is congruent to another newform in $S_4(p)$.*
2. *$\overline{h}$ is the simultaneous reduction of a newform in $S_4^+(p, \overline{\mathbb{Z}}_p)$ and a newform in $S_4^-(p, \overline{\mathbb{Z}}_p)$.*
3. *$h$ is congruent to a modular form of level 1 and weight $p + 3$.*
4. *$\overline{h}$ is not in the image of the theta-operator from $M_2(p, \overline{\mathbb{Z}}_p)$.*

*Under these assumptions, the number of pairs of eigenforms which satisfy a congruence is exactly $\lfloor \frac{p}{12} \rfloor$. Moreover, $2 \implies 1$ trivially, and the implications $2 \implies 4 \iff 3$ hold without the assumption of Hypothesis 1.*

*Remark.* Many of these results and methods can be extended to more general spaces of modular forms, and in particular to spaces $S_k^{\text{new},p}(Np)$, where $p \nmid N$ is prime. (A recent paper of Barcau and Paşol [4] contains results in this direction.) We restrict our attention to the simpler case here to reduce the number of hypotheses, and to produce hypotheses which can be tested computationally.

*Remark.* Frank Calegari has described to us a deep framework based on recent advances in modularity in which to consider these conjectures. Calegari's outline (which involves, among many other elements, recent work of Kisin on local deformation rings) provides a conceptual reason to believe in their truth.

In Section 2, we review basic facts about modular forms mod $p$, and provide background about Hecke algebras over $\mathbb{Z}_p$. In Section 3, we prove Theorem 3, and in Section 4, we deduce Theorem 1 from Theorem 3. In Section 5, we discuss computations in the weight 4 case. Sections 6 and 7 contain the results about forms of weight 6.

**Acknowledgments.** The authors thank Frank Calegari for his helpful comments, and they thank the referee for a number of suggestions which improved the exposition.

## 2. Preliminaries on modular forms and Hecke algebras

We will use the notation for spaces of modular forms given in the introduction. If $f \in M_k(1, \overline{\mathbb{F}}_p)$ then we define the *filtration* of $f$ by

$$w(f) := \inf\{k' \ : \ f(z) \pmod p \in M_{k'}(1, \overline{\mathbb{F}}_p)\}.$$

We require some basic facts about filtrations.

**Proposition 4** (Swinnerton-Dyer [15])**.** *If $f \in M_k(1, \overline{\mathbb{F}}_p)$ then the following are true.*

(1) $w(f) \equiv k \pmod{p-1}$.
(2) $w(\Theta f) \equiv w(f) + 2 \pmod{p-1}$.
(3) $w(\Theta f) \leq w(f) + p + 1$, *with equality if and only if* $w(f) \not\equiv 0 \pmod p$.

Although the discussion of Hecke algebras below may be well-known to experts, we have chosen to give a fairly complete exposition for the benefit of the readers. *For simplicity we restrict the discussion to those values of $k$ for which $S_k(p)$ contains no oldforms.* For some of this material one may consult the survey articles of Darmon, Diamond, and Taylor [8] or of Diamond and Im [9].

The ring $\mathbb{T}$ is finitely generated and free as a $\mathbb{Z}_p$-module. The minimal primes $\mathfrak{p}$ of $\mathbb{T}$ are those with $\mathfrak{p} \cap \mathbb{Z}_p = (0)$, and the maximal primes are those with $\mathfrak{p} \cap \mathbb{Z}_p = (p)$. Each normalized eigenform $f = \sum a(n) q^n \in S_k(p, \overline{\mathbb{Z}}_p)$ gives rise to a map $\mathbb{T} \to \overline{\mathbb{Z}}_p$ defined via $T_n \mapsto a(n)$. The image of this map is an order in the ring of integers of a finite extension of $\overline{\mathbb{Q}}_p$, and the kernel is a minimal prime ideal which depends only on the $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ conjugacy class of the eigenform $f$. This gives a correspondence between such conjugacy classes and minimal primes of $\mathbb{T}$. Similarly, there is a correspondence between $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ conjugacy classes of eigenforms in $S_k(p, \overline{\mathbb{F}}_p)$ and maximal primes of $\mathbb{T}$.

Each minimal prime of $\mathbb{T}$ is contained in a unique maximal ideal. If $\mathfrak{m}$ is a maximal ideal, then the minimal primes contained in $\mathfrak{m}$ correspond to distinct Galois conjugacy classes of characteristic zero eigenforms with the same characteristic $p$ reductions. Assuming Hypothesis 1, the number of such minimal primes is either one or two (if there were three or more

characteristic zero eigenforms with the same reduction then two would have the same Fricke eigenvalue).

Theorems 8.7 and 8.15 of Matsumura [11] show that

$$\mathbb{T} \cong \prod_{\mathfrak{m}} \mathbb{T}_{\mathfrak{m}}, \tag{2.1}$$

where the product runs over maximal ideals $\mathfrak{m}$ of $\mathbb{T}$. Each $\mathbb{T}_{\mathfrak{m}}$ is a finitely generated, free $\mathbb{Z}_p$-module (see, for example, §12 of [9]).

