*LMS J. Comput. Math.* 14 (2011) 214–231 © 2011 Author
doi:10.1112/S1461157011000155

# Computations with classical and $p$-adic modular forms

Alan G. B. Lauder

*Dedicated to Daqing Wan*

Abstract

We present $p$-adic algorithms for computing Hecke polynomials and Hecke eigenforms associated to spaces of classical modular forms, using the theory of overconvergent modular forms. The algorithms have a running time which grows linearly with the logarithm of the weight and are well suited to investigating the dimension variation of certain $p$-adically defined spaces of classical modular forms.

## 1. *Introduction*

In this article we present some simple $p$-adic algorithms for computing with modular forms based upon the work of Katz, Coleman and Wan. The algorithms have the unusual property that their running time is polynomial in the $p$-adic precision and also grows linearly with the logarithm of the weight. Our methods rely upon the theory of overconvergent modular forms, but let us turn first to applications of these methods to classical modular forms.

### 1.1. *Classical modular forms*

Let $p$ be a prime number and $N$ be a positive integer coprime to $p$. Denote by $\mathbf{P}_k(t) \in \mathbb{Z}[t]$ the reverse characteristic polynomial of the Atkin operator $U_p$ acting upon the space $\mathbf{M}_k(Np, \mathbb{C})$ of classical modular forms of level $\Gamma_1(N) \cap \Gamma_0(p)$ and weight $k$. We show the following (see also Note 1.5).

Theorem 1.1. *There exists an explicit algorithm which takes as input positive integers $N, k$ and $m$ and a prime number $p \geqslant 5$ not dividing $N$ and gives as output the integer polynomial $\mathbf{P}_k(t)$ with coefficients modulo $p^m$ and runs in time polynomial in $N, p$ and $m$ and in time linear in* $\log(k)$.

For non-negative $\alpha \in \mathbb{Q}$ write $\mathbf{d}(k, \alpha)$ for the number of reciprocal roots of $\mathbf{P}_k(t)$ of $p$-adic valuation $\alpha$. (This is the dimension of a certain 'slope $\alpha$' subspace of the space of classical modular forms over the field of $p$-adic numbers [**21**, p. 450].) From Theorem 1.1 and a result of Wan [**21**, Lemma 3.1] one deduces the next result.

Theorem 1.2. *There exists an explicit algorithm which takes, as input, positive integers $N, k$ and $\beta$ and a prime number $p \geqslant 5$ not dividing $N$ and gives, as output, $\mathbf{d}(k, \alpha)$ for all $\alpha \leqslant \beta$, and runs in time polynomial in $N, p$ and $\beta$ and in time linear in* $\log(k)$.

The linear dependence on $\log(k)$ makes the algorithm well suited to studying experimentally the following conjecture of Gouvêa and Mazur on the variation of $\mathbf{d}(k, \alpha)$ as $k$ moves $p$-adically in a fixed residue class modulo $(p-1)$.

Received 18 March 2011.

*2000 Mathematics Subject Classification* 11G18 (primary), 11Y16, 11-04 (secondary).

The author is a Royal Society University Research Fellow. His work is supported in part by a grant from the European Research Council (204083).

CONJECTURE 1.3 (Gouvêa–Mazur). *If $k_0, k_1 \in \mathbb{Z}$ with $k_0, k_1 \geqslant 2\alpha + 2$ for some rational number $\alpha$ and $k_0 \equiv k_1 \bmod p^n(p-1)$ for some integer $n \geqslant \alpha$ then $\mathbf{d}(k_0, \alpha) = \mathbf{d}(k_1, \alpha)$.*

The above conjecture is difficult to investigate with classical algorithms since their time requirement grows as a polynomial function of the weight $k$.

To each eigenvalue $\lambda$ of $U_p$ on $\mathbf{M}_k(Np, \mathbb{C})$ one may associate a (generalised) eigenspace; that is, the union over positive integers $j$ of the kernel of $(U_p - \lambda)^j$. The elements in this space are called (generalised) eigenforms. An adaptation of the algorithm underlying Theorem 1.1 yields the following. (In this theorem we assume that the matrix $A_{i,s}^{u,v}(j)$ for the $U_p$ operator in § 2.3 is $p$-adically integral.)

THEOREM 1.4. *There exists an explicit algorithm with the following input, output and complexity. The input comprises positive integers $N, k$ and a prime $p \geqslant 5$ not dividing $N$, and, in addition, positive integers $m$ and $\nu$. The output is the image in $\mathbb{Z}[[q]]/(p^m, q^\nu)$ of a basis of (normalised) eigenforms for the $U_p$ operator acting upon $\mathbf{M}_k(Np, \mathbb{C})$ for all eigenvalues of valuation zero which have multiplicity one as a reciprocal root of $\mathbf{P}_k(t)$ modulo $p$. The algorithm runs in time polynomial in $N, p, m$ and $\nu$ and in time linear in $\log(k)$.*

The integrality assumption underlying this theorem implies that our main algorithms (Algorithms 1 and 2) compute an *integral* matrix $A$ for the $U_p$ operator (step (6)). Given that the latter is true (which the author has found in practice, cf. Note 3.1), and provided one is restricted to eigenvalues of slope zero which can be approximated by Newton lifting, various complications disappear. More generally, we sketch (without rigorous proofs) an algorithm which computes the image in $\mathbb{Z}[[q]]/(p^m, q^\nu)$ of a basis of eigenforms for any eigenvalue $\lambda \in \mathbb{Z}_p$ which can be approximated by Newton lifting and runs in time polynomial in $N, p, \mathrm{ord}_p(\lambda), m$ and $\nu$ and in time linear in $\log(k)$ (§ 3.4.2). The output of this latter algorithm is provably correct (we just do not prove that it always works).

The explicit relationship between the Atkin $U_p$ operator acting upon classical forms of weight $k$ and level $\Gamma_1(N) \cap \Gamma_0(p)$ and the Hecke $T_p$ operator acting upon classical forms of weight $k$ and level $\Gamma_1(N)$ is explained in [**12**, Section 4]. This allows one to deduce the same results for the latter case from our theorems above for the former. That is, one may replace '$U_p$ acting upon $\mathbf{M}_k(Np, \mathbb{C})$' by '$T_p$ acting upon $\mathbf{M}_k(N, \mathbb{C})$' and modify the statements of these theorems accordingly.

Our theorems for classical modular forms follow from analogous results for overconvergent modular forms along with the theorem of Coleman which tells us that overconvergent eigenforms of slope less than $k-1$ are classical modular forms [**5**].

NOTE 1.5. All complexity estimates are measured in bit operations, unless stated otherwise. We *assume* for all our theorems that there exists an algorithm which computes a basis of $q$-expansions in $\mathbb{Z}_p[[q]]$ modulo $(p^a, q^b)$ for the space $\mathbf{M}_k(N, \mathbb{Z}_p)$ (§ 2.1) of classical modular forms of level $N$ and weight $k$ in time polynomial in $a, b, N, k$ and $\log(p)$ (or $p$). (Our theorems transform such an algorithm into one for related problems which have running time linear in the logarithm of the weight.) For level $N = 1$ this can be done deterministically [**20**, Lemma 2.20], and so for level 1 all the algorithms in this paper are deterministic. For a general level, the author's own analysis suggests one can just use [**20**, Algorithms 5.11, 9.12] to compute a basis over the integers and reduce coefficients, cf. [**9**, pp. 1–2]. (These algorithms seem to require some randomisation, and the author does not know if there exist deterministic algorithms.) However, computing coefficients over the integers is not very good in practice and one really desires an algorithm which directly computes the coefficients modulo any desired power of $p$ (see also Notes 3.4 and 3.5).

Daqing Wan has observed that since $\mathbf{P}_k(t) \equiv \mathbf{P}_{k+(p-1)p^{m-1}}(t) \bmod p^m$, see [**21**, Lemma 2.4], one may restrict the input to $0 \leqslant k < (p-1)p^{m-1}$, and thus remove the dependence upon $k$

in all of our theorems. In practice, though, the time of one step of the algorithm does grow linearly with $\log(k)$ (step (4) of Algorithms 1 and 2), so we prefer the theorems as stated.

### 1.2. *Overconvergent modular forms*

Let $\mathbb{Q}_p$ denote the field of $p$-adic numbers and $\mathbb{Z}_p$ its ring of integers. Choose a finite extension $K$ of $\mathbb{Q}_p$ with ring of integers $B$ such that there exists $r \in B$ with $0 < \mathrm{ord}_p(r) < p/(p+1)$. The space $M_k(N, K, r)$ of $r$-overconvergent modular forms of level $N$ and weight $k$ is defined in § 2.1. It contains all classical modular forms of weight $k$ for $\Gamma_1(N) \cap \Gamma_0(p)$. Elements $f \in M_k(N, K, r)$ have $q$-expansions and the Atkin $U_p$ operator acts upon them in the usual manner, see (2.1). The characteristic series

$$P_k(t) := \det(1 - tU_p \mid M_k(N, K, r))$$

is a $p$-adically entire function lying in $1 + t\mathbb{Z}_p[[t]]$ which is independent of the auxiliary choice of $K$ and $r$. For each positive integer $m$ reducing the coefficients of this series modulo $p^m$, one obtains a polynomial, which we denote $P_k(t) \bmod p^m$. The central result of this paper is the following theorem.

THEOREM 1.6. *There exists an explicit algorithm which takes, as input, integers $N, k$, $m$ and a prime number $p \geqslant 5$ not dividing $N$ and gives, as output, $P_k(t) \bmod p^m$ and runs in time polynomial in $N, p$ and $m$ and in time linear in* $\log(k)$.

The algorithm underlying this theorem is given explicitly, for level $N = 1$ in Algorithm 1 and for a general level $N$ in Algorithm 2. In particular, for level 1 it is quite elementary and straightforward to implement.

For non-negative $\alpha \in \mathbb{Q}$, write $d(k, \alpha)$ for the number of reciprocal roots of $P_k(t)$ of $p$-adic valuation $\alpha$. As before we have the following two associated results. (The latter depends upon the same integrality assumption as Theorem 1.4, and again we explain how to proceed more generally in § 3.4.2.)

