# On the computation of the coefficients of modular forms

Bas Edixhoven, Mathematisch Instituut, Universiteit Leiden

November 29, 2008

## 1 Introduction

The aim of this article is to give an overview of joint work with Jean-Marc Couveignes, Robin de Jong, Franz Merkl, and Johan Bosman. Details of this joint work can be found in [9] (that text will be updated soon, and will eventually appear as a book in the series "Annals of Mathematics Studies" of Princeton University Press), in [7] and in [3] and [2]. The updated version of [9] will contain the results mentioned in the last sections of this text. The book version will contain deterministic variants of the probabilistic algorithms given in [9]. In this overview, by *algorithm* we mean deterministic algorithm. We will focus on the main results and ideas, skipping technical details, and we will also mention some future developments. In comparison to the previous overview [10] of this joint work, this text discusses the developments since 2006: more examples by Johan Bosman, generalisation to forms of level one of arbitrary weight, and application to theta functions of lattices; it says much less about the method by which Galois representations are computed.

An important example of our main results can be formulated easily. Ramanujan's $\tau$-function $\tau : \mathbb{N}_{>0} \to \mathbb{Z}$ is defined by the equality of formal power series with integer coefficients:

$$(1.1) \qquad q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n = q - 24q^2 + 252q^3 + \cdots \quad \text{in } \mathbb{Z}[[q]].$$

Hecke already showed that $|\tau(n)| = O(n^6)$ as $n$ tends to infinity. One can then ask how fast $\tau(n)$ can be computed, as a function of $n$. More precisely, one can ask if there is an algorithm that on input $n \in \mathbb{N}_{>0}$ computes $\tau(n)$ in time polynomial in $\log n$, i.e., in a running time that is bounded by a fixed power of $\log n$. As a partial answer to this question we have the following result.

**1.2 Theorem** *There exists an algorithm that on input a prime number $p$ gives $\tau(p)$, in running time polynomial in $\log p$.*

Let us first indicate why this is fast. For $n \in \mathbb{N}$, a straightforward way to compute $\tau(n)$ is to compute the product in (1.1) up to order $q^n$, i.e., to do the necessary multiplications in the ring $\mathbb{Z}[[q]]/(q^{n+1})$. Clearly, this takes time at least linear in $n$, hence exponential in $\log n$. A faster algorithm for computing $\tau(n)$, based on computation of class numbers, is given in [5]; but, even assuming the generalised Riemann hypothesis (GRH), that algorithm has running time approximately $O(n^{1/2})$, which is still exponential in $\log n$.

Let us emphasise that in Theorem 1.2 the integer $p$ must be a prime number. This condition is not there for some artificial reason. For $n \in \mathbb{N}_{>0}$, the computation of $\tau(n)$ is reduced to the computation of the $\tau(p)$ for $p$ dividing $n$ via well-known properties of the $\tau$-function. These are summarised in the identity of (formal) Dirichlet series

$$(1.3) \qquad \sum_{n\geq 1} \tau(n) n^{-s} = \prod_{p} (1 - \tau(p){\cdot}p^{-s} + p^{11}{\cdot}p^{-2s})^{-1},$$

where the index $p$ of the Euler product on the right ranges over the set of prime numbers. On the other hand, if $p$ and $q$ are distinct prime numbers and $n = pq$, then one can easily compute $\tau(p)^2/p^{11}$ and $\tau(q)^2/q^{11}$ from $\tau(n)$ and $\tau(n^2)$, which shows that factoring $n$ is equivalent to computing $\tau(n)$ and $\tau(n^2)$, provided $\tau(n) \neq 0$. See [1] for details.

The importance of the series $\sum_{n\geq 1} \tau(n) q^n$ in (1.1) comes from the fact that the complex analytic function $\Delta\colon \mathbb{H} \to \mathbb{C}$ on the complex upper half plane defined by

$$(1.4) \qquad \Delta\colon \mathbb{H} \to \mathbb{C}, \quad z \mapsto \sum_{n\geq 1} \tau(n) e^{2\pi i n z}$$

is a modular form of level 1 and weight 12, the so-called discriminant modular form. This means that for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$ and all $z \in \mathbb{H}$ one has

$$(1.5) \qquad \Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12} \Delta(z).$$

Behind our proof of Theorem 1.2 is the existence of Galois representations associated to modular forms. This will be explained in some detail in the next section.

In our opinion, the fact that such Galois representations are accessible to computation is of much interest. We get congruences for $\tau(p)$ modulo all primes $\ell$. The classical congruences only involve the primes 2, 3, 5, 7, 23, and 691. Whereas the classical congruences are given by explicit formulas, these other congruences are "encoded" by number fields $K_\ell$, and can now, in theory, be made explicit. More generally, one can hope that non-solvable global field extensions whose existence is guaranteed by the Langlands program can be made accessible to computation. Our result gives an example of the computation of higher degree étale cohomology with $\mathbb{F}_\ell$-coefficients together with its Galois action. It provides some evidence towards the existence of polynomial time algorithms for computing the number of solutions in $\mathbb{F}_p$ of a fixed system of polynomial equations over $\mathbb{Z}$, when $p$ varies.