If $R$ is a commutative ring with unity, and $S$ is the multiplicative system of all non-zero-divisors, then the total ring of fractions of $R$ is the ring $S^{-1}R$. The normalization of $R$, which we denote by $\widetilde{R}$, is the integral closure of $R$ in its total ring of fractions. In order to address Theorem 1, we would like to determine as explicitly as possible the rings $\mathbb{T}$ and $\widetilde{\mathbb{T}}$. Using (2.1), a moment's thought (or Exercise 2.5.1 of [10]) shows that

$$\widetilde{\mathbb{T}} \cong \prod_{\mathfrak{m}} \widetilde{\mathbb{T}}_{\mathfrak{m}}.$$

Corollary 2.1.13 of [10] states that if $R$ is a reduced ring, and $P_1, \dots, P_s$ are the minimal prime ideals of $R$, then

$$\widetilde{R} \cong \widetilde{R/P_1} \times \widetilde{R/P_2} \times \cdots \times \widetilde{R/P_s}.$$

Recalling our assumption that $S_k(p)$ contains no oldforms, we see that the operators $\{T_n\}$ are simultaneously diagonalizable, and therefore that $\mathbb{T}$ is reduced (i.e. contains no non-zero nilpotents). Thus, for each $\mathfrak{m}$, we either have

$$\widetilde{\mathbb{T}}_{\mathfrak{m}} \cong \widetilde{\mathbb{T}_{\mathfrak{m}}/\mathfrak{p}_1\mathbb{T}_{\mathfrak{m}}} \tag{2.2}$$

or

$$\widetilde{\mathbb{T}}_{\mathfrak{m}} \cong \widetilde{\mathbb{T}_{\mathfrak{m}}/\mathfrak{p}_1\mathbb{T}_{\mathfrak{m}}} \times \widetilde{\mathbb{T}_{\mathfrak{m}}/\mathfrak{p}_2\mathbb{T}_{\mathfrak{m}}}, \tag{2.3}$$

according to the number of minimal primes which $\mathfrak{m}$ contains (i.e. the number of characteristic zero eigenforms which reduce to the characteristic $p$ eigenform corresponding to $\mathfrak{m}$).

Assume Hypothesis 1, and let $\mathfrak{p}$ be a minimal prime ideal; then $\mathfrak{p}$ corresponds to a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ class of eigenforms, say $f_1, f_2, \dots, f_r$. Let $K$ be the field generated by the coefficients of one of these eigenforms, and let $\mathcal{O}_K$ be its ring of integers. We have the following important fact.

**Lemma 5.** *Assume Hypothesis 1. Then, $K/\mathbb{Q}_p$ is unramified.*

*Proof.* Suppose to the contrary that Hypothesis 1 holds and that $K/\mathbb{Q}_p$ is ramified. Then there is a non-trivial element $\sigma$ in the inertia subgroup of $\mathrm{Gal}(K/\mathbb{Q}_p)$. Let $f_i$ be an eigenform with the property that the field obtained by adjoining the coefficients of $f_i$ to $\mathbb{Q}_p$ is ramified. Let $\sigma(f_i)$ denote the form obtained by applying $\sigma$ to each coefficient of $f_i$. Then $\sigma(f_i)$ is a newform with the property that $\sigma(f_i) \equiv f_i \pmod{p}$. Moreover, since the $p$th coefficient of $f_i$ is $-p^{k-1}$ times the Fricke eigenvalue of $f_i$, it follows that the Fricke eigenvalue of $\sigma(f_i)$ is the same as that of $f_i$. This contradicts Hypothesis 1. □

As mentioned in the introduction, Hypothesis 1 is equivalent to Conjecture 3 of [6] with the extra hypothesis that $K/\mathbb{Q}_p$ is unramified. Congruences between newforms with the same Fricke eigenvalue arise in one of two ways: from ramification of the field of definition

(as demonstrated in the proof of Lemma 5), or from the failure of $\mathbb{T}^+$ and $\mathbb{T}^-$ to be integrally closed. Hypothesis 1 asserts that neither occurs, while Conjecture 3 of [6] precludes only the latter.

It follows from Lemma 5 with the notation above that $K$ is the unique unramified extension of $\mathbb{Q}_p$ of degree $r$. In particular, $K$ is Galois and is the field generated by the coefficients of any one of the eigenforms $f_1, f_2, \dots, f_r$.

**Lemma 6.** *Assume Hypothesis 1, and suppose that $\mathfrak{m}$ is a maximal ideal which contains a unique minimal prime ideal $\mathfrak{p}$. Suppose that $\mathfrak{p}$ corresponds to the field $K$ as in the last paragraph. Then we have*

$$\mathbb{T}_{\mathfrak{m}} \cong \widetilde{\mathbb{T}}_{\mathfrak{m}} \cong \widetilde{\mathbb{T}_{\mathfrak{m}}/\mathfrak{p}_{\mathfrak{m}}} \cong \mathcal{O}_K.$$

*Proof.* Adopt the assumptions and the notation in the statement of the lemma. By the discussion at the start of this section, we know that $\mathbb{T}/\mathfrak{p}$ is the subring of $K$ generated by the coefficients of the eigenforms $f_1, \dots, f_r$, and and is hence an order $\mathcal{O}$ in $\mathcal{O}_K$. Moreover, with $\mathfrak{p}_{\mathfrak{m}} = \mathfrak{p}\mathbb{T}_{\mathfrak{m}}$, we have

$$\mathbb{T}_{\mathfrak{m}}/\mathfrak{p}_{\mathfrak{m}} \cong \mathbb{T}/\mathfrak{p} \cong \mathcal{O}. \tag{2.4}$$

Since $\widetilde{\mathcal{O}} = \mathcal{O}_K$, this together with (2.2) establishes all but the first of the claimed isomorphisms.

