LMS J. Comput. Math. 16 (2013) 246–270
doi:10.1112/S1461157013000132

Computing level one Hecke eigensystems (mod p)

Craig Citro and Alexandru Ghitza

Abstract

We describe an algorithm for enumerating the set of level one systems of Hecke eigenvalues arising from modular forms (mod p).

Supplementary materials are available with this article.

1. *Introduction*

One of the cornerstone results of the modern arithmetic theory of modular forms associates to every level one Hecke eigensystem mod p a unique odd semisimple 2-dimensional Galois representation (mod p) unramified outside p. This follows from the corresponding results of Deligne (and Serre, and Eichler–Shimura) for eigenforms over $\mathbb{Z}$; a more direct approach that avoids using the full machinery of Deligne's characteristic zero theorem can be found in [**8**, Proposition 11.1].

Serre's conjecture (now a theorem of Khare–Wintenberger) says that all Galois representations described above arise from level one eigensystems. In [**14**, § 8], Khare recalls the well-known fact that the set of level one eigensystems (mod p) is finite of cardinality $O(p^3)$ as $p \to \infty$, and he outlines an argument due to Serre showing that this cardinality is $\Omega(p^2)$ as $p \to \infty$. Khare adds that 'It will be of interest to get quantitative refinements of this', and guesses that the cardinality is in fact asymptotic to $p^3/48$ as $p \to \infty$. In his PhD thesis, Centeleghe studies this question and proposes a precise conjecture for the asymptotic behavior of the number of representations of fixed conductor N (see [**3**, Conjecture 4.1.1]).

The present paper describes an efficient algorithm for enumerating the set of level one eigensystems (mod p), and hence also the set of odd semisimple 2-dimensional Galois representations (mod p) unramified outside of p. The theoretical framework underlying our approach is based on Tate's theory of theta cycles. We use two alternative computational methods: the Victor Miller basis for modular forms of level one and modular symbols over finite fields.

In a recent paper [**4**], Centeleghe attacks the problem of counting the number of irreducible Galois representations by an ingenious approach that requires computing with a single Hecke operator for each prime p. Unfortunately, this method only gives a lower bound on the number of representations. It is worth noting, however, that this lower bound is generally very close to the known upper bound, and in many cases (200 of the 374 cases considered in [**4**]) allows one to deduce the exact number. An unexpected result of our computations is that Centeleghe's lower bounds are equal to the exact numbers in many more cases; see § 8 for more details.

We remark that our algorithm computes only as many traces of Frobenius as are needed to distinguish different representations. For the orthogonal problem of efficient computation of lots of traces of Frobenius for a given Galois representation, we refer the reader to the recent monograph [**5**].

Received 18 November 2011; revised 31 March 2013.

2010 Mathematics Subject Classification 11F11 (primary), 11F25, 11F33, 11F80, 11Y40 (secondary).

The first author was partially supported by NSF grant DMS-0713225. The second author was supported by an Early Career Researcher grant from the University of Melbourne and Discovery Grant DP120101942 from the Australian Research Council. Some of the computations described in this paper were performed on W. Stein's machines `mod` and `geom`, supported by NSF grant DMS-0821725.

2. *Review of modular forms mod p*

We recall the definition of modular forms mod p of level one and of their Hecke operators.

Let $M_k(\mathbb{C})$ denote the complex vector space of holomorphic modular forms of weight k and level one. There is a $\mathbb{C}$-linear map that associates to each modular form its q-expansion at the (only) cusp ∞:

$$Q\colon M_k(\mathbb{C}) \longrightarrow \mathbb{C}[[q]], \quad f \longmapsto f(q) = \sum_{n=0}^{\infty} a_n q^n.$$

By the q-expansion principle [**12**, Theorem 1.6.1], this map is injective. We let $S_k(\mathbb{C})$ denote the subspace of cusp forms, that is of forms f whose q-expansion has no constant term.

We define the $\mathbb{Z}$-module of forms with integer coefficients by

$$M_k(\mathbb{Z}) = Q^{-1}(\mathbb{Z}[[q]])$$

and, for any $\mathbb{Z}$-module R, we define the R-module of forms with R-coefficients by

$$M_k(R) = M_k(\mathbb{Z}) \otimes_{\mathbb{Z}} R.$$

In particular, we define[†] the space of modular forms mod p of level one and weight k to be $M_k = M_k(\overline{\mathbb{F}}_p)$. These are obtained by reducing modulo p the q-expansions of the modular forms with coefficients in the ring of algebraic integers.

In a similar way, we define the subspace $S_k = S_k(\overline{\mathbb{F}}_p)$ of cusp forms mod p of level one and weight k.

2.1. *Eisenstein series mod p*

There are two normalizations for Eisenstein series in characteristic zero. The first makes the coefficient of q be one:

$$G_k = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \quad \text{where } \sigma_i(n) = \sum_{d|n} d^i. \tag{2.1}$$

The second makes the constant coefficient be one:

$$E_k = -\frac{2k}{B_k} G_k = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \tag{2.2}$$

We define Eisenstein series (mod p) by reducing the characteristic zero Eisenstein series modulo p. The first normalization is problematic for primes dividing the denominator of $B_k/(2k)$; by the von Staudt–Kummer congruences (see [**21**, Lemma 4]), this happens if and only if k is a multiple of $p-1$.

Convention. To simplify notation, we will always write G_k to denote the Eisenstein series (mod p) of weight k, keeping in mind that it is the reduction modulo p of the q-expansion in (2.1) if k is not a multiple of $p-1$, and the reduction modulo p of the q-expansion in (2.2) if k is a multiple of $p-1$.

Since we will soon restrict our attention to forms of weight at most $p+1$, the latter situation will only occur for the *Hasse invariant* A, which is the reduction modulo p of E_{p-1}. The von Staudt–Kummer congruences tell us that, apart from the constant coefficient, all coefficients of E_{p-1} are divisible by p, so the q-expansion of A is simply $A(q) = 1 \in \overline{\mathbb{F}}_p[[q]]$.

[†] Morally, the appropriate definition of modular forms mod p is intrinsic, as global sections of line bundles over the moduli stack of elliptic curves over $\overline{\mathbb{F}}_p$ (see [**12**, § 1.1], [**8**, § 10], or [**6**, § 2.1]). The naive definition we use is equivalent in level one for $p \geqslant 5$, by [**12**, Theorem 1.8.2, Remark 1.8.2.2].

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

2.2. *Operators*

The spaces M_k are equipped with a number of interesting linear maps. We will define them in the most economical way, by describing their effect on q-expansions. Suppose that $f \in M_k$ has q-expansion

$$f(q) = \sum_{n=0}^{\infty} a_n q^n.$$

For every prime ℓ, there is a Hecke operator $T_\ell \colon M_k \longrightarrow M_k$ given by

$$(T_\ell f)(q) = \sum_{n=0}^{\infty} a_{n\ell} q^n + \ell^{k-1} \sum_{n=0}^{\infty} a_n q^{n\ell}.$$

A *Hecke eigenform* is an element $f \in M_k$ which is an eigenvector for T_ℓ for all primes ℓ.

An important map is multiplication by the Hasse invariant A, defined in § 2.1. As we mentioned above, A has q-expansion $A(q) = 1$. Multiplication by A is an injective linear map

$$M_k \longrightarrow M_{k+(p-1)}, \quad f \longmapsto Af.$$

Of course, it behaves like the identity map on the level of q-expansions, and therefore commutes with the Hecke operators T_ℓ.

If f is a modular form (mod p), its *filtration* is defined by

$$w(f) = \min\{k \in \mathbb{N} \mid f = A^i g \text{ for some } g \in M_k, i \in \mathbb{N}\}.$$

2.3. *The algebra of modular forms*

The product of a form of weight k_1 and a form of weight k_2 is a modular form of weight $k_1 + k_2$. We take this multiplicative structure into account by setting

$$M = \bigoplus_{k \in \mathbb{Z}} M_k.$$

This is a graded $\overline{\mathbb{F}}_p$-algebra of Krull dimension 2. The q-expansion map

$$M \longrightarrow \overline{\mathbb{F}}_p[[q]], \quad f \longmapsto f(q)$$

is an algebra homomorphism with kernel $(A-1)M$ (see [**21**, Theorem 2]).

2.4. *The theta operator*

There is a derivation on M, raising degrees by $p+1$:

$$\vartheta \colon M_k \longrightarrow M_{k+(p+1)}, \quad f \longmapsto q\frac{d}{dq} f,$$

whose effect on q-expansions is

$$(\vartheta f)(q) = \sum_{n=0}^{\infty} n a_n q^n. \tag{2.3}$$

Katz gave a geometric construction of this operator and described some of its properties in [**13**]. Of these, we will need the following result.

PROPOSITION 1 [**13**, Theorem (2) and Corollary (5)]. *We have the following conditions.*
(a) *If $f \in M_k$ has filtration k and p does not divide k, then ϑf has filtration $k+p+1$.*
(b) *If $f \in M_k$ has $\vartheta(f) = 0$, then f has a unique expression of the form*

$$f = A^r g^p,$$

where $0 \leqslant r \leqslant p-1$, $r + k \equiv 0 \pmod p$, $g \in M_\ell$ and $p\ell + r(p-1) = k$.

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

Another important feature of the theta operator is that it commutes with Hecke operators 'up to twist', that is $T_\ell \circ \vartheta = \ell\vartheta \circ T_\ell$ (see [**8**, equations (4.8)]).

We use these properties to find out whether an *eigenform* can be in the kernel of ϑ.

PROPOSITION 2. *If f is a Hecke eigenform and $\vartheta^i(f) = 0$ for some i, then f is a scalar multiple of some power of the Hasse invariant A.*

Proof. We start by proving the case $i = 1$.

By equation (2.3), the q-expansion of $f \in \ker \vartheta$ is of the form

$$f(q) = a_0 + a_p q^p + a_{2p} q^{2p} + \dots.$$

Since f is an eigenvector for T_p (say with eigenvalue $a(p)$), we have

$$a(p)a_0 + a(p)a_p q^p + \dots = a(p)f(q) = (T_p f)(q) = a_0 + a_p q + \dots.$$

We conclude that $a_p = 0$, but then $a_{np} = 0$ for all $n \geqslant 1$. So the q-expansion of f is actually constant $f(q) = a_0$. We normalize f so that $f(q) = 1$. Then $A - f$ is in the kernel of the q-expansion homomorphism, so

$$A - f = (A-1)h \quad \text{for some } h = \sum_{j=0}^{N} h_j \in M,$$

where h_j is homogeneous of degree j.