THEOREM 1.7. *There exists an explicit algorithm which takes, as input, integers $N, k$ and $\beta$ and a prime number $p \geqslant 5$ not dividing $N$ and gives, as output, $d(k, \alpha)$ for all $\alpha \leqslant \beta$ and runs in time polynomial in $N, p$ and $\beta$ and in time linear in* $\log(k)$.

THEOREM 1.8. *There exists an explicit algorithm with the following input, output and complexity. The input comprises integers $N$,$k$ and a prime $p \geqslant 5$ not dividing $N$, and, in addition, positive integers $m$ and $\nu$. The output is the image in $\mathbb{Z}[[q]]/(p^m, q^\nu)$ of a basis of (normalised) eigenforms for the $U_p$ operator acting upon $M_k(N, K, r)$ for all eigenvalues of valuation zero which have multiplicity one as a reciprocal root of $P_k(t)$ modulo $p$. The algorithm runs in time polynomial in $N, p, m$ and $\nu$ and in time linear in* $\log(k)$.

Let us now give a brief summary of results in the literature which are relevant to the work in this paper.

### 1.3. *The literature*

The Gouvêa–Mazur conjecture was made in [**12**, Conjecture 1], and was motivated mainly by experimental work for level 1 in collaboration with Mestre. Further numerical evidence strongly supporting the original conjecture was presented in [**11**] (see also the webpages of Gouvêa and Stein). An analogue of this conjecture for overconvergent modular forms was stated in [**13**, Conjecture 2], and is now known to imply the original conjecture by work of Coleman [**5**].

Coleman and Wan proved a version of the Gouvêa–Mazur conjecture in which the linear bound $n \geqslant \alpha$ is replaced by a bound with a quadratic function of $\alpha$ with coefficients depending upon $N$ and $p$; see [**6, 21**]. This is the strongest current result toward the conjecture. Buzzard defined the notion of a regular prime $p$ for each level $N$, and gave an algorithm which conjecturally gives as output the sequence of slopes ($p$-adic valuations of reciprocal roots of $\mathbf{P}_k(t)$) at different weights $k$ for a prime $p$ which is regular with respect to the level [**2**]. The smallest prime which is not regular in level 1 is $p = 59$, and Buzzard and Calegari found a counterexample to the conjecture in this case [**3**]. Namely, for $k_0 = 16$ and $k_1 = 16 + 58 \times 59$ we have $d(k_0, 1) = 1$ and $d(k_1, 1) > 1$ but $k_0 \equiv k_1 \bmod (p-1)p$. Note that this counterexample still leaves open the possibility that one can replace '$n \geqslant \alpha$' by '$n \geqslant \alpha + 1$', so there remains a large gap between what has been observed experimentally and the quadratic bound of Coleman and Wan.

The experimental work for computing slopes in [**3, 11, 12**] is based upon classical algorithms. These classical algorithms run in polynomial time in $p$, $m$ (and $N$, cf. Note 1.5) but exponential time in $\log(k)$. An algorithm for computing the characteristic series $P_k(t)$ modulo $p^m$ using a formula due to Koike is applied in [**7**]. This is useful for small $p$ and $m$ but has the drawback that the complexity grows exponentially with $m$. Methods for computing $P_k(t)$ modulo $p^m$ which have polynomial running time in $m$ are available for small primes ($p \leqslant 19$) in level 1 through work of Buzzard (unpublished), Loeffler [**18**] and Kilford [**17**]. (The algorithm based upon Koike's formula should run in linear time in $\log(k)$ and the methods for small primes in level 1 might also (suitably adapted), although these papers do not address this question.) The problem of computing eigenfunctions is discussed in [**14**], [**18**, Section 4] and [**17**, § 4.2]. A powerful general method for working with overconvergent modular forms has been developed by Pollack and Stevens, based upon overconvergent modular symbols, and used to compute approximations to $p$-adic $L$-functions in time polynomial in $m$; see [**19**] and, for certain efficient computations related to Stark–Heegner points, see [**8**]. (One can also compute invariants related to $p$-adic $L$-functions in some special cases with our methods, see § 3.4.4.) From the complexity analysis in [**8**, Proposition 2.14] it seems that the methods of Pollack and Stevens may be comparable to our own in terms at least of the running time dependence on $p$ and $m$, but the author is not sufficiently expert to make a clear comparison. In any case, our methods are completely different and we hope they will be a useful complement to those currently in the literature.

### 1.4. *The structure of the paper*

This paper is organised in a straightforward manner. The theory lying behind our results is described in Section 2, the algorithms themselves are presented and our theorems proved in Section 3, and we conclude with some illustrative examples in Section 4.

## 2. *Theory*

In this section we present the ideas underpinning out main algorithms (Algorithms 1 and 2) and consequently the proof of Theorem 1.6. We shall follow closely the notation and exposition of Wan [**21**].

### 2.1. *Katz expansions*

For each integer $k$ let $\mathbf{M}_k(N, \mathbb{Z}_p)$ denote the space of classical modular forms on $\Gamma_1(N)$ whose $q$-expansions at infinity have coefficients in $\mathbb{Z}_p$. This is a free $\mathbb{Z}_p$-module of finite rank. Let $E_{p-1}$ be the classical Eisenstein series of weight $p-1$ and level 1 normalised to have constant term 1. For each integer $i > 0$, Katz showed that one may choose a free $\mathbb{Z}_p$-module $\mathbf{W}_i(N, \mathbb{Z}_p)$ of $\mathbf{M}_{k+i(p-1)}(N, \mathbb{Z}_p)$ such that

$$\mathbf{M}_{k+i(p-1)}(N, \mathbb{Z}_p) = E_{p-1} \cdot \mathbf{M}_{k+(i-1)(p-1)}(N, \mathbb{Z}_p) \oplus \mathbf{W}_i(N, \mathbb{Z}_p).$$

(This choice is not canonical; see [15, p. 105].) Define $\mathbf{W}_0(N, \mathbb{Z}_p) := \mathbf{M}_k(N, \mathbb{Z}_p)$. Let $K$ be a finite extension of $\mathbb{Q}_p$ with ring of integers $B$. Define $\mathbf{W}_i(N, B) := \mathbf{W}_i(N, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} B$. For $r \in B$ the space $M_k(N, B, r)$ of $r$-overconvergent modular forms is by (our) definition the space of all 'Katz expansions' of the form

$$f = \sum_{i=0}^{\infty} r^i \frac{b_i}{E_{p-1}^i}, \quad b_i \in \mathbf{W}_i(N, B), \lim_{i\to\infty} b_i = 0$$

where $b_i \to 0$ as $i \to \infty$ means the $q$-expansions of $b_i$ are more and more divisible by $p$ as $i$ goes to infinity. We define $M_k(N, K, r) := M_k(N, B, r) \otimes_B K$, a $p$-adic Banach space.

### 2.2. *Atkin's operator and Coleman's trick*

One can write elements in $M_k(N, K, r)$ as $q$-expansions. (Note that $E_{p-1}$ has constant term 1 so $E_{p-1}^{-i}$ has a $q$-expansion in $1 + q\mathbb{Z}_p[[q]]$.) We define the action of Atkin's $U_p$ operator on $q$-expansions in the usual manner:

$$U_p : \sum_{n=0}^{\infty} a_n q^n \mapsto \sum_{n=0}^{\infty} a_{pn} q^n. \tag{2.1}$$

A crucial point which underlies the analysis by Wan is that

$$pU_p(M_k(N, B, r)) \subset M_k(N, B, r^p) \tag{2.2}$$

provided $0 < \mathrm{ord}_p(r) < 1/(p+1)$; see [21, Equation (2.6)]. Let us from now on assume that $0 < \mathrm{ord}_p(r) < p/(p+1)$ and so, in particular, since we have a natural injection

$$i : M_k(N, B, r^p) \hookrightarrow M_k(N, B, r),$$

the space $M_k(N, K, r)$ is stable under $U_p (= U_p \circ i)$. We define

$$P_k(t) := \det(1 - tU_p \mid M_k(N, K, r)),$$

a $p$-adic entire function with $p$-adically integral coefficients [21, p. 454, Lines 13–15].

Now write $k := k_0 + j(p-1)$ where $0 \leqslant k_0 < p-1$. Using Katz expansions one sees that the multiplication map

$$E_{p-1}^j : M_{k_0}(N, K, r) \to M_k(N, K, r)$$

is an isomorphism of $p$-adic Banach spaces. Since conjugate operators have the same characteristic series, it follows that

$$P_k(t) = P_{k_0+j(p-1)}(t) = \det(1 - tE_{p-1}^{-j} \circ U_p \circ E_{p-1}^j \mid M_{k_0}(N, K, r)).$$

The operator $U_p$ is Frobenius linear, so $E_{p-1}^{-j} \circ U_p = U_p \circ E_{p-1}^{-j}(q^p)$. Defining

$$G(q) := \frac{E_{p-1}(q)}{E_{p-1}(q^p)},$$

we see that

$$P_k(t) = \det(1 - tU_p \circ G(q)^j \mid M_{k_0}(N, B, r)).$$

We note that the fact that $G(q)$ is (a 1-unit) in the ring $M_0(N, B, r)$ provided $0 < \mathrm{ord}_p(r) < 1/(p+1)$ is key to the analysis of Wan [21, Lemma 2.1].