We next show that $\mathcal{O} = \mathcal{O}_K$. To this end, recall that the $p$th Fourier coefficient of $f_i$ is equal to $-\lambda_p p^{\frac{k}{2}-1}$, where $\lambda_p$ is the Fricke eigenvalue of $f_i$. Since the $f_i$ are Galois-conjugate, the forms $f_1, \dots, f_r$ have the same Fricke eigenvalue. By Hypothesis 1, none of them are congruent mod $p$, and hence the reductions

$$\overline{f}_1, \overline{f}_2, \dots, \overline{f}_r$$

are distinct. Set $\mathbb{F} = \mathcal{O}/p\mathcal{O}$. Since $K$ is unramified, the action of $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ on the reduced eigenforms $\overline{f}_i$ is the same as that of $\mathrm{Gal}(K/\mathbb{Q}_p)$ on the eigenforms $f_1, \dots, f_r$. This implies that $|\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)| \geq r$, and hence $\mathbb{F} = \mathbb{F}_{p^r}$. We conclude that $\mathcal{O}/p\mathcal{O} \cong \mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_{p^r}$. Therefore $\mathcal{O}_K = \mathcal{O} + p\mathcal{O}_K$, and Nakayama's lemma implies that $\mathcal{O} = \mathcal{O}_K$, as desired.

Using (2.4), the proof will be complete once we show that $\mathfrak{p}_{\mathfrak{m}} = 0$. Since $\mathbb{T}$ is reduced, (2.1) shows that $\mathbb{T}_{\mathfrak{m}}$ is reduced. Therefore the nilradical of $\mathbb{T}_{\mathfrak{m}}$ (which is the intersection of the two prime ideals of $\mathbb{T}_{\mathfrak{m}}$) is 0, and the result follows. □

Suppose now that we are in the case when there are two minimal primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ contained in $\mathfrak{m}$. We will prove the following lemma.

**Lemma 7.** *Suppose that $k = 4$. Assume Hypothesis 1 and let $K_1$ and $K_2$ be the coefficient fields of the conjugacy classes of newforms corresponding to $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Then $K_1 = K_2$, and if $\mathcal{O}$ denotes the ring of integers of $K := K_1 = K_2$, we have*

$$\mathbb{T}_{\mathfrak{m}} \cong \{(a, b) \in \mathcal{O} \times \mathcal{O} : a \equiv b \pmod{p}\}.$$

*Proof.* The fields $K_1$ and $K_2$ are unramified, and $\mathcal{O}_1/p\mathcal{O}_1$ (respectively $\mathcal{O}_2/p\mathcal{O}_2$) is the extension of $\mathbb{F}_p$ generated by the coefficients of the reduction of the first (respectively second) conjugacy class of congruent eigenforms. Thus

$$[K_1 : \mathbb{Q}_p] = [\mathcal{O}_1/p\mathcal{O}_1 : \mathbb{F}_p] = [\mathcal{O}_2/p\mathcal{O}_2 : \mathbb{F}_p] = [K_2 : \mathbb{Q}_p],$$

from which it follows that $K_1 = K_2 = K$.

From (2.3) we have an embedding

$$\mathbb{T}_{\mathfrak{m}} \to \widetilde{\mathbb{T}}_{\mathfrak{m}} \cong \widetilde{\mathbb{T}_{\mathfrak{m}}/\mathfrak{p}_1\mathbb{T}_{\mathfrak{m}}} \times \widetilde{\mathbb{T}_{\mathfrak{m}}/\mathfrak{p}_2\mathbb{T}_{\mathfrak{m}}}.$$

The argument in the proof of Lemma 6 shows that $\mathbb{T}_{\mathfrak{m}}/\mathfrak{p}_1\mathbb{T}_{\mathfrak{m}} \cong \mathbb{T}_{\mathfrak{m}}/\mathfrak{p}_2\mathbb{T}_{\mathfrak{m}} \cong \mathcal{O}$, and hence we have an embedding

$$\mathbb{T}_{\mathfrak{m}} \to \mathcal{O} \times \mathcal{O}.$$

Moreover, both projections $p_1 : \mathbb{T}_{\mathfrak{m}} \to \mathcal{O}$ and $p_2 : \mathbb{T}_{\mathfrak{m}} \to \mathcal{O}$ are surjective. Let $I_1 = \ker p_2$ and $I_2 = \ker p_1$; via this embedding we may view each of $I_1$ and $I_2$ as a subset of $\mathcal{O}$. In fact, $I_1$ and $I_2$ are ideals of $\mathcal{O}$. If, for example, $a \in I_1$, then $(a, 0) \in \mathbb{T}_{\mathfrak{m}}$. Since $p_1$ is surjective, for any $b \in \mathcal{O}$, there is some $c \in \mathcal{O}$ with $(b, c) \in \mathbb{T}_{\mathfrak{m}}$. Then, $(a, 0)(b, c) = (ab, 0) \in \mathbb{T}_{\mathfrak{m}}$ and hence $ab \in I_1$.

Define a map $\phi : \mathcal{O}/I_1 \to \mathcal{O}/I_2$ by sending the coset $a + I_1$ to $b + I_2$, where $(a, b)$ is any element of $\mathbb{T}_{\mathfrak{m}}$. If $(a_1, b_1)$ and $(a_2, b_2)$ are two elements of $\mathbb{T}_{\mathfrak{m}}$ with $a_1 + I_1 = a_2 + I_1$, then $(a_1 - a_2, 0) \in \mathbb{T}_{\mathfrak{m}}$, and so

$$(a_1, b_1) - (a_2, b_2) - (a_1 - a_2, 0) = (0, b_1 - b_2) \in \mathbb{T}_{\mathfrak{m}}.$$

Since $b_1 - b_2 \in I_2$ it follows that $\phi$ is well-defined. It is easy to check that $\phi$ is a ring homomorphism, which is surjective since $p_2$ is surjective.