We distinguish three possibilities.

(a) The weight of f is $p-1$. Then f and A are both in M_{p-1} and have the same q-expansion, so by the q-expansion principle $f = A$.

(b) The weight of f is less than $p-1$. Then comparing the highest degree terms in $A - f = Ah - h$ we see that $A = Ah_N$, which means that $h = 1$ and $f = 1$.

(c) The weight of f is greater than $p-1$. By looking at the highest degree terms in $-f + A = Ah - h$ we get $f = -Ah_N$. Note that $0 = \vartheta(f) = \vartheta(h_N)$ and h_N is a Hecke eigenform with weight strictly less than the weight of f. We repeat the whole argument with f replaced by h_N, until we fall in one of the cases (a) or (b), and we are done since each step peels off a factor of $-A$.

To finish the proof, we need to consider the case $i > 1$. So suppose that $\vartheta^i(f) = 0$, and let $g = \vartheta^{i-1}(f)$. Suppose that $g \neq 0$, then g is a Hecke eigenform satisfying $\vartheta(g) = 0$, so by the case $i = 1$ proved above, we know that $g = cA^n$ for some c, n. However, since $i > 1$, g is in the image of ϑ, hence $g = cA^n$ is a cusp form, which implies that $g = 0$. We can therefore move all of the way down to $\vartheta(f) = 0$, from which we conclude by using the case $i = 1$. □

2.5. *Hecke eigensystems*

In view of our interest in Galois representations unramified outside p, we define the (away-from-p) Hecke algebra by

$$\mathscr{H} = \mathbb{Z}[T_\ell \mid \ell \neq p].$$

By a *Hecke eigensystem* we will mean a ring homomorphism

$$\Phi \colon \mathscr{H} \longrightarrow \overline{\mathbb{F}}_p.$$

It is clear that the spaces M_k are $\overline{\mathbb{F}}_p\mathscr{H}$-modules. We say that an eigensystem Φ occurs in M_k if there exists a non-zero $f \in M_k$ such that

$$Tf = \Phi(T)f \quad \text{for all } T \in \mathscr{H}.$$

We write Φ_f for the eigensystem given by the eigenform f.

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

If Φ is an eigensystem, we define the (first) *twist* of Φ by

$$\Phi[1]\colon \mathscr{H} \longrightarrow \overline{\mathbb{F}}_p, \quad T_\ell \longmapsto \ell\Phi(T_\ell).$$

It is clear that this operation can be repeated (at most) $p-1$ times before getting back to Φ. The resulting eigensystems are called the *twists* of Φ. The twisting operation has a modular interpretation: for any eigenform f we have

$$\Phi_f[1] = \Phi_{\vartheta f}.$$

We will say that two eigensystems Φ and Ψ are *equivalent* (write $\Phi \sim \Psi$) if Φ is a twist of Ψ, that is if there exists i such that $\Phi = \Psi[i]$.

One of the crucial results for our computational work is due to Jochnowitz [10, Theorem 4.1] in the level one case, and to Ash and Stevens [1, Theorems 3.4, 3.5] in the general case. See also [6, Theorem 3.4].

THEOREM 3. *Every modular eigensystem has a twist that occurs in weight at most $p+1$.*

This indicates that, instead of having to work with spaces of arbitrary weight, it suffices to restrict to weight at most $p+1$ and take twists.

2.6. *The Sturm–Murty bound*

We need to be able to decide whether two eigensystems are equal by comparing only finitely many of the eigenvalues. The following result (due to Sturm and revisited by Murty) solves this problem in the case of two eigenforms of the same weight.

THEOREM 4 (Special case of [15, Theorem 1]). *Let f and g be holomorphic modular forms of weight k and level one, with Fourier coefficients $a_f(n)$ and $a_g(n)$. Let $\beta(k) = k/12$ and suppose that*

$$a_f(n) = a_g(n) \quad \text{for all } n \leqslant \beta(k).$$

Then $f = g$.

The proof works in any characteristic; via the relation between Fourier coefficients and Hecke operators we arrive at the form in which we will use the following result.

PROPOSITION 5. *Let Φ and Ψ be eigensystems occurring in the same weight k and suppose that*

$$\Phi(\ell) = \Psi(\ell) \quad \text{for all primes } \ell \leqslant \beta(k).$$

Then $\Phi = \Psi$.

3. *Some consequences of the theory of theta cycles*

Let f be a modular form which is not in the kernel of the theta operator. The *ϑ-cycle* of f is defined to be the $(p-1)$-tuple of integers

$$(w(\vartheta f), w(\vartheta^2 f), \dots, w(\vartheta^{p-1} f)).$$

It is clear from the effect of ϑ on q-expansions that $\vartheta^p f = \vartheta f$, which justifies the use of the word *cycle*. Note, however, that $\vartheta^{p-1} f = f$ only in special circumstances (when all of the Fourier coefficients of f of index divisible by p vanish), which explains why the cycle does not include $w(f)$ in general.

A lot is known about the structure of ϑ-cycles, which were introduced by Tate and appear for the first time in a paper of Jochnowitz [11]. For low weights, we will use the following classification given by Edixhoven (and based on Jochnowitz's analysis in [11, § 7]).

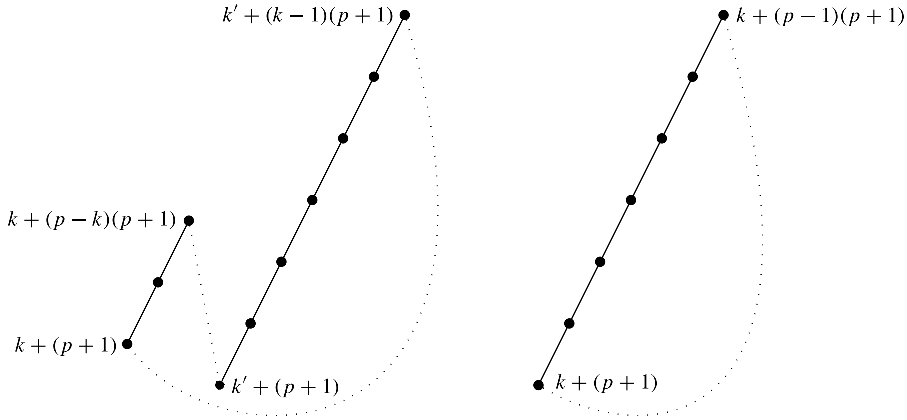


FIGURE 1. *Theta cycles of ordinary forms:* $4 \leqslant k \leqslant p-1$ *(left,* $k' = p+1-k$*) and* $k = p+1$ *(right). The lines correspond to applications of the theta operator: a solid line indicates that the filtration increases, while a dotted line indicates a drop in the filtration.*

PROPOSITION 6 (Edixhoven [6, Proposition 3.3]). *Let* $p \geqslant 5$ *be prime. Let* f *be an eigenform* (mod p) *of weight and filtration* k*, where* $k \leqslant p+1$*. Let* (a_ℓ) *denote the eigenvalues of* f*.*

(1) *If* $a_p \neq 0$ *(*f *is* ordinary*), then the* ϑ*-cycle of* f *is given by*

weight	ϑ*-cycle*
$4 \leqslant k \leqslant p-1$	$(k+(p+1), \ldots, k+(p-k)(p+1),$ $k'+(p+1), \ldots, k'+(k-1)(p+1))$
$k = p+1$	$(p+1+(p+1), \ldots, p+1+(p-1)(p+1))$

where $k' = p+1-k$*. See Figure 1.*

(2) *If* $a_p = 0$ *(*f *is* non-ordinary*), then the* ϑ*-cycle of* f *is given by*

weight	ϑ*-cycle*
$4 \leqslant k \leqslant p-1$	$(k+(p+1), \ldots, k+(p-k)(p+1), k'',$ $k''+(p+1), \ldots, k''+(k-3)(p+1), k)$
$k = p+1$	*does not occur*

where $k'' = p+3-k$*. See Figure 2.*

REMARK 7. We have extracted from the statement of [6, Proposition 3.3] only the parts that are relevant to level one. We have also eliminated the unnecessary requirement that f be a cusp form (see [11, § 7]).

LEMMA 8. *Let* f_1 *and* f_2 *be eigenforms with equivalent eigensystems. Then the* ϑ*-cycles of* f_1 *and* f_2 *are the same up to a cyclic permutation.*

Proof. We start by reducing to the case where neither f_1 nor f_2 is in the kernel of ϑ. Suppose that $f_1 \in \ker(\vartheta)$, then by Proposition 2 we know that $f_1 = cA^n$ for some c, n. Therefore, $\Phi_{f_1} = \Phi_A = \Phi_{G_{p+1}}[p-2]$, so we may replace f_1 by G_{p+1}, which is not in the kernel of ϑ. The same goes for f_2.

Since the eigensystems are equivalent, there exists an integer i such that $\Phi_{f_1} = \Phi_{\vartheta^i f_2}$. In particular, the weight of f_1 and the weight of $\vartheta^i f_2$ are congruent modulo $p-1$. We have that $\vartheta(f_1) \neq 0$ and $\vartheta(\vartheta^i f_2) \neq 0$, so $\vartheta(f_1)$ and $\vartheta^{i+1}(f_2)$ have the same q-expansion, and their weights

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

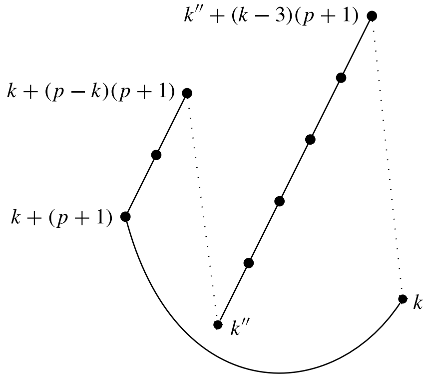


FIGURE 2. *Theta cycle of a non-ordinary form:* $4 \leqslant k \leqslant p-1$ *and* $k'' = p+3-k$. *The lines correspond to applications of the theta operator: a solid line indicates that the filtration increases, while a dotted line indicates a drop in the filtration.*

are congruent modulo $p-1$. Without loss of generality, the weight of $\vartheta(f_1)$ is less than or equal to the weight of $\vartheta^{i+1}(f_2)$, so there exists j such that $A^j\vartheta(f_1)$ has the same weight as $\vartheta^{i+1}(f_2)$. These forms also have the same q-expansion, so they must be equal:

$$A^j \vartheta f_1 = \vartheta^{i+1} f_2.$$

But then for all $a \geqslant 1$ we have

$$A^j \vartheta^a f_1 = \vartheta^{i+a} f_2.$$

Since $w(Ag) = w(g)$ for all modular forms g, we conclude that the ϑ-cycles of f_1 and f_2 are the same up to a cyclic permutation. □

We use Edixhoven's result to determine when two eigensystems are equivalent, and to estimate the number of twists of a given eigensystem.