### 2.3. *Wan's analysis*

Let us now assume then that $0 < \mathrm{ord}_p(r) < 1/(p+1)$. Write $m_i$ for the rank of the free $B$-module $\mathbf{W}_i(N, B)$ and choose an (ordered) basis $\{b_{i,1}, \ldots, b_{i,m_i}\}$. Then the elements

$$e_{i,s} := \frac{r^i}{E_{p-1}^i} b_{i,s}, \quad i \geqslant 0, 1 \leqslant s \leqslant m_i$$

(ordered in the obvious manner), form an orthonormal basis for the $p$-adic Banach space $M_{k_0}(N, K, r)$. Write

$$U_p \circ G^j(e_{i,s}) = \sum_{u,v} A_{i,s}^{u,v}(j) e_{u,v}$$

where $A_{i,s}^{u,v}(j) \in K$. Since $G^j \in M(N, B, r)$, Wan easily deduces [**21**, p. 457], using (2.2),

$$\mathrm{ord}_p(A_{i,s}^{u,v}(j)) \geqslant u(p-1)\mathrm{ord}_p(r) - 1. \tag{2.3}$$

This is the final ingredient we shall need in our algorithm

### 2.4. *An outline of the algorithm*

With this theory in place the algorithm is quite straightforward. Using (2.3) one finds an appropriate subset of the basis of $M_{k_0}(N, B, r)$, depending on the required precision, and computes the action of $U_p \circ G(q)^j$ on the elements in this set using $q$-expansions and a fast exponentiation routine. The only non-trivial algorithmic problem which needs to be solved is for certain $i$ to compute a basis of $q$-expansions for the spaces $\mathbf{W}_i(N, B)$ modulo $(p^m, q^{\ell' p})$ for a suitable integer $\ell'$ which one must determine. When the level $N$ is 1, this is not difficult as the Miller basis [**20**, Lemma 2.20] allows one to determine the necessary $\ell'$ and directly compute the bases.

## 3. *Algorithms*

In this section we present explicitly the algorithm underlying the proof of Theorem 1.6. We consider first the case of level $N = 1$ since then the whole algorithm can be worked out and implemented using completely elementary methods.

### 3.1. *Preliminaries*

We shall use the notation $\mathcal{O}(\,\cdot\,)$ and $\tilde{\mathcal{O}}(\,\cdot\,)$ to measure the running time and space requirements of algorithms, usually in bit operations and bits of space, respectively, unless stated otherwise [**10**, § 25.7]. For $\alpha \in \mathbb{Q}$ we define $\lfloor \alpha \rfloor$ to be the greatest integer not greater than $\alpha$, and $\lceil \alpha \rceil$ to be the least integer not less than $\alpha$. By a 'row-reduced basis of $q$-expansions' of some space of modular forms over a ring, we shall mean a set of $q$-expansions (modulo some power of $q$) which when placed in a matrix are in row-reduced form over that ring. We shall of course not work with $q$-expansions in $\mathbb{Z}_p[[q]]$ exactly but rather with their images in the finite ring $\mathbb{Z}_p[[q]]/(p^a, q^b) \cong \mathbb{Z}[[q]]/(p^a, q^b)$ for different integers $a$ and $b$.

### 3.2. *Level* 1

We now present and give a detailed analysis of the algorithm underlying Theorem 1.6 for the case of level $N = 1$.

ALGORITHM 1. Given a prime number $p \geqslant 5$, an integer $k$ and a positive integer $m$, this algorithm computes the reverse characteristic series modulo $p^m$ of the Atkin $U_p$ operator (or of the operator $pU_p$) on the space of overconvergent $p$-adic modular forms of weight $k$ and level 1.

(1) *Dimensions.* Compute the unique $k_0, j \in \mathbb{Z}$ with $0 \leqslant k_0 < p-1$ and $k = k_0 + j(p-1)$. Compute $n := \lfloor ((p+1)/(p-1))(m+1) \rfloor$. For $i = 0, 1, \ldots, n$ compute $d_i$, the dimension of the space of classical modular forms of level 1 and weight $k_0 + i(p-1)$. Compute $m_i := d_i - d_{i-1}$, for $i \geqslant 1$, $m_0 := d_0$, and $\ell := m_0 + m_1 + \cdots + m_n = d_n$. Compute working precision $m' := m + \lceil n/(p+1) \rceil$.

(2) *Complementary spaces.* For each $0 \leqslant i \leqslant n$ denote by $M_{k_0+i(p-1)}$ a row-reduced basis of $q$-expansions in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$ of the space of classical modular forms of weight $k_0 + i(p-1)$ and level 1. Compute the last $m_i$ elements in $M_{k_0+i(p-1)}$ and call this ordered set $W_i$.

(3) *Katz expansions.* Compute the $q$-expansion in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$ of the Eisenstein series $E_{p-1}(q)$. For each $0 \leqslant i \leqslant n$, let $b_{i,1}, \ldots, b_{i,m_i}$ denote the elements in $W_i$. Compute $e_{i,s} := p^{\lfloor i/(p+1) \rfloor} E_{p-1}^{-i} b_{i,s}$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$.

(4) *Coleman's trick.* Define $G(q) := E_{p-1}(q)/E_{p-1}(q^p)$ and compute $G(q)^j$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$ using a fast exponentiation routine. For each $0 \leqslant i \leqslant n$ and $1 \leqslant s \leqslant m_i$ compute $u_{i,s} := G(q)^j e_{i,s}$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$.

(5) *Atkin operator.* For each $0 \leqslant i \leqslant n$ and $1 \leqslant s \leqslant m_i$ compute $t_{i,s} := U_p(u_{i,s})$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell})$, where $U_p$ is the Atkin operator on $q$-expansions.

(6) *Linear algebra.* Compute $T$, the $\ell \times \ell$ matrix over $\mathbb{Z}/(p^{m'})$ whose entries are the coefficients in the $q$-expansions modulo $q^\ell$ of the $\ell$ elements $t_{i,s}$. Compute $E$, the $\ell \times \ell$ upper-triangular matrix over $\mathbb{Z}/(p^{m'})$ whose entries are the coefficients in the $q$-expansions modulo $q^\ell$ of the $\ell$ elements $e_{i,s}$. Use linear algebra over $\mathbb{Z}/(p^{m'})$ to compute the matrix $A$ over $\mathbb{Z}/(p^{m'})$ such that $T = AE$. (One may need to multiply $T$ by $p$ and solve $pT = AE$.) Return $\det(1 - At) \bmod p^m$.

NOTE 3.1. The ambiguity over the output ($\det(1 - U_p t)$ or $\det(1 - pU_p t)$) arises since (2.3) only guarantees that the matrix for $pU_p$ has integral coefficients. However, in the author's experiments the matrix for $U_p$ always has integral coefficients, and in theory one can in any case deduce $\det(1 - U_p t) \bmod p^m$ from $\det(1 - pU_p t) \bmod p^{c(p)m}$ where $c(p)$ is an explicit polynomial function of $p$.

3.2.1. *Proof of correctness.* For each $i \geqslant 0$, let $d_i$ denote the dimension of $\mathbf{M}_{k_0+i(p-1)}(1, \mathbb{Z}_p)$ and $m_i$ that of $\mathbf{W}_i(1, \mathbb{Z}_p)$. Thus $d_0 = m_0$ and $d_i = m_i - m_{i-1}$ for $i \geqslant 1$. We first need a lemma.

LEMMA 3.2. *For $0 \leqslant i \leqslant n$ the elements in $W_i$ (step (2) of Algorithm 1) are the reduction modulo $(p^{m'}, q^{\ell p})$ of a basis for some choice of the space $\mathbf{W}_i(1, \mathbb{Z}_p)$.*

*Proof.* Let $M_{k_0+i(p-1)}$ denote the ordered set of elements in the row-reduced form of the basis modulo $(p^{m'}, q^{\ell p})$ in step (2). Then the $r$th element in $M_{k_0+i(p-1)}$ has lowest coefficient $q^{r-1}$; see [**20**, Remark 2.21]. Hence, since $E_{p-1}$ has lowest term 1, the ordered set

$$\{E_{p-1} f \mid f \in M_{k_0+(i-1)(p-1)}\}$$

is such that the $r$th element has lowest term $q^{r-1}$. The $m_i = d_i - d_{i-1}$ elements in the ordered set $W_i$ have leading term $q^{r-1}$ for $r > d_{i-1} = \#M_{k_0+(i-1)(p-1)}$. Thus no non-zero $\mathbb{Z}/(p^{m'})$-linear combination of them can be the reduction modulo $(p^{m'}, q^{\ell p})$ of an element in $E_{p-1} \cdot \mathbf{M}_{k_0+(i-1)(p-1)}(1, \mathbb{Z}_p)$. Hence they are the reduction modulo $(p^{m'}, q^{\ell p})$ of a basis for some choice of space $\mathbf{W}_i(1, \mathbb{Z}_p)$. □

Let us now prove the correctness of an idealised form of our algorithm in which one makes the following modifications. First, let us choose a rational number $\varepsilon > 0$ and define $n_\varepsilon := \lfloor (((p+1) + \varepsilon)/(p-1))(m+1) \rfloor$ and $\ell_\varepsilon := d_{n_\varepsilon}$, and replace $n$ and $\ell$ throughout the algorithm by $n_\varepsilon$ and $\ell_\varepsilon$. Second, choose an element $r$ in some extension $B$ of $\mathbb{Z}_p$ such that $\mathrm{ord}_p(r) = 1/((p+1) + \varepsilon)$ and in step (3) define $e_{i,s} := r^i E_{p-1}^{-i} b_{i,s}$. Third, assume that all computations are done exactly with elements in $B$ rather than in $B/(p^{m'})$. Then by Lemma 3.2 one observes that we have computed exactly the top $\ell_\varepsilon \times \ell_\varepsilon$ lefthand corner of the infinite matrix $(A_{i,s}^{u,v}(j))$ from § 2.3 for a particular choice of $r$ with $0 < \mathrm{ord}_p(r) < 1/(p+1)$. (Recall $(A_{i,s}^{u,v}(j))$ is the matrix for $U_p \circ G^j$ on our orthonormal basis and $\det(1 - U_p \circ G^j t)$ is the characteristic series of the $U_p$ operator on the space of overconvergent modular forms of level 1

and weight $k = k_0 + j(p-1)$.) From (2.3) one sees that for

$$u \geqslant \frac{(p+1)+\varepsilon}{p-1}(m+1)$$

the coefficients in the rows of $A_{i,s}^{u,v}(j)$ labelled by pairs $(u,v)$ $(1 \leqslant v \leqslant m_u)$ have $p$-adic valuation at least $m$. Now by (2.3) either the matrix $(A_{i,s}^{u,v}(j))$ has integral entries, or if not then $p(A_{i,s}^{u,v}(j))$ does. In the former case we see that this matrix reduces modulo $p^m$ to an $\ell_\varepsilon \times \infty$ matrix. Thus its characteristic series is equal modulo $p^m$ to the reverse characteristic polynomial of the $\ell_\varepsilon \times \ell_\varepsilon$ submatrix in the top lefthand corner. However, this is exactly what our idealised algorithm has computed. In the latter case, the same argument shows that our idealised algorithm outputs the characteristic series of $pU_p$ modulo $p^m$ acting on overconvergent modular forms of weight $k$.