Moreover, if $\phi(a + I_1) = b + I_2 = 0$, then $b \in I_2$ and so $(0, b) \in \mathbb{T}_{\mathfrak{m}}$. Thus,

$$(a, b) - (0, b) = (a, 0) \in \mathbb{T}_{\mathfrak{m}}$$

and so $a \in I_1$ and $a + I_1 = 0$. Thus, $\phi$ is injective and hence an isomorphism. Since every non-zero ideal of $\mathcal{O}$ has finite index and there is at most one ideal of $\mathcal{O}$ of any given index, it follows that $I_1 = I_2$. This implies that

$$\mathbb{T}_{\mathfrak{m}} = \{(a, b) \in \mathcal{O} \times \mathcal{O} : b + I_2 = \phi(a + I_1)\}.$$

Finally, the image in $\mathbb{T}_{\mathfrak{m}}$ of the Hecke operator $T_1$ is $(1, 1)$, and the image in $\mathbb{T}_{\mathfrak{m}}$ of the Hecke operator $T_p$ is $\pm(p, -p)$. Therefore $(2p, 0) \in \mathbb{T}_{\mathfrak{m}}$, and since $p > 2$ we conclude that $I_1 = I_2 = (p)$. Hence

$$\mathbb{T}_{\mathfrak{m}} = \{(a, b) \in \mathcal{O} \times \mathcal{O} : b \equiv \phi(a) \pmod{p}\}.$$

Since $\phi : \mathcal{O}/p\mathcal{O} \to \mathcal{O}/p\mathcal{O}$ is an automorphism, we have that

$$\mathbb{T}_{\mathfrak{m}} \cong \{(a, b) \in \mathcal{O} \times \mathcal{O} : a \equiv b \pmod{p}\}.$$

□

## 3. Proof of Theorem 3

*Proof of Theorem 3.* To begin, we note that (2) $\iff$ (1) is an immediate consequence of Hypothesis 1.

We turn to the implications which can be proved without the assumption of Hypothesis 1. Ahlgren and Barcau [2] have proved the following, which is Conjecture 4 of [6] (this result has been generalized to higher level in [4]). Let $\mathfrak{p}$ be the maximal ideal in $\overline{\mathbb{Z}}_p$.

**Theorem 8.** *Suppose that $f \in S_2(p, \overline{\mathbb{Z}}_p)$ and $h \in S_4(p, \overline{\mathbb{Z}}_p)$ are eigenforms of $w_p$, are not identically zero modulo $\mathfrak{p}$, and satisfy*

$$\Theta f \equiv h \pmod{\mathfrak{p}}.$$

*Then the eigenvalues of $f$ and $h$ under $w_p$ have opposite signs.*

An inspection of the proof shows that the same conclusion holds when $f = E_2^*(z) = E_2(z) - pE_2(pz)$, the weight 2 Eisenstein series in $M_2(p)$.

To see that (2) $\implies$ (4), suppose that we have a congruence

$$h^+ \equiv h^- \pmod{\mathfrak{p}} \tag{3.1}$$

between forms in $S_4^+(p, \overline{\mathbb{Z}}_p)$ and $S_4^-(p, \overline{\mathbb{Z}}_p)$. If $\overline{h^+}$ is in the image of $\Theta$ then we would have

$$h^+ \equiv h^- \equiv \Theta f \pmod{\mathfrak{p}} \tag{3.2}$$

for some form $f \in S_2(p, \overline{\mathbb{Z}}_p)$. However, this is impossible by Theorem 8.

To see that (3) $\implies$ (4), suppose that $h \equiv \Theta f \pmod{\mathfrak{p}}$ where $f \in M_2(p, \overline{\mathbb{Z}}_p)$ and $h \in S_4(p, \overline{\mathbb{Z}}_p)$. We have $w(f) = p + 1 \not\equiv 0 \pmod{p}$, so by Proposition 4 we must have $w(h) = 2p + 2$ (recall that the filtration is either $p + 3$ or $2p + 2$).

For the reverse implication, suppose that (3) is false, so that $w(h) = 2p + 2$. Write $h = \sum a(n)q^n$. By a result of Serre and Tate (see Théorème 3 of [14]) we know that the mod $\mathfrak{p}$ system of eigenvalues

$$\{a(\ell) \pmod{\mathfrak{p}} \ : \ \ell \text{ prime}\}$$

arises via twisting from a system of weight $\leq p + 1$ and level one. In other words, there is a level one eigenform $g$ with $w(\overline{g}) \leq p + 1$ and with the property that

$$\overline{h} = \Theta^i \overline{g} \tag{3.3}$$

for some $i \in \{0, \dots, p - 1\}$.