THEOREM 9. *For* $i = 1, 2$, *let* f_i *be an eigenform of weight and filtration* k_i, *where*

$$1 \leqslant k_1 \leqslant k_2 \leqslant p+1.$$

Suppose that the eigensystems of f_1 *and* f_2 *are equal after a non-trivial twist, that is that* $\Phi_{f_1}[x] = \Phi_{f_2}$ *for some non-zero* $x \in \mathbb{Z}/(p-1)\mathbb{Z}$. *Then we must be in one of the following two situations:*

(a) $a_p(f_1) \neq 0 \neq a_p(f_2)$, $k_1 + k_2 = p+1$ *and* $x = p - k_1$;
(b) $a_p(f_1) = 0 = a_p(f_2)$, $k_1 + k_2 = p+3$ *and* $x = p - k_1 + 1$.

Proof. By Lemma 8, the ϑ-cycles of f_1 and f_2 are the same up to a cyclic permutation. The two cases now follow by comparing the general shape and the low points of the cycles in Edixhoven's classification. □

REMARK 10. In relation to case (b) of Theorem 9, note that if f_1 is non-ordinary, that is $a_p(f_1) = 0$, then there is always a form f_2 of weight $p + 3 - k_1$ such that $\Phi_{f_1}[p - k_1 + 1] = \Phi_{f_2}$.

PROPOSITION 11. *Let* f *be an eigenform of weight and filtration* k, *where* $1 \leqslant k \leqslant p+1$. *Let* $n(\Phi_f)$ *denote the number of distinct twists of the corresponding eigensystem* Φ_f. *Then*

$$n(\Phi_f) \in \left\{ \frac{p-1}{2}, p-1 \right\}.$$

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

The case $n(\Phi_f) = (p-1)/2$ *is only possible in the following situations:*

(a) $a_p \neq 0$ *and* $k = (p+1)/2$ *(so* $p \equiv 3 \pmod 4$*);*

(b) $a_p = 0$ *and* $k = (p+3)/2$ *(so* $p \equiv 1 \pmod 4$*).*

Moreover, case (b) *never occurs.*

Proof. Suppose that $n(\Phi_f) \neq p-1$. Then $n(\Phi_f)$ is a divisor of $p-1$, and the ϑ-cycle of f consists of copies of subcycles of length $n(\Phi_f)$.

Looking at the ϑ-cycle pictures (Figures 1 and 2), we note that the ordinary case with $k = p+1$ has only one low point, so here $n(\Phi_f) = p-1$; and the other two cases have two low points, so $n(\Phi_f) \geqslant (p-1)/2$. In order to have equality, the two low points must agree, that is we must have either

$$a_p \neq 0 \text{ and } k + p + 1 = k' + p + 1 = 2p + 2 - k, \text{ so } k = \frac{p+1}{2},$$

or

$$a_p = 0 \text{ and } k = k'' = p + 3 - k, \text{ so } k = \frac{p+3}{2}.$$

Since we do not use the last statement of the Proposition in our computations, we relegate its proof to § 9. □

EXAMPLE 12. In § 4 we prove that if $p \equiv 3 \pmod 4$, $G_{(p+1)/2}$ always has ϑ-cycle of length $(p-1)/2$.

If f is a cusp form of weight $(p+1)/2$, its ϑ-cycle length can be either $(p-1)/2$ or $p-1$. We give an explicit example for each of these two cases.

(a) The smallest example of a cusp form of weight $(p+1)/2$ with ϑ-cycle of length $(p-1)/2$ is Δ mod 23:

$$\Delta(q) = q + 22q^2 + 22q^3 + q^6 + q^8 + 22q^{13} + 22q^{16} + q^{23} + 22q^{24} + q^{25} + O(q^{26}).$$

We claim that $\vartheta^{12}\Delta = A^{12}\vartheta\Delta$ and, hence, the ϑ-cycle of Δ has length 11. This alleged equality takes place in weight 300, where the Sturm bound is 25, so it suffices to check it on q-expansions up to that precision:

$$(\vartheta^{12}\Delta)(q) = q + 21q^2 + 20q^3 + 6q^6 + 8q^8 + 10q^{13} + 7q^{16} + 22q^{24} + 2q^{25} + O(q^{26}),$$
$$(A^{12}\vartheta\Delta)(q) = q + 21q^2 + 20q^3 + 6q^6 + 8q^8 + 10q^{13} + 7q^{16} + 22q^{24} + 2q^{25} + O(q^{26}).$$

(b) The smallest example of a cusp form of weight $(p+1)/2$ with ϑ-cycle of length $p-1$ occurs for $p = 43$. The space of cusp forms of weight 22 is one-dimensional; denote its normalized generator by Δ_{22} (an explicit expression for it is $\Delta_{22} = 41G_4^4G_6 + 18G_4G_6^3$). The beginning of its q-expansion is

$$\Delta_{22}(q) = q + 13q^2 + 27q^3 + 41q^4 + 39q^5 + O(q^6).$$

The following shows that the ϑ-cycle length is not 21:

$$(\vartheta^{22}\Delta_{22})(q) = q + 13q^2 + 4q^3 + 18q^4 + 16q^5 + O(q^6),$$
$$(A^{22}\vartheta\Delta_{22})(q) = q + 3q^2 + 12q^3 + 3q^4 + 11q^5 + O(q^6).$$

4. *Eigensystems coming from Eisenstein series*

PROPOSITION 13. *Let* $4 \leqslant k_1 < k_2 \leqslant p+1$ *and let* Φ_1, Φ_2 *denote the eigensystems of the Eisenstein series* G_{k_1} *and* G_{k_2}*. Then* $\Phi_1 \sim \Phi_2$ *if and only if* $k_1 + k_2 \equiv 2 \pmod{p-1}$*. In this case,* $\Phi_2 = \Phi_1[p - k_1]$*.*

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

Proof. Suppose that $k_1 + k_2 \equiv 2 \pmod{p-1}$. On the one hand we have

$$\Phi_1[p-k_1](T_\ell) = \ell^{p-k_1}(1+\ell^{k_1-1}) = \ell^{p-k_1}+1.$$

On the other hand, we have

$$k_1 + k_2 \equiv 2 \pmod{p-1} \Rightarrow k_2 \equiv p+1-k_1 \pmod{p-1},$$

so

$$\Phi_2(T_\ell) = 1+\ell^{k_2-1} = 1+\ell^{p+1-k_1-1}.$$

For the other implication, suppose that $\Phi_2 = \Phi_1[i]$ for some i. This means that

$$\ell^i + \ell^{i+k_1-1} \equiv 1+\ell^{k_2-1} \pmod{p}$$

for all primes $\ell \neq p$. Let a, b, c be the respective remainders of the division by $p-1$ of i, $i+k_1-1$, k_2-1. (In particular, $a, b, c < p-1$.) Then in $\mathbb{F}_p$ we have

$$\alpha^a + \alpha^b = 1+\alpha^c \quad \text{for all } \alpha \in \mathbb{F}_p^\times. \tag{4.1}$$

Consider the polynomial

$$f(x) = x^a + x^b - 1 - x^c \in \mathbb{F}_p[x].$$

The degree of f is at most $p-2$ (or f is the zero polynomial). If $f \neq 0$, then f has at most $p-2$ roots in $\mathbb{F}_p$. However, equation (4.1) implies that f has $p-1$ roots in $\mathbb{F}_p$, so we must have that $f = 0$.

We have two possibilities: (i) $a = 0$ and $b = c$, which implies $i = 0$ and $k_1 = k_2$, contradicting the assumption that $k_1 < k_2$; (ii) $b = 0$ and $a = c$, which implies

$$k_1 + k_2 \equiv 2 \pmod{p-1} \quad \text{and} \quad i \equiv k_2 - 1 \equiv p + k_2 - 2 \equiv p - k_1 \pmod{p-1}. \qquad \square$$

PROPOSITION 14. *Let $4 \leqslant k \leqslant p+1$. The Eisenstein series G_k has $p-1$ twists, unless $p \equiv 3 \pmod 4$ and $k = (p+1)/2$, in which case G_k has $(p-1)/2$ twists.*

Proof. We start by noting that Eisenstein series are always ordinary, so $a_p \neq 0$. So according to Proposition 11, the number of twists is $p-1$, except possibly if $p \equiv 3 \pmod 4$ and $k = (p+1)/2$. Suppose that we are in this case, and let Φ be the eigensystem of G_k. We easily see that

$$\Phi(T_\ell) = 1+\ell^{(p+1)/2-1} = 1+\ell^{(p-1)/2}$$
$$\Phi[(p-1)/2](T_\ell) = \ell^{(p-1)/2}(1+\ell^{(p-1)/2}) = \ell^{(p-1)/2}+1,$$

so Φ has $(p-1)/2$ twists. $\square$

COROLLARY 15. *The number of distinct eigensystems* $\pmod p$ *coming from Eisenstein series is* $(p-1)^2/4$.

Proof. This follows via simple arithmetic from Propositions 13 and 14. $\square$

We end this section by discussing the possibility that an Eisenstein series and a cuspidal eigenform of small weights have equivalent eigensystems.

PROPOSITION 16. *Let G_k be the Eisenstein series of weight $k \leqslant p+1$ and fix an even integer $k' \neq 14$ with $12 \leqslant k' \leqslant p+1$. A cuspidal eigenform f of weight k' with $\Phi_{G_k} \sim \Phi_f$ exists if and only if $k' = k$ and p divides the numerator of the kth Bernoulli number B_k.*

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

Proof. The argument can be extracted from [**18**, proof of Theorem 10]; we include it here for completeness.

