COMPUTING COEFFICIENTS OF MODULAR FORMS

by

Peter Bruin

Abstract. — We prove that coefficients of q-expansions of modular forms can be computed in polynomial time under certain assumptions, the most important of which is the Riemann hypothesis for ζ-functions of number fields. We give applications to computing Hecke operators, counting points on modular curves over finite fields, and computing the number of representations of an integer as a sum of a given number of squares.

***Résumé* (Sur le calcul des coefficients des formes modulaires).** — On démontre que les coefficients des q-développements des formes modulaires peuvent être calculés en temps polynomial sous certaines conditions, dont la plus importante est l'hypothèse de Riemann pour les fonctions ζ des corps de nombres. On donne des applications aux problèmes suivants : calculer des opérateurs de Hecke ; compter le nombre de points d'une courbe modulaire sur un corps fini ; calculer le nombre de représentations d'un entier comme somme d'un nombre donné de carrés.

1. Introduction

Let n and k be positive integers, and let $\mathrm{M}_k(\Gamma_1(n))$ be the complex vector space of modular forms of weight k for the group $\Gamma_1(n)$. A modular form $f \in \mathrm{M}_k(\Gamma_1(n))$ is determined by n, k and its q-expansion coefficients $a_m(f)$ for $0 \leq m \leq k \cdot d(\Gamma_1(n))$, where $d(\Gamma_1(n))$ is a function growing roughly quadratically in n.

A natural question to ask is whether, given $a_m(f)$ for $0 \leq m \leq k \cdot d(\Gamma_1(n))$, one can efficiently compute $a_m(f)$ for large m. In the case $n = 1$, Couveignes, Edixhoven et al. [**2**] described a deterministic algorithm that accomplishes this in time polynomial in $\log m$ for fixed k. Under the generalised Riemann hypothesis, their algorithm runs in time polynomial in k and $\log m$. Earlier algorithms, based on modular symbols, require time polynomial in m. The

2000 ***Mathematics Subject Classification.*** — 11E25, 11F11, 11F30, 11F80, 11Y16.
Key words and phrases. — Algorithms, Hecke algebras, modular forms, sums of squares.

The results of this article are based on those of my thesis [**1**]. I am much indebted to my advisors Bas Edixhoven and Robin de Jong for their support. I would also like to thank the organisers of the conference *Théorie des nombres et applications* for the opportunity to speak about this subject, which has led to this article.
The research for this article was supported by the Netherlands Organisation for Scientific Research.

method of [**2**] is, very briefly, to compute two-dimensional Galois representations associated to eigenforms of level 1 over finite fields.
In this article, results from the author's thesis [**1**] on computing Galois representations associated to eigenforms of higher levels are used to generalise the result of Couveignes, Edixhoven et al., be it that we can currently only give a probabilistic algorithm. The precise result from [**1**] that we need is Theorem 3.1 below. We will use this to prove our main result, which reads as follows.

Theorem 1.1. — *Let n_0 be a positive integer. There exists a probabilistic algorithm that, given*

- *a positive integer k,*
- *a squarefree positive integer n_1 coprime to n_0,*
- *a number field K,*
- *a modular form f of weight k for $\Gamma_1(n)$ over K, where $n = n_0 n_1$, and*
- *a positive integer m in factored form,*

computes $a_m(f)$, and whose expected running time is bounded by a polynomial in the length of the input under the Riemann hypothesis for ζ-functions of number fields.

Let us make precise how the number field K and the form f should be given to the algorithm and how it returns $a_m(f)$. We represent K by its multiplication table with respect to some $\mathbf{Q}$-basis $(b_1, \ldots, b_r)$ of K. By this we mean the rational numbers $c_{i,j,k}$ with $1 \leq i, j, k \leq r$ such that

$$b_i b_j = \sum_{k=1}^{r} c_{i,j,k} b_k.$$

We represent elements of K as $\mathbf{Q}$-linear combinations of $(b_1, \ldots, b_r)$. We represent f by its coefficients $a_0(f)$, …, $a_{k \cdot d(\Gamma_1(n))}(f)$; these, as well as the output $a_m(f)$, are elements of K.
We should also make precise what the word 'probabilistic' in Theorem 1.1 means. The correct interpretation is that the result is guaranteed to be correct, but that the running time depends on random choices made during execution. Probabilistic algorithms with this property are commonly called *Las Vegas* algorithms. These are to be contrasted with *Monte Carlo* algorithms, where the randomness influences the correctness of the output instead of the running time. It is worth emphasising that the expected running time is defined by averaging *only* over the random choices made during execution, *not* over the possible inputs. For any input x, the actual running time of the algorithm given this input can be modelled as a random variable T_x. The claim that the expected running time is polynomial in the length of the input means that there exists a polynomial P such that for any input x, the expectation of T_x is at most $P(\text{length of } x)$. We refer to Lenstra and Pomerance [**10**, § 12] for an enlightening discussion of probabilistic algorithms.

Remark 1.2. — The length of the input depends not only on k, n_0, n_1, $\log m$ and K, but also on the complexity of the given coefficients of the modular form f. For example, if f is a primitive form f_0 multiplied by an integer A, then for fixed f_0 and A tending to ∞, the length

of the input increases approximately by a multiple of $\log A$, and the running time increases approximately by a polynomial in $\log A$.

Remark 1.3. — Without the generalised Riemann hypothesis, we are only able to prove that the running time of our algorithm is polynomial in $\exp(n_1)$, $\exp(k)$ and the length of the input. In other words, we are still able to prove unconditionally that if not only n_0, but also n_1 and k are fixed, then the expected running time is polynomial in the length of the input.

Remark 1.4. — Omitting the condition that m be given in factored form would be equivalent to claiming that integers that are products of two prime numbers can be factored in polynomial time. Namely, suppose that the theorem holds without this condition. Applying the hypothetical stronger version of the theorem with

- k a fixed even integer greater than 2,
- $n_0 = n_1 = 1$,
- $K = \mathbf{Q}$,
- $f = E_k$, the classical Eisenstein series E_k of weight k for $\Gamma_1(1) = \mathrm{SL}_2(\mathbf{Z})$, and
- $m = pq$, where p and q are two distinct prime numbers,

we conclude that there exists a probabilistic algorithm that computes $a_m(E_k)$ in time polynomial in $\log m$. From the formula

$$\begin{aligned} a_m(E_k) &= \sum_{d|m} d^{k-1} \\ &= 1 + p^{k-1} + q^{k-1} + m^{k-1}, \end{aligned}$$

it follows that $\{p^{k-1}, q^{k-1}\}$ can be computed quickly as the set of roots of the polynomial $x^2 - (a_m(E_k) - m^{k-1} - 1)x + m^{k-1} \in \mathbf{Z}[x]$. Hence we would be able to compute $\{p, q\}$ from m in time polynomial in $\log m$, which is a claim we certainly do not wish to make.

Remark 1.5. — The reason why our algorithm is probabilistic is that this is the current state of affairs for the algorithm to which Theorem 3.1 refers. This algorithm can perhaps be turned into a deterministic one by replacing the arithmetic over finite fields that is used in [**1**] by approximate arithmetic over the complex numbers. The latter approach is taken by Couveignes, Edixhoven et al. [**2**, Chapter 12] for modular forms of level 1. There are currently still some difficulties with this approach for modular forms of higher level. We refer to [**1**, Introduction] for a discussion of these.