Let us now deduce the correctness of Algorithm 1 from that of our idealised algorithm. First observe that the idealised algorithm would output correctly even performing computations in $B/(p^{m'})$ rather than $B$. (Note that over $K$ one can rewrite $T = AE$ as $A = TE^{-1}$ and since $E$ is upper-triangular one sees that the valuation of $E^{-1}$ at least $-n_\varepsilon/(p+1)$. Thus there is a loss of precision of $n_\varepsilon/(p+1) \leqslant \lceil n_\varepsilon/(p+1) \rceil = m' - m$ $p$-adic coefficients when solving this system. This accounts for the slightly higher working precision needed in the algorithm.) Next, let us choose $\varepsilon > 0$ small enough so that $n_\varepsilon = n$ and so $\ell_\varepsilon = \ell$. Then our idealised algorithm (revised to perform computations over $B/(p^{m'})$) only differs from Algorithm 1 in the choice of basis $e_{i,s}$ in step (3). Precisely, there is a diagonal change of basis matrix $P_\varepsilon$ with entries $\delta_{i,s} := r^i p^{-\lfloor i/(p+1) \rfloor}$ where $0 \leqslant \mathrm{ord}_p(\delta_{i,s}) < 1$ (shrinking $\varepsilon$ further if required). Let $\gamma := \max\{\mathrm{ord}_p \delta_{i,s}\} < 1$ be the maximum valuation of non-zero entries in $P_\varepsilon$. Let $A_\varepsilon$ denote the matrix computed in step (6) of the (revised) idealised algorithm and $A$ that computed by our actual algorithm, both with entries reduced modulo $p^m$. Then $A_\varepsilon \equiv P_\varepsilon^{-1} A P_\varepsilon \bmod p^{m-\gamma}$. Thus in the case in which $U_p$ acts by an integral matrix $A_{i,s}^{u,v}(j)$ we have

$$\det(1 - At) \equiv \det(1 - A_\varepsilon t) \equiv \det(1 - A_{i,s}^{u,v}(j)t) \mod p^m$$

since $m - \gamma > m - 1$. The same argument works when $A_{i,s}^{u,v}(j)$ has valuation $-1$ and one instead computes the characteristic series of $pU_p$ modulo $p^m$.

3.2.2. *Analysis of the complexity.* Let us first examine the space requirements of the algorithm. Observe that $n, m' \in \mathcal{O}(m)$ and so $\ell \in \mathcal{O}(pm)$ by the dimension formula [**20**, Corollary 2.16]. Thus $q$-expansions in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$ require $\mathcal{O}(p^2 m^2 \log(p))$ bits of space. We shall need $\mathcal{O}(\ell)$ such $q$-expansions ($b_{i,s}$, $e_{i,s}$ and $u_{i,s}$ for $0 \leqslant i \leqslant n$ and $1 \leqslant s \leqslant m_i$) and hence the main space requirement is $\mathcal{O}(p^3 m^3 \log(p))$ bits. (This absorbs the auxiliary space required for performing quasi-linear time multiplication in the ring $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$.) We shall of course need $\mathcal{O}(\log(k))$ bits of space for the integer $k$, giving a total space requirement of $\mathcal{O}(p^3 m^3 \log(p) + \log(k))$ bits. (Here and elsewhere for $k < 0$ by '$\log(k)$' we mean $\log(-k)$ and for $k = 0$ we just take '$\log(0)$' to mean 1.)

We now consider the running time of the different steps of the algorithm. Recall that one can multiply two elements in the ring $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$ in time $\tilde{\mathcal{O}}(mp\ell)$ bit operations using FFT-based methods [**1**, Section 3], and that for any finite ring $R$ and element $a \in R$ one can compute an integer power $a^j \in R$ within $2\log_2(j)$ ring multiplications [**10**, § 4.3].

(1) The formula for these dimensions is given in [**20**, Corollary 2.16].

(2) Computation of $q$-expansions in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$ for the whole row-reduced basis $M_{k_0+i(p-1)}$ of the space of modular forms of weight $k_0 + i(p-1)$ for each $i = 0, 1, \ldots, n$ is unnecessary, since one only requires the last $m_i$ elements of the basis in each case. The last $m_i$ elements in the basis can be computed directly by using the Miller basis (for cusp forms) described in [**20**, Lemma 2.20]. Each element in $W_i$ can then be computed in time $\tilde{\mathcal{O}}(\ell p \times m) = \tilde{\mathcal{O}}(p^2 m^2)$ bit operations, provided that one first precomputes the Eisenstein series $E_4(q)$ and $E_6(q)$ and also $\Delta(q)$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$. Ignoring the precomputation, this gives a total running time of $\mathcal{O}(p^2 m^2 \times \ell) = \mathcal{O}(p^3 m^3)$ bit operations. Precomputation of $E_4$, $E_6$ and $\Delta$ can certainly be done within this bound, even using naive algorithms. (Recall $\Delta = (E_4^3 - E_6^2)/1728$.)

(3) Computation of the Eisenstein series $E_{p-1}(q)$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{lp})$ can naively be done in $\tilde{\mathcal{O}}((\ell p)^{1/2} \times (\ell p) \times m) = \tilde{\mathcal{O}}(p^{3/2}m^{5/2})$ bit operations. One can then find all $e_{i,s}$ in time $\tilde{\mathcal{O}}(\ell \times m \times \ell p) = \tilde{\mathcal{O}}(p^3m^3)$ bit operations.

(4) Computation of $G(q)$ is straightforward and $G(q)^j$ can be found in $\mathcal{O}(\log(j)) = \mathcal{O}(\log(k))$ operations in the ring $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell p})$; that is, $\tilde{\mathcal{O}}(\ell p \times m \times \log(k)) = \tilde{\mathcal{O}}(p^2m^2\log(k))$ bit operations. One now finds all $u_{i,s}$ in $\tilde{\mathcal{O}}(p^3m^3)$ further bit operations.

(5) Computation of the Atkin operator on $q$-expansions is trivial.

(6) Since $E$ is in upper-triangular form the computation of $A$ is simple and can certainly be done in $\tilde{\mathcal{O}}(\ell^3 \times m) = \tilde{\mathcal{O}}(p^3m^4)$ bit operations. One can compute the reverse characteristic polynomial of $A$ in $\mathcal{O}(\ell^3) = \mathcal{O}(p^3m^3)$ operations in the ring $\mathbb{Z}/(p^{m'})$ using a classical algorithm based upon Hessenberg form [4, § 2.2.4]; that is, $\tilde{\mathcal{O}}(p^3m^4)$ bit operations.

In conclusion the algorithm requires $\tilde{\mathcal{O}}(p^3m^4 + p^2m^2\log(k))$ bit operations where the dependence upon $\log(k)$ (step (4)) is in fact linear rather than quasi-linear.

NOTE 3.3. In the author's experiments the most time consuming part was step (2). The matrix computations in step (6) were very fast; in particular, using Wan's bound [21, Lemma 3.1] one only needs to compute the initial few coefficients in $\det(1 - At) \bmod p^m$ since all the higher coefficients vanish, and this can be done naively by taking small powers of the matrix.

### 3.3. *Level N*

The main complications in level $N > 1$ are that one cannot write down a basis for the complementary spaces $\mathbf{W}_i(N, \mathbb{Z}_p)$ so easily, and one needs to do computations modulo $q^{\ell' p}$ where $\ell' \geqslant \ell$ is at least the Sturm bound [16, Theorems 3.13, 6.19] for the space $\mathbf{M}_{k_0+n(p-1)}(N, \mathbb{Z}_p)$ with, as before, $n := \lfloor((p+1)/(p-1))(m+1)\rfloor$. Although the algorithm is otherwise very similar, for clarity we shall write it out in full.

ALGORITHM 2. Given a positive integer $N$, a prime number $p \geqslant 5$ not dividing $N$, an integer $k$ and a positive integer $m$, this algorithm computes the reverse characteristic series modulo $p^m$ of the Atkin $U_p$ operator (or of the operator $pU_p$) on the space of overconvergent $p$-adic modular forms of weight $k$ and level $N$.

(1) *Dimensions.* Compute the unique $k_0, j \in \mathbb{Z}$ with $0 \leqslant k_0 < p-1$ and $k = k_0 + j(p-1)$. Compute $n := \lfloor((p+1)/(p-1))(m+1)\rfloor$. For $i = 0, 1, \ldots, n$ compute $d_i$, the dimension of the space of classical modular forms of level $N$ and weight $k_0 + i(p-1)$. Compute $m_i := d_i - d_{i-1}$, for $i \geqslant 1$, $m_0 := d_0$, and $\ell := m_0 + m_1 + \ldots + m_n = d_n$. Compute working precision $m' := m + \lceil n/(p+1)\rceil$. Compute $\ell' \geqslant \ell$, the Sturm bound for the space of classical modular forms of level $N$ and weight $k_0 + (p-1)n$.

(2) *Complementary spaces.* For each $0 \leqslant i \leqslant n$ compute $M_{k_0+i(p-1)}$, a row-reduced basis of $q$-expansions in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$ of the space of classical modular forms of weight $k_0 + i(p-1)$ and level $N$. Set $W_i := \emptyset$ and, for each $1 \leqslant w \leqslant d_i$, if the valuation (degree of lowest term) of the $w$th element in $M_{k_0+i(p-1)}$ does not occur as the valuation of an element in $M_{k_0+(i-1)(p-1)}$ then adjoin that element to $W_i$.

(3) *Katz expansions.* Compute the $q$-expansion in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$ of the Eisenstein series $E_{p-1}(q)$. For each $0 \leqslant i \leqslant n$, let $b_{i,1}, \ldots, b_{i,m_i}$ denote the elements in $W_i$. Compute $e_{i,s} := p^{\lfloor i/(p+1)\rfloor} E_{p-1}^{-i} b_{i,s}$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$.