Suppose that there exists a form f with the given properties. Then there is some integer i such that $\Phi_f = \Phi_{G_k}[i]$, that is $\vartheta f = \vartheta^{i+1} G_k$. The conditions imposed on k' exclude the possibility of it being divisible by p, therefore the filtration of ϑf is $k' + p + 1$. Similarly, the filtration of $\vartheta^{i+1} G_k$ is $k + (i+1)(p+1)$. Therefore,

$$k' + p + 1 = k + (i+1)(p+1).$$

However, $k' \leqslant p + 1$ so $k' + p + 1 \leqslant 2(p+1)$, from which we conclude that $i = 0$, so $k' = k$.

Therefore, $\vartheta(f - G_k) = 0$. Again since k is not divisible by p we get that $f = G_k$, in particular the constant term of G_k is zero; but this constant term is the reduction modulo p of $B_k/(2k)$, therefore p must divide the numerator of $B_k/(2k)$. Using one last time the condition $k \leqslant p + 1$ we conclude that p divides the numerator of $B_k/(2k)$ if and only if it divides the numerator of B_k. □

5. *Bounds on the number of eigensystems*

In this section, we derive an explicit formula for the well-known upper bound on the number[†] $N(2, p)$ of level one Hecke eigensystems modulo p.

Let $N_{\text{twist}}(2, p)$ be the number of equivalence classes up to twist of level one Hecke eigensystems modulo p. We have seen that any eigensystem has at most $p - 1$ twists, so we get the inequality

$$N(2, p) \leqslant N_{\text{twist}}(2, p) \cdot (p - 1).$$

We know that each eigensystem occurs, up to twist, in weights at most $p + 1$. Therefore we can bound $N_{\text{twist}}(2, p)$ by the sum of the dimensions of the spaces M_k for $k \leqslant p + 1$:

$$N_{\text{twist}}(2, p) \leqslant \sum_{k=4}^{p+1} \dim M_k.$$

We now use the classical dimension formulas (see, e.g., [**22**, Corollary 1 in § 1.3]):

$$\dim M_k = \begin{cases} 0 & \text{if } k < 0 \text{ or } k \text{ is odd} \\ \left\lfloor \dfrac{k}{12} \right\rfloor & \text{if } k \equiv 2 \pmod{12} \\ \left\lfloor \dfrac{k}{12} \right\rfloor + 1 & \text{otherwise.} \end{cases}$$

After a straightforward calculation, we obtain the following expression for the sum of dimensions (write Q for the quotient of the integer division of $p + 1$ by 12):

$$\sum_{k=4}^{p+1} \dim M_k = \begin{cases} 3Q^2 + 4Q & \text{if } p \equiv 1 \pmod{12} \\ 3Q^2 + 6Q + 2 & \text{if } p \equiv 5 \pmod{12} \\ 3Q^2 + 7Q + 3 & \text{if } p \equiv 7 \pmod{12} \\ 3Q^2 + 3Q & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

It remains to multiply this value by $p - 1$ in order to obtain the desired upper bound on $N(2, p)$. Note that this upper bound is asymptotic to $p^3/48$ as $p \to \infty$.

[†] We use Khare's notation, which is motivated by the fact that this is the number of continuous semisimple odd representations

$$\rho\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{GL}_2(\overline{\mathbb{F}}_p)$$

that are unramified outside p. Note that we do not restrict our attention to irreducible representations here, but by Corollary 15 the difference is known to be $(p-1)^2/4$.

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

When $p \equiv 3 \pmod 4$, it is possible to give a slightly lower, more precise upper bound, as we indicate at the end of § 9.

6. *Special features*

Several factors can contribute to the number of eigensystems being smaller than the upper bound. We describe them here and explain how we detect their presence computationally. (We recall that $\beta(k)$ denotes the Sturm–Murty bound for the space of cusp forms of weight k.)

6.1. *Eisenstein-cuspidal congruences* (**E**)

We already discussed the possibility of an Eisenstein series mod p to be congruent to a cusp form in § 4. We detect this in our computation by using Serre's criterion from Proposition 16. More precisely, if Serre's criterion is satisfied in weight k (which can be checked very quickly), we know that such a cusp form f exists. Finding it requires checking Fourier coefficients up to precision $\beta(k)$.

These cusp forms give rise to reducible Galois representations.

6.2. *Non-semisimple Hecke action* (**NS**)

It can happen that the action of the Hecke operators on the spaces of cusp forms (mod p) is not semisimple; in this case, a simple subspace of dimension d will contribute fewer than d eigensystems. The first time this phenomenon occurs in our computations is for $p = 57$, weight $k = 32$. The space S_{32} has dimension 2; with respect to the Victor Miller basis, the matrices of the first few Hecke operators are

$$T_2 = \begin{pmatrix} 0 & 5 \\ 1 & 28 \end{pmatrix} \quad T_3 = \begin{pmatrix} 37 & 16 \\ 30 & 6 \end{pmatrix} \quad T_5 = \begin{pmatrix} 19 & 21 \\ 31 & 16 \end{pmatrix} \quad T_7 = \begin{pmatrix} 57 & 22 \\ 58 & 6 \end{pmatrix}$$

with respective Jordan normal forms

$$\begin{pmatrix} 14 & 1 \\ 0 & 14 \end{pmatrix} \quad \begin{pmatrix} 55 & 1 \\ 0 & 55 \end{pmatrix} \quad \begin{pmatrix} 51 & 1 \\ 0 & 51 \end{pmatrix} \quad \begin{pmatrix} 65 & 1 \\ 0 & 65 \end{pmatrix}$$

This two-dimensional space contributes only one Hecke eigensystem.

We detect non-semisimple spaces during the decomposition of S_k into simple Hecke submodules.

6.3. *Companion forms* (**C**, **Q**)

This is related to part (a) of Theorem 9. Suppose that f has weight $k \leqslant p + 1$ and $a_p(f) \neq 0$. It can happen that f has a *companion*, that is a form g of weight $p + 1 - k$ such that

$$\Phi_g = \Phi_f[p - k].$$

The system Φ_g appears in the space S_{p+1-k}, but it has already been counted as a twist of Φ_f. We check this by comparing ordinary forms f in weight k with ordinary forms of weight $p + 1 - k$, up to precision $\beta(k + p + 1)$.

Here is the justification for the comparison bound: we have f of weight $k > (p + 1)/2$ and g of weight $p + 1 - k$. We want to check whether the q-expansions ϑf (in weight $k + p + 1$) and $\vartheta^k g$ (in weight $kp + p + 1$) are equal. *A priori* it seems that this must be checked in weight $kp + p + 1$, where we are verifying the equality $A^k \vartheta f = \vartheta^k g$. However, as Buzzard pointed out to us, we can do much better by using ϑ-cycles. We are in the situation illustrated in Figure 1: ϑf is the first low point of the cycle, and ϑg is the second low point. Following the cycle, we see that $\vartheta^k g$ is back at the first low point, that is that $\vartheta^k g$ has filtration $k + p + 1$. Therefore, it suffices to perform the comparison in weight $k + p + 1$, checking q-expansions up to $\beta(k + p + 1)$.

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

In the 'central' case $k = p + 1 - k$, there are two possibilities:

(a) $g = f$, in which case f has $(p-1)/2$ twists and gives rise to a dihedral representation; this case is well-understood, as described in § 9;

(b) $g \neq f$, in which case we count f with its $p-1$ twists and ignore g; in all such cases we observed, the Galois orbit of f has size 2 and the Galois conjugate of f is g, so that f and g are defined over the quadratic extension $\mathbb{F}_{p^2}$; we call the span of f and g a *quadratic-twist eigenspace*.

Companion forms give rise to Galois representations whose restriction to the decomposition subgroup at p is diagonalizable (see [**8**, Proposition 13.8]).

6.4. *Non-ordinary forms* (**NO**)

This is related to part (b) of Theorem 9. If f has weight $k \leqslant p + 1$ and $a_p(f) = 0$, then there exists a form g of weight $p + 3 - k$ such that

$$\Phi_g = \Phi_f[p - k + 1].$$

The system Φ_g appears in the space S_{p+3-k}, but it should be ignored, since it has already been counted as a twist of Φ_f. This includes the 'central' case $k = p + 3 - k$, where we check computationally that $f \neq g$ (this is mostly a sanity check, since $f = g$ never occurs in the non-ordinary case, as we see in Proposition 11 and § 9).

We find g computationally by checking coefficients up to precision $\beta(p + 3 - k)$.

Non-ordinary forms give rise to Galois representations whose restriction to the decomposition subgroup at p is irreducible.

7. *Description of the algorithm*

Step 1. *Obtain the eigensystems coming from Eisenstein series*

According to Proposition 13, the complete list of such eigensystems up to twist is G_k for $4 \leqslant k \leqslant (p+1)/2$, together with G_{p+1}.

Step 2. *Obtain the eigensystems coming from cusp forms of weight up to* $p + 1$

Fix a weight k with $12 \leqslant k \leqslant p + 1$. We took two different approaches.

(1) Compute the (cuspidal) Victor Miller basis over $\mathbb{F}_p$ of weight k up to and including the pth coefficient, then decompose the span of this basis into Hecke eigensystems.

(2) Compute the (cuspidal) modular symbols of weight k and sign -1 over $\mathbb{F}_p$, then decompose into Hecke eigenspaces.

Either of these gives us a list of cuspidal eigenforms $f_1, \ldots, f_n$ with $n \leqslant \dim S_k$, for the spaces of cusp forms S_k of weight $k \leqslant p + 1$.

Step 3. *Remove duplicates* (*up to twist*)

Check for the special circumstances listed in § 6 and remove any eigensystems that have a twist already on the list.

We now have the list of all eigensystems up to twist.

8. *Summary and discussion of results*

We produced two distinct implementations of this algorithm, a higher-level one in Sage [**20**], and a lower-level one written in C and using the library FLINT2 [**9**] for arithmetic and factorization of polynomials over $\mathbb{F}_p$, and basic linear algebra mod p.