To end this introduction, let us note that as a consequence of Theorem 1.2, for $m \in \mathbb{N}$ given together with its factorisation into primes, the number of elements $x$ of the Leech lattice with $\|x\|^2 = 2m$ can be computed in time polynomial in $\log m$. This will be explained in section 5.

## 2 Galois representations

Our proof of Theorem 1.2 uses that $\Delta$ is an eigenform for certain operators named after Hecke, that such an eigenform implies the existence of certain Galois representations (Deligne), and that, for $p$ prime, $\tau(p)$ is the trace of the Frobenius conjugacy class. We make this more explicit.

Deligne has shown in 1969 (see [8]) that for each prime number $\ell$ there exists a number field $K_\ell$ (i.e., finite extension of $\mathbb{Q}$), Galois over $\mathbb{Q}$, together with a faithful representation

$$\rho_\ell\colon\ \mathrm{Gal}(K_\ell/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell), \tag{2.1}$$

uniquely determined by the modular form $\Delta$ by the following conditions. First of all, the representation $\rho_\ell$ is semisimple (i.e., irreducible, or the direct sum of two 1-dimensional representations). Secondly, the extension $\mathbb{Q} \to K_\ell$ is unramified at all primes $p \neq \ell$. Lastly, for all $p \neq \ell$ the characteristic polynomial of the Frobenius element $\rho_\ell(\mathrm{Frob}_p)$ is given by

$$\det(1 - x{\cdot}\rho_\ell(\mathrm{Frob}_p)) = 1 - \tau(p)x + p^{11}x^2. \tag{2.2}$$

The notions "unramified" and "Frobenius element" will be made explicit in a moment. What is important now is that we have a description of $\tau(p)$ mod $\ell$:

$$\text{for all } \ell \neq p\text{:} \quad \mathrm{trace}(\rho_\ell(\mathrm{Frob}_p)) = \tau(p) \quad \text{in } \mathbb{F}_\ell. \tag{2.3}$$

The fields $K_\ell$, which encode non-explicit congruences mod $\ell$ for $\tau(p)$, for all $p \neq \ell$, can be thought of as an analog in the $\mathrm{GL}_2$ context of the fields $\mathbb{Q}(\zeta_\ell)$ generated by the roots of unity of order $\ell$. Serre and Swinnerton-Dyer have shown that for $\ell$ not in $\{2, 3, 5, 7, 23, 691\}$ we have $\mathrm{im}(\rho_\ell) \supset \mathrm{SL}_2(\mathbb{F}_\ell)$, hence for these $\ell$ (called non-exceptional) the extension $\mathbb{Q} \to K_\ell$ is not solvable. Nevertheless, these $K_\ell$ can now be computed efficiently.

**2.4 Theorem** *There exists an algorithm that on input $\ell$ computes $\rho_\ell$ in time polynomial in $\ell$. More precisely, it gives:*

- *the extension* $\mathbb{Q} \to K_\ell$*, given in terms of the "structure constants"* $a_{i,j,k} \in \mathbb{Q}$ *with respect to a* $\mathbb{Q}$*-basis* $e$*:* $e_i e_j = \sum_k a_{i,j,k} e_k$*;*

- *a list of the elements* $\sigma$ *of* $\mathrm{Gal}(K_\ell/\mathbb{Q})$*, where each* $\sigma$ *is given as its matrix with respect to* $e$*;*

- *the injective morphism* $\rho_\ell\colon\ \mathrm{Gal}(K_\ell/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$.

Before discussing the proof of this result, let us describe how it implies Theorem 1.2, via standard methods from computational number theory. So, let $p$ be a prime number. The strategy is then to compute $\tau(p)$ mod $\ell$ for all $\ell$ up to some sufficiently large number $x(p)$. One knows that $|\tau(p)| < 2p^{11/2}$ by Deligne, and that $\prod_{\ell<x(p)} \ell \approx e^{x(p)}$. So, in order to deduce $\tau(p)$ from the congruences modulo all $\ell < x(p)$, it is sufficient to take $x(p)$ a suitable constant times $\log p$. Hence, for proving Theorem 1.2, it suffices to show that for primes $p$ and $\ell$, one can compute $\tau(p)$ mod $\ell$ in time polynomial in $\ell\cdot \log p$. Theorem 2.4 gives us $\rho_\ell$ in time polynomial in $\ell$. Then one computes a $\mathbb{Q}$-basis $e'$ of $K_\ell$ such that the denominators of the structure constants $a'_{i,j,k}$ with respect to $e'$ are not divisible by $p$ and such that the $\mathbb{F}_p$-algebra obtained by reduction mod $p$ of the $a'_{i,j,k}$ is a product of fields (unramifiedness at $p$ means that such a basis $e'$ exists); here one uses an algorithm of Buchmann and Lenstra (see [4]). The group $\mathrm{Gal}(K_\ell/\mathbb{Q})$ then permutes these fields, and for each of them, there is a unique element in $\mathrm{Gal}(K_\ell/\mathbb{Q})$ that induces the $p$-power automorphism on it. This gives, up to conjugation, an element $\mathrm{Frob}_p$ in $\mathrm{Gal}(K_\ell/\mathbb{Q})$. Then one has $\tau(p) = \mathrm{trace}(\rho_\ell(\mathrm{Frob}_p))$ in $\mathbb{F}_l$.