(4) *Coleman's trick.* Define $G(q) := E_{p-1}(q)/E_{p-1}(q^p)$ and compute $G(q)^j$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$ using a fast exponentiation routine. For each $0 \leqslant i \leqslant n$ and $1 \leqslant s \leqslant m_i$, compute $u_{i,s} := G(q)^j e_{i,s}$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$.

(5) *Atkin operator.* For each $0 \leqslant i \leqslant n$ and $1 \leqslant s \leqslant m_i$ compute $t_{i,s} := U_p(u_{i,s})$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell'})$, where $U_p$ is the Atkin operator on $q$-expansions.

(6) *Linear algebra.*, Compute $T$, the $\ell \times \ell'$ matrix over $\mathbb{Z}/(p^{m'})$ whose entries are the coefficients in the $q$-expansions modulo $q^{\ell'}$ of the $\ell$ elements $t_{i,s}$. Compute $E$, the $\ell \times \ell'$ matrix over $\mathbb{Z}/(p^{m'})$ whose entries are the coefficients in the $q$-expansions modulo $q^{\ell'}$ of the $\ell$ elements $e_{i,s}$. Use linear algebra over $\mathbb{Z}/(p^{m'})$ to compute the matrix $A$ over $\mathbb{Z}/(p^{m'})$ such that $T = AE$. (One may need to multiply $T$ by $p$ and solve $pT = AE$.) Return $\det(1 - At) \bmod p^m$.

NOTE 3.4. In step (2) one could compute $M_{k_0+i(p-1)}$ by first computing $E_{p-1}m$ for all $m \in M_{k_0+(i-1)(p-1)}$ and then generating $m_i$ further elements in weight $k_0 + i(p-1)$ at random to (hopefully) complete the basis. It would be better still though to find a direct method of computing only the complementary space, as in Algorithm 1. Unfortunately, in the author's MAGMA implementation for level $N > 1$, the whole basis in weight $k_0 + i(p-1)$ is generated over $\mathbb{Z}$ for each $0 \leqslant i \leqslant n$ and then reduced modulo $p^{m'}$, making it practical for only small values of $N$, $p$ and $m$ (although $k$ can be large).

NOTE 3.5. The difficulty in using modular symbols methods to compute modular form expansions directly modulo $p^{m'}$ is that when the weight becomes larger than $p$ the space of Manin symbols [**20**, Theorem 8.4] computed modulo $p$ sometimes does not have the expected dimension, and then existing implementations fail. (This was pointed out to the author by Buzzard.) In Algorithm 2 one needs to compute up to weight approximately $mp$. Loeffler has suggested instead computing modular forms in small weight (with coefficients modulo $p^{m'}$) and then, using the ring structure, multiplying them together to generate the required modular forms in higher weight. One may also be able to construct the complementary spaces directly using such ideas. The author's preliminary implementation suggests this is a very promising approach for making the algorithm much more practical for a general level.

3.3.1. *Analysis of the algorithm.* As before, for each $i \geqslant 0$, let $d_i$ denote the dimension of $\mathbf{M}_{k_0+i(p-1)}(N, \mathbb{Z}_p)$ and $m_i$ that of $\mathbf{W}_i(N, \mathbb{Z}_p)$. Thus $d_0 = m_0$ and $d_i = m_i - m_{i-1}$ for $i \geqslant 1$.

LEMMA 3.6. *For $0 \leqslant i \leqslant n$, the elements in $W_i$ (step (2) of Algorithm 2) are the reduction modulo $(p^{m'}, q^{\ell' p})$ of a basis for some choice of the space $\mathbf{W}_i(N, \mathbb{Z}_p)$.*

*Proof.* Since $E_{p-1}(q)$ has constant term 1, working with a row-reduced form of bases one can identify a complementary space to $E_{p-1} \cdot \mathbf{M}_{k_0+(i-1)(p-1)}(N, \mathbb{Z}_p)$ in $\mathbf{M}_{k_0+i(p-1)}(N, \mathbb{Z}_p)$ simply by looking at the position of leading entries in the rows of the matrices corresponding to the bases $M_{k_0+(i-1)(p-1)}$ and $M_{k_0+i(p-1)}$. Note that the choice of $\ell'$ equal to the Sturm bound ensures that none of the rows in the matrix corresponding to a row-reduced basis for the space of classical modular forms of weight $k_0 + n(p-1)$ and level $N$ vanish when reduced as $q$-series modulo $q^{\ell'}$. Thus every element in our choice of space $\mathbf{W}_i(N, \mathbb{Z}_p)$ can be uniquely identified (modulo $p^{m'}$) via its image in the $\mathbb{Z}/(p^{m'})$-span of the elements in $W_i$. □

The proof of correctness now follows exactly the argument in § 3.2.1, using Lemma 3.6 in place of Lemma 3.2.

Regarding the complexity of the algorithm, observe that $\ell$ and $\ell'$ are polynomially bounded by $N, p$ and $m$, and one can compute $q$-expansions modulo $(p^{m'}, q^{\ell' p})$ of the basis $M_{k_0+i(p-1)}$ in time polynomial in $N, p$ and $m$ (by our assumption in Note 1.5). The complexity analysis then follows that for the case $N = 1$.

NOTE 3.7. For the sake of simplicity of presentation, the author has glossed over one minor point relating to the loss of precision in Algorithm 2. The working precision $m'$ is at least correct when the row-reduced form of a basis for the space of classical modular forms of level $N$ and weight $k_0 + n(p-1)$ has leading entries which are $p$-adic units. Otherwise, in

certain exceptional cases there may be a small additional (but computable) loss of precision in step (6) (the author does not know if these cases actually occur). For theoretical purposes, one can show using naive estimates on the size of the coefficients in a basis over $\mathbb{Z}$ for this space of modular forms that one can take $m'$ to equal $m$ plus an explicit polynomial function of $N, p$ and $m$, and then be sure that the output is correct modulo $p^m$.

### 3.4. *Deductions from Theorems 1.6*

We now explain how to deduce the remaining theorems in Section 1 from Theorem 1.6.

3.4.1. *Proof of Theorem 1.7.* We explain how to deduce Theorem 1.7 from Theorem 1.6. For each positive integer $m$, let $w(m)$ denote the point of intersection of the Wan polygon from [**21**, Lemma 3.1] with the line '$y = m$'. Choose $m$ sufficiently large that the gradient of the line segment joining the origin to the point $w(m)$ is greater than $\beta$. (Wan's polygon gives a quadratic lower bound on the Newton polygon $P_k(t)$ depending only upon $k_0 = k \bmod (p-1)$, and the coefficients in this quadratic lower bound are polynomial in $N$ and $p$. Thus $m$ is a polynomial in $N, p$ and $\beta$.) By Wan's analysis, all slopes of $P_k(t) \bmod p^m$ (thought of as an integer polynomial) which are less than $\beta$ must be slopes of $P_k(t)$ itself, and vice-versa. So one deduces Theorem 1.7 by applying Theorem 1.6 with this choice of $m$. (In actual computations a more careful comparison of the Newton polygon of the matrix $A$ computed in step (6) when lifted to $\mathbb{Z}_p$ and Wan's polygon allows one to provably compute more slopes of $P_k(t)$ itself.)

3.4.2. *Proof of Theorem 1.8.* Let us first outline the algorithm for constructing eigenforms (Theorem 1.8). One works throughout Algorithm 2 (or Algorithm 1) to the desired $q$-adic precision $\nu$ (at least $\ell'$) and computes 'eigenvalues' for the finite matrix $A$ (step (6)) and the $q$-expansions of their associated 'eigenvectors'. If $v \in \mathbb{Z}[[q]]/(p^m, q^\nu)$ is such an eigenvector for $U_p \circ G^j$ on overconvergent modular forms of weight $k_0$ then $E_{p-1}^j v \in \mathbb{Z}[[q]]/(p^m, q^\nu)$ is the desired eigenform for $U_p$ on overconvergent modular forms of weight $k$.

Two difficulties arise in practice. First, one may lose precision when computing the 'eigenvalues'. Second, the corresponding 'eigenspaces' may have additional irrelevant elements in them. These problems disappear under the assumption that the integral matrix $A$ (step (6)) is for the action of $U_p$ (rather than $pU_p$), and one restricts attention to eigenvalues of valuation zero which are simple reciprocal roots of $P_k(t) \bmod p$. For under these assumptions certainly one may compute the eigenvalues without losing precision. Assume then that $\lambda \in \mathbb{Z}/(p^m)$ with $\det(A - \lambda I) = 0$, and $\mathrm{ord}_p(\lambda) = 0$. Since $\lambda$ is a simple reciprocal root of $P_k(t) \bmod p$, we see that the matrix $(A - \lambda I) \bmod p$ has a kernel of dimension one. Moreover, we know that there exists some vector $v$ over $\mathbb{Z}/(p^m)$ which is non-zero modulo $p$ with $(A - \lambda I)v = 0$ (coming from the unique normalised eigenform we wish to approximate). The following simple lemma then guarantees that $\ker(A - \lambda I)$ is as expected.