Remark 1.6. — It would be more satisfactory if we could prove the theorem with the level ranging over all positive integers n. We currently cannot do this for the following reason. The modular curve $\mathrm{X}_1(n)$ has a regular and semi-stable model over the ring of integers $\mathbf{Z}_L$ of a suitable number field L, but in general we do not know a good bound on the number of irreducible components of the geometric fibres of such a model at primes of $\mathbf{Z}_L$ that divide n. If we could prove the theorem in this more general form, then the restriction to modular forms for congruence subgroups of the form $\Gamma_1(n)$ could also be removed. The reason for this is that

the space of modular forms of weight k for the principal congruence subgroup $\Gamma(n) \subseteq \mathrm{SL}_2(\mathbf{Z})$ can be embedded into $\mathrm{M}_k(\Gamma_1(n^2))$ by a map that on q-expansions is given by $q \mapsto q^n$.

We now turn to some applications of Theorem 1.1. We will prove that there exist probabilistic algorithms that solve the following problems in expected polynomial time in the input, assuming the Riemann hypothesis for ζ-functions of number fields:

- Given a positive integer k, a squarefree positive integer n and a positive integer m in factored form, compute the matrix of the Hecke operator T_m in $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$ with respect to a fixed $\mathbf{Z}$-basis of $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$.
- Given a squarefree positive integer n and a prime number $p \nmid n$, compute the zeta function of the modular curve $\mathrm{X}_1(n)$ over $\mathbf{F}_p$.
- Given an even positive integer k and a positive integer m in factored form, compute the number of ways in which m can be written as a sum of k squares of integers.

Actually, we do not prove our results in exactly the same order as presented above. We first prove Theorem 1.1 in the special case where f is an Eisenstein series or a primitive cusp form. This suffices to solve (a slightly more general version of) the above problem of computing Hecke operators. We then prove Theorem 1.1 in general. Finally, we show how to solve the problems of computing zeta functions of modular curves and finding the number of representations of an integer as a sum of squares.
To conclude this introduction, we remark that in order to keep this article at a reasonable length, we have omitted, or only briefly touched upon, much material that can be found in [**1**] and [**2**]. This means that the contents of this article are largely disjoint from those of [**1**] and [**2**].

2. Background

We begin by collecting the necessary preliminaries and introducing our notation. For definitions and more background, we refer to the many texts on modular forms, such as Diamond and Im [**5**] or Diamond and Shurman [**6**].

2.1. Modular forms. — Let n and k be positive integers. Let $\mathrm{M}_k(\Gamma_1(n))$ denote the $\mathbf{C}$-vector space of modular forms of weight k for the group

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; \begin{array}{rl} a \equiv d \equiv 1 & \pmod{n}, \\ c \equiv 0 & \pmod{n} \end{array} \right\}.$$

For every $f \in \mathrm{M}_k(\Gamma_1(n))$ and every $m \geq 0$, we write $a_m(f)$ for the coefficient of q^m in the q-expansion of f, so the q-expansion of f is the power series $\sum_{m=0}^{\infty} a_m(f) q^m$ in $K[[q]]$. For every divisor d of n and every divisor e of n/d, there exists an injective $\mathbf{C}$-linear map

$$b_e^{d,n} \colon \mathrm{M}_k(\Gamma_1(d)) \rightarrowtail \mathrm{M}_k(\Gamma_1(n))$$

that, on q-expansions, has the effect of sending q to q^e.

We define

$$d(\Gamma_1(n)) = \frac{1}{12}[\mathrm{SL}_2(\mathbf{Z}) : \{\pm 1\}\Gamma_1(n)]. \tag{1}$$

This $d(\Gamma_1(n))$ grows roughly quadratically in n. A basic fact that we will need often is the following.

Lemma 2.1. — *Any $f \in \mathrm{M}_k(\Gamma_1(n))$ is determined by n, k and the coefficients $a_m(f)$ for $0 \leq m \leq k \cdot d(\Gamma_1(n))$.*

Proof. — If $n \geq 5$, then $d(\Gamma_1(n))$ is the degree of the line bundle ω of modular forms of weight 1 on the modular curve $\mathrm{X}_1(n)$. In that case, we can view modular forms as global sections of $\omega^{\otimes k}$. If $f, g \in \mathrm{M}_k(\Gamma_1(n))$ are such that $a_m(f) = a_m(g)$ for $0 \leq m \leq k \cdot d(\Gamma_1(n))$, then $f - g$ has a zero of order at least $k \cdot d(\Gamma_1(n)) + 1$ at the cusp ∞ of $\mathrm{X}_1(n)$, and we conclude that $f = g$. One can prove the lemma in general by reducing to the case $n \geq 5$. We refer to Sturm [**14**] for a full proof. □

2.2. Hecke algebras. — Let $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$ be the Hecke algebra on $\mathrm{M}_k(\Gamma_1(n))$. This is a commutative ring, free of finite rank as a $\mathbf{Z}$-module and generated as a $\mathbf{Z}$-algebra by the Hecke operators T_m for $m \in \{1, 2, \ldots\}$ and the diamond operators $\langle d \rangle$ for $d \in (\mathbf{Z}/n\mathbf{Z})^\times$. It acts on the $\mathbf{C}$-vector space $\mathrm{M}_k(\Gamma_1(n))$ of modular forms.
Let us give some useful formulae. We have

$$T_{m_1 m_2} = T_{m_1} T_{m_2} \quad \text{if } \gcd(m_1, m_2) = 1 \tag{2}$$

and

$$T_{p^{i+2}} = T_p T_{p^{i+1}} - p^{k-1} \langle p \rangle T_{p^i} \quad (p \text{ prime and } i \geq 0), \tag{3}$$

where $\langle p \rangle$ is to be interpreted as 0 if p divides n. For all $f \in \mathrm{M}_k(\Gamma_1(n))$, we have

$$a_m(T_p(f)) = a_{pm}(f) + p^{k-1} a_{m/p}(\langle p \rangle f) \quad (p \text{ prime and } m \geq 1), \tag{4}$$

where the second term is 0 if p divides n or if p does not divide m, and

$$a_1(T_m f) = a_m(f) \quad (m \geq 1). \tag{5}$$

There exists a canonical bilinear map

$$\begin{aligned} \mathbf{T}(\mathrm{M}_k(\Gamma_1(n))) \times \mathrm{M}_k(\Gamma_1(n)) &\longrightarrow \mathbf{C} \\ (t, f) &\longmapsto a_1(tf), \end{aligned}$$

inducing an isomorphism

$$\mathrm{M}_k(\Gamma_1(n)) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}\text{-modules}}(\mathbf{T}(\mathrm{M}_k(\Gamma_1(n))), \mathbf{C}) \tag{6}$$

of $\mathbf{C} \otimes_{\mathbf{Z}} \mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$-modules.
An eigenform of weight k for $\Gamma_1(n)$ is an element of $\mathrm{M}_k(\Gamma_1(n))$ spanning a one-dimensional eigenspace for the action of $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$. Let f be such a form. Then $a_1(f) \neq 0$, and we may scale f such that $a_1(f) = 1$. Now (5) implies that

$$T_m f = a_m(f) f \quad \text{for all } m \geq 1.$$

Furthermore, there exists a unique group homomorphism

$$\epsilon\colon (\mathbf{Z}/n\mathbf{Z})^\times \to \mathbf{C}^\times,$$

called the character of f, such that

$$\langle d\rangle f = \epsilon(d) f \quad \text{for all } d \in (\mathbf{Z}/n\mathbf{Z})^\times.$$

Under the isomorphism (6), the eigenforms $f \in \mathrm{M}_k(\Gamma_1(n))$ with $a_1(f) = 1$ correspond to the *ring* homomorphisms $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n))) \to \mathbf{C}$.
The $\mathbf{C}$-vector space $\mathrm{M}_k(\Gamma_1(n))$ can be written as a direct sum

$$\mathrm{M}_k(\Gamma_1(n)) = \mathrm{E}_k(\Gamma_1(n)) \oplus \mathrm{S}_k(\Gamma_1(n)).$$

Here $\mathrm{S}_k(\Gamma_1(n))$ denotes the subspace of cusp forms and $\mathrm{E}_k(\Gamma_1(n))$ denotes the subspace of Eisenstein series. The action of $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$ respects these subspaces, and we get a corresponding decomposition

$$\mathbf{T}(\mathrm{M}_k(\Gamma_1(n))) = \mathbf{T}(\mathrm{E}_k(\Gamma_1(n))) \times \mathbf{T}(\mathrm{S}_k(\Gamma_1(n)))$$

of $\mathbf{Z}$-algebras.