Let us now discuss how one proves Theorem 2.4. As this will become somewhat technical, some readers may want to skip it from some point on and continue with the next section.

So, let $\ell$ be a prime number. We may and do assume that the image of $\rho_\ell$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$. According to [8], $\rho_\ell$ is realised on a 2-dimensional sub-$\mathbb{F}_\ell$-vector space $V_\ell$ of the dual of the étale cohomology group $H^{11}(E^{10}_{\overline{\mathbb{Q}},\mathrm{et}}, \mathbb{F}_\ell)$, where $E^{10}$ is the 10-fold self-product of the "universal elliptic curve". In particular, $E^{10}$ is an 11-dimensional algebraic variety, defined over $\mathbb{Q}$, and independent of $\ell$. At this point, the reader is not required to know what all this is; we just want to convince him/her that this realisation of $\rho_\ell$ is not easily accessible for computation in a direct way.

Via some standard methods in étale cohomology (the Leray spectral sequence, and passing to a finite cover to trivialise a locally constant sheaf of finite dimensional $\mathbb{F}_\ell$-vector spaces), or from the theory of congruences between modular forms, it is well known that $V_\ell$ also occurs in the $\ell$-torsion $J_\ell(\overline{\mathbb{Q}})[\ell]$ of the Jacobian variety $J_\ell$ of some modular curve $X_\ell$ defined over $\mathbb{Q}$. The field $K_\ell$ is then the field generated by suitable "coordinates" of the points $x \in V_\ell \subset J_\ell(\overline{\mathbb{Q}})[\ell]$.

The Riemann surface $X_\ell(\mathbb{C})$ of complex points of $X_\ell$ can be described as:

$$X_\ell(\mathbb{C}) = \Gamma_1(\ell)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})), \tag{2.5}$$

where $\Gamma_1(\ell) = \{(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \mathrm{SL}_2(\mathbb{Z}) \mid a \equiv 1 \pmod{\ell} \text{ and } c \equiv 0 \pmod{\ell}\}$.

We are now in the more familiar situation of torsion points on abelian varieties. But the price that we have paid for this is that the abelian variety $J_\ell$ depends on $\ell$, and that its dimension, equal to the genus of $X_\ell$, i.e., equal to $(\ell-5)(\ell-7)/24$, grows quadratically with $\ell$. This makes it impossible to directly compute the $x \in V_\ell$ using computer algebra: known algorithms for solving systems of non-linear polynomial equations take time exponential in the dimension.

At this point, Couveignes suggested to use approximations and height bounds. This is an important idea. In its simplest form, it works as follows. Suppose that $x$ is a rational number, $x = a/b$, with $a$ and $b$ in $\mathbb{Z}$ coprime. Suppose that we have an upper bound $M$ for $\max(|a|, |b|)$. Then $x$ is determined by any approximation $y \in \mathbb{R}$ of $x$ such that $|y - x| < 1/2M^2$, simply because for all $x' \neq x$ with $x' = a'/b'$, where $a'$ and $b'$ in $\mathbb{Z}$ satisfy $\max(|a'|, |b'|) < M$, we have $|x' - x| = |(a'b - ab')/bb'| \geq 1/M^2$.

For the computation of $K_\ell$, we consider the minimal polynomial $P_\ell$ in $\mathbb{Q}[T]$ of a carefully theoretically constructed generator $\alpha$ of $K_\ell$. We use approximations of all Galois conjugates of $\alpha$, i.e., of all roots of $P_\ell$. Instead of working directly with torsion points of $J_\ell$, we work with divisors on the curve $X_\ell$. Using this strategy, the problem of showing that $P_\ell$ can be computed in time polynomial in $\ell$ is divided into two different tasks. Firstly, to show that the number of digits necessary for a good enough approximation of $P_\ell$ is bounded by a fixed power of $\ell$. Secondly, to show that, given $\ell$ and $n$, the coefficients of $P_\ell$ can be approximated with a precision of $n$ digits in time polynomial in $n{\cdot}\ell$. The first problem was solved by Bas Edixhoven and Robin de Jong, with some help by Franz Merkl, using Arakelov geometry. The second problem was solved by Jean-Marc Couveignes, in two ways: complex approximations (numerical analysis), and approximations in the sense of reductions modulo many small primes, using exact computations in Jacobians of modular curves over finite fields. We emphasise that the solutions to each of these problems required much work, which occupies most of the pages of [9] and of [7].

# 3 Johan Bosman's examples

Using the Magma system to do computer computations over $\mathbb{C}$, Johan Bosman has found, for all $\ell \leq 23$ and for every normalised cuspidal eigenform $f_k$ of level one and weight $k \leq 22$, a polynomial $P_{k,\ell}$ of degree $\ell + 1$ that gives the projective Galois representation over $\mathbb{F}_\ell$ associated to $f_k$:

$$\overline{\rho}_{f_k,\ell}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell) \to \mathrm{PGL}_2(\mathbb{F}_\ell).$$

More precisely, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the roots of $P_{k,\ell}$ corresponds to the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ via $\rho_{f_k,\ell}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ on the set of 1-dimensional sub-$\mathbb{F}_\ell$-vector spaces of $\mathbb{F}_\ell^2$. We refer to [3] for these examples, where the 13 cases with non-solvable image are listed in a table at the end. Three of the examples come from $\ell$-torsion of elliptic curves. For the 10 other cases, one must really work with the Jacobian $J_\ell$, which is of dimension 12 for $\ell = 23$.