If $i = 0$ then $\overline{h} = \overline{g}$, which is impossible since $w(\overline{h}) = 2p + 2$. If $i > 0$ then $\overline{h}$ is a member of its own theta-cycle (i.e. $\overline{h} = \Theta^{p-1}\overline{h}$). Straightforward considerations using Proposition 4 show that the filtrations in this theta cycle are

$$2p + 2 = w(\overline{h}),\ 3p + 3 = w(\Theta\overline{h}),\ \dots\ ,\ p^2 + p = w(\Theta^{p-2}\overline{h}). \tag{3.4}$$

Suppose by way of contradiction that $i \geq 2$. From (3.3) we see that

$$\Theta^{p-i}\overline{h} = \Theta^p \overline{g} = \Theta\overline{g}.$$

With (3.4), this yields a contradiction since $1 \leq p - i \leq p - 2$. We conclude that $i = 1$. Therefore $w(\overline{g}) = p + 1$. Since $S_2(p, \overline{\mathbb{F}}_p) = S_{p+1}(1, \overline{\mathbb{F}}_p)$ as $\overline{\mathbb{F}}_p$-vector spaces, we conclude that $\overline{h}$ is the reduction of a form in $\Theta\left(S_2(p, \overline{\mathbb{Z}}_p)\right)$, showing that (4) $\implies$ (3) unconditionally.

To complete the proof of the theorem, we will show that (1) $\iff$ (3) under the assumption of Hypothesis 1. To this end, we introduce some notation. Let $D := \dim S_4(\Gamma_0(p))$; since the old space is trivial, there are exactly $D$ newforms in this space. We enumerate them as follows:

$$\begin{aligned} &h_1^+, \dots, h_s^+ \\ &h_1^-, \dots, h_s^-, \end{aligned} \tag{3.5}$$

and

$$g_1, \dots, g_t. \tag{3.6}$$

Here the forms $h_i^+$, $h_i^-$ are all of the newforms (with Fricke eigenvalues $+1$ and $-1$, respectively) in $S_4(\Gamma_0(p))$ which have a congruence, and the $g_j$ are those newforms without a congruence. By Hypothesis 1, we may list the forms in such a way that

$$h_i^+ \equiv h_i^- \pmod{\mathfrak{p}} \text{ for all } i \tag{3.7}$$

and such that the forms $h_i^+$, $h_i^-$ satisfy no other congruences.

To show that (1) $\implies$ (3) it will suffice to show that each form $h_i^+$ has filtration $p+3$. To this end, we define

$$E(z) := E_{p-1}(z) - p^{p-1}E_{p-1}(pz) \in M_{p-1}(p, \overline{\mathbb{Z}}_p). \tag{3.8}$$

Then we have $E(z) \equiv 1 \pmod{p}$ and

$$E(z)|_{p-1}w_p \equiv 0 \pmod{p^{\frac{p+1}{2}}}. \tag{3.9}$$

We recall that under Hypothesis 1, the fields of definition of the newforms in $S_4(p)$ are unramified over $\mathbb{Q}_p$. Let $K$ be the field generated over $\mathbb{Q}_p$ by the coefficients of all of these newforms, and let $\mathcal{O}$ be its ring of integers. Since $p$ is a uniformizer for $\mathcal{O}$, we conclude from (3.7) that there exists a form $h \in S_4(p, \mathcal{O})$ with the property that

$$h^+ - h^- = ph. \tag{3.10}$$

Applying $w_p$ to (3.10) we conclude that

$$h^+ + h^- = ph|_4 w_p. \tag{3.11}$$

Combining (3.10) and (3.11) gives

$$2h^+ = ph|_4 w_p + ph.$$

It follows that $ph|_4 w_p \in S_4(p, \mathcal{O})$ and that $w(h^+) = w(ph|_4 w_p)$. To see that this filtration is $p+3$, we use the trace map from $S_k(p)$ to $S_k(1)$, which is given by

$$\mathrm{Tr}(f) := f + p^{1-\frac{k}{2}} \left(f|_k w_p\right) |U_p.$$

Then by (3.9) we obtain

$$\begin{aligned}
\mathrm{Tr}(p(h\,|_4\, w_p)E) - p(h\,|_4\, w_p)E &= p^{1-\frac{p+3}{2}} \left( (p(h\,|_4\, w_p)E)|_{p+3} w_p \right) |U_p \\
&= p^{-\frac{p-1}{2}} h(E|_{p-1} w_p)|U_p \\
&\equiv 0 \pmod{p}.
\end{aligned}$$

Set $H := \mathrm{Tr}(p(h\,|_4\, w_p)E) \in S_{p+3}(1, \mathcal{O})$. Then $H \equiv p(h\,|_4\, w_p) \pmod{p}$, so $w(h^+) = w(ph|_4 w_p) = p+3$, as desired. This shows that (1) $\implies$ (3).

We turn to the implication (3) $\implies$ (1). From (3.5) and (3.6) we have

$$D = 2s + t. \tag{3.12}$$

Each of the eigenforms $h_j^+$ have filtration $p+3$ and are distinct modulo $p$. It follows that

$$\dim S_{p+3} \geq s \tag{3.13}$$

On the other hand, the forms $h_1^+, \ldots, h_s^+, g_1, \ldots, g_t$ are congruent modulo $p$ to forms in $S_{2p+2}$, and are pairwise incongruent. Therefore

$$\dim S_{2p+2} \geq s + t. \tag{3.14}$$

On the other hand, standard dimension formulas and (3.12) give the equality

$$\dim S_{2p+2} + \dim S_{p+3} = \dim S_4(p) = 2s + t. \tag{3.15}$$

Combining (3.13), (3.14) and (3.15) gives

$$\dim S_{p+3} = s, \quad \dim S_{2p+2} = s + t. \tag{3.16}$$

We conclude that

$$h \text{ satisfies a congruence} \iff w(h) = p + 3.$$

The last assertion follows since $\dim S_{p+3} = \left\lfloor \frac{p}{12} \right\rfloor$. □

## 4. Proof of Theorem 1

Theorem 1 follows easily from Theorem 3. By Lemmas 6 and 7, a conjugacy class of eigenforms with no congruence does not contribute to the index of $\mathbb{T}$ in its normalization, while a pair of conjugacy classes of eigenforms of size $r$ with a congruence contributes a factor of $p^r$ to the index. By Theorem 3 the total number of pairs of newforms with a congruence is $\left\lfloor \frac{p}{12} \right\rfloor$, and Theorem 1 follows.