2.3. Eisenstein series. — Let d_1 and d_2 be positive integers such that $d_1 d_2$ divides n, and consider primitive characters

$$\epsilon_1\colon (\mathbf{Z}/d_1\mathbf{Z})^\times \to \mathbf{C}^\times, \quad \epsilon_2\colon (\mathbf{Z}/d_2\mathbf{Z})^\times \to \mathbf{C}^\times.$$

(A character $\epsilon\colon (\mathbf{Z}/d\mathbf{Z})^\times \to \mathbf{C}^\times$, with d a positive integer, is called primitive if there is no strict divisor $e \mid d$ such that ϵ factors through the quotient $(\mathbf{Z}/d\mathbf{Z})^\times \to (\mathbf{Z}/e\mathbf{Z})^\times$.) We define the formal power series

$$E_k^{\epsilon_1,\epsilon_2}(q) = -\delta_{d_1,1}\frac{B_k^{\epsilon_2}}{2k} + \sum_{m=1}^{\infty}\left(\sum_{d\mid m}\epsilon_1(m/d)\epsilon_2(d)d^{k-1}\right)q^m \in \mathbf{C}[[q]]. \tag{7}$$

Here $B_k^{\epsilon_2}$ is a generalised Bernoulli number and $\delta_{d_1,1}$ is 1 or 0 depending on whether $d_1 = 1$ or $d_1 > 1$.
If $k \neq 2$, or if $k = 2$ and at least one of ϵ_1 and ϵ_2 is non-trivial, then $E_k^{\epsilon_1,\epsilon_2}(q)$ is the q-expansion of an eigenform in $\mathrm{E}_k(\Gamma_1(d_1 d_2))$ with character $\epsilon_1\epsilon_2$. For any divisor e of $n/(d_1 d_2)$, the map $b_e^{d_1 d_2, n}\colon \mathrm{M}_k(\Gamma_1(d_1 d_2)) \to \mathrm{M}_k(\Gamma_1(n))$ sends this form to an element of $\mathrm{M}_k(\Gamma_1(n))$ with q-expansion $E_k^{\epsilon_1,\epsilon_2}(q^e)$. As for the case where $k = 2$ and both ϵ_1 and ϵ_2 are trivial, for every divisor $e \mid n$ with $e > 1$ there is an element of $\mathrm{E}_2(\Gamma_1(n))$ with q-expansion $E_2(q) - eE_2(q^e)$, where $E_2(q)$ is the power series

$$E_2(q) = -\frac{1}{24} + \sum_{m=1}^{\infty}\left(\sum_{d\mid m} d\right)q^m. \tag{8}$$

For $k \neq 2$, the finite set

$$F_k(\Gamma_1(n)) = \bigsqcup_{d_1 d_2 \mid n}\ \bigsqcup_{e\mid(n/d_1 d_2)} \left\{E_k^{\epsilon_1,\epsilon_2}(q^e) \mid \epsilon_i\colon (\mathbf{Z}/d_i\mathbf{Z})^\times \to \mathbf{C}^\times \text{ primitive}\right\} \tag{9}$$

is a $\mathbf{C}$-basis of $\mathrm{E}_k(\Gamma_1(n))$. For $k = 2$, we take all $E_k^{\epsilon_1\epsilon_2}(q^e)$ for ϵ_1, ϵ_2 not both trivial, together with the $E_2(q) - eE_2(q^e)$ for all $e \mid n$ with $e > 1$.

2.4. Cusp forms. — We write $\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n))$ for the orthogonal complement, with respect to the Petersson inner product, of the subspace of $\mathrm{S}_k(\Gamma_1(n))$ spanned by the images of all the $b_e^{d,n}$ with d strictly dividing n. The space $\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n))$ is preserved by the action of $\mathbf{T}(\mathrm{S}_k(\Gamma_1(n)))$. The unique quotient of $\mathbf{T}(\mathrm{S}_k(\Gamma_1(n)))$ that acts faithfully on $\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n))$ is denoted by $\mathbf{T}(\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n)))$.
An eigenform $f \in \mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n))$ with $a_1(f) = 1$ is called a primitive cusp form. The finite set

$$B_k(\Gamma_1(n)) = \bigsqcup_{d \mid n} \bigsqcup_{e \mid (n/d)} b_e^{d,n}\{\text{primitive cusp forms in } \mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n))\} \tag{10}$$

is a $\mathbf{C}$-basis for $\mathrm{S}_k(\Gamma_1(n))$.

2.5. Modular forms over other rings. — We define

$$\mathrm{M}_k^{\mathrm{int}}(\Gamma_1(n)) = \{\text{forms in } \mathrm{M}_k(\Gamma_1(n)) \text{ with } q\text{-expansion in } \mathbf{Z}[[q]]\}.$$

This is a $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$-module that is free of finite rank as a $\mathbf{Z}$-module. For any commutative $\mathbf{Z}[1/n]$-algebra R, we define the R-module of modular forms of weight k for $\Gamma_1(n)$ with coefficients in R as

$$\mathrm{M}_k(\Gamma_1(n), R) = R \otimes_{\mathbf{Z}} \mathrm{M}_k^{\mathrm{int}}(\Gamma_1(n)).$$

Apart from the complex numbers, the important examples for us are number fields and finite fields of characteristic not dividing n. If R is any field of characteristic not dividing n, we define eigenforms over R in the same way as in the case $R = \mathbf{C}$.
If R is a sub-$\mathbf{Z}[1/n]$-algebra of $\mathbf{C}$, we identify $\mathrm{M}_k(\Gamma_1(n), R)$ with the submodule of $\mathrm{M}_k(\Gamma_1(n))$ consisting of forms with q-expansion in $R[[q]]$.

3. Modular Galois representations

Let n and k be positive integers, let $\mathbf{F}$ be a finite field of characteristic not dividing n, and let $f \in \mathrm{M}_k(\Gamma_1(n), \mathbf{F})$ be an eigenform over $\mathbf{F}$.
It follows from work of Eichler, Shimura, Igusa, Deligne and Serre that there exists a continuous semi-simple representation

$$\rho_f \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}_{\mathbf{F}} V_f,$$

where V_f is a two-dimensional $\mathbf{F}$-vector space, with the following properties:

- ρ_f is unramified at all prime numbers p not dividing nl;
- if p is such a prime number, then the characteristic polynomial of the Frobenius conjugacy class at p equals $t^2 - a_p(f)t + \epsilon(p)p^{k-1}$, where ϵ is the character of f.