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

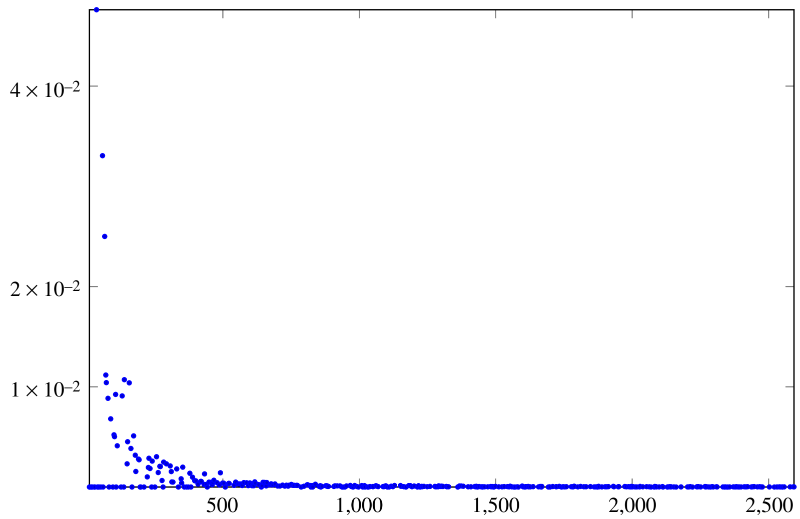


FIGURE 3. *The relative difference (as a percentage) between the actual number of eigensystems and the upper bound, for all primes less than* 2595. *See also the file reldiff.out in the online supplementary material available for download from the publisher's website.*

The table in the appendix records, for all the primes under 2595, the number of distinct non-Eisenstein[†] eigensystems mod p, the upper bound on this number, as well as any interesting features that each prime might have: companion forms, Eisenstein-cuspidal congruence, non-ordinary forms, non-semisimple Hecke module or a quadratic-twist. The raw data, as well as some results on primes above 2595, are available at

https://bitbucket.org/aghitza/eigensystems_data

The first explicit examples of companion forms appear in [**8**], resulting from computations performed by Elkies and Atkin. They focused on finding primes at which the reduction of the six cuspidal eigenforms with rational coefficients have companions. Higher-degree examples were given by Centeleghe in his thesis [**3**], going up to $p = 619$. Our results extend this range to all $p < 2595$.

Similarly, we find new examples of non-ordinary forms mod $p < 2595$ of weight $k \leqslant p + 1$, extending those listed in [**3**, Tables 5 and 6] and the results of Gouvêa in [**7**].

It is interesting to compare our results with Centeleghe's table in [**4**]. Out of the 374 lower bounds he computes, 200 are marked with a star in his table, meaning that they are proved to give the actual number of representations. Our results indicate that a further 164 of his lower bounds coincide with the exact numbers, for a total of 364 out of 374. We have marked with a star the 10 primes for which Centeleghe's lower bound is not equal to the actual number of eigensystems.

Finally, we note that the 'interesting' phenomena described above are quite rare, and the actual number of eigensystems deviates very little from the explicit upper bound given in § 5. We have plotted the relative difference between the actual number and the upper bound in Figures 3 and 4 at two different zoom levels.

[†]We decided to exclude the Eisenstein eigensystems from the count in order to ease comparison with Centeleghe's results. As Corollary 15 indicates, the number of Eisenstein eigensystems (mod p) is $(p-1)^2/4$.

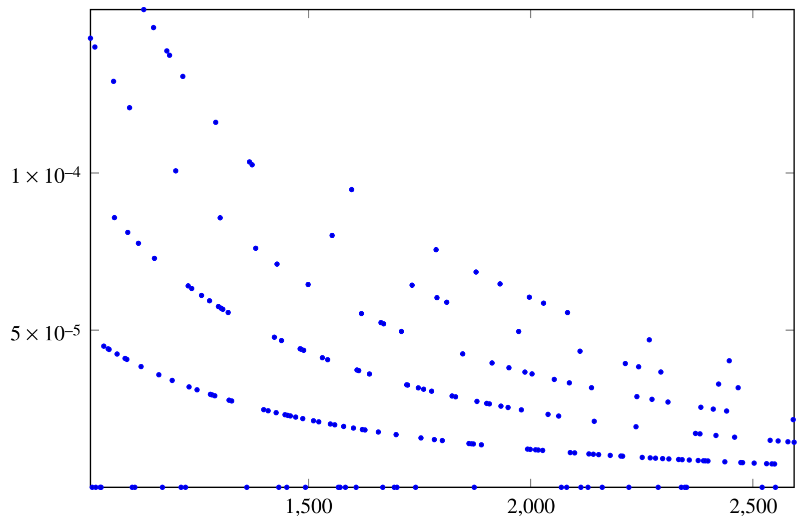


FIGURE 4. *The relative difference (as a percentage) between the actual number of eigensystems and the upper bound, for the primes between* 1000 *and* 2595. *See also the file reldiff.zoom in the online supplementary material.*

9. *The dihedral case*

We recall the situation described in Proposition 11: let f be an eigenform of weight and filtration k with $1 \leqslant k \leqslant p+1$. Let Φ_f be the corresponding eigensystem and let $n(\Phi_f)$ denote the number of its distinct twists. We proved already that $n(\Phi_f)$ is either $p-1$ or $(p-1)/2$, and the classification of ϑ-cycles tells us that the latter can occur only in the cases

(a) $a_p \neq 0$ and $k = (p+1)/2$ (so $p \equiv 3 \pmod 4$);
(b) $a_p = 0$ and $k = (p+3)/2$ (so $p \equiv 1 \pmod 4$).

This section is dedicated to proving that case (b) never occurs and obtaining more precise information about case (a). We are indebted to T. Centeleghe and the anonymous referee for indicating how the proof goes.

PROPOSITION 17. *Let $p \geqslant 11$ be prime. Let f be a cuspidal eigenform $\pmod p$ of level one and weight k, where $2 \leqslant k \leqslant p+1$. Let $\Phi = (a_\ell)$ be the eigensystem of f, ρ the Galois representation $\pmod p$ attached to f, and $\tilde{\rho}$ the corresponding projective representation. Suppose that Φ has $(p-1)/2$ twists.*

(a) *The image of $\tilde{\rho}$ is a dihedral group.*
(b) *We must have $p \equiv 3 \pmod 4$, $k = (p+1)/2$ and $a_p \neq 0$.*

Proof. (a) We start by noting that, under the assumptions, ρ cannot be reducible. If it were, then Φ would also be the eigensystem of the Eisenstein series G_k; but according to Proposition 14 the only Eisenstein series with $(p-1)/2$ twists and $k \leqslant p+1$ is $G_{(p+1)/2}$. By Proposition 16, p would have to divide the numerator of the Bernoulli number $B_{(p+1)/2}$. It is however known (see [**2**, equation (5.2)]) that

$$-2B_{(p+1)/2} \equiv h \pmod p$$

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

where h is the class number of $\mathbb{Q}(\sqrt{-p})$. By the von Staudt–Clausen congruence, p does not divide the denominator of $B_{(p+1)/2}$, since $p-1$ does not divide $(p+1)/2$. As $0<h<p$, we conclude that p also does not divide the numerator of $B_{(p+1)/2}$, contradiction.

So ρ is an irreducible representation.

The assumption on the number of twists of Φ implies that

$$\begin{aligned} (\ell^{(p-1)/2}-1)a_\ell = 0 &\qquad \text{for all } \ell \neq p \\ \Rightarrow \operatorname{trace}(\rho(\mathrm{Frob}_\ell)) = a_\ell = 0 &\qquad \text{for all } \ell \text{ such that } \ell^{(p-1)/2} = -1 \\ \Rightarrow \tilde{\rho}(\mathrm{Frob}_\ell) \text{ has order } 2 &\qquad \text{for all } \ell \text{ such that } \ell^{(p-1)/2} = -1 \end{aligned}$$

where we used the fact that a trace zero element of PGL_2 must have order two. We conclude that half of the elements of image($\tilde{\rho}$) have order two. Therefore, this image is either $\mathbb{Z}/2\mathbb{Z}$ or a dihedral group D_n of order $2n$ with $n \geqslant 2$.

If the image were $\mathbb{Z}/2\mathbb{Z}$, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is simply given by one trace zero element of PGL_2; but such an element is diagonalizable and hence fixes a line, contradicting the irreducibility of ρ.

(b) Fix a decomposition subgroup G_p at p and let ρ_p be the restriction of ρ to G_p. In the ordinary case $a_p \neq 0$, Deligne proved (see [**8**, Proposition 12.1]) that

$$\rho_p \sim \begin{pmatrix} \chi^{k-1}\lambda(1/a_p) & * \\ 0 & \lambda(a_p) \end{pmatrix}$$

where $\chi\colon G_p \longrightarrow \mathbb{F}_p^\times$ is the mod p cyclotomic character. But our assumption on the number of twists of Φ means that $\rho_p \otimes \chi^{(p-1)/2} \cong \rho_p$, which forces $*$ above to be zero. In other words, ρ_p is a semisimple representation of G_p, which by a result of Serre (see [**17**, Proposition 4]) implies that ρ_p is tamely ramified.
In the non-ordinary case $a_p = 0$, Fontaine proved (see [**6**, § 6]) that ρ_p is irreducible; in particular, ρ_p is semisimple and we can again conclude that it is tamely ramified.
Let $K/\mathbb{Q}$ be the number field defined by the projective representation $\tilde{\rho}$. By part (a), $K/\mathbb{Q}$ is a dihedral extension; since ρ is odd, complex conjugations act non-trivially so K is not a totally real field; since f has level one, ρ and K are unramified outside p; and we have just seen that K is tamely ramified at p.
We fix a decomposition subgroup D of K at p, and normal subgroups

$$I^w \lhd I \lhd D$$

where I is the inertia subgroup of D and let I^w is the wild inertia subgroup. It is known that the quotient I/I^w is a cyclic group (see [**16**, Corollaire 1 of Proposition IV.7]); but I^w is trivial since K is tamely ramified at p. Therefore, I is cyclic.
Let $\mathbb{Q}^{(p)}$ be the unique quadratic field unramified outside p. It must be ramified at p, so its discriminant is $\pm p$. Therefore,

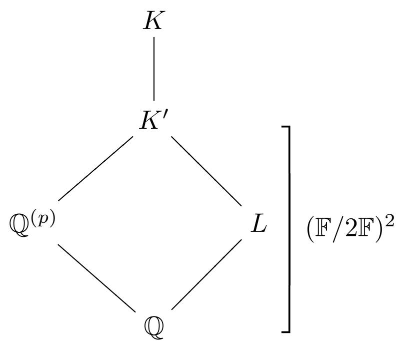
$$\mathbb{Q}^{(p)} = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } p \equiv 1 \pmod 4 \\ \mathbb{Q}(\sqrt{-p}) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We know that $\mathbb{Q}^{(p)}$ is contained in K (the group $\mathrm{Gal}(K/\mathbb{Q})$ is dihedral so it surjects onto $\mathbb{Z}/2\mathbb{Z}$, so K contains a quadratic field; since K is ramified only at p, so is this quadratic field, which must then be isomorphic to $\mathbb{Q}^{(p)}$).

