COUNTING LATTICE VECTORS

DENIS XAVIER CHARLES

Abstract. We consider the problem of counting the number of lattice vectors of a given length and prove several results regarding its computational complexity. We show that the problem is ♯P-complete resolving an open problem. Furthermore, we show that the problem is at least as hard as integer factorization even for lattices of bounded rank or lattices generated by vectors of bounded norm. Next, we discuss a deterministic algorithm for counting the number of lattice vectors of length d in time $2^{O(rs+\log d)}$, where r is the rank of the lattice, s is the number of bits that encode the basis of the lattice. The algorithm is based on the theory of modular forms.

Date: January 2005.

Research supported in part by NSF grant CCR-9988202. A preliminary version of this work was presented as a contributed talk at the Banff conference in honour of Prof. Hugh C. Williams (May 2003).

1. Introduction

Lattices are a source of some remarkably hard computational problems. For example, finding the shortest vector in a lattice or finding a closest lattice vector to a given point seem to be difficult tasks. See [Cai99] for a survey of results in this area. In this article we consider the problem of exactly counting the number of vectors in a lattice at a given distance (under the L_2-norm). We show the following hardness results regarding this problem.

(1) Counting lattice vectors is $\sharp\mathsf{P}$-complete.
(2) There is a randomized polynomial time reduction from integer factorization to the problem of counting lattice vectors in lattices of fixed rank $r \geq 8$.
(3) There is a randomized polynomial time reduction from integer factorization to the problem of counting lattice vectors in lattices generated by vectors of bounded norm.

The first result resolves an open question posed by Ravi Kumar and Sivakumar in [RS01]. It is known that for fixed rank lattices the problem of counting the lattice points of a given length in L_1-norm is in P (see [DyK97]). The second result shows that in L_2-norm the problem is essentially harder. Our third result shows that even with short basis vectors (where the shortest vector problem is trivial) the problem remains hard.

We also give a deterministic algorithm for this problem that has a running time of $2^{O(rs+\log d)}$, where r is the rank of the lattice, s is the the number of bits in the encoding of the basis and d is the square of the norm of the vectors. Though the problem is $\sharp\mathsf{P}$-hard and our algorithm has an exponential running time, we believe that the algorithm has its own merit and is interesting. In particular, note that any algorithm that exhaustively counts the lattice vectors of norm d requires $2^{\Omega(r \log d)}$ time, since there are lattices that have $2^{\Omega(r \log d)}$ vectors of norm d (for example the Gaussian lattice of rank r). The algorithm we propose uses the deep theory of modular forms that has been developed over the past century. In particular, we use the fact that the *theta series* of a lattice is a modular form. The Fourier coefficients of the theta series encode the number of vectors of a given norm in the lattice. We then make use of recent developments that allow one to compute the space of modular forms to find the Fourier coefficients of this theta series. One can also interpret our algorithm, in conjunction with the hardness results, as providing a family of modular forms whose Fourier coefficients are $\sharp\mathsf{P}$-hard to compute. This seems to be the first result regarding the computational complexity of computing Fourier coefficients of modular forms.

The outline of the rest of the article is as follows. In section (§2) we define the problem formally and describe our results. Section (§3) deals with the $\sharp\mathsf{P}$-hardness result. The reductions involving integer factorization require more machinery and we discuss them later in (§7). In section (§4) we discuss an obvious algorithm to solve this problem. We use this simple algorithm as a part of our main algorithm. Next, we review the relevant facts about modular forms that we need in section (§5). Subsequently, in section (§6) we discuss a version of our algorithm that works for special lattices, where it is easy to see all the general features of the algorithm. Finally, in section (§8) we generalize this method to work for all lattices.