This ρ_f is unique up to isomorphism.
The end product of [**1**] is a probabilistic algorithm for computing representations of the form ρ_f, where f is an eigenform over a finite field $\mathbf{F}$. This allows us to state the following theorem.

Theorem 3.1. — *Let n_0 be a positive integer. There exists a probabilistic algorithm that, given*

- *a positive integer k,*
- *a squarefree positive integer n_1 coprime to n_0,*
- *a finite field $\mathbf{F}$ of characteristic greater than k, and*
- *an eigenform $f \in \mathrm{M}_k(\Gamma_1(n))$, given by its coefficients $a_m(f)$ for $0 \leq m \leq k \cdot d(\Gamma_1(n))$,*

computes ρ_f in the form of the following data:

- *the finite Galois extension K_f of $\mathbf{Q}$ such that ρ_f factors as*

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \twoheadrightarrow \mathrm{Gal}(K_f/\mathbf{Q}) \rightarrowtail \mathrm{Aut}_{\mathbf{F}}\, V_f,$$

  given by the multiplication table of some $\mathbf{Q}$-basis $(b_1, \ldots, b_r)$ of K_f;
- *for every $\sigma \in \mathrm{Gal}(K_f/\mathbf{Q})$, the matrix of σ with respect to the basis $(b_1, \ldots, b_r)$ and the matrix of $\rho_f(\sigma)$ with respect to some fixed $\mathbf{F}$-basis of V_f,*

and that runs in expected time polynomial in k, n_1 and $\#\mathbf{F}$.
Moreover, once ρ_f has been computed, one can compute $\rho_f(\mathrm{Frob}_p)$ using a deterministic algorithm in time polynomial in k, n_1, $\#\mathbf{F}$ and $\log p$.

Remark 3.2. — This running time is optimal from a certain perspective, given the fact that the length of the input and output of such an algorithm is necessarily at least polynomial in k, n_1 and $\#\mathbf{F}$ (and $\log p$ for the second part).

4. Some bounds

In this section we collect some bounds that we will need in § 5 below to prove Theorem 1.1.

4.1. The discriminant of the new quotient of the Hecke algebra. — Let n and k be positive integers. The $\mathbf{Z}$-algebra $\mathbf{T}(\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n)))$ is reduced, because there is a basis of eigenforms for its action on $\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n))$. Furthermore, it is free of finite rank as a $\mathbf{Z}$-module. In particular, it has a non-zero discriminant $\mathrm{disc}\,\mathbf{T}(\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n)))$.

Lemma 4.1. — *The logarithm of $|\mathrm{disc}\,\mathbf{T}(\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n)))|$ is bounded by a polynomial in n and k.*

Proof. — The method of Ullmo [**15**], who considered cusp forms of weight 2 for $\Gamma_0(n)$ with n squarefree, extends without difficulty to our situation. For completeness, let us give a proof in this more general setting.
We abbreviate

$$\mathbf{T} = \mathbf{T}(\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n)))$$

and

$$\begin{aligned} r &= \dim_{\mathbf{C}} \mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n)) \\ &= \operatorname{rank}_{\mathbf{Z}} \mathbf{T}. \end{aligned}$$

It follows from Lemma 2.1 and (6) that the $\mathbf{Q}$-vector space $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{T}$ is spanned by the elements $T_1, \dots, T_{k \cdot d(\Gamma_1(n))}$, with $d(\Gamma_1(n))$ as in (1). We can therefore choose integers

$$1 \leq m_1 \leq \cdots \leq m_r \leq k \cdot d(\Gamma_1(n))$$

such that the elements $T_{m_1}, \dots, T_{m_r}$ of $\mathbf{T}$ are $\mathbf{Z}$-linearly independent. We let $\mathbf{T}'$ denote the subgroup of $\mathbf{T}$ spanned by $T_{m_1}, \dots, T_{m_r}$. This $\mathbf{T}'$ is free of rank r as a $\mathbf{Z}$-module, so it has finite index $(\mathbf{T} : \mathbf{T}')$ in $\mathbf{T}$, and

$$\operatorname{disc} \mathbf{T} = \frac{\operatorname{disc} \mathbf{T}'}{(\mathbf{T}' : \mathbf{T})^2}.$$

In particular, this implies

$$|\operatorname{disc} \mathbf{T}| \leq \left|\operatorname{disc} \mathbf{T}'\right|.$$

We next use the definition of the discriminant:

$$\operatorname{disc} \mathbf{T}' = \det\bigl(\operatorname{tr}(T_{m_u} T_{m_v})_{u,v=1}^{r}\bigr),$$

where $\operatorname{tr}(e)$ denotes the trace of the $\mathbf{Z}$-linear map $\mathbf{T}' \to \mathbf{T}'$ sending t to et. Now the trace of an endomorphism e of $\mathbf{T}'$ equals the trace of the endomorphism dual to e on the $\mathbf{C}$-vector space

$$\operatorname{Hom}_{\mathbf{Z}\text{-modules}}(\mathbf{T}', \mathbf{C}) \cong \mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n)).$$

We let $f_1, \dots, f_r$ be the primitive cusp forms in $\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n))$, and we abbreviate

$$\alpha_{t,u} = a_{m_t}(f_u).$$

Then we get

$$\operatorname{tr}(T_{m_u} T_{m_v}) = \sum_{t=1}^{r} \alpha_{t,u} \alpha_{t,v}.$$

We then compute $\operatorname{disc} \mathbf{T}'$ as follows:

$$\begin{aligned} \operatorname{disc} \mathbf{T}' &= \det\left(\sum_{t=1}^{r} \alpha_{t,u}\alpha_{t,v}\right)_{u,v=1}^{r} \\ &= \det\left(\begin{pmatrix} \alpha_{1,1} & \alpha_{2,1} & \dots & \alpha_{r,1} \\ \alpha_{1,2} & \alpha_{2,2} & \dots & \alpha_{r,2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{1,r} & \alpha_{2,r} & \dots & \alpha_{r,r} \end{pmatrix} \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \dots & \alpha_{1,r} \\ \alpha_{2,1} & \alpha_{2,2} & \dots & \alpha_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{r,1} & \alpha_{r,2} & \dots & \alpha_{r,r} \end{pmatrix}\right) \\ &= \det\bigl((\alpha_{t,u})_{t,u=1}^{r}\bigr)^2. \end{aligned}$$

Deligne's bound for the coefficients of eigenforms, proved in [**3**] and [**4**], implies the inequality

$$\begin{aligned} |\alpha_{t,u}| &= |a_{m_t}(f_u)| \\ &\leq \sigma_0(m_t) m_t^{(k-1)/2}. \end{aligned}$$

Here $\sigma_0(m)$ denotes the number of positive divisors of m. Elementary estimates now show that $\log|\mathrm{disc}\,\mathbf{T}|$ is bounded by a polynomial in n and k. □

4.2. Primes of small norm in number fields. — The Riemann hypothesis for the ζ-function of a number field K has the following well-known implication of for the existence of prime ideals of small norm in the ring of integers of K.