In order to find the polynomials $P_{k,\ell}$, Bosman computed, with a high precision, approximations of them, which allowed him to *guess* the $P_{k,\ell}$. The theoretically proved sufficient precision is not really made explicit in [9], and even if it was, it would not be practical. The $P_{k,\ell}$ thus obtained do have the property that their splitting field is unramified outside $\ell$, and that it has the right Galois group. To really *prove* that his $P_{k,\ell}$ are correct, he then uses the recent progress by Khare, Wintenberger, Kisin (see [11] and [12]) on Serre's conjecture on modularity of 2-dimensional Galois representations over finite fields. The projective representations to $\mathrm{PGL}_2(\mathbb{F}_\ell)$ coming from the $P_{k,\ell}$ can be lifted to $\mathrm{GL}_2(\mathbb{F}_\ell)$, still being unramified outside $\ell$, and thus come from a modular form of level one and of minimal weight, which is then shown to be $f_k$.

We list some of Bosman's examples. The polynomials given here are not the approximated ones, but have been obtained by taking suitable elements in the ring of integers of the field given by the approximated polynomials.

$$\begin{aligned}P_{12,17} = {} & x^{18} - 9x^{17} + 51x^{16} - 170x^{15} + 374x^{14} - 578x^{13} + 493x^{12} - 901x^{11} + 578x^{10} \\ & - 51x^9 + 986x^8 + 1105x^7 + 476x^6 + 510x^5 + 119x^4 + 68x^3 + 306x^2 \\ & + 273x + 76.\end{aligned}$$

$$\begin{aligned}P_{12,19} = {} & x^{20} - 7x^{19} + 76x^{17} - 38x^{16} - 380x^{15} + 114x^{14} + 1121x^{13} - 798x^{12} - 1425x^{11} \\ & + 6517x^{10} + 152x^9 - 19266x^8 - 11096x^7 + 16340x^6 + 37240x^5 + 30020x^4 \\ & - 17841x^3 - 47443x^2 - 31323x - 8055.\end{aligned}$$

$$\begin{aligned}P_{22,23} = {} & x^{24} - 11x^{23} + 46x^{22} - 1127x^{20} + 6555x^{19} - 7222x^{18} - 140737x^{17} \\ & + 1170700x^{16} - 2490371x^{15} - 16380692x^{14} + 99341324x^{13} + 109304533x^{12} \\ & - 2612466661x^{11} + 4265317961x^{10} + 48774919226x^9 \\ & - 244688866763x^8 - 88695572727x^7 + 4199550444457x^6 \\ & - 10606348053144x^5 - 25203414653024x^4 + 185843346182048x^3 \\ & - 228822955123883x^2 - 1021047515459130x + 2786655204876088.\end{aligned}$$

As an application of his computation of the $P_{12,\ell}$ for $\ell$ in $\{13, 17, 19\}$, Bosman has verified Lehmer's conjecture that for all $n \in \mathbb{Z}_{\geq 1}$, $\tau(n) \neq 0$ up to a higher bound than what was done before. More precisely, he has shown that for all $n < 22798241520242687999 \approx 2 \cdot 10^{19}$ one has $\tau(n) \neq 0$. The previous bound was $22689242781695999 \approx 2 \cdot 10^{16}$.

Using the same methods, Johan Bosman could also produce a polynomial that gives an $\mathrm{SL}_2(\mathbb{F}_{16})$ extension of $\mathbb{Q}$, corresponding to a weight 2 modular form on $\Gamma_0(137)$ (genus 11). Such an example was still missing in tables of Jürgen Klüners. See [2].

# 4 Modular forms of level 1 and arbitrary weight

In this section we present the generalisation of Theorem 1.2 on fast computation of $\tau(p)$ to forms of level 1 and arbitrary weight.

For $k \in \mathbb{Z}$, a holomorphic function $f\colon \mathbb{H} \to \mathbb{C}$ is called a modular form of level 1 and weight $k$ if it satisfies the following two conditions. The first condition is that for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$ and for all $z$ in $\mathbb{H}$ we have $f((az+b)/(cz+d)) = (cz+d)^k f(z)$. This implies that for all $z \in \mathbb{H}$ we have $f(z+1) = f(z)$, hence that $f$ has a $q$-expansion $f = \sum_{n \in \mathbb{Z}} a_n(f) q^n$ (recall that $q(z) = \exp(2\pi i z)$). The second condition is that $f$ is "holomorphic at the cusp", i.e., that for all $n < 0$ we have $a_n(f) = 0$.