LEMMA 3.8. *Let $M$ be a matrix over $\mathbb{Z}/(p^m)$ and denote its reduction modulo $p^j$ by $M_j$, for $1 \leqslant j \leqslant m$. Assume that $\ker(M_1)$ has dimension one and that there exists $v$ over $\mathbb{Z}/(p^m)$ which is non-zero modulo $p$ such that $Mv = 0$. Then $\ker(M)$ is free of rank one generated by $v$.*

*Proof.* We prove by induction on $j$ that $\ker(M_j)$ is free of rank one. That is, assume $w_j$ is over $\mathbb{Z}/(p^j)$ with $M_j w_j = 0$. We show $w_j \equiv \alpha_j v \bmod p^j$ for some $\alpha_j \in \mathbb{Z}/(p^j)$. This is true for $j = 1$. For $j > 1$ we have $M_{j-1} w_{j-1} = 0$ where $w_{j-1} := w_j \bmod p^{j-1}$. By induction $w_{j-1} \equiv \alpha_{j-1} v \bmod p^{j-1}$ for some $\alpha_{j-1}$, say defined over $\mathbb{Z}/(p^j)$. Then $p^{j-1}$ divides $w_j - \alpha_{j-1} v$ so writing $u$ for the quotient we have $M_1 u = 0 \bmod p$, since $M_j(w_j - \alpha_{j-1} v) \equiv 0 \bmod p^j$. As $\ker(M_1)$ has dimension one we have $u \equiv \beta v \bmod p$ for some $\beta \in \mathbb{Z}/(p)$. Thus $w_j \equiv (\alpha_{j-1} + p^{j-1}\beta)v \bmod p^j$, as required. □

This completes the proof of Theorem 1.8. We now explain how to proceed in general. Let us assume that we have correctly computed the matrix $A$ over $\mathbb{Z}/(p^m)$ and successfully used Newton lifting to obtain an 'eigenvalue' $\lambda \in \mathbb{Z}/(p^m)$ with $\mathrm{ord}_p(\lambda) = \alpha$, bearing in mind possible precision loss here. (Of course, the same method will work for eigenvalues lying in a finite extension of $\mathbb{Z}_p$.) That is, $\det(A - \lambda I) = 0$. We wish to find the elements in the kernel of the matrix $A - \lambda I$ which come from the reduction modulo $p^m$ of an eigenform. If $\alpha > 0$ then given any element $v \in \ker(A)$ we find that $(A - \lambda I)(p^{m-\alpha}v) = 0$. The kernel of $A$ is typically very large, so in this case $E_\lambda := \ker(A - \lambda I)$ will have many elements. However, if all the additional elements in $E_\lambda$ arise in the trivial way just described, then computing a generating set for $E_\lambda$ over $\mathbb{Z}/(p^m)$ and then reducing the entries in these vectors modulo $p^{m-\alpha}$ will leave only the 'true' eigenvectors. If we assume the dimension of the space of $\lambda$-eigenforms equals the multiplicity $r_\lambda$ of $\lambda$ as a root of $P_k(t) \bmod p^m$ then what we require is that *when one reduces the vectors in the generating set for $E_\lambda$ modulo $p^{m-\alpha}$ we are left with $r_\lambda$ distinct non-zero vectors.* Notice that given that our assumption is true, one must compute the matrix $A$ to precision $p^{m+\alpha}$ to determine the eigenforms for $\lambda$ modulo $p^m$.

The method in the above paragraph should also work when the matrix $A$ computed in step (6) is for the action of $pU_p$, although the author has not encountered this situation.

We conclude with the following observation. The ring $M(k, B, r)$ is stable under $pU_p \circ G^j$ provided $0 < \mathrm{ord}_p(r) < p/(p+1)$, by [**21**, Lemma 2.1, Equation (2.6)]. However, in our algorithm we use a 'step function' decay rate which approximates the case of $r$-overconvergence for $\mathrm{ord}_p(r) = 1/(p+1)$. Thus with respect to the basis we choose, the coefficient of $p^{\lfloor i/(p+1) \rfloor} E_{p-1}^{-i} b_{i,s}$ in our eigenform (normalised in such a way that at least one entry in the eigenvector is a $p$-adic unit) will have $p$-adic order at least $ip/(p+1) - \lfloor i/(p+1) \rfloor$, which is approximately $((p-1)/(p+1))i$. Since we take $0 \leqslant i \leqslant n$ with $n$ of size around $((p+1)/(p-1))(m+1)$ the coefficients in the 'true' eigenvector(s) for $A$ will decay linearly to around zero modulo $p^m$, making them rather easy to spot.

Note 3.9. Darmon has asked the author whether the methods in this paper can be used to compute the ordinary projection of a $p$-adic modular form. (The existing (heuristic) method for this is to iterate the Atkin $U_p$ operator on the $q$-expansion, but this requires an exponential number of terms in the $p$-adic precision desired.) The author can do this in certain examples, by applying the $U_p$ operator just once and solving a linear system (given that one has already computed $q$-expansions of all eigenforms of slope less than the required precision using our algorithm). However, the author's method (and the existing one) are complicated by the existence of congruences between eigenforms; in particular, one cannot assume (as one would like) that a cusp form with $p$-adically integral coefficients is a $p$-adically integral linearly combination of normalised eigenforms.

3.4.3. *Proof of Theorems 1.1, 1.2 and 1.4.* One deduces the results in § 1.1 from those in § 1.2 using Coleman's theorem that (generalised) overconvergent eigenforms of slope less than $k-1$ are classical [**5**]. Thus for $m \leqslant k-1$ we have $\mathbf{P}_k(t) \equiv P_k(t) \bmod p^m$ and for $\alpha < k-1$ we have $\mathbf{d}(k, \alpha) = d(k, \alpha)$; see [**21**, Lemma 2.3]. If one chooses $m \geqslant k-1$ then classical algorithms will compute the desired output in time polynomial in $N$, $p$ and $m$ for Theorem 1.1 and likewise for the other two results (recall here our assumption in Note 1.5).

3.4.4. *Invariants related to p-adic L-functions.* We now show how one can efficiently compute $(\partial/\partial k)P_k(t)$ for variable weight $k$ evaluated at $k := k_0$, and present an application of this to computing invariants associated to $p$-adic $L$-functions in certain special cases.

The derivative of $P_k(t)$ with respect to $k$ at the point $k := k_0$ equals

$$\lim_{m \to \infty} \frac{P_{k_0 + (p-1)p^m}(t) - P_{k_0}(t)}{(p-1)p^m}.$$

We may compute this using the following lemma.

LEMMA 3.10. *Letting* $s := (p-1)p^m$ *we have*

$$\frac{P_{k_0+s}(t) - P_{k_0}(t)}{s} \equiv \frac{P_{k_0+ps}(t) - P_{k_0}(t)}{ps} \mod p^{m+1}.$$

*Proof.* This is equivalent to

$$p(P_{k_0+s}(t) - P_{k_0}(t)) \equiv P_{k_0+ps}(t) - P_{k_0}(t) \mod p^{2m+2}.$$

We prove this using the congruences in [**13**, Section 3]. For arbitrary $k$ write $P_k(t) = \sum_{i=0}^{\infty} a_i(k)t^i$. To ease notation fix a choice of $0 \leqslant i < \infty$ and, omitting the subscript $i$, note that we need to show

$$p(a(k_0+s) - a(k_0)) \equiv a(k_0+ps) - a(k_0) \mod p^{2m+2}. \tag{3.1}$$

Define the difference functions $\delta_j(a, k_0)$ by

$$\begin{aligned} \delta_1(a, k_0) &:= a(k_0+s) - a(k_0) \\ \delta_j(a, k_0) &:= \delta_{j-1}(a, k_0+s) - \delta_{j-1}(a, k_0) \quad (j \geqslant 2). \end{aligned}$$

By [**13**, Theorem 2] we have $\delta_j(a, k_0) \equiv 0 \bmod p^{j(m+1)}$. We rewrite (3.1) as $a(k_0+ps) - pa(k_0+s) + (p-1)a(k_0) \equiv 0 \bmod p^{2m+2}$. Thus it suffices to show that $a(k_0+ps) - pa(k_0+s) + (p-1)a(k_0)$ is a $\mathbb{Z}$-linear combination of $\delta_j(a, k_0)$ for $j \geqslant 2$. Let $X$ be a variable and write $(X-1)^j = \sum_{\ell=0}^{j} \binom{j}{l}(-1)^{j-\ell}X^\ell$. Then one proves easily from its definition that $\delta_j(a, k_0) = \sum_{\ell=0}^{j} \binom{j}{l}(-1)^{j-\ell}a(k_0+\ell s)$. Hence we must equivalently prove that $X^p - pX + (p-1)$ is a $\mathbb{Z}$-linear combination of $(X-1)^j$ for $j \geqslant 2$. This follows since it vanishes to order two at $X = 1$. (Indeed, it vanishes to order $p$ modulo $p$ so one can replace $m+1$ by $m+2$ in the congruence in the lemma.) □

Since one can compute $P_{k_0+(p-1)p^m}(t) \bmod p^{2m+1}$ in time polynomial in $m$, by the above lemma we can find $(\partial/\partial k)P_k(t)|_{k:=k_0} \bmod p^m$ in time polynomial in $m$ (and $N$ and $p$, and in time linear in $\log(k_0)$).

Let us conclude by explaining how to compute invariants related to $p$-adic $L$-functions in certain cases (see Note 3.11) using a method due to Coleman, Stevens and Teitelbaum. We restrict to prime level $p$ so we can follow the exposition in [**7**, Section IV]. Let $f = \sum_n a_n q^n$ be a newform of level $p$ and weight $k_0$ which is split multiplicative at $p$, so $a_p(f) = p^{(k_0-2)/2}$. There is a $p$-adic invariant $\mathcal{L}_p(f)$ which according to [**7**, p. 155, Proposition] is equal to

$$-2a_p(f)\frac{(\partial/\partial k)P_k(t)}{(\partial/\partial t)P_k(t)} \tag{3.2}$$

evaluated at $k := k_0$ and $t := 1/a_p(f)$. Here $P_k(t)$ is the characteristic series of the $U_p$ operator on overconvergent modular forms of level 1 and (variable) weight $k$. Since derivation with respect to $t$ commutes with specialisation $k := k_0$ the denominator of (3.2) evaluates to $(\partial/\partial t)P_{k_0}(t)$ evaluated at $t := 1/a_p(f)$. Hence it can be computed using Algorithm 1. For the numerator, we compute the derivative of $P_k(t)$ with respect to $k$ at the point $k := k_0$ using the above method. Thus we can find $\mathcal{L}_p(f) \bmod p^m$ in time polynomial in $m$.

NOTE 3.11. This method for approximating $\mathcal{L}_p(f)$ is unfortunately limited to certain very special cases for the following reason. Except when there is a unique split multiplicative cusp form in level $p$ and weight $k_0$, the denominator (and hence the numerator) in (3.2) will vanish and so the equation is not useful for computing $\mathcal{L}_p(f)$. (For weight $k_0 := 2$ one should replace $P_k(t)$ by the characteristic series $Q_k(t)$ on overconvergent cusp forms (so $P_k(t) = (1-t)Q_k(t)$) to avoid the denominator vanishing even when there is a unique split multiplicative cusp form.)

However, we hope the fact that we can efficiently approximate $(\partial/\partial k)P_k(t)$ evaluated at $k := k_0$ may be of independent interest.