2. Definition of the problem

A lattice $\mathcal{L} \subseteq \mathbb{Q}^n$ is the integer linear span of $r \leq n$ linearly independent vectors of $\mathbb{Q}^n$. In other words $\mathcal{L}$ is a $\mathbb{Z}-$submodule of $\mathbb{Q}^n$, not necessarily of full rank. Our encoding of a lattice lists the basis vectors whose entries are given in binary. Throughout this article when we refer to norm we mean the L_2 norm i.e., if $\mathbf{v} = (a_1, \cdots, a_n) \in \mathbb{Q}^n$ then $\|\mathbf{v}\|^2 = \sum_{1 \leq i \leq n} a_i^2$. If $\mathcal{L}$ is a lattice, then we define a function $\vartheta_{\mathcal{L}} : \mathbb{N} \to \mathbb{N}$ by $\vartheta_{\mathcal{L}}(d) = \sharp\{\mathbf{v} \in \mathcal{L} \ : \ \|\mathbf{v}\|^2 = d\}$. The computational problem that

we are interested in is the following:

Counting Lattice Vectors

Input: A lattice $\mathcal{L} \subseteq \mathbb{Z}^n$ (all the basis vectors have integer coordinates), and an integer d in binary.
Question: What is $\vartheta_{\mathcal{L}}(d)$?

The assumption on the lattices is mild since any lattice can be scaled up (say by $\alpha \in \mathbb{Z}$) so that every basis vector has integer coordinates and furthermore $\vartheta_{\mathcal{L}}(d) = \vartheta_{\alpha\mathcal{L}}(\alpha^2 d)$.

Ajtai showed in [Aj97] that finding the shortest non-zero vector in a lattice in L_2-norm is NP-hard. But the reduction he obtained is randomized and non-parsimonious, thus the ♯P-hardness of the counting version of this problem remained open. In [RS01] Ravi Kumar and Sivakumar asked whether counting lattice vectors is ♯P−hard. Our first result is that indeed the problem is ♯P-hard under polynomial time Turing reductions, resolving the question. We also show that certain restricted versions of the counting lattice vectors problem remain as hard as integer factorization. Next, we describe an algorithm to compute $\vartheta_{\mathcal{L}}(d)$ in time $2^{O(rs+\log d)}$, where r is the rank of the lattice and s is the number of bits of the encoding of $\mathcal{L}$. The exhaustive search method leads to an algorithm that requires $2^{O(r \log d)}$ time, thus our method is faster for large rank r and norm d.

Remark 2.1. One could consider a variant of the problem which is perhaps more natural, namely that of counting the number of vectors of norm *at most* d for a lattice $\mathcal{L}$. It is evident that computing $\vartheta_{\mathcal{L}}(d)$ (polynomial time Turing) reduces to this problem. Thus this variant of the problem is also ♯P-complete as a consequence of Theorem 3.1. Furthermore, our algorithm for computing $\vartheta_{\mathcal{L}}(d)$ can be used to solve this problem by computing $\sum_{\ell \leq d} \vartheta_{\mathcal{L}}(\ell)$ in the same asymptotic running time. Thus both variants are equivalent for our considerations.

3. ♯P-hardness result

We refer the reader to [Pap94] Chapter 18 for the definition of the complexity class ♯P and the notion of ♯P-hardness.

Theorem 3.1. *Counting lattice vectors is* ♯P*-complete under polynomial time Turing reductions.*

Proof : It is easy to see that the problem of Counting lattice vectors is in ♯P, so we concentrate on showing that the problem is hard for the class ♯P.

It is known that computing the permanent of an $n \times n$-matrix with entries in $\{0, 1\}$ is ♯P-complete ([Val79]). Our aim is to give a polynomial time reduction from computing the permanent of such matrices to counting lattice vectors in suitable lattices.

We are given a matrix $M = \{a_{ij}\}_{1 \leq i,j \leq n}$, where $a_{ij} \in \{0, 1\}$. We wish to compute Per $M = \sum_{\sigma \in S_n} \prod_{1 \leq i \leq n} a_{i\sigma(i)}$ where S_n denotes the full group of permutations of n letters.

Let $\log n < \alpha_1 < \alpha_2 < \alpha_3 < \cdots < \alpha_n < \beta_1 < \beta_2 < \cdots < \beta_n < \gamma$ be a sequence of $2n + 1$ integers. Consider the lattice $\mathcal{L} \subseteq \mathbb{Q}^{3n^2}$ of rank n^2 given by basis vectors that are defined below. A vector in $\mathbb{Q}^{3n^2}$ is given by a tuple of $3n^2$ rational numbers. We treat this tuple as being made up of three blocks each of n^2 consecutive entries of the vector. Each block in turn can be thought of as an $n \times n$ matrix. We will call these blocks the A, B and C blocks respectively. We now define the basis vector $\mathbf{v}_{ij}$ for $1 \leq i, j \leq n$. Each block will have *at most one* non-zero entry. The $\langle i, j \rangle$-th entry of the A-block of $\mathbf{v}_{ij}$ is a_{ij} from the matrix M. The $\langle i, j \rangle$-th entry of the B-block of $\mathbf{v}_{ij}$ is