For $k \in \mathbb{Z}$, we let $M_k$ denote the $\mathbb{C}$-vector space of modular forms of level 1 and weight $k$. The subspace $S_k$ consisting of the $f$ with $a_0(f) = 0$ is called the space of cuspforms. The direct sum $M$ of all $M_k$ is a graded $\mathbb{C}$-algebra, and it is well known to be generated by the Eisenstein series of weights 4 and 6, together with $\Delta$, satisfying one relation:

$$M = \mathbb{C}[E_4, \Delta] \oplus E_6 {\cdot} \mathbb{C}[E_4, \Delta],$$

where:

$$E_4 = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n, \quad E_6 = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n, \quad \text{and} \quad \Delta = \frac{E_4^3 - E_6^2}{1728},$$

and where, for $m$ and $n$ in $\mathbb{N}$, $\sigma_m(n) = \sum_{0<d|n} d^m$. The space $M_k$ is zero if $k < 0$, and, for $k \geq 0$ its dimension grows linearly with $k$: $\dim M_k - k/12$ is bounded. For each $k$ in $\mathbb{Z}$ we have $S_k = \Delta M_{k-12}$. For $k \geq 4$, $S_k$ has codimension one in $M_k$.

For each $k \in \mathbb{N}$, the space $M_k$ is equipped with Hecke operators, coming from the action of $\mathrm{GL}_2(\mathbb{Q})^+$ on $\mathbb{H}$. These operators preserve $S_k$. For each $i \in \mathbb{N}_{>0}$ one has an operator $T_i$ (we do not include $k$ in the notation). The $\mathbb{Z}$-algebra in $\mathrm{End}_{\mathbb{C}}(S_k)$ generated by the $T_i$ is called the Hecke algebra $\mathbb{T}_k$ acting on cuspforms of level 1 and weight $k$. It is commutative, generated by the $T_p$ with $p$ prime. For $p$ prime, the action of $T_p$ on $M_k$ is as follows:

$$\text{for } f \text{ in } M_k \text{ and } p \text{ prime:} \quad T_p f = \sum_{n\geq 0} a_{np}(f)q^n + \sum_{n\geq 0} p^{k-1}a_n(f)q^{np}.$$

The Hecke algebra $\mathbb{T}_k$, together with its elements $T_i$, $i \in \mathbb{N}_{>0}$, gives us another interpretation of $S_k$: the pairing $S_k \times \mathbb{T}_k \to \mathbb{C}$, $(f,t) \mapsto a_1(t(f))$, identifies $S_k$ with the space of $\mathbb{Z}$-linear maps from $\mathbb{T}_k$ to $\mathbb{C}$. The subset of morphisms of $\mathbb{Z}$-algebras corresponds to the set of normalised cuspidal eigenforms: the $f$ in $S_k$ such that $a_1(f) = 1$ and $T_i(f) = a_i(f)\cdot f$ for all $i$. Each $S_k$ has a natural inner product, for which the $T_i$ are self-adjoint, hence $S_k$ has a basis of eigenforms, and all eigenvalues are real.

The structure of $M$ given above implies that as a $\mathbb{Z}$-module, $\mathbb{T}_k$ is generated by the $T_i$ with $i \leq k/12$, and that it is free of rank $\dim_{\mathbb{C}} S_k$. Therefore, an element $f$ of $S_k$ is determined by its values on the $T_i$ with $i \leq k/12$. The following theorem is the generalisation of Theorem 1.2 to arbitrary weights: it says that the coefficients $a_p(f)$ can be computed quickly, if the $a_m(f)$ for $m \leq k/12$ are given.

**4.1 Theorem** *Assume the generalised Riemann hypothesis for number fields, or, in the following, assume that $k$ bounded. There is an algorithm that on input $k \in \mathbb{N}$ and $p$ prime gives the element $T_p$ of $\mathbb{T}_k$ as a $\mathbb{Z}$-linear combination of the $T_i$ with $i \leq k/12$, in time polynomial in $k \log p$.*

The principle of the proof of Theorem 4.1 is simply to compute the image of $T_p$ in sufficiently many quotients $\mathbb{T}_k/m$ of $\mathbb{T}_k$ by maximal ideals. We only consider maximal ideals $m$ of $\mathbb{T}_k$ with $\mathbb{T}_k/m$ a prime field, and with $\#(\mathbb{T}_k/m) \leq x$ for a suitable bound $x$ to be specified later. We let $P(k,x)$ be the set of these $m$. We will use the LLL-algorithm (see [13]) to compute $T_p$ from all these congruences, replacing the Chinese remainder theorem that we used in the case $k = 12$, where $\mathbb{T}_{12} = \mathbb{Z}$.

The $\mathbb{Z}$-algebra $\mathbb{T}_k$ can be computed, in the form of a $\mathbb{Z}$-basis and a multiplication table, in time polynomial in $k$, using algorithms for computing with modular symbols (see [15]).

For each maximal ideal $m$ of $\mathbb{T}_k$ there is a unique semi-simple Galois representation $\rho_m$ from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{GL}_2(\mathbb{T}_k/m)$ that is unramified at all primes $q$ not equal to the characteristic of $\mathbb{T}_k/m$, and such that for all such $q$ the Frobenius element $\rho_m(\mathrm{Frob}_q)$ has trace $T_q$ and determinant $q^{k-1}$ in $\mathbb{T}_k/m$. Just as in Theorem 2.4, for $m$ with $\mathbb{T}/m$ a prime field, $\rho_m$ can be computed in time polynomial in $k\cdot \log(\#\mathbb{T}_k/m)$. Hence we can compute the image of $T_p$ in all the $\mathbb{T}_k/m$ with $m$ in $P(k,x)$ in time polynomial in $kx$. We let $\mathbb{I}_{k,x}$ be the intersection in $\mathbb{T}_k$ of all $m$ in $P(k,x)$. Then we have the exact sequence:

$$0 \to \mathbb{I}_{k,x} \to \mathbb{T}_k \to \prod_{m\in P(k,x)} \mathbb{T}_k/m \to 0,$$

and we can compute the image $\overline{T_p}$ of $T_p$ in $\mathbb{T}_k/\mathbb{I}_{k,x}$, as well as a pre-image $T'_p$ in $\mathbb{T}_k$ of $\overline{T_p}$ in time polynomial in $kx$. We will now address the problem of how to choose $x$ so that we can efficiently compute $T_p$ from $T'_p$.