## 4. *Examples*

All computations were done using an implementation, in the MAGMA programming language, written by the author. We shall focus mainly on the case of level $N = 1$, since our present implementation for that case is much better than for $N > 1$, for the reasons explained in Note 3.4 (but see also Note 3.5).

### 4.1. *The Gouvêa–Mazur conjecture*

Let us first look at some examples illustrating Theorems 1.2 and 1.7. Primes $p < 59$ are regular [**2**, Definition 1.2] for level $N = 1$, and Buzzard has a conjectural recipe for the slopes of $P_k(t)$ (or $\mathbf{P}_k(t)$) in this situation; that is, the sequence of $p$-adic absolute values of the reciprocal roots. The author found experimentally that slopes sequences for these primes agree with this conjecture and the Gouvêa–Mazur conjecture. Here are some examples.

EXAMPLE 4.1. Let $p := 5$, $k := 0$ in level $N := 1$. Then the slope sequence for $P_k(t)$ begins

$$0, 1, 4, 5, 8, 9, 10, 13, 14, 19, 20, 21, 24, 25, 28, 29, 30, 35, 36, 39, 40, 41, 44, \ldots .$$

This agrees with the conjecture of Buzzard and the conjectural formula of Clay [**17**, Equation (4)].

EXAMPLE 4.2. Let $p := 23$, $k_1 := 100000$ and $k_2 := 100000 + (p - 1)$. Then the slope sequences for $P_k(t)$ begin

$$\begin{aligned} k_1 &: 0, 1, 1, 2, 2, 3, 3, 4, 4, 4, 4, 4, 5, 5, 6, 6, 7, 7, 9, 10, 10, 10, 11, 12, 12, 13, 13,\\ &\quad 15, 15, 16, 16, 16, 16, 16, 17, \ldots\\ k_2 &: 0, 1, 1, 2, 2, 3, 3, 4, 4, 4, 4, 4, 5, 5, 6, 6, 7, 7, 9, 10, 10, 10, 11, 12, 12, 13, 13,\\ &\quad 14, 14, 16, 16, 16, 16, 16, 17, \ldots . \end{aligned}$$

This agreement is similar to that observed in [**11**] for other examples, and is entirely mysterious.

Let us consider now the first irregular primes, $p = 59$ and 79.

EXAMPLE 4.3. Let $p := 59$ and $k_a := 16 + (p - 1)p^a$ for $1 \leqslant a \leqslant 7$ and $a = \infty$ with $k_\infty := 16$, in level $N = 1$. Write $\mathbf{7}_n$ for a sequence of $n$ sevens. One finds that the slope sequences for $P_k(t)$ appear to begin as follows (these sequences are not provably correct in their entirety, just experimentally observed):

$$\begin{aligned} k_\infty &: 0, 1, \mathbf{7}_{72}, 14, 15, 15, 15, 15, 16, 16, 16, 16, 16, 17, 17, \ldots\\ k_1 &: 0, 1, 1, 2, 2, 2, 3, 3, 3, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, \mathbf{7}_{24},\\ &\quad 8, 8, 8, 8, 8, 9, 9, 9, 9, 9, 10, 10, 10, 10, 11, 11, 11, 11, 11, 11,\\ &\quad 12, 12, 12, 13, 14, 15, 15, 15, 15, 16, 16, 16, 16, 16, 17, 17, \ldots\\ k_2 &: 0, 1, 2, 3, 3, 3, 4, 4, 4, 4, 4, 5, 5, 5, 5, 6, 6, 6, 6, 6, \mathbf{7}_{34},\\ &\quad 8, 8, 8, 8, 8, 9, 9, 9, 9, 10, 10, 10, 10, 10, 10, 11, 11, 11, 12, 14\\ &\quad 15, 15, 15, 15, 16, 16, 16, 16, 16, 17, 17, \ldots\\ k_3 &: 0, 1, 3, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, \mathbf{7}_{44}, 8, 8, 8, 8, 9, 9, 9, 9, 9, 9\\ &\quad 10, 10, 10, 11, 14, 15, 15, 15, 15, 16, 16, 16, 16, 16, 17, 17, \ldots\\ k_4 &: 0, 1, 4, 5, 5, 5, 6, 6, 6, 6, 6, 6, \mathbf{7}_{52}, 8, 8, 8, 8, 8, 8, 9, 9, 9, 10,\\ &\quad 14, 15, 15, 15, 15, 16, 16, 16, 16, 16, 17, 17, \ldots\\ k_5 &: 0, 1, 5, 6, 6, 6, \mathbf{7}_{64}, 8, 8, 8, 9, 14, 15, 15, 15, 15, 16, 16, 16, 16, 16, 17, 17, \ldots\\ k_6 &: 0, 1, 6, \mathbf{7}_{70}, 8, 14, 15, 15, 15, 15, 16, 16, 16, 16, 16, 17, 17, \ldots\\ k_7 &: 0, 1, \mathbf{7}_{72}, 14, 15, 15, 15, 15, 16, 16, 16, 16, 16, 17, 17, \ldots . \end{aligned}$$

The case $k_\infty$ and $k_1$ is exactly the counterexample of Buzzard and Calegari [3]. In fact, comparing each $k_a$, $(1 \leqslant a \leqslant 6)$ to $k_\infty$ gives us a counterexample to the Gouvêa–Mazur conjecture, but not to a weaker conjecture where one replaces '$n \geqslant \alpha$' by '$n \geqslant \alpha + 1$'. The symmetry in the sequence for $k_\infty$ around the run of sevens is predicted by the theory of twin eigenforms [11], but the symmetries in the other sequences are not understood by the author.

A similar picture emerges for $p := 79$ when $k_a := 38 + (p-1)p^a$ for $a = \infty, 1, 2$. We find $\mathbf{d}(38, 1) = 1$ but $\mathbf{d}(38 + (p-1)p, 1) = 2$, and $\mathbf{d}(38 + (p-1)p^2, 1) = 1$ but $\mathbf{d}(38 + (p-1)p^2, 2) = 1 \neq 0 = \mathbf{d}(38, 2)$.

Thus our initial experiments for $N = 1$ support Buzzard's conjectures for regular primes and a slight weakening of the Gouvêa–Mazur conjecture in general.

### 4.2. *Hecke polynomials and eigenforms*

Let us now consider some examples illustrating Theorems 1.1, 1.4, 1.6 and 1.8. We recall that our conclusions for classical modular forms follow from those for overconvergent modular forms (and vice versa) by the theorem of Coleman that overconvergent eigenforms of small slopes are classical [5].

We first look at some small examples where the output of our algorithm can be compared directly with that from existing Magma programs. In these examples we remove the trivial factors coming from the Eisenstein subspaces and work with classical and overconvergent cusp forms.

Example 4.4. Let $p := 5$, $k := 4$ and $N := 1$. The space $\mathbf{S}_k(p, \mathbb{C})$ of cusp forms of level $p$ and weight $k$ has dimension one and is spanned by the form

$$f_\lambda = q - 4q^2 + 2q^3 + 8q^4 - 5q^5 - 8q^6 + 6q^7 - 23q^9 + 20q^{10} + 32q^{11} + \dots.$$

This is an eigenform for $U_p$ acting on $\mathbf{S}_k(p, \mathbb{C})$ with eigenvalue $\lambda = -5$. If one computes $P_k(t)$ (modulo $p^5$, say) one discovers $-5$ is a reciprocal root and the above form is also an eigenform for $U_p$ acting upon overconvergent modular forms of weight 4 and level 1, within the precision of the computation.

Example 4.5. Let $p := 13$, $k := 24$ and $N := 1$. Then $\mathbf{S}_k(p, \mathbb{C})$ has dimension 27. Write $\mathbf{Q}_k(t)$ for the reverse characteristic polynomial of $U_p$ acting on $\mathbf{S}_k(p, \mathbb{C})$, and $Q_k(t)$ for the characteristic series of $U_p$ acting on the space of overconvergent cusp forms of weight $k$ and level 1 (so $P_k(t) = (1-t)Q_k(t)$). One checks that $\mathbf{Q}_k(t) \equiv Q_k(t) \bmod p^{k-1}$. Moreover, there is a unique slope zero eigenvalue $\lambda \in \mathbb{Z}_p$ of $U_p$ on overconvergent cusp forms, and we compute $\lambda \equiv -5417682171 \bmod p^{10}$ and that the corresponding eigenform $f_\lambda$ satisfies

$$\begin{aligned} f_\lambda \equiv\ & q + 11497121859q^2 - 427686176q^3 + 9639421438q^4 - 42119324604q^5 \\ & + 4033205146q^6 + 34959083328q^7 - 6918687549q^8 + 36824348083q^9 \\ & - 68609559472q^{10} - 17625583781q^{11} + 14252847841q^{12} - 5417682171q^{13} \\ & + 3056148420q^{14} + \dots + 15384475756q^{168} \mod (p^{10}, q^{169}). \end{aligned}$$

As expected, this is an eigenform of weight $k$ for the Hecke operators $T_\ell$ (prime $\ell \neq p$), within the precision of the computation. By Coleman's theorem, $f_\lambda \in \mathbf{S}_k(p, \mathbb{C})$. One checks the eigenvalues $\lambda_\ell$ computed for $T_\ell$ are indeed eigenvalues for the Hecke operator $T_\ell$ on $\mathbf{S}_k(p, \mathbb{C})$ modulo $p^{10}$. Similarly, there is a unique slope-one eigenvalue $\mu \in \mathbb{Z}_p$, and we find $\mu \equiv -29944734937 \bmod p^{10}$ and that the corresponding eigenform $f_\mu$ satisfies

$$\begin{aligned} f_\mu \equiv\ & q - 11497120779q^2 + 428025656q^3 - 9614094782q^4 + 42192393624q^5 \\ & - 42141698202q^6 - \dots + 45068609300q^{168} \mod (p^{10}, q^{169}). \end{aligned}$$

Again, one checks this is a Hecke eigenform of weight $k$, within the precision of the computation, and by Coleman's theorem $f_\mu \in \mathbf{S}_k(p, \mathbb{C})$. Finally, one checks that these two eigenforms $f_\lambda$ and $f_\mu$ are congruent modulo $p^{10}$ to the (normalised) eigenforms of slope zero and one, respectively, for the $T_p$ operator acting on the two-dimensional space $\mathbf{S}_k(1, \mathbb{C})$, as predicted (modulo $p^{k-1}$ and modulo $p^{k-2}$, respectively, in fact) in [**12**, Section 4].