Under the composition

$$I \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}^{(p)}/\mathbb{Q})$$

the cyclic group I surjects onto $\mathrm{Gal}(\mathbb{Q}^{(p)}/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$; since $I \subset \mathrm{Gal}(K/\mathbb{Q}) \cong D_n$ we conclude that $I \cong \mathbb{Z}/2\mathbb{Z}$.
Therefore, $\mathrm{Gal}(K/\mathbb{Q}^{(p)})$ is unramified at $\mathfrak{p}$, where $p = \mathfrak{p}^2$ in $\mathbb{Q}^{(p)}$. (Because the ramification index of p is 2, so all of the ramification above p happens in the quadratic extension $\mathbb{Q}^{(p)}$.)
This means that $\mathrm{Gal}(K/\mathbb{Q}^{(p)})$ is unramified at every finite place.
The order of $\mathrm{Gal}(K/\mathbb{Q}^{(p)})$ must be odd; otherwise, $\mathrm{Gal}(K/\mathbb{Q})$ would have a quotient isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, and a second quadratic extension unramified at p, non-isomorphic to $\mathbb{Q}^{(p)}$:



This is absurd, as it contradicts the uniqueness of $\mathbb{Q}^{(p)}$.
Since ρ is an odd representation, the image $c \in \mathrm{Gal}(K/\mathbb{Q})$ of a complex conjugation is non-trivial; since the order of $\mathrm{Gal}(K/\mathbb{Q}^{(p)})$ is odd, we must have $c \notin \mathrm{Gal}(K/\mathbb{Q}^{(p)})$, so c stays non-trivial in the quotient $\mathrm{Gal}(\mathbb{Q}^{(p)}/\mathbb{Q})$. We conclude that $\mathbb{Q}^{(p)}$ is an imaginary quadratic field, so it must be $\mathbb{Q}(\sqrt{-p})$, so $p \equiv 3 \pmod 4$ and $k = (p+1)/2$. □

Furthermore, it is known that every dihedral representation as described in Proposition 17 is induced from an unramified character of the quadratic field $\mathbb{Q}(\sqrt{-p})$, and therefore that the number of (mod p) dihedral representations is $(h-1)/2$, where h is the class number of $\mathbb{Q}(\sqrt{-p})$. The result goes back to Hecke; we refer the interested reader to [**19**, § 8.1] or [**3**, Proposition 3.3.7]. This allows us to obtain a more precise upper bound on the number of eigensystems: in the case $p \equiv 3 \pmod 4$, our estimate from § 5 overcounts the contribution of the dihedral representations, so we need to refine it by subtracting $(p-1)(h-1)/4$. It is this refined upper bound that we use in the table of results and in Figures 3 and 4.

Appendix. *Table of results*

The following table gives the exact number of eigensystems mod p, the refined upper bound on this number as described at the end of § 9, and indicates the presence of the following special features:

- **C**: companion form;
- **E**: Eisenstein-cuspidal congruence;
- **NO**: non-ordinary form;
- **NS**: non-semisimple Hecke module;
- **Q**: quadratic-twist eigenspace (two companion forms that are Galois conjugate);
- *: number is strictly greater than Centeleghe's lower bound;
- (d): corresponding eigenform is defined over $\mathbb{F}_{p^d}$ (omitted if $d = 1$).

The interested reader can find the raw data that were used in constructing the table at

https://bitbucket.org/aghitza/eigensystems_data

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

p	Number	Bound	Special features
11	10	10	
13	12	12	
17	48	48	
19	72	72	
23	143	143	
29	336	336	
31	405	405	
37	720	756	**E**: 32
41	1080	1080	
43	1260	1260	
47	1656	1656	
53	2496	2496	
59	3393	3509	**E**: 44 **NO**: 16
61	3900	3900	
67	5148	5280	**E**: 58 **NS**: 32
71	6195	6265	**NS**: 54
73	6840	6912	**NS**: 40
79	8736	8814	**NO**: 38
83	10 373	10 373	
89	12 848	12 936	**NS**: 68
97	16 896	16 896	
101	19 100	19 200	**E**: 68
103	20 196	20 298	**E**: 24
107	22 737	22 949	**C**: 26 **NO**: 28
109	24 300	24 300	
113	27 104	27 216	**NS**: 84
127	38 934	38 934	
131	42 510	42 900	**E**: 22 **NO**: 40 **NS**: 28
137	49 368	49 368	
139	50 991	51 543	**C**: 20 **NO**: 36 **NS**: 28 138
149	63 788	63 936	**E**: 130
151	66 075	66 375	**C**: 52 **NO**: 60
157	74 256	75 036	**E**: 62 110 **NS**: 70 70 74
163	83 916	84 240	**NS**: 80 146
167	90 387	90 387	
173	100 620	101 136	**C**: 68 **NO**: 24 **NS**: 74
179	111 784	112 140	**C**: 30 **NS**: 70
181	115 920	116 100	**NS**: 38
191	136 040	136 420	**C**: 30(2)
193	140 928	141 312	**C**: 48 **NO**: 72
197	150 528	150 528	
199	154 836	154 836	
211	185 535	185 535	
223	219 225	219 447	**NO**: 72
227	231 424	231 876	**NS**: 46 220
229	237 576	238 260	**C**: 58 58 **NO**: 116
233	250 792	251 256	**E**: 84 **NS**: 148
239	270 725	270 725	

p	Number	Bound	Special features
241	277 680	278 400	**C**: 98 **NS**: 96 198
251	314 875	314 875	
257	337 664	338 688	**E**: 164 **NO**: 50 100 **Q**: 130(2)
263	362 084	362 608	**E**: 100 **NO**: 98
269	388 332	389 136	**C**: 84 **NO**: 78 **NS**: 114
271	396 495	397 305	**C**: 18 40 **E**: 84
277	425 040	425 316	**NO**: 92
281	444 360	444 360	
283	452 751	453 879	**C**: 142 **E**: 20 **NO**: 72 72
293	503 408	504 576	**E**: 156 **NS**: 76 156 266
307	580 023	581 247	**C**: 52 **E**: 88 **NO**: 78 **NS**: 88
311	602 485	603 415	**C**: 32 126 **E**: 292
313	616 200	616 512	**NO**: 114
317	640 532	640 848	**NS**: 198
331	729 135	730 455	**C**: 164 166 **NO**: 84 84
337	771 456	771 456	
347	842 164	842 856	**C**: 74 **E**: 280
349	857 472	857 820	**NS**: 38
353	886 336	888 096	**E**: 186 300 **NO**: 76(2) **NS**: 92
359	933 127	933 127	
367	998 448	998 448	
373	1 049 412	1 049 412	*
379	1 099 791	1 101 303	**C**: 20 **E**: 100 174 **NO**: 56
383	1 135 686	1 135 686	
389	1 190 772	1 191 936	**E**: 200 **NS**: 124 390
397	1 266 804	1 267 596	**C**: 16 **NS**: 358
401	1 306 000	1 306 800	**E**: 382 **NS**: 220
409	1 386 792	1 387 200	**E**: 126
419	1 491 006	1 491 842	**NO**: 106 **NS**: 258
421	1 513 260	1 514 100	**C**: 112 **E**: 240
431	1 623 250	1 623 680	**C**: 80
433	1 646 352	1 648 512	**C**: 188 **E**: 366 **NS**: 126 322 352
439	1 716 741	1 717 179	* **C**: 214
443	1 766 232	1 766 232	
449	1 839 040	1 839 936	**NS**: 108 374
457	1 939 824	1 940 736	**NS**: 202 266
461	1 992 260	1 992 720	**E**: 196
463	2 017 323	2 018 247	**E**: 130 **NO**: 182
467	2 070 205	2 071 603	**E**: 94 194 **NS**: 376
479	2 233 694	2 234 650	* **NO**: 236 **NS**: 34
487	2 351 025	2 351 511	**NS**: 228
491	2 406 880	2 410 310	**C**: 124 246 **E**: 292 336 338 **NO**: 124 124
499	2 530 587	2 531 583	**NO**: 126 **NS**: 70
503	2 590 320	2 591 324	**C**: 162 **NS**: 204
509	2 688 336	2 688 336	
521	2 883 400	2 884 440	**NS**: 350 358
523	2 916 414	2 917 458	**E**: 400 **NS**: 424
541	3 231 360	3 231 900	* **E**: 86

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

p	Number	Bound	Special features
547	3 339 609	3 341 247	**E**: 270 486
557	3 528 376	3 529 488	**E**: 222 **NS**: 82
563	3 643 446	3 644 570	**C**: 282 **NS**: 476
569	3 763 000	3 764 136	**C**: 86 **NS**: 108
571	3 803 040	3 803 610	**NS**: 422
577	3 924 288	3 926 016	**C**: 54 **E**: 52 **NO**: 36
587	4 132 765	4 134 523	**E**: 90 92 **NS**: 220
593	4 263 584	4 264 176	**E**: 22
599	4 390 516	4 392 310	* **NO**: 222 **NS**: 128 388
601	4 438 800	4 440 000	**NO**: 136 **NS**: 528
607	4 572 876	4 573 482	**E**: 592
613	4 712 400	4 713 012	**E**: 522
617	4 804 184	4 806 648	**E**: 20 174 338 **NS**: 288
619	4 851 300	4 853 154	**C**: 158 216 **E**: 428
631	5 140 170	5 141 430	**E**: 80 226
641	5 393 280	5 393 280	
643	5 443 197	5 443 839	**C**: 322
647	5 541 065	5 543 649	**E**: 236 242 554 **NO**: 268
653	5 701 088	5 703 696	**E**: 48 **NO**: 66 328(2)
659	5 861 135	5 861 793	**E**: 224
661	5 914 260	5 916 900	**NS**: 92 130 312 424
673	6 245 568	6 246 912	**E**: 408 502
677	6 357 780	6 359 808	**E**: 628 **NS**: 64 658
683	6 529 468	6 530 832	**E**: 32 **NS**: 280
691	6 762 000	6 764 070	**E**: 12 200 **NS**: 214
701	7 063 700	7 064 400	**NO**: 268
709	7 309 392	7 310 100	**NS**: 174
719	7 619 057	7 620 493	**NO**: 358 **NS**: 570
727	7 881 456	7 882 182	**E**: 378
733	8 080 548	8 082 012	**C**: 184 **NS**: 332
739	8 281 836	8 282 574	**NS**: 692
743	8 414 280	8 415 764	**C**: 134 **NS**: 640
751	8 690 625	8 692 875	**C**: 158 **E**: 290
757	8 904 924	8 906 436	**E**: 514 **NS**: 750
761	9 047 800	9 049 320	**E**: 260 **Q**: 382(2)
769	9 337 344	9 338 880	**NO**: 62 **NS**: 78
773	9 484 792	9 486 336	**C**: 280 **E**: 732
787	10 012 854	10 012 854	
797	10 401 332	10 402 128	**E**: 220
809	10 878 912	10 881 336	**E**: 330 628 **NS**: 520
811	10 958 895	10 961 325	**E**: 544 **NO**: 140 **NS**: 244
821	11 373 400	11 375 040	**E**: 744 **NS**: 438
823	11 457 036	11 457 036	
827	11 624 711	11 626 363	**E**: 102 **NS**: 522
829	11 712 060	11 712 060	
839	12 133 402	12 136 754	**E**: 66 **NO**: 140 **NS**: 242 738
853	12 762 960	12 763 812	**NO**: 68
857	12 943 576	12 945 288	**C**: 264 **NS**: 804