In the case where $k$ is not fixed, we will use the assumption of GRH to show that there are sufficiently many $m$'s, in the form of the following effective prime number theorem for number fields (see [16]).

**4.2 Theorem (Weinberger)** *Assume GRH for number fields. For $K$ a number field and $x$ in $\mathbb{R}$ let $\pi_1(x, K)$ denote the number of maximal ideals $m$ of the ring of integers $O_K$ of $K$ with $O_K/m$ a prime field and with $|O_K/m| \leq x$. For $x > 2$ in $\mathbb{R}$ let $\mathrm{li}(x) = \int_2^x (1/\log y)dy$. Then there exists $c_1$ in $\mathbb{R}$ such that for every number field $K$ and for every $x > 2$ one has*

$$|\pi_1(x, K) - \mathrm{li}(x)| \leq c_1\sqrt{x}\log\left(|\operatorname{discr}(O_K)x^{\dim_{\mathbb{Q}} K}|\right),$$

*where $\operatorname{discr}(O_K) \in \mathbb{Z}$ denotes the discriminant of $O_K$.*

As all eigenvalues of all $T_i$ on all $S_k$ are real, we have, for each $k$, an isomorphism of $\mathbb{R}$-algebras $\mathbb{R} \otimes \mathbb{T}_k \to \mathbb{R}^{\dim S_k}$, unique up to permutation of the factors. The standard inner product on $\mathbb{R}^{\dim S_k}$ is the trace form of this $\mathbb{R}$-algebra, hence is obtained by extension of scalars from $\mathbb{Z}$ to $\mathbb{R}$ of the trace form of $\mathbb{T}_k$. We will view each $\mathbb{T}_k$ as a lattice in $\mathbb{R} \otimes \mathbb{T}_k$, and we equip each $\mathbb{R} \otimes \mathbb{T}_k$ with the standard volume form, i.e., the one for which the unit cube has volume one. From the Ramanujan bound on the eigenvalues of the $T_i$, proved by Deligne, one easily derives that

$$\log \mathrm{Vol}(\mathbb{R} \otimes \mathbb{T}_k/\mathbb{T}_k) = \frac{1}{2}\log \operatorname{discr}|\mathbb{T}_k| \leq \frac{k^2}{24}\log k.$$

Let us now explain how we choose $x$ as a function of $k$ and $p$, assuming GRH for number fields. Let $n_k$ be the rank of $\mathbb{T}_k$, i.e., $n_k = \dim_{\mathbb{C}} S_k$. We can and do assume that $n_k > 0$. The norm of the element $T_p$ that we want to compute from a congruence modulo $\mathbb{I}_{k,x}$ is bounded, by Deligne, as follows:

$$\|T_p\| \leq 2n_k^{1/2}p^{(k-1)/2}.$$

Applying Theorem 4.2 to the number fields of which $\mathbb{Q} \otimes \mathbb{T}_k$ is a product, one proves that for $x$ a suitable constant times fixed powers of $k$ and $\log(p)$, one has the following lower bound for the length of a shortest non-zero element of $\mathbb{I}_{k,x}$:

$$\mu_1(\mathbb{I}_{k,x}) > 2^{(n_k+1)/2}{\cdot}\|T_p\|, \quad \text{where} \quad \mu_1(\mathbb{I}_{k,x}) = \min\{\|t\| \mid t \in \mathbb{I}_{k,x} - \{0\}\}.$$

Under these conditions, the standard approach for using the LLL-algorithm for the "closest vector problem" shows that $T_p$ can be computed from our element $T'_p$ in $T_p + \mathbb{I}_{k,x}$, in time polynomial in $k\log(p)$, as follows.

Let $b$ denote our inner product on $\mathbb{T}_k$, i.e., the trace form. Let $e = (e_1, \ldots, e_n)$ be an "LLL-reduced basis" of $\mathbb{I}_{k,x}$: if $e^* = (e_1^*, \ldots, e_n^*)$ denotes the orthogonal $\mathbb{R}$-basis of $\mathbb{R} \otimes \mathbb{T}_k$ obtained from $e$ by letting $e_i^*$ be the orthogonal projection of $e_i$ to the orthogonal complement of the subspace of $\mathbb{R} \otimes \mathbb{T}_k$ generated by $\{e_j \,|\, j < i\}$ (i.e., by the Gram-Schmidt orthogonalisation process), and $\mu_{i,j} := b(e_i, e_j^*)/b(e_j^*, e_j^*)$, then we have:

$$
\begin{aligned}
&|\mu_{i,j}| \leq \frac{1}{2} \quad \text{for } 1 \leq j < i \leq n, \text{ and} \\
&\|e_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|e_{i-1}^*\|^2 \quad \text{for } 1 < i \leq n.
\end{aligned}
$$

Then $T_p$ can be recovered from $T_p'$ as follows:

- put $x_n := T_p'$;
- for $i$ going down from $n$ to 1 let $x_{i-1} := x_i - [b(x_i, e_i^*)/b(e_i^*, e_i^*)]e_i$, where, for $y$ in $\mathbb{Q}$, $[y]$ denotes the largest of the (one or two) integers nearest to $y$;
- then $T_p = x_0$.