## 5. Computations

In this section we describe the computations which lead to Corollary 2. To check that there is no congruence between two forms in $S_4^+(p)$, it suffices to find a prime $\ell$ so that the $\ell$th coefficients of the newforms in $S_4^+(p)$ are distinct mod $p$. This is equivalent to the statement that $p$ does not divide the discriminant of $T_\ell$, restricted to $S_4^+(p)$. Similarly, to show there is no congruence between two forms in $S_4^-(p)$, it suffices to find a prime $q$ so that the discriminant of the characteristic polynomial of $T_q$ acting on $S_4^-(p)$ is coprime to $p$.

Numerical evidence suggests that for primes $\ell \neq p$, the characteristic polynomial of $T_\ell$ will have few irreducible factors. In particular, it should be possible to determine the characteristic polynomial of $T_\ell$ restricted to either of these spaces using the following algorithm:

(1) Compute the dimension of $S_4^+(p)$ (using standard dimension formulas and the formula for the genus of $X_0^+(p)$).
(2) Compute the characteristic polynomial $r(x)$ of $T_\ell$ on $S_4(p)$ using the algorithm of Kohel and Stein (implemented in MAGMA [5]).
(3) Factor $r(x)$ in $\mathbb{Q}[x]$.
(4) Find all collections of irreducible factors of $r(x)$ whose cumulative degrees sum to the dimension of $S_4^+(p)$ (in practice there is only one such collection, usually consisting of a single factor).

For example, the dimension of $S_4^+(89)$ is 14. The characteristic polynomial of $T_2$ factors as a product of four irreducible factors, of degrees 1, 1, 6, and 14. Since there is only one partition of 14 with parts from the above set, we are able to compute the characteristic polynomials of $T_2$ acting on $S_4^+(89)$ and $S_4^-(89)$.

For all primes $p \leq 5000$ the collection of irreducible factors of $r(x)$ described in step (4) was unique, and so it was possible to determine the characteristic polynomial restricted to the desired subspaces. In fact, $p = 1531$ was the only prime larger than 1000 for which any characteristic polynomial was found to have more than two irreducible factors.

Apart from the cases $p = 139$ and $p = 389$, the algorithm shows that the discriminant of the characteristic polynomial of $T_\ell$ restricted to $S_4^+(p)$ is coprime to $p$ for some $\ell \leq 19$, and similarly for $S_4^-(p)$. When $p = 139$, there is a pair of conjugacy classes of eigenforms (with opposite Fricke eigenvalue) over $\mathbb{Q}_{139}(\sqrt{139})$ which are congruent. When $p = 389$, there is a single conjugacy class of eigenforms over $\mathbb{Q}_{389}(\sqrt{389})$ which contains a congruence. These forms arise as the image under the $\Theta$ operator of the pair of eigenforms in $S_2(389)$ which are congruent.

## 6. Results in weight six

In this section we describe the extension of these ideas to higher weight by considering the case of $k = 6$ in detail. The situation here is complicated by the fact that there are both $\pmod p$ and $\pmod{p^2}$ congruences between newforms. In principle, these ideas could be extended to higher weights, although without further insight the results would become increasingly less satisfying, since stronger hypotheses would be required.

We recall (see for example Theorem 4.1 of [3]) that if $f \in S_6(p)$ is a newform, then $w(\overline{f})$ is one of $p+5$, $2p+4$, or $3p+3$. As in the previous case, it seems that the filtration determines the type of congruence which $f$ satisfies. In particular, we will prove the following.

**Theorem 9.** *Suppose that $p \geq 5$ is prime and that Hypothesis 1 is true for $S_6(p)$. If $f$ is a normalized eigenform in $S_6(p)$, then we have*

(1) $w(\overline{f}) = 3p+3 \iff f$ *has no congruences.*
(2) $w(\overline{f}) = 2p+4 \implies f$ *has a congruence modulo $p$ but not modulo $p^2$.*
(3) $w(\overline{f}) = p+5 \impliedby f$ *has a congruence modulo $p^2$.*

As before, the theta operator plays a key role. In particular, we have the following.

**Proposition 10.** *Suppose that $f \in S_6(p)$. Then*

(1) $w(\overline{f}) = 3p+3 \iff \overline{f} \in \Theta^2 \overline{M}_2(p)$.
(2) $w(\overline{f}) = 2p+4 \iff \overline{f} \in \Theta \overline{M}_4(p) \setminus \Theta^2 \overline{M}_2(p)$.
(3) $w(\overline{f}) = p+5 \iff \overline{f} \notin \Theta \overline{M}_4(p)$.

We suspect that more is true.

**Conjecture 11.** *All of the implications in Theorem 9 can be replaced by equivalences.*

Hypothesis 1 and Conjecture 11 together imply the $k = 6$ case of Conjecture 1 of [6].