2^{α_i} if $a_{ij} = 1$ and 2^{γ} otherwise, and the $\langle i, j\rangle$-th entry of the C-block of $\mathbf{v}_{ij}$ is 2^{β_j} if $a_{ij} = 1$ and 2^{γ} otherwise. The rest of the entries of the A, B and C blocks are zeroes. This completes the definition of the lattice. It is clear that the rank of $\mathcal{L}$ is n^2.

We make the following key claim:
Claim: There are choices of the sequence $\langle \alpha_i, \beta_j\rangle_{1\le i,j\le n}$ and γ such that the following is true. Suppose $\mathbf{v} = \theta_{11}\mathbf{v}_{11} + \theta_{12}\mathbf{v}_{12} + \cdots + \theta_{nn}\mathbf{v}_{nn}$. Then $\|\mathbf{v}\|^2 = n + \sum_{1\le i\le n}(2^{2\alpha_i} + 2^{2\beta_i})$ iff there is a $\sigma \in S_n$ such that $\prod_{1\le i\le n} a_{i\sigma(i)} = 1$.
Proof of Claim: First suppose there is a $\sigma \in S_n$ such that $\prod_{1\le i\le n} a_{i\sigma(i)} = 1$, then the vector $\mathbf{v} = \sum_{1\le i\le n} \mathbf{v}_{i\sigma(i)}$ has $\|\mathbf{v}\|^2 = n + \sum_{1\le i\le n}(2^{2\alpha_i} + 2^{2\beta_i})$.

Let $D = n + \sum_{1\le i\le n}(2^{2\alpha_i} + 2^{2\beta_i})$, and let $\mathbf{v} = \theta_{11}\mathbf{v}_{11} + \theta_{12}\mathbf{v}_{12} + \cdots + \theta_{nn}\mathbf{v}_{nn}$ be a vector in the lattice $\mathcal{L}$ such that $\|\mathbf{v}\|^2 = D$.

As the $\mathbf{v}_{ij}$ are orthogonal we get that

$$D = \|\mathbf{v}\|^2 = \langle \mathbf{v}, \mathbf{v}\rangle = \sum_{1\le i,j\le n} \theta_{ij}^2 \|\mathbf{v}_{ij}\|^2. \tag{1}$$

Note that if $\theta_{ij} \neq 0$ this implies that $a_{ij} = 1$, for otherwise $\|\mathbf{v}\|^2 \ge \|\mathbf{v}_{ij}\|^2 \ge 2^{2\gamma+1} > D$. Let $\delta_{ij} = \theta_{ij}^2\|\mathbf{v}_{ij}\|$, so that if $\theta_{ij} \neq 0$ then $\delta_{ij} = \theta_{ij}^2(1 + 2^{2\alpha_i} + 2^{2\beta_j})$. Reducing both sides of equation (1) modulo $2^{2\alpha_1}$ we get: $\sum_{1\le i,j\le n} \theta_{ij}^2 \equiv n \mod 2^{2\alpha_1}$. If $\sum_{1\le i,j\le n} \theta_{ij}^2 = n + k2^{2\alpha_1}$ with $k \ge 1$ then there is a θ_{rs} such that $\theta_{rs}^2 \ge \frac{2^{2\alpha_1}}{n^2}$. This implies that $\delta_{rs} \ge 2^{2\alpha_1 + 2\alpha_r - 2\log n}$. Suppose we select α_i and β_j such that $\beta_n < 2^{2\alpha_1 - \log n}$ then $\delta_{rs} > D$ which is impossible. Thus $k = 0$ and the congruence is an equality, so that