Lemma 4.2. — *Let ϵ and δ be positive real numbers. There exist positive real numbers A and B such that the following holds. Let K be an number field such that the Riemann hypothesis is true for the ζ-function of K. Let $\mathbf{Z}_K$ denote the ring of integers of K, and for every prime number p let $\lambda_K(p)$ denote the number of prime ideals of $\mathbf{Z}_K$ of norm equal to p. Then for all real numbers $x \geq 2$ such that*

$$\frac{x^\delta}{(\log x)^2} \geq A[K:\mathbf{Q}] \quad \textit{and} \quad \frac{x^\delta}{\log x} \geq B \log|\mathrm{disc}\,\mathbf{Z}_K|$$

we have

$$\left| \sum_{p \leq x \text{ prime}} \lambda_K(p) \log p - x \right| \leq \epsilon x^{1/2+\delta}.$$

Proof. — For every prime number p and every positive integer m, we define

$$\Lambda_K(p^m) = \sum_{t|m} t \cdot \#\{\text{prime ideals of norm } p^t \text{ in } \mathbf{Z}_K\} \cdot \log p.$$

In particular, this implies $\Lambda_K(p) = \lambda_K(p)\log p$ for every prime number p. We define $\Lambda_K(n) = 0$ if n is not a prime power. The relation between ζ_K and Λ_K is the Dirichlet series

$$-\frac{\zeta_K'(s)}{\zeta_K(s)} = \sum_{n=1}^{\infty} \Lambda_K(n) n^{-s}.$$

We define

$$\begin{aligned} \psi_K \colon [1,\infty) &\longrightarrow \mathbf{R} \\ x &\mapsto \sum_{n \leq x} \Lambda_K(n). \end{aligned}$$

Now there exists a positive real number c, independent of K, such that the generalised Riemann hypothesis for ζ_K implies the estimate

$$|\psi_K(x) - x| \leq c\sqrt{x}\log(x)\log\bigl(x^{[K:\mathbf{Q}]}\,|\mathrm{disc}\,\mathbf{Z}_K|\bigr) \quad \text{for all } x \geq 2;$$

see Iwaniec and Kowalski [**9**, Theorem 5.15]. By elementary arguments, it follows that there exists a positive real number c', also independent of K, such that

$$\left| \sum_{p \leq x \text{ prime}} \lambda_K(p) \log p - x \right| \leq c' \sqrt{x} \log(x) \log\bigl(x^{[K:\mathbf{Q}]} |\operatorname{disc} \mathbf{Z}_K|\bigr) \quad \text{for all } x \geq 2.$$

It is now straightforward to check that taking $A = B = 2c'/\epsilon$ works. □

5. Proof of Theorem 1.1

As already mentioned briefly in the introduction, Theorem 1.1 will be proved as follows. We first prove the following basic cases:

- f is an element of the form $E_k^{\epsilon_1,\epsilon_2}$ in $\mathrm{E}_k(\Gamma_1(d_1 d_2))$, where $\epsilon_1 \colon (\mathbf{Z}/d_1\mathbf{Z})^\times \to \mathbf{C}^\times$ and $\epsilon_2 \colon (\mathbf{Z}/d_2\mathbf{Z})^\times \to \mathbf{C}^\times$ are primitive characters;
- f is a primitive cusp form in $\mathrm{S}_k(\Gamma_1(n))$.

In each case, we take K to be the number field generated by the coefficients of f, and we assume that m is a prime number. After proving these special cases, we show that we can compute the Hecke algebra $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$ in a sense that will be explained in § 5.3 below. It is then straightforward to deduce Theorem 1.1 in general.

5.1. Eisenstein series. — We start by considering the Eisenstein series $E_k^{\epsilon_1,\epsilon_2}$, where $\epsilon_1 \colon (\mathbf{Z}/d_1\mathbf{Z})^\times \to \mathbf{C}^\times$ and $\epsilon_2 \colon (\mathbf{Z}/d_2\mathbf{Z})^\times \to \mathbf{C}^\times$ are primitive characters and e is a divisor of $n/(d_1 d_2)$. For convenience, we also allow the case of the 'pseudo-Eisenstein series' E_2 defined by (8). Let K be the cyclotomic extension of $\mathbf{Q}$ generated by the images of ϵ_1 and ϵ_2. The formula (7) shows that for every prime number p, we can compute the element $a_p(E_k^{\epsilon_1,\epsilon_2}) \in K$ in time polynomial in n, k and $\log p$.

5.2. Primitive forms. — We continue with the case where f is a primitive cusp form in $\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n))$ and K is the number field generated by the coefficients of f. Let $\mathbf{Z}_K$ denote the ring of integers of K. There exists a unique ring homomorphism

$$e_f \colon \mathbf{T}(\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n))) \to \mathbf{Z}_K$$

sending each Hecke operator to its eigenvalue on f. Let A denote the image of e_f. It is of finite index $(\mathbf{Z}_K : A)$ in $\mathbf{Z}_K$, and we have

$$\operatorname{disc} A = (\mathbf{Z}_K : A)^2 \operatorname{disc} \mathbf{Z}_K.$$

Furthermore, we have

$$|\operatorname{disc} A| \leq |\operatorname{disc} \mathbf{T}(\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n)))| \quad \text{and} \quad [K : \mathbf{Q}] \leq \operatorname{rank}_{\mathbf{Z}} \mathbf{T}(\mathrm{S}_k^{\mathrm{new}}(\Gamma_1(n))).$$

Lemma 4.1 now implies that $\log|\operatorname{disc} A|$, and hence also $\log|\operatorname{disc} \mathbf{Z}_K|$ and $\log(\mathbf{Z}_K : A)$, are bounded by a polynomial in n and k. The same clearly holds for $[K : \mathbf{Q}]$.

Now let p be a prime number. We have to show that we can compute $a_p(f)$ in time polynomial in n, k and $\log p$. In Couveignes, Edixhoven et al. [**2**, § 15.2] it is explained in detail how to do this. We only give a sketch.
We may assume that p does not divide n; namely, if p does divide n, then we can spend time polynomial in p, so using modular symbols is fast enough; see § 5.3 below.
By Lemma 4.2 applied to K and the fact that $\log(\mathbf{Z}_K : A)$ is bounded by a polynomial in n and k, we can choose x sufficiently large, but bounded by a polynomial in n and k, such that if M is the set of maximal ideals of A whose norm is a prime number lying in the interval $(k, x]$ and different from p, we have

$$\prod_{\mathfrak{m}\in M} \mathrm{Norm}(\mathfrak{m}) \geq \left(2^{([K:\mathbf{Q}]+1)/2} \cdot 2p^{(k-1)/2}\right)^{[K:\mathbf{Q}]}. \tag{11}$$

An explanation for the right-hand side will be given below. We compute $a_p(f)$ using the following algorithm.

1. Compute a $\mathbf{Z}$-basis for A.
2. Compute a bound x and the set M of maximal ideals of A such that the set M defined above satisfies (11).
3. For all $\mathfrak{m} \in M$, compute the Galois representation $\rho_{f \bmod \mathfrak{m}}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(A/\mathfrak{m})$ using Theorem 3.1.
4. For all $\mathfrak{m} \in M$, compute
$$(a_p(f) \bmod \mathfrak{m}) = \mathrm{tr}(\rho_{f \bmod \mathfrak{m}}(\mathrm{Frob}_p)) \in A/\mathfrak{m},$$
again using Theorem 3.1.
5. Compute an LLL-reduced $\mathbf{Z}$-basis for the ideal $\mathfrak{a} = \prod_{\mathfrak{m}\in M} \mathfrak{m}$ of A.
6. From the $a_p(f) \bmod \mathfrak{m}$, compute the image of $a_p(f)$ in $A/\mathfrak{a}$.
7. Using the LLL algorithm, reconstruct $a_p(f)$ as the shortest representative in A of the image of $a_p(f)$ in $A/\mathfrak{a}$. This works because of the inequality (11).