**Theorem 12.** *Suppose that $p \geq 5$ is prime and that Hypothesis 1 and Conjecture 11 are true for $S_6(p)$. Then, the index of $\mathbb{T}$ in its normalization is*

$$\begin{cases} p^{3\lfloor \frac{p}{12} \rfloor} & p \equiv 1, 5 \pmod{12}, \\ p^{3\lfloor \frac{p}{12} \rfloor + 2} & p \equiv 7, 11 \pmod{12}. \end{cases}$$

We have computed all of the $p$-adic eigenforms and their filtrations for $k = 6$ and $p < 191$ with the exception of $p = 139$. In all of these cases, Conjecture 11 is true. In particular, Theorem 9 is true for $p$ in this range.

## 7. Proofs of results for weight 6

We begin by proving Proposition 10 since it involves no additional hypotheses.

*Proof of Proposition 10.* We begin with the first equivalence. Suppose that $\overline{f} \in \Theta^2 \overline{M}_2(p)$. Then there is a form $F \in S_{p+1}$ with $\overline{f} = \Theta^2 \overline{F}$, from which we conclude that $w(f) = 3p+3$.

Conversely, suppose that $w(f) = 3p+3$, and let $F \in S_{3p+3}$ be a form whose reduction is $\overline{f}$. Using the result of Serre and Tate mentioned above, we have

$$\overline{F} = \Theta^k \overline{G}$$

for some level-one eigenform $G$ with $w(G) \leq p+1$ (so that $k \geq 2$). From this we conclude that

$$w(\Theta^{p-k} \overline{F}) = w(\Theta G) \leq 2p+2.$$

It follows from Proposition 4 that $k \leq 2$. Therefore $k = 2$ and $w(G) = p + 1$, so that $G$ is congruent to a form in $M_2(p)$. This proves the first equivalence.

We turn to the second. If $\overline{f} \in \Theta\overline{M}_4(p) \setminus \Theta^2\overline{M}_2(p)$ then there is a form $F \in S_{2p+2}$ with $\overline{f} = \Theta\overline{F}$. Since $w(F) = p+3$ or $w(F) = 2p+2$, we have $w(\Theta F) = 2p+4$ or $w(\Theta F) = 3p+3$. However, the latter possibility is ruled out by the first equivalence.

Conversely, suppose that $w(f) = 2p + 4$, let $F \in S_{2p+4}$ be a form whose reduction is $\overline{f}$, and let $G$ be a level-one eigenform with $w(G) \leq p + 1$ such that

$$\overline{F} = \Theta^k\overline{G}$$

As above we conclude that $k \leq 3$. Since $w(\Theta G) \leq 2p + 2$, we cannot have $k = 1$. Since $k \geq 2$, there must be a drop in the theta cycle (and hence a filtration which is zero modulo $p$) between $G$ and $\Theta^{k-1}G$. Using this fact, it is easy to deduce that $k = 3$ and

$$w(G) = p - 1, \quad w(\Theta G) = 2p, \quad w(\Theta^2 G) = p + 3, \quad w(\Theta^3 G) = 2p + 4.$$

Since $S_4(p, \overline{\mathbb{F}}_p) = S_{3p+1}(1, \overline{\mathbb{F}}_p)$ as $\overline{\mathbb{F}}_p$ vector spaces (see for example Theorem 4.1 of [3]) and $S_{p+3}(1, \overline{\mathbb{F}}_p) \subseteq S_{3p+1}(1, \overline{\mathbb{F}}_p)$, it follows that $\Theta^2 G$ is congruent to a form in $M_4(p)$, so that $f \in \Theta\overline{M}_4(p)$. The second equivalence (and with it the third) follows. □

Let $D := \dim S_6(p)$. Since the old space is trivial, there are exactly $D$ newforms in this space. We assume that Hypothesis 1 is true for $S_6(p)$. It follows that these newforms have coefficients in the maximal unramified extension of $\mathbb{Q}_p$. We enumerate them as follows:

$$\begin{aligned} &h_1^+, \dots, h_s^+, \qquad g_1^+, \dots, g_t^+, \qquad f_1, \dots, f_r, \\ &h_1^-, \dots, h_s^-, \qquad g_1^-, \dots, g_t^-, \end{aligned} \tag{7.1}$$

in such a way that

$$h_i^+ \equiv h_i^- \pmod{p^2}, \tag{7.2}$$

$$g_j^+ \equiv g_j^- \pmod{p} \text{ but } g_j^+ \not\equiv g_j^- \pmod{p^2}, \tag{7.3}$$

and

$$\text{the } f_k \text{ have no congruence.} \tag{7.4}$$

As before, the superscript + or − denotes the sign of the $w_p$-eigenvalue. By Hypothesis 1, (7.2) and (7.3) describe all of the congruences between newforms in $S_6(p)$.

We have the following.

**Lemma 13.** *With notation as in* (7.1), (7.2), *and* (7.3), *we have*

$$\begin{aligned} w(h_i) &= p + 5, \\ w(g_j) &\leq 2p + 4, \\ w(f_k) &\leq 3p + 3, \end{aligned}$$

*for all $i$, $j$, and $k$.*

*Proof of Lemma 13.* Each newform has filtration at most $3p + 3$. The first two assertions in the lemma follow from the $p$-adic properties of the trace operator as in in the proof of Theorem 3. For example, if we write $h^\pm$ for one of the pairs $h_i^\pm$ in (7.1), then we have

$$h^+ - h^- = p^2 h \tag{7.5}$$

for some weight 6 form $h$ with $p$-integral coefficients. Applying $w_p$ to (7.5) and adding the resulting equation yields

$$2h^+ = p^2 h + p^2 h|w_p. \tag{7.6}$$

From this we conclude that $p^2 h|w_p$ has integral coefficients, and that

$$w(h^+) = w(p^2 h|w_p). \tag{7.7}$$

Using the form $E$ from (3.8), we see that

$$\mathrm{Tr}(p^2(h|w_p)\cdot E) - p^2(h|w_p)\cdot E = p^{3-\frac{p+5}{2}}\left(h(E|w_p)\right)|U_p = ph'$$

for some form $h'$ with integral coefficients. Using (7.6), this shows that $w(h^+) \leq p+5$. Equality follows since there are no weight 6 cusp forms of level one.