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

p	Number	Bound	Special features
859	13 035 165	13 035 165	
863	13 215 322	13 216 184	**NS**: 706
877	13 874 964	13 876 716	**E**: 868 **NS**: 100
881	14 066 800	14 068 560	**E**: 162 **NS**: 144
883	14 163 597	14 164 479	**NO**: 222
887	14 352 314	14353200	**E**: 418
907	15 355 341	15 356 247	**NO**: 228
911	15 553 265	15 555 085	**C**: 366 **NS**: 820
919	15 970 905	15 972 741	**C**: 120
929	16 504 480	16 506 336	**E**: 520 820
937	16 937 856	16 937 856	
941	17 156 880	17 156 880	
947	17 487 756	17 487 756	
953	17 822 392	17 824 296	**E**: 156 **NS**: 268
967	18 619 167	18 622 065	**C**: 376 378 **NS**: 362
971	18 853 405	18 854 375	**E**: 166
977	19 210 608	19 210 608	
983	19 558 985	19 561 931	**C**: 144 **NS**: 676 742
991	20 046 510	20 047 500	**C**: 166
997	20 418 996	20 418 996	
1009	21 164 976	21 168 000	**C**: 126 **NS**: 38 294
1013	21 422 016	21 422 016	
1019	21 800 470	21 803 524	**C**: 356 **NS**: 60 952
1021	21 9351 00	21 935 100	
1031	22 580 175	22 580 175	
1033	22 720 512	22720512	
1039	23 113 665	23 114 703	**NS**: 586
1049	23 795 888	23 796 936	**NO**: 426
1051	23 931 600	23 932 650	**NO**: 368
1061	24 622 740	24 625 920	**E**: 474 **Q**: 532(2) 532(2)
1063	24 758 937	24 761 061	**NO**: 352 **NS**: 584
1069	25 187 712	25 188 780	**NO**: 280
1087	26 484 282	26 485 368	**NO**: 52
1091	26 776 940	26 778 030	**E**: 888
1093	26 927 628	26 929 812	**C**: 164 460
1097	27 224 640	27 227 928	**C**: 324 408 **NS**: 1010
1103	27 672 873	27 672 873	
1109	28 134 336	28 134 336	
1117	28 747 044	28 749 276	**E**: 794 **NO**: 476
1123	29 214 636	29 215 758	**NO**: 152
1129	29 684 448	29 688 960	**E**: 348 **NO**: 192 **NS**: 730 **Q**: 566(2)
1151	31 449 050	31 453 650	**E**: 534 784 968 **NS**: 1038
1153	31 627 008	31 629 312	**E**: 802 **NS**: 1136
1163	32 459 889	32 461 051	**NS**: 896
1171	33 137 325	33 137 325	
1181	33 993 440	33 998 160	* **C**: 360 **NO**: 182 **NS**: 954 1008
1187	34 513 786	34 518 530	**NO**: 114 254 298 **NS**: 472
1193	35 047 184	35 048 376	**E**: 262

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

p	Number	Bound	Special features
1201	35 756 400	35 760 000	**C**: 460 **E**: 676 **NS**: 338
1213	36 846 012	36 846 012	
1217	37 208 384	37 213 248	**E**: 784 866 1118 **NS**: 492
1223	37 757 967	37 757 967	
1229	38 325 880	38 328 336	**E**: 784 **NO**: 616
1231	38 506 995	38 508 225	**NO**: 100
1237	39 081 084	39 083 556	**E**: 874 **NS**: 1094
1249	40 234 272	40 235 520	**NO**: 224
1259	41 206 419	41 208 935	**NO**: 316 **NS**: 36
1277	43 008 856	43 011 408	**C**: 540 **NO**: 532
1279	43 205 985	43 207 263	**E**: 518
1283	43 618 127	43 619 409	**E**: 510
1289	44 237 648	44 238 936	**NS**: 544
1291	44 437 920	44 443 080	**E**: 206 824 **NO**: 324 **NS**: 308
1297	45 067 104	45 069 696	**E**: 202 220
1301	45 485 700	45 489 600	**E**: 176 **NS**: 246 728
1303	45 694 341	45 696 945	**C**: 410 **NS**: 1280
1307	46 118 125	46 120 737	**E**: 382 852
1319	47 392 644	47 395 280	**E**: 304 **NS**: 1080
1321	47 624 280	47 625 600	* **C**: 168
1327	48 273 693	48 275 019	**E**: 466
1361	52 097 520	52 097 520	
1367	52 778 142	52 783 606	**E**: 234 **NS**: 84 118 266
1373	53 486 048	53 491 536	**C**: 344 **NO**: 444 520 **NS**: 902
1381	54 429 960	54 434 100	**E**: 266 **Q**: 692(2) 692(2)
1399	56 586 147	56 587 545	
1409	57 820 928	57 822 336	**E**: 358
1423	59 561 892	59 564 736	**NS**: 1140
1427	60 066 685	60 068 111	**NO**: 358
1429	60 321 576	60 325 860	**C**: 94 **E**: 996 **NS**: 390
1433	60 835 656	60 835 656	
1439	61 588 821	61 591 697	**E**: 574 **NO**: 674
1447	62 631 321	62 632 767	**NS**: 792
1451	63 159 100	63 159 100	
1453	63 423 360	63 424 812	**NO**: 702
1459	64 211 049	64 212 507	**NS**: 234
1471	65 808 225	65 809 695	**NS**: 854
1481	67 169 800	67 172 760	**NO**: 530 **NS**: 202
1483	67 440 633	67 443 597	**E**: 224 **NO**: 694
1487	67 980 042	67 981 528	**NS**: 956
1489	68 266 464	68 269 440	**NS**: 252 **Q**: 746(2)
1493	68 822 976	68 822 976	
1499	69 649 510	69 654 004	**E**: 94 **NS**: 90 1366
1511	71 329 380	71 330 890	**C**: 498
1523	73 062 849	73 064 371	**E**: 1310
1531	74 219 535	74 222 595	**NO**: 252 **NS**: 1250
1543	75 979 737	75 982 821	**C**: 732 **NS**: 222
1549	76 879 872	76 881 420	**C**: 110

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

p	Number	Bound	Special features
1553	77 474 288	77 480 496	**NO**: 620 778(2) **NS**: 1034
1559	78 363 505	78 365 063	**E**: 862
1567	79 594 299	79 594 299	
1571	80 206 590	80 206 590	
1579	81 442 158	81 443 736	**NO**: 396
1583	82 056 758	82 056 758	
1597	84 262 416	84 270 396	**C**: 168 196 398 **E**: 842 **NS**: 1198
1601	84 905 600	84 907 200	**NS**: 798
1607	85 857 563	85 857 563	
1609	86 185 584	86 188 800	**E**: 1356 **NS**: 892
1613	86 831 992	86 835 216	**E**: 172 **NS**: 1146
1619	87 799 961	87 804 815	**E**: 560 **NO**: 406 **NS**: 1506
1621	88 134 480	88 136 100	**E**: 980
1627	89 116 995	89 118 621	**NO**: 644
1637	90 775 096	90 778 368	**E**: 718 **NO**: 714
1657	94 151 880	94 153 536	**C**: 176
1663	95 171 106	95 176 092	**C**: 396 **E**: 270 1508
1667	95 868 304	95 868 304	
1669	96 213 576	96 218 580	**C**: 652 **E**: 388 1086
1693	100 438 812	100 438 812	
1697	101 152 832	101 154 528	**C**: 432
1699	101 508 987	101 508 987	
1709	103 315 212	103 320 336	**C**: 72 514 **NS**: 308
1721	105 513 400	105 516 840	**E**: 30 **NS**: 1514
1723	105 880 614	105 884 058	**NO**: 488 **NS**: 380
1733	107 737 328	107 744 256	**E**: 810 942 **NO**: 868(2)
1741	109 245 900	109 245 900	
1747	110 376 882	110 380 374	**NS**: 442 902
1753	111 523 560	111 525 312	**E**: 712
1759	112 662 309	112 665 825	**E**: 1520 **NS**: 720
1777	116 175 264	116 178 816	**E**: 1192 **NS**: 1682
1783	117 353 610	117 355 392	**C**: 762
1787	118 144 793	118 153 723	**E**: 1606 **NO**: 358 498 **NS**: 262 1372
1789	118 546 188	118 553 340	**E**: 848 1442 **NS**: 568 712
1801	120 958 200	120 960 000	**C**: 728
1811	122 974 115	122 981 355	**E**: 550 698 1520 **NO**: 824
1823	125 433 768	125 437 412	**NS**: 68
1831	127 107 225	127 110 885	**E**: 1274 **NS**: 532
1847	130 463 281	130 468 819	**E**: 954 1016 1558
1861	133 481 040	133 482 900	**NS**: 274
1867	134 777 448	134 779 314	**NS**: 1564
1871	135 629 230	135 631 100	**E**: 1794
1873	136 086 912	136 086 912	
1877	136 953 628	136 963 008	**C**: 516 **E**: 1026 **NO**: 278 **NS**: 116 1042
1879	137 386 029	137 389 785	**E**: 1260
1889	139 610 048	139 611 936	**E**: 242
1901	142 291 000	142 294 800	**C**: 476 **E**: 1722
1907	143 639 972	143 643 784	**C**: 368 **NS**: 106