5.3. Computing Hecke operators. — We represent $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$ in the following form: we specify its multiplication table with respect to a suitable $\mathbf{Z}$-basis $(b_1, \ldots, b_r)$, together with the Hecke operators T_m for $1 \leq m \leq k \cdot d(\Gamma_1(n))$ and the diamond operators $\langle d\rangle$ for all $d \in (\mathbf{Z}/n\mathbf{Z})^\times$ as $\mathbf{Z}$-linear combinations of $(b_1, \ldots, b_r)$. These data specify $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$ uniquely because the above operators generate $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$. In other words, if the same data are given with respect to a different basis of $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$, there exists exactly one change of $\mathbf{Z}$-basis compatible with the given T_m and $\langle d\rangle$.

Theorem 5.1. — *Let n_0 be a positive integer. There exists a probabilistic algorithm that, given*

- *a positive integer k,*
- *a squarefree positive integer n_1 coprime to n_0, and*
- *a positive integer m in factored form,*

computes

– *the Hecke algebra* $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$ *as above, where* $n = n_0 n_1$, *and*
– *the element* T_m *on the basis* $(b_1, \dots, b_r)$,

and that runs in expected time polynomial in k, n_1 *and* $\log m$ *under the Riemann hypothesis for* ζ*-functions of number fields.*

Proof. — We need some more information about the action of Hecke operators on q-expansions. As a basis for $\mathrm{M}_k(\Gamma_1(n))$ we take the union of the basis $F_k(\Gamma_1(n))$ of $\mathrm{E}_k(\Gamma_1(n))$ defined by (9) and the basis $B_k(\Gamma_1(n))$ of $\mathrm{S}_k(\Gamma_1(n))$ defined by (10).
Let f be either an Eisenstein series $E_k^{\epsilon_1,\epsilon_2} \in \mathrm{E}_k(\Gamma_1(d_1 d_2))$ as above or a primitive form in $\mathrm{S}_k(\Gamma_1(d))$. In the first case, we put $d = d_1 d_2$. The formula (4) for the action of the Hecke operator T_p shows that the relation between T_p and the maps $b_e^{d,n} \colon \mathrm{M}_k(\Gamma_1(d)) \to \mathrm{M}_k(\Gamma_1(n))$, where e runs through the divisors of n/d, is as follows:

$$T_p(b_e^{d,n} f) = \begin{cases} a_p \cdot b_e^{d,n} f & \text{if } p \nmid n; \\ b_{e/p}^{d,n} f & \text{if } p \mid e; \\ a_p \cdot b_e^{d,n} f - p^{k-1} \epsilon(p) b_{pe}^{d,n} f & \text{if } p \nmid d,\ p \nmid e \text{ and } p \mid n; \\ a_p \cdot b_e^{d,n} f & \text{if } p \mid d \text{ and } p \nmid e. \end{cases} \tag{12}$$

This formula gives the matrix of T_p with respect to the basis $F_k(\Gamma_1(n))$ of $\mathrm{E}_k(\Gamma_1(n))$ and the basis $B_k(\Gamma_1(n))$ of $\mathrm{S}_k(\Gamma_1(n))$.
We first compute the q-expansions of the Eisenstein series $E_k^{\epsilon_1,\epsilon_2} \in \mathrm{E}_k(\Gamma_1(d_1 d_2))$, with $\epsilon_i \colon (\mathbf{Z}/d_i\mathbf{Z})^\times \to \mathbf{C}^\times$ primitive characters such that $d_1 d_2 \mid n$, as in § 2.3. From these q-expansions and (12) we then compute the Hecke algebra $\mathbf{T}(\mathrm{E}_k(\Gamma_1(n)))$ in the form described above in time polynomial in n and k.
Given a prime number p, we compute all the $a_p(E_k^{\epsilon_1,\epsilon_2})$ as in § 5.1, and we find the matrix of T_p using (12). We then express T_p on the basis of $\mathbf{T}(\mathrm{E}_k(\Gamma_1(n)))$ that we computed earlier. In this way, we can compute the Hecke operator $T_p \in \mathbf{T}(\mathrm{E}_k(\Gamma_1(n)))$ in time polynomial in n, k and $\log p$.
For cusp forms, the q-expansions are computed from the Hecke algebra instead of vice versa. We compute the Hecke algebras $\mathbf{T}(\mathrm{S}_k(\Gamma_1(d)))$, where d runs through the divisors of n, in the form described above. These data can be computed in time polynomial in n and k using deterministic algorithms based on modular symbols and the LLL lattice basis reduction algorithm; see Stein [**13**, Chapter 8] and the author's thesis [**1**, § IV.4.1]. From each $\mathbf{T}(\mathrm{S}_k(\Gamma_1(d)))$, we compute the q-expansions of the primitive cusp forms in $\mathrm{S}_k(\Gamma_1(d))$.
So far, we have only used existing methods. To compute the Hecke operator $T_p \in \mathbf{T}(\mathrm{S}_k(\Gamma_1(n)))$ for a prime number p in time polynomial in $\log p$, we need our new tools. For every divisor d of n and every primitive form $f \in \mathrm{S}_k(\Gamma_1(d))$, we compute $a_p(f)$ as in § 5.2. Using (12), we obtain the matrix of T_p with respect to the basis $B_k(\Gamma_1(n))$. We finally express T_p on the basis of $\mathbf{T}(\mathrm{S}_k(\Gamma_1(n)))$ that we computed earlier.

Now let m be an arbitrary positive integer, and suppose that we know the factorisation of m. Then we can compute the element

$$T_m \in \mathbf{T}(\mathrm{M}_k(\Gamma_1(n))) = \mathbf{T}(\mathrm{E}_k(\Gamma_1(n))) \times \mathbf{T}(\mathrm{S}_k(\Gamma_1(n)))$$

from the T_p for for $p \mid m$ prime in time polynomial in $\log m$ using the identities (2) and (3). □

5.4. Proof of Theorem 1.1 in general. — Given n, k, K, f and m as in the theorem, we compute $a_m(f)$ as follows. We first compute $\mathbf{T}(\mathrm{M}_k(\Gamma_1(n)))$ using modular symbols. From f we then determine the unique $\mathbf{Z}$-linear map

$$e_f \colon \mathbf{T}(\mathrm{M}_k(\Gamma_1(n))) \to K$$

sending T_i to $a_i(f)$ for all i with $1 \leq i \leq k \cdot d(\Gamma_1(n))$. Using Theorem 5.1, we then compute the Hecke operator T_m. Finally, we compute $a_m(f)$ as

$$a_m(f) = e_f(T_m).$$

It is straightforward to check that all these computations can be done in time polynomial in the length of the input.

Remark 5.2. — The proof shows that the Riemann hypothesis only needs to be assumed for the ζ-functions of number fields that arise as fields of coefficients of primitive cusp forms.

6. Applications

6.1. Counting points on modular curves. — The case $k = 2$ of Theorem 5.1 implies a new result on counting points on modular curves over finite fields.