The assertion about the $g_j$ is proved with the same argument, (using $E^2$ in place of $E$) and we omit the details. □

*Proof of Theorem 9.* We know that each of the eigenforms $h_i^+$ have filtration $p+5$ and are distinct modulo $p$. It follows that

$$\dim S_{p+5} \geq s. \tag{7.8}$$

Similarly, we conclude that

$$\begin{aligned} \dim S_{2p+4} &\geq s+t, \\ \dim S_{3p+3} &\geq s+t+r. \end{aligned} \tag{7.9}$$

Using dimension formulas, we compute that

$$\dim S_{2p+4} + \dim S_{3p+3} = \dim S_6(p) = 2r+2s+t, \tag{7.10}$$

from which it follows that

$$\begin{aligned} \dim S_{2p+4} &= s+t, \\ \dim S_{3p+3} &= s+t+r. \end{aligned}$$

The claims in the theorem now follow. □

*Proof of Theorem 12.* The discussion in Section 2 applies to all weights with suitable modification. For example, in weight 6, distinct newforms may be congruent mod $p$ or mod $p^2$. In the case where a characteristic $p$ eigenform arises from two characteristic zero eigenforms with a congruence mod $p$, but not mod $p^2$, the corresponding localized Hecke algebra is

$$\mathbb{T}_{\mathfrak{m}} \cong \{(a,b) \in \mathcal{O}\times\mathcal{O} : a \equiv b \pmod{p}\},$$

and in the case of a mod $p^2$ congruence, the localized Hecke algebra is

$$\mathbb{T}_{\mathfrak{m}} \cong \{(a,b) \in \mathcal{O}\times\mathcal{O} : a \equiv b \pmod{p^2}\}.$$

A pair of conjugacy classes of eigenforms of size $r$ contributes the factor $p^r$ or $p^{2r}$ to the index in the respective cases.

By Conjecture 11, the sum of the sizes of the conjugacy classes with mod $p^2$ congruences is $\dim S_{p+5}$, and the sum of the sizes of the conjugacy classes with mod $p$ congruences but not mod $p^2$ congruences is $\dim S_{2p+4} - \dim S_{p+5}$. Hence, the $p$-adic valuation of the index of the Hecke algebra is

$$\dim S_{p+5} + \dim S_{2p+4} = \begin{cases} 3\lfloor \frac{p}{12} \rfloor & p \equiv 1,5 \pmod{12}, \\ 3\lfloor \frac{p}{12} \rfloor + 2 & p \equiv 7,11 \pmod{12}. \end{cases}$$

□

## References


[1] Ahmed Abbes and Emmanuel Ullmo. À propos de la conjecture de Manin pour les courbes elliptiques modulaires. *Compositio Math.*, 103(3):269–286, 1996.

[2] Scott Ahlgren and Mugurel Barcau. Congruences for modular forms of weights two and four. *J. Number Theory*, 126(2):193–199, 2007.

[3] Scott Ahlgren and Matthew Papanikolas. Higher Weierstrass points on $X_0(p)$. *Trans. Amer. Math. Soc.*, 355(4):1521–1535, 2003.

[4] M. Barcau and V. Pacşol. Mod $p$ congruences for modular forms of weight two and four for $\Gamma_0(pN)$. Preprint.

[5] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[6] Frank Calegari and William A. Stein. Conjectures about discriminants of Hecke algebras of prime level. In *Algorithmic number theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 140–152. Springer, Berlin, 2004.

[7] Alina Carmen Cojocaru and Ernst Kani. The modular degree and the congruence number of a weight 2 cusp form. *Acta Arith.*, 114(2):159–167, 2004.

[8] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[9] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 39–133. Amer. Math. Soc., Providence, RI, 1995.

[10] Craig Huneke and Irena Swanson. *Integral closure of ideals, rings, and modules*, volume 336 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2006.

[11] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[12] Loïc Merel and William A. Stein. The field generated by the points of small prime order on an elliptic curve. *Internat. Math. Res. Notices*, (20):1075–1082, 2001.

[13] Marusia Rebolledo Hochart. Corps engendré par les points de 13-torsion des courbes elliptiques. *Acta Arith.*, 109(3):219–230, 2003.

[14] Jean-Pierre Serre. Valeurs propres des opérateurs de Hecke modulo $l$. In *Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, 1974)*, pages 109–117. Astérisque, Nos. 24–25. Soc. Math. France, Paris, 1975.

[15] 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)*, pages 1–55. Lecture Notes in Math., Vol. 350. Springer, Berlin, 1973.

[16] Mark Watkins. Computing the modular degree of an elliptic curve. *Experiment. Math.*, 11(4):487–502 (2003), 2002.

[17] D. Zagier. Modular parametrizations of elliptic curves. *Canad. Math. Bull.*, 28(3):372–384, 1985.



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

Department of Mathematics, Wake Forest University, Winston-Salem, NC 27109
*E-mail address*: rouseja@wfu.edu