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

p	Number	Bound	Special features
1913	145 006 080	145 011 816	**C**: 702 **NO**: 872 **NS**: 1210
1931	149 133 030	149 142 680	**C**: 296 966 **NO**: 456 484 484
1933	149 612 148	149 616 012	**E**: 1058 1320
1949	153 366 040	153 369 936	**C**: 44 170
1951	153 821 850	153 827 700	**E**: 1656 **NS**: 716 1920
1973	159 108 848	159 116 736	**C**: 900 **NO**: 70 248 **NS**: 1204
1979	160 561 183	160 565 139	**E**: 148 **NS**: 110
1987	162 525 303	162 531 261	**C**: 770 **E**: 510 **NS**: 1948
1993	164 011 320	164 013 312	**E**: 912
1997	164 995 348	165 005 328	**E**: 772 1888 **NO**: 562 **NS**: 1298 1300
1999	165 487 347	165 489 345	**NS**: 992
2003	166 490 324	166 496 330	**C**: 350 **E**: 60 600
2011	168 501 315	168 503 325	**C**: 100
2017	170 019 360	170 021 376	**E**: 1204
2027	172 561 511	172 563 537	**NS**: 156
2029	173 069 520	173 079 660	**NO**: 396 **NS**: 914 1458 **Q**: 1016(2) 1016(2)
2039	175 630 764	175 634 840	* **E**: 1300 **NS**: 1980
2053	179 299 656	179 305 812	**E**: 1932 **NO**: 1028(2)
2063	181 917 888	181 922 012	**C**: 852 **NO**: 664
2069	183 539 136	183 539 136	
2081	186 756 960	186 756 960	
2083	187 283 187	187 293 597	**C**: 1042(2) **NS**: 906 1088 1738
2087	188 356 413	188 362 671	**E**: 376 1298 **NO**: 170
2089	188 920 152	188 922 240	**Q**: 1046(2)
2099	191 642 859	191 644 957	**E**: 1230
2111	194 932 350	194 940 790	**E**: 1038 **NO**: 98 506 **NS**: 146
2113	195 520 512	195 520 512	
2129	200 004 336	200 004 336	
2131	200 560 800	200 562 930	**NS**: 1694
2137	202 264 248	202 270 656	**E**: 1624 **NO**: 798 **NS**: 1984
2141	203 409 140	203 411 280	**C**: 222
2143	203 971 950	203 976 234	**E**: 1916 **NS**: 258
2153	206 854 544	206 856 696	**E**: 1832
2161	209 174 400	209 174 400	
2179	214 449 147	214 451 325	**NS**: 384
2203	221 626 896	221 629 098	**NO**: 706
2207	222 820 339	222 822 545	**C**: 316
2213	224 659 568	224 668 416	**C**: 554 554 **E**: 154 **NO**: 1108
2221	227 117 100	227 117 100	
2237	232 065 496	232 069 968	**C**: 340 **NO**: 88
2239	232 668 075	232 674 789	**C**: 898 **E**: 1826 **NS**: 512
2243	233 929 159	233 938 127	**C**: 236 1122 **NO**: 562 562
2251	236 455 875	236 458 125	**NO**: 918
2267	241 531 807	241 543 137	**E**: 2234 **NO**: 220 **NS**: 1760 2094 2224
2269	242 186 112	242 188 380	**NO**: 220
2273	243 467 520	243 474 336	**E**: 876 2166 **NS**: 208
2281	246 055 320	246 057 600	**NS**: 622
2287	247 992 138	247 992 138	

https://doi.org/10.1112/S1461157013000132 Published online by Cambridge University Press

p	Number	Bound	Special features
2293	249 958 644	249 967 812	**E**: 2040 **NO**: 842 1148(2)
2297	251 278 832	251 281 128	**NS**: 2058
2309	255 239 412	255 246 336	**E**: 1660 1772 **NS**: 1014
2311	255 892 560	255 894 870	**C**: 184
2333	263 299 124	263 301 456	**NS**: 678
2339	265 331 437	265 331 437	
2341	266 020 560	266 022 900	**NS**: 1914
2347	268 075 074	268 075 074	
2351	269 416 925	269 416 925	
2357	271 521 932	271 524 288	**E**: 2204
2371	276 387 030	276 391 770	**E**: 242 2274
2377	278 502 840	278 505 216	**E**: 1226
2381	279 911 800	279 916 560	**C**: 868 **E**: 2060
2383	280 599 600	280 6067 46	**E**: 842 2278 **NO**: 722
2389	282 748 752	282 751 140	**E**: 776
2393	284 174 384	284 176 776	**C**: 126
2399	286 286 429	286 288 827	* **NS**: 946
2411	290 627 925	290 635 155	**E**: 2126 **NO**: 12 **NS**: 1192
2417	292 821 616	292 826 448	* **NO**: 896 **NS**: 146
2423	294 987 490	294 9971 78	**E**: 290 884 **NS**: 248 2084
2437	300 163 920	300 166 356	**NS**: 2352
2441	301 642 560	301 649 880	**E**: 366 1750 **NS**: 200
2447	303 849 458	303 861 688	**C**: 218 430 694 868 **NS**: 1764
2459	308 367 161	308 372 077	**NO**: 1074 **NS**: 712
2467	311 392 917	311 402 781	**NO**: 372 **NS**: 226 584 640
2473	313 684 440	313 686 912	**NO**: 1236
2477	315 212 132	315 214 608	**NS**: 1490
2503	325 244 988	325 247 490	**E**: 1044
2521	332 337 600	332 337 600	
2531	336 302 780	336 305 310	**NO**: 286
2539	339 506 991	339 512 067	**C**: 1138 **NS**: 2426
2543	341 104 625	341 107 167	**E**: 2374
2549	343 549 388	343 551 936	**C**: 934
2551	344 336 700	344 336 700	
2557	346 795 524	346 800 636	**C**: 640 **E**: 1464
2579	355 825 872	355 831 028	**E**: 1730 **NO**: 606
2591	360 797 360	360 805 130	**E**: 854 2574 **NS**: 448
2593	361 672 128	361 677 312	**C**: 180 764

Acknowledgements. The authors wish to thank the referees for their thorough and insightful comments, in particular for pointing out a gap in the original version of the algorithm in § 7 and for suggesting the arguments given in § 9, C. Khare for motivating and encouraging our work, W. Stein for suggesting the use of the Victor Miller basis and useful discussions about decompositions into Hecke eigenspaces, and K. Buzzard, T. Centeleghe and M. Flander for suggestions and corrections.

The collaboration on this project started during the Sage Days 7 workshop in February 2008, hosted by the Institute for Pure and Applied Mathematics (IPAM) at UCLA. The authors thank IPAM for facilitating this meeting.

References

1. A. Ash and G. Stevens, 'Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues', *J. reine angew. Math.* 365 (1986) 192–220.
2. L. Carlitz, 'The class number of an imaginary quadratic field', *Comment. Math. Helv.* 27 (1953) 338–345.
3. T. G. Centeleghe, 'A conjectural mass formula for mod p Galois representations'. PhD Thesis, University of Utah, May 2009.
4. T. G. Centeleghe, 'Computing the number of certain Galois representations mod p', *J. Théor. Nombres Bordeaux* 23 (2011) no. 3, 603–627.
5. J-M. Couveignes and B. Edixhoven (eds), *Computational aspects of modular forms and Galois representations* (Princeton University Press, Princeton, NJ, 2011).
6. B. Edixhoven, 'The weight in Serre's conjectures on modular forms', *Invent. Math.* 109 (1992) no. 3, 563–594.
7. F. Q. Gouvêa, 'Non-ordinary primes: a story', *Experiment. Math.* 6 (1997) no. 3, 195–205.
8. B. H. Gross, 'A tameness criterion for Galois representations associated to modular forms (mod p)', *Duke Math. J.* 61 (1990) no. 2, 445–517.
9. W. Hart, 'Fast library for number theory: an introduction', *Mathematical Software – ICMS 2010*, Lecture Notes in Computer Science 6327 (Springer, Heidelberg, 2010) 88–91, http://www.flintlib.org/.
10. N. Jochnowitz, 'Congruences between systems of eigenvalues of modular forms', *Trans. Amer. Math. Soc.* 270 (1982) no. 1, 269–285.
11. N. Jochnowitz, 'A study of the local components of the Hecke algebra mod ℓ', *Trans. Amer. Math. Soc.* 270 (1982) no. 1, 253–267.
12. N. M. Katz, 'p-adic properties of modular schemes and modular forms', *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Mathematics 350 (Springer, Berlin, 1973) 69–190.
13. N. M. Katz, 'A result on modular forms in characteristic p', *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, Lecture Notes in Mathematics 601 (Springer, Berlin, 1977) 53–61.
14. C. Khare, 'Modularity of Galois representations and motives with good reduction properties', *J. Ramanujan Math. Soc.* 22 (2007) no. 1, 75–100.
15. M. Ram Murty, 'Congruences between modular forms', *Analytic number theory (Kyoto, 1996)*, London Mathematical Society Lecture Note Series 247 (Cambridge University Press, Cambridge, 1997) 309–320.
16. J-P. Serre, '*Corps locaux*'. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.
17. J-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* 15 (1972) no. 4, 259–331.
18. J-P. Serre, 'Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]', *Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416*, Lecture Notes in Mathematics 317 (Springer, Berlin, 1973) 319–338.
19. J-P. Serre, 'Modular forms of weight one and Galois representations', *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)* (Academic Press, London, 1977) 193–268.
20. W. A. Stein *et al.*, Sage Mathematics Software (Version 4.6.1). The Sage Development Team, 2011, http://www.sagemath.org.
21. H. P. F. Swinnerton-Dyer, 'On ℓ-adic representations and congruences for coefficients of modular forms', *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, Lecture Notes in Mathematics 350 (Springer, Berlin, 1973) 1–55.
22. D. Zagier, 'Elliptic modular forms and their applications', *The 1-2-3 of modular forms*, Universitext (Springer, Berlin, 2008) 1–103.

Craig Citro
Google
651 North 34th Street
Seattle, WA 98103
USA

craigcitro@gmail.com

Alexandru Ghitza
Department of Mathematics and Statistics
The University of Melbourne
Parkville, VIC, 3010
Australia

aghitza@alum.mit.edu