Theorem 6.1. — *There exists a probabilistic algorithm that, given a squarefree positive integer n and a prime number $p \nmid n$, computes the zeta function of the modular curve $\mathrm{X}_1(n)$ over $\mathbf{F}_p$, and that runs in time polynomial in n and $\log p$ under the Riemann hypothesis for ζ-functions of number fields.*

Proof. — Let $\mathrm{J}_1(n)_{\mathbf{F}_p}$ denote the Jacobian of $\mathrm{X}_1(n)_{\mathbf{F}_p}$. Let χ be the characteristic polynomial of the Frobenius endomorphism of the l-adic Tate module $\mathrm{T}_l\mathrm{J}_1(n)_{\mathbf{F}_p}$, where l is any prime number different from p; then χ has integral coefficients and does not depend on the choice of l. Because of the well-known identity

$$\mathrm{Z}_{\mathrm{X}_1(n)/\mathbf{F}_p}(t) = \frac{\chi^*(t)}{(1-t)(1-pt)},$$

where $\chi^*(t) = t^{\deg \chi}\chi(1/t)$ is the reciprocal polynomial of χ, it suffices to compute χ.
Let $\mathbf{T}_1(n)$ denote the Hecke algebra acting on $\mathrm{J}_1(n)_{\mathbf{F}_p}$. Then $\mathbf{Q}_l \otimes_{\mathbf{Z}_l} \mathrm{T}_l\mathrm{J}_1(n)_{\mathbf{F}_p}$ is a free $\mathbf{Q}_l \otimes_{\mathbf{Z}} \mathbf{T}_1(n)$-module of rank 2. By the Eichler–Shimura relation, the characteristic polynomial of Frob_p on it equals $x^2 - T_p x + p\langle p \rangle \in \mathbf{T}_1(n)[x]$. This implies that the characteristic polynomial of Frob_p viewed as a $\mathbf{Q}_l$-linear map equals

$$\chi = \mathrm{Norm}_{\mathbf{T}_1(n)[x]/\mathbf{Z}[x]}(x^2 - T_p x + p\langle p \rangle) \in \mathbf{Z}[x].$$

To compute the right-hand side, we use the fact that the Hecke algebras $\mathbf{T}(\mathrm{S}_2(\Gamma_1(n)))$ and $\mathbf{T}_1(n)$ are isomorphic. By Theorem 5.1, we can therefore compute $\mathbf{T}_1(n)$ and the matrices M_{T_p} and $M_{\langle p\rangle}$ of T_p and $\langle p\rangle$ with respect to some $\mathbf{Z}$-basis $(b_1, \dots, b_r)$ of $\mathbf{T}_1(n)$. We interpret $(b_1, \dots, b_r)$ as a $\mathbf{Z}[x]$-basis of $\mathbf{T}_1(n)[x]$, and we compute χ as the determinant of the matrix $x^2 \cdot \mathrm{id} - x \cdot M_{T_p} + p \cdot M_{\langle p\rangle}$ with coefficients in $\mathbf{Z}[x]$. □

Corollary 6.2. — *There exists a probabilistic algorithm that, given a squarefree positive integer n and a prime power q coprime to n, computes the number of rational points on $\mathrm{X}_1(n)$ over the field of q elements, and that runs in time polynomial in n and $\log q$ under the Riemann hypothesis for ζ-functions of number fields.*

6.2. Lattices. — A particularly interesting family of modular forms consists of *θ-series* associated to integral lattices. An *integral lattice* is a free Abelian group L of finite rank together with a symmetric, positive-definite, bilinear form

$$\langle\ ,\ \rangle \colon L \times L \to \mathbf{Z}.$$

We identify a lattice L with its image in the Euclidean space

$$L_{\mathbf{R}} = \mathbf{R} \otimes_{\mathbf{Z}} L.$$

The form $\langle\ ,\ \rangle$ extends uniquely to an inner product $\langle\ ,\ \rangle_{\mathbf{R}}$ on $L_{\mathbf{R}}$. The *dual lattice* of L is

$$L^\vee = \{v \in L_{\mathbf{R}} \mid \langle v, L\rangle \subseteq \mathbf{Z}\}$$

equipped with the symmetric positive definite bilinear form $\langle\ ,\ \rangle^\vee$ obtained by restricting $\langle\ ,\ \rangle_{\mathbf{R}}$. The *level* of L is the exponent of the group $L^\vee/L$, i.e. the least positive integer c such that $cL^\vee \subseteq L$. It can be computed as the least common denominator of the entries of the inverse of the matrix of $\langle\ ,\ \rangle$ with respect to some $\mathbf{Z}$-basis of L.

Let $(L, \langle\ ,\ \rangle)$ be an integral lattice of even rank k and level n. For every non-negative integer m we define

$$r_L(m) = \#\{x \in L \mid \langle x, x\rangle = m\}.$$

The θ-series of L is the element of $\mathbf{Z}[[q]]$ defined by

$$\begin{aligned}\theta_L &= \sum_{x \in L} q^{\langle x,x\rangle} \\ &= \sum_{m=0}^{\infty} r_L(m) q^m.\end{aligned}$$

This power series is the q-expansion of a modular form of weight $k/2$ for $\Gamma_1(4n)$. The lattice L is called *even* if the integer $\langle x, x\rangle$ is even for all $x \in L$. If L is even, then the level $4n$ can be replaced by $2n$; if both L and $L^\vee$ are even, then it can be replaced by $\Gamma_1(n)$. For proofs of these results, we refer to Miyake [**12**, § 4.9].

Couveignes, Edixhoven et al. [**2**, § 15.3] treat the following application of their result on computing coefficients of modular forms for $\mathrm{SL}_2(\mathbf{Z})$. They take L equal to the Leech lattice, which is the unique self-dual even lattice of rank 24. Its θ-series is a linear combination

of the Eisenstein series E_{12} and the discriminant modular form Δ. The latter is the unique element of $\mathrm{S}_{12}(\mathrm{SL}_2(\mathbf{Z}))$ with $a_1(\Delta) = 1$. Its q-expansion coefficients are given by Ramanujan's τ-function:

$$\begin{aligned}\Delta &= q\prod_{m=1}^{\infty}(1-q^m)^{24}\\ &= \sum_{m=1}^{\infty}\tau(m)q^m.\end{aligned}$$

As mentioned before, the coefficients of Eisenstein series can be computed from the formulae in § 2.3. It is proved in [**2**] that given a positive integer m in factored form, the integer $\tau(m)$, and hence the representation number $r_L(m)$, can be computed deterministically in time polynomial in $\log m$.

The corresponding generalisation that is made possible by Theorem 1.1 is the following result.

Theorem 6.3. — *Let n_0 be a positive integer. There exists a probabilistic algorithm that, given*

- *an even positive integer k,*
- *a squarefree positive integer n_1 coprime to n_0,*
- *the representation numbers $r_L(0), \ldots, r_L(k/2 \cdot d(\Gamma_1(4n))$ for a lattice L of even rank k and level n, where $4n = n_0n_1$, and*
- *a positive integer m in factored form,*

computes $r_L(m)$, and that runs in time polynomial in k, n_1 and $\log m$ under the Riemann hypothesis for ζ-functions of number fields.

Remark 6.4. — Unfortunately, in general it is not clear how one can efficiently compute θ_L to sufficient order, given only the matrix of $\langle\ ,\ \rangle$ with respect to some $\mathbf{Z}$-basis of L.