In the case where $k$ is fixed, in Theorem 4.1, the $\mathbb{Z}$-algebra $\mathbb{T}_k$ is fixed, and the ordinary asymptotic prime number theorem for each of the factors of $\mathbb{Q} \otimes \mathbb{T}_k$ suffices for what we do.

**4.3 Theorem** *Assume GRH for number fields, or, in the following, assume that $k$ is bounded. There exists an algorithm that on input positive integers $k$ and $n$, together with the factorisation of $n$ into prime factors, computes the element $T_n$ of $\mathbb{T}_k$ as $\mathbb{Z}$-linear combination of the $T_i$ with $i \leq k/12$.*

Theorem 4.3 follows from Theorem 4.1 by using the standard way to express $T_n$ in the $T_p$ for the prime numbers $p$ dividing $n$:

$$
T_m = \prod_{p|m} T_{p^{v_p(m)}}, \quad T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} T_{p^{r-2}}.
$$

# 5 Lattices

Theorem 4.3 has an interesting application to certain modular forms that come from lattices: theta functions of even unimodular lattices.

Let us consider a free $\mathbb{Z}$-module $L$ of finite rank $n_L$, equipped with a positive definite symmetric bilinear form $b\colon L \times L \to \mathbb{Z}$. Then $L_{\mathbb{R}} := \mathbb{R} \otimes L$ is an $\mathbb{R}$-vector space of dimension $n_L$

on which $b$ gives an inner product, and hence $L$ is a lattice in the euclidean space $L_{\mathbb{R}}$. For $m$ in $\mathbb{Z}$ we define:

$$r_L(m) := \#\{x \in L \mid b(x,x) = m\}. \tag{5.1}$$

In this situation, one considers the so-called *theta-function* $\theta_L \colon \mathbb{H} \to \mathbb{C}$ associated to $(L, b)$:

$$\theta_L = \sum_{x \in L} q^{b(x,x)/2} = \sum_{m \geq 0} r_L(m) q^{m/2}, \quad \text{where } q \colon z \mapsto \exp(2\pi i z). \tag{5.2}$$

The form $b$ is called *even* if $b(x, x)$ is even for all $x$ in $L$. Equivalently, $b$ is even if and only if the matrix of $b$ with respect to a basis of $L$ has only even numbers on the diagonal. The form $b$ is called *unimodular* if the map $x \mapsto (y \mapsto b(x, y))$ from $L$ to its dual $L^\vee$ is an isomorphism of $\mathbb{Z}$-modules. Equivalently, $b$ is unimodular if and only if the matrix of $b$ with respect to a basis of $L$ has determinant 1. If $(L, b)$ is even and unimodular, then $n_L$ is even, and $\theta_L$ is a modular form of level 1 and weight $n_L/2$ (see [14, VII,§6]). This explains that Theorem 4.3 has the following consequence.

**5.3 Theorem** *Assume GRH, or, in the following, consider only $(L, b)$ whose ranks $n_L$ are bounded. There is an algorithm that, on input the rank $n_L$ and the integers $r_L(i)$ for $1 \leq i \leq n_L/24$ of an even unimodular lattice $(L, b)$, and an integer $m > 0$ together with its factorisation into primes, computes $r_L(m)$ in time polynomial in $n_L \log(m)$.*

To prove this theorem, one writes $\theta_L$ as a rational multiple of the Eisenstein series $E_{n_L/2}$ of weight $n_L/2$ plus a cuspform $f$ with rational coefficients. The coefficient $a_m(E_{n_L/2})$ can be computed easily, because $m$ is given with its factorisation. For $a_m(f)$ one first computes the $a_i(f)$ for $i \leq n_L/24$, using the $r_L(i)$. Then, viewing $f$ as a $\mathbb{Z}$-linear map $\mathbb{T}_{n_L/2} \to \mathbb{Q}$, one has $a_m(f) = f(T_m)$ and one applies Theorem 4.3.

We give an example. Let $L$ be the *Leech lattice*. It is the unimodular lattice of rank 24 that, according to Henry Cohn and Abhinav Kumar [6], gives the densest lattice sphere packing in dimension 24. As $M_{12}$ is two-dimensional, generated by $E_{12}$ and $\Delta$, $\theta_L$ is a linear combination of these two. Comparing the coefficients of $q^m$ for $m = 0$ and $m = 1$ gives:

$$\theta_L = E_{12} - \frac{65520}{691}\Delta, \quad \text{with } E_{12} = 1 + \frac{65520}{691}\sum_{n \geq 1} \sigma_{11}(n) q^n.$$

Theorem 5.3 says that if $m > 0$ is given, with its factorisation into primes, then $r_L(m)$ can be computed in time polynomial in $\log(m)$.