EXAMPLE 4.6. Let $p := 5$, $k := 8$ and level $N := 4$. Write $\mathbf{Q}_k(t)$ for the reverse characteristic polynomial of $U_p$ acting on $\mathbf{S}_k(\Gamma_0(pN), \mathbb{C})$. (Note that here, and in Algorithm 2, we replace $\Gamma_1(N)$ by $\Gamma_0(N)$ since MAGMA can compute with $\Gamma_0(pN)$ but not $\Gamma_0(p) \cap \Gamma_1(N)$.) Let $Q_k(t)$ denote the characteristic series of $U_p$ acting on the space of overconvergent cusp forms of weight $k$ for $\Gamma_0(N)$ (so $P_k(t) = (1-t)^3 Q_k(t)$). Then one finds

$$Q_k(t) \equiv \mathbf{Q}_k(t) \equiv 1 + 420t + 12850t^2 \mod p^{k-1},$$

as predicted by Coleman.

We conclude with a few slightly larger examples.

EXAMPLE 4.7. For $p := 31$, $k := 20000$ and $N := 1$ we find that there is an eigenform $f_\lambda$ for the $U_p$ operator on overconvergent cusp forms with slopes zero eigenvalue $\lambda \equiv 386999 \bmod 31^4$ and

$$\begin{aligned} f_\lambda \equiv q &- 426011q^2 - 354487q^3 - 225553q^4 - 444281q^5 + 283916q^6 - 58349q^7 - 308209q^8 \\ &- 308892q^9 + 352309q^{10} - 108755q^{11} - 71306q^{12} + 69802q^{13} - 175397q^{14} \\ &+ 108633q^{15} - 149157q^{16} - 12105q^{17} - 193957q^{18} + 353356q^{19} + 419246q^{20} \\ &- 137874q^{21} - 375223q^{22} + 268222q^{23} - 144601q^{24} - 286014q^{25} + 32857q^{26} \\ &+ 279753q^{27} - 305774q^{28} - 157214q^{29} - 292132q^{30} + 386999q^{31} + \ldots \mod (p^4, q^{434}). \end{aligned}$$

It is an eigenform of weight $k$ for the Hecke operator $T_\ell$ (for prime $\ell \neq p$), within the precision of the computation. By Coleman's theorem, $f_\lambda$ is a classical eigenform of level $p$ and weight $k$ and it is congruent modulo $p^{k-1}$ to a classical eigenform of level 1 and weight $k$.

EXAMPLE 4.8. For $p := 7$, $k := 3141592654$ and $N := 1$, the slope sequence for the $U_p$ operator on overconvergent cusp forms begins $1, 3, 4, 6, 7, \ldots$ and thus there are unique cuspidal eigenforms $f_{\lambda_1}, f_{\lambda_3}$ and $f_{\lambda_4}$ of slopes $1, 3$ and $4$, respectively. We compute the eigenvalues to be $\lambda_1 \equiv -24525190293240 \bmod 7^{17}$, $\lambda_3 \equiv 112276712302636 \bmod 7^{17}$ and $\lambda_4 \equiv -112303394072667 \bmod 7^{17}$ and the eigenforms to be

$$\begin{aligned} f_{\lambda_1} &\equiv q + 62446499273038q^2 + 67809209427118q^3 + \ldots \\ f_{\lambda_3} &\equiv q - 114643186896404q^2 + 108422174471877q^3 + \ldots \\ f_{\lambda_4} &\equiv q + 11716060772632q^2 - 86506782486717q^3 + \ldots \end{aligned}$$

modulo $(7^{17}, q^{100})$. They are, as expected, eigenforms of weight $k$ for the Hecke operator $T_\ell$ (for prime $\ell \neq p$), within the precision of the computation, which, by Coleman's theorem, are classical.

EXAMPLE 4.9. For $p := 23$, $k := 1234728$ and $N := 1$, we find that there is an eigenform $f_\lambda$ for the $U_p$ operator on overconvergent cusp forms with slopes zero eigenvalue $\lambda \equiv 11639528745283 \bmod 23^{10}$. The author computed the eigenvalues of $T_\ell$ (prime $\ell \neq p$) on this eigenform for $\ell < 529$, each modulo $23^{10}$. By Coleman's theorem, $f_\lambda$ is a classical eigenform of level $p$ and weight $k$ and it is congruent modulo $p^{k-1}$ to a classical eigenform of level 1 and weight $k$.

EXAMPLE 4.10. For $p := 41$, $k := 0$ and $N := 1$ we find there is a unique cuspidal overconvergent eigenform $f_\lambda$ with slope zero eigenvalue $\lambda \in \mathbb{Z}_p$ (and in addition two further cuspidal eigenforms of slope zero defined over a quadratic extension of $\mathbb{Z}_p$). We compute $\lambda \equiv -88357391431 \bmod 41^7$ and

$$f_\lambda \equiv q + 17353260525q^2 + 3857679517q^3 + 44173066834q^4 + \dots$$

modulo $(41^7, q^{1107})$. We check it is a (non-classical) eigenform of weight $k$ for the Hecke operator $T_\ell$ (for prime $\ell \neq p$), within the precision of the computation.

The experiments were carried out on a 2.60 GHz machine with 64 GB RAM. The computations for Example 4.3 took over one day for each choice of $k_a$ (and up to around 500 MB of RAM), Example 4.2 took about 4 hours for each $k_i$, Examples 4.6 and 4.9 took around one minute, and Example 4.10 about five minutes. The remaining examples took a matter of seconds to compute.

*Acknowledgements.* The author would like to thank the following people: Kevin Buzzard for sharing his expertise and enthusiasm without stint; David Loeffler for his idea on how to make the algorithm more practical in general level; Denis Charles, John Cremona and William Stein for helpful communications on the complexity of computing with classical modular forms; Henri Darmon and Robert Pollack for their keen interest and stimulating questions (and patient answers); the anonymous referee and the editors; and Daqing Wan for introducing the author to this topic and many others. It is a pleasure to dedicate this paper to Daqing Wan, a generous and inspiring mathematician.

## *References*

**1.** D. BERNSTEIN, 'Fast multiplication and its applications', *Algorithmic number theory: lattices, number fields, curves and cryptography*, Mathematical Sciences Research Institute Publications 44 (eds J. P. Buhler and P. Stevenhagen; Cambridge University Press, Cambridge, 2008) 325–384.
**2.** K. BUZZARD, 'Questions about slopes of modular forms', *Astérique* 298 (2005) 1–15.
**3.** K. BUZZARD and F. CALEGARI, 'A counterexample to the Gouvéa–Mazur conjecture', *C. R. Math. Acad. Sci. Paris* 338 (2004) no. 10, 751–753.
**4.** H. COHEN, *A course in computational algebraic number theory*, Graduate Texts in Mathematics 138 (Springer, Berlin, 1993).
**5.** R. COLEMAN, 'Classical and overconvergent modular forms', *Invent. Math.* 124 (1996) 215–241.
**6.** R. COLEMAN, '$p$-adic Banach spaces and families of modular forms', *Invent. Math.* 127 (1997) 417–479.
**7.** R. COLEMAN, G. STEVENS and J. TEITELBAUM, 'Numerical experiments on families of $p$-adic modular forms', *Computational perspectives on number theory*, AMS/IP Studies in Advanced Mathematics 7 (American Mathematical Society, Providence, RI, 1998) 143–158.
**8.** H. DARMON and R. POLLACK, 'Efficient calculation of Stark–Heegner points via overconvergent modular symbols', *Israel J. Math.* 153 (2006) 319–354.
**9.** B. EDIXHOVEN, 'Introduction, main results, context', *Computational aspects of modular forms and galois representations*, Annals of Mathematics Studies 176 (eds J.-M. Couveignes and B. Edixhoven; Princeton University Press, Princeton, NJ, 2011).
**10.** J. VON ZUR GATHEN and J. GERHARD, *Modern computer algebra* (Cambridge University Press, Cambridge, 1999).
**11.** F. GOUVÊA, 'Where the slopes are', *J. Ramanujan Math. Soc.* 16 (2001) no. 1, 75–99.
**12.** F. GOUVÊA and B. MAZUR, 'Families of modular eigenforms', *Math. Comp.* 58 (1992) no. 198, 793–805.
**13.** F. GOUVÊA and B. MAZUR, 'On the characteristic power series of the $U$ operator', *Ann. Inst. Fourier (Grenoble)* 43 (1993) no. 2, 301–312.
**14.** F. GOUVÊA and B. MAZUR, 'Searching for $p$-adic eigenfunctions', *Math. Res. Lett.* 2 (1995) 515–536.
**15.** N. M. KATZ, '$p$-adic properties of modular schemes and modular forms', *Modular forms in one variable III*, Lecture Notes in Mathematics 350 (eds P. Deligne and W. Kuyk; Springer, New York, 1973) 69–190.
**16.** L. KILFORD, *Modular forms: a classical and computational introduction* (Imperial College Press, London, 2008).
**17.** L. KILFORD, 'On the $U_p$ operator acting on $p$-adic overconvergent modular forms when $X_0(p)$ has genus 1', *J. Number Theory* 130 (2010) 586–594.
**18.** D. LOEFFLER, 'Spectral expansions of overconvergent modular functions', *Int. Math. Res. Not. IMRN* 2007 (2007) doi:10.1093/imrn/rnm050.

**19.** R. Pollack and G. Stevens, "Overconvergent modular symbols and $p$-adic $L$-functions',', *Ann. Sci. Éc. Norm. Supér.* (4) 44 (2011) 1–42.
**20.** W. Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics 79 (American Mathematical Society, Providence, RI, 2007).
**21.** D. Wan, 'Dimension variation of classical and $p$-adic modular forms', *Invent. Math.* 133 (1998) 449–463.

*Alan G. B. Lauder*
*Mathematical Institute*
*24-29 St Giles, Oxford*
*United Kingdom*

lauder@maths.ox.ac.uk