6.3. Sums of squares. — Now consider the lattice $\mathbf{Z}^k$, equipped with the standard bilinear form, so that the standard basis is orthonormal. Its θ-series is

$$\theta_{\mathbf{Z}^k} = \theta^k, \tag{13}$$

where θ is Jacobi's θ-series:

$$\theta = \sum_{m\in\mathbf{Z}} q^{m^2} = 1 + 2\sum_{m=1}^{\infty} q^{m^2}.$$

We let $r_k(m)$ denote the m-th coefficient of $\theta_{\mathbf{Z}^k}$, so that

$$r_k(m) = \#\{(x_1,\ldots,x_k) \in \mathbf{Z}^k \mid x_1^2 + \cdots + x_k^2 = m\}.$$

The problem of finding $r_k(m)$ is the classical problem of determining the number of ways in which m can be written as a sum of k squares. This question has a long and interesting history, which involves (among many others) Fermat, Legendre, Gauß, Jacobi, Eisenstein and Liouville. There is a large volume of literature devoted to this problem; we refer only to Dickson [**7**], Grosswald [**8**] and Milne [**11**].

From now on we restrict to *even* values of k. This restriction is imposed on us by the fact that θ is a modular form of weight $1/2$, and our results on computing coefficients of modular forms only hold for forms of integral weight.
For $k = 2, 4, 6, 8, 10$, there exist formulae for $r_k(m)$. One set of such formulae is the following:

$$\begin{aligned}
r_2(m) &= 4\sum_{d|m} \epsilon(d), \\
r_4(m) &= 8\sum_{d|m} d - 32 \sum_{d|(m/4)} d, \\
r_6(m) &= 16\sum_{d|m} \epsilon(m/d)d^2 - 4\sum_{d|m} \epsilon(d)d^2, \\
r_8(m) &= 16\sum_{d|m} d^3 - 32 \sum_{d|(m/2)} d^3 + 256 \sum_{d|(m/4)} d^3, \\
r_{10}(m) &= \frac{4}{5}\sum_{d|m} \epsilon(d)d^4 + \frac{64}{5}\sum_{d|m} \epsilon(m/d)d^4 + \frac{8}{5} \sum_{\substack{z \in \mathbf{Z}[\sqrt{-1}] \\ |z|^2 = m}} z^4.
\end{aligned}$$

Here d runs over the positive divisors of m, $m/2$ or $m/4$; if $m/2$ or $m/4$ is not an integer, the corresponding sum is omitted. Furthermore, ϵ denotes the unique non-trivial Dirichlet character modulo 4:

$$\epsilon(d) = \left(\frac{-1}{d}\right) = \begin{cases} 1 & \text{if } d \equiv 1 \bmod 4, \\ -1 & \text{if } d \equiv 3 \bmod 4, \\ 0 & \text{if } d \equiv 0 \bmod 2. \end{cases}$$

One way to interpret the existence of the above formulae is as follows. For $k = 2, 4, 6, 8$, the space $\mathrm{S}_{k/2}(\Gamma_1(4))$ is trivial; in other words, $\theta_{\mathbf{Z}^k} \in \mathrm{M}_{k/2}(\Gamma_1(4))$ is a linear combination of Eisenstein series. Although $\mathrm{S}_5(\Gamma_1(4))$ is non-trivial, it is spanned by a cusp form with *complex multiplication*, explaining the last term in the formula for $r_{10}(m)$.
For $k \geq 12$, it is true that various formulae have been proposed for $r_k(m)$, but it seems that none of these makes it possible to compute $r_k(m)$ time polynomial in k and $\log m$. This may be understood, from our perspective, in light of the fact that for every even $k \geq 12$, the decomposition of θ^k as as a linear combination of eigenforms contains cusp forms without complex multiplication. The latter fact was proved recently by I. Varma [**16**]. No method was previously known for computing the coefficients of such cusp forms in polynomial time.
Using (13), we can quickly compute $\theta_{\mathbf{Z}^k}$ to sufficient order to determine it uniquely as an element of $\mathrm{M}_{k/2}(\Gamma_1(4))$. The following result is therefore a special case ($n_0 = 4$, $n_1 = 1$) of Theorem 6.3.

Theorem 6.5. — *There exists a probabilistic algorithm that, given an even positive integer k and a positive integer m in factored form, computes the number of representations of m as a sum of k squares of integers, and that runs in time polynomial in k and $\log m$ under the Riemann hypothesis for ζ-functions of number fields.*

As in Remark 1.3, without assuming the generalised Riemann hypothesis we can still prove that for fixed k, the expected running time is polynomial in $\log m$.

References

[1] P. J. Bruin, *Modular curves, Arakelov theory, algorithmic applications*. Proefschrift (Ph. D. thesis), Universiteit Leiden, 2010. Available online: `http://hdl.handle.net/1887/15915`.

[2] J.-M. Couveignes and S. J. Edixhoven (with J. G. Bosman, R. S. de Jong and F. Merkl), *Computational aspects of modular forms and Galois representations*. Princeton University Press, to appear. Preprint available on arXiv: `math/0605244`.

[3] P. Deligne, Formes modulaires et représentations l-adiques. Séminaire Bourbaki, 21e année (1968/1969), exposé 355. Lecture Notes in Mathematics **179**, 139–172. Springer-Verlag, Berlin/Heidelberg/New York, 1971.

[4] P. Deligne, La conjecture de Weil. I. *Publications mathématiques de l'I.H.É.S.* **43** (1973), 273–307.

[5] F. Diamond and J. Im, Modular forms and modular curves. In: V. Kumar Murty (editor), *Seminar on Fermat's Last Theorem* (Fields Institute for Research in Mathematical Sciences, Toronto, ON, 1993–1994), 39–133. CMS Conference Proceedings **17**. American Mathematical Society, Providence, RI, 1995.

[6] F. Diamond and J. Shurman, *A First Course in Modular Forms*. Springer-Verlag, Berlin/Heidelberg/New York, 2005.

[7] L. E. Dickson, *History of the theory of numbers*. Volume II: Diophantine analysis. Carnegie Institute, Washington, D.C., 1920. Reprinted by Chelsea Publishing Co., New York, 1966.

[8] E. Grosswald, *Representations of Integers as Sums of Squares*. Springer-Verlag, Berlin/Heidelberg/New York, 1985.

[9] H. Iwaniec and E. Kowalski, *Analytic Number Theory*. AMS Colloquium Publications **53**. American Mathematical Society, Providence, RI, 2004.

[10] H. W. Lenstra, Jr. and C. Pomerance, A rigorous time bound for factoring integers. *Journal of the American Mathematical Society* **5** (1992), no. 3, 483–516.

[11] S. C. Milne, Infinite families of exact sums of squares formulas, Jacobi elliptic functions, continued fractions, and Schur functions. *Ramanujan Journal* **6** (2002), no. 1, 7–149.

[12] T. Miyake, *Modular Forms*. Springer-Verlag, Berlin/Heidelberg, 1989.

[13] W. A. Stein, *Modular Forms, a Computational Approach*. With an appendix by P. E. Gunnells. American Mathematical Society, Providence, RI, 2007.

[14] J. Sturm, On the congruence of modular forms. In: D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn and M. B. Nathanson (editors), *Number Theory (New York, 1984–1985)*. Lecture Notes in Mathematics **1240**, 275–280. Springer-Verlag, Berlin/Heidelberg, 1987.

[15] E. Ullmo, Hauteur de Faltings de quotients de $J_0(N)$, discriminants d'algèbres de Hecke et congruences entre formes modulaires. *American Journal of Mathematics* **122** (2000), no. 1, 83–115.

[16] I. Varma, *Sums of Squares, Modular Forms, and Hecke Characters*. Master's thesis, Universiteit Leiden, 2010.

1er octobre 2010

Peter Bruin, Département de Mathématiques d'Orsay, Bâtiment 425, Université Paris-Sud 11, 91405 Orsay cedex, France • *E-mail :* `Peter.Bruin@math.u-psud.fr`