We can also consider direct sums of copies of $L$. For $n \in \mathbb{N}$, we have:

$$\theta_{L^n} = \sum_{x_1, \ldots, x_n \in L} q^{(b(x_1,x_1) + \cdots + b(x_n,x_n))/2} = \left(\sum_{x \in L} q^{b(x,x)/2}\right)^n = \theta_L^n.$$

This means that we can compute the $r_{L^n}(i)$ for $1 \leq i \leq n$ in time polynomial in $n$ by doing our multiplications in $\mathbb{Z}[[q]]/(q^{n+1})$. Hence, assuming GRH, if $m > 0$ is given, with its factorisation into primes, then $r_{L^n}(m)$ can be computed in time polynomial in $n \log(m)$.

It is interesting to note that, theta functions are usually considered as modular forms whose coefficients are easy to compute. As such, they can be used to compute coefficients of cuspforms. But for coefficients $a_m$ with $m$ large, one now concludes that the situation is reversed.

# 6 Future perspectives

It is to be expected that Theorem 4.3 will be generalised to the spaces of cuspforms of varying level and weight, with running time for computing $T_n$ polynomial in $\log(n)$, the level and the weight. A PhD-student, Peter Bruin, is working on this.

Hence, it is also to be expected that, assuming GRH, there is an algorithm that on input positive integers $n$ and $m$, together with the factorisation of $m$ into primes, computes the number:

$$r_{\mathbb{Z}^{2n}}(m) = \#\{x \in \mathbb{Z}^{2n} \mid x_1^2 + \cdots + x_{2n}^2 = m\}$$

in time polynomial in $n$ and $\log(m)$. Hence, even in the absence of explicit simple formulas for the $r_{\mathbb{Z}^{2n}}(m)$ as one has for $n \leq 5$, there will be an algorithm that computes the $r_{\mathbb{Z}^{2n}}(m)$ as fast as if one had such formulas.

Another consequence of the expected generalisation of Theorem 4.3 mentioned above is that, again assuming GRH, there is an algorithm that on input a positive number $n$ and a finite field $\mathbb{F}_q$ computes the number $\#X_1(n)(\mathbb{F}_q)$ in time polynomial in $n$ and $\log q$. Indeed, this is a matter of computing the element $T_p$ (where $p$ is the prime dividing $q$) in the Hecke algebra acting on the space $S_2(\Gamma_1(n))$ of modular forms of weight 2 on $\Gamma_1(n)$. At this moment, there is no algorithm known for point counting on curves $C$ over $\mathbb{F}_q$ that has running time polynomial in $\log(q)$ and the genus of $C$, if both the genus and the characteristic of $\mathbb{F}_q$ are not bounded. The case of modular curves is interesting, but does not indicate how to solve this for general curves.

# References

[1] E. Bach and D. Charles. *The hardness of computing an eigenform.* arXiv:0708.1192.

[2] J. Bosman. *A polynomial with Galois group* $\mathrm{SL}_2(\mathbb{F}_{16})$. arXiv:math/0701442.

[3] J. Bosman. *On the computation of Galois representations associated to level one modular forms.* arXiv:0710.1237

[4] J.A. Buchmann and H.W. Lenstra. *Approximating rings of integers in number fields.* J. Théor. Nombres Bordeaux 6 (1994), no. 2, 221–260.

[5] D. Charles. *Computing the Ramanujan tau function.* Ramanujan J. 11 (2006), no. 2, 221–224.

[6] H. Cohn and A. Kumar. *The densest lattice in twenty-four dimensions.* Electron. Res. Announc. Amer. Math. Soc. 10 (2004), 58–67 (electronic).

[7] J-M. Couveignes. *Linearizing torsion classes in the Picard group of algebraic curves over finite fields.* arXiv:0706.0272

[8] P. Deligne. *Formes modulaires et représentations $l$-adiques.* Séminaire Bourbaki, 355, Février 1969.

[9] S.J. Edixhoven, J-M. Couveignes, R. de Jong, F. Merkl and J. Bosman. *On the computation of coefficients of a modular form.* Arxiv:math.NT/0605244.

[10] S.J. Edixhoven. *On the computation of the coefficients of a modular form.* Algorithmic number theory, 30–39, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006.

[11] C. Khare. *Serre's modularity conjecture: the level one case.* Duke Math. J. 134 (2006), no. 3, 557–589.

[12] M. Kisin. *Modularity of 2-dimensional Galois representations.* Current Developments in Mathematics 2005, 191-230.

[13] A.K. Lenstra, H.W. Lenstra, and L. Lovász. *Factoring polynomials with rational coefficients.* Math. Ann. 261 (1982), no. 4, 515–534.

[14] J-P. Serre. *Cours d'arithmétique.* Deuxième édition revue et corrigée. Le Mathématicien, No. 2. Presses Universitaires de France, Paris, 1977.

[15] W. Stein. *Modular forms, a computational approach,* with an appendix by Paul E. Gunnells. Graduate Studies in Mathematics, 79. American Mathematical Society, Providence, RI, 2007.

[16] P.J. Weinberger. *Finding the number of factors of a polynomial.* J. Algorithms 5 (1984), no. 2, 180–186.