$$\sum_{1\le i,j\le n} \theta_{ij}^2 = n.$$

Thus we get that $|\theta_{ij}| \le \sqrt{n}$ and since they are integers there are at most n θ_{ij}'s that are non-zero. If, in addition, we have $n^3 2^{\alpha_i} < 2^{\alpha_{i+1}}$ and $n^3 2^{\beta_i} < 2^{\beta_{i+1}}$ then we argue that in fact $|\theta_{ij}| \le 1$. Suppose to the contrary we had a vector with $1 < |\theta_{ij}|^2 \le n$, then $\delta_{ij} = \theta_{ij}^2 + \theta_{ij}^2 2^{2\alpha_i} + \theta_{ij}^2 2^{2\beta_j}$. Now $\theta_{ij}^2 2^{2\alpha_i} > 2^{2\alpha_i}$ so there must be at least one other vector which helps this vector "cheat" so that the sum adds to a valid power $2^{2\alpha_k}$ (say). Let S be the set of basis vectors that help to make $\theta_{ij}^2 2^{2\alpha_i}$ another valid power of 2. But $|S| \le n^2$ and each of these vectors can add a factor of at most $n2^{2\alpha_i}$ to the norm to boost it to the next valid power of 2, but then since $n^3 2^{\alpha_i} < 2^{\alpha_{i+1}}$ this is impossible. Thus the set S is empty and all the $|\theta_{ij}| \le 1$.

But now we have $\sum_{1\le i,j\le n} \theta_{ij}^2 = n$, with each $|\theta_{ij}| \le 1$ and θ_{ij} are integers. This implies that there must be exactly n non-zero θ_{ij}. Suppose $\theta_{ij_1}, \theta_{ij_2}, \cdots, \theta_{ij_k}$ with $1 < k \le n$ are all non-zero. Then clearly the $2^{2\alpha_i}$ term of the norm of $\mathbf{v}$ cannot be accounted for by any of the basis elements, thus for each i there is exactly one j such that $|\theta_{ij}| = 1$. This defines for us a permutation $\sigma \in S_n$ such that for each i, $1 \le i \le n$ $|\theta_{i\sigma(i)}| = 1$. It is now evident that $\prod_{1\le i\le n} a_{i\sigma(i)} = 1$. Thus we have proved the claim.

To finish the proof of the theorem note that for each $\sigma \in S_n$ if $\prod_{1\le i\le n} a_{i\sigma(i)} = 1$ then there are 2^n vectors given by $\sum_{1\le i\le n} \pm\mathbf{v}_{i\sigma(i)}$ of norm square $n + \sum_{1\le i\le n}(2^{2\alpha_i} + 2^{2\beta_i})$.

Hence we have that:

$$2^n \text{Per } M = \left| \left\{ \mathbf{v} \in \mathcal{L} \;\middle|\; \|\mathbf{v}\|^2 = n + \sum_{1 \le i \le n} (2^{2\alpha_i} + 2^{2\beta_i}) \right\} \right|.$$

Since a sequence α_i, β_j and γ that satisfies all the conditions imposed in our proof can be picked in polynomial time, this proves the theorem. In particular, an acceptable sequence would be $\alpha_1 = cn^2$, for some constant $c > 0$; $\alpha_i = cn^2 + ib \log n$, for $b > 3$ another constant and $1 < i \le n$; $\beta_i = cn^2 + (i+n)b \log n$ and $\gamma > \beta_n$. $\square$

4. A Naïve algorithm

Let $\mathcal{L} \subseteq \mathbb{Q}^n$ be a lattice with basis $\mathbf{v}_1, \cdots, \mathbf{v}_r$ and $\mathbf{v} = \langle \alpha_1, \cdots, \alpha_n \rangle \in \mathcal{L}$ be such that $\|\mathbf{v}\|^2 = d$ then we have that $|\alpha_i| \le \sqrt{d}$. Suppose we are given a vector $\mathbf{v}$ we can check if it belongs to the lattice $\mathcal{L}$ by solving for $\mathbf{v} = e_1\mathbf{v}_1 + \cdots + e_r\mathbf{v}_r$ for the e_i and checking whether $e_i \in \mathbb{Z}$. We can thus evaluate $\vartheta_{\mathcal{L}}(d)$ by exhaustive search in time $2^{O(n \log d)}$. We can improve the exhaustive search in the case where the lattice is not full rank as follows. Suppose $\mathbf{v}_i = \langle \gamma_{i1}, \cdots, \gamma_{in} \rangle$ and assume (without loss of generality) that the $r \times r$ minor $(\gamma_{ij})_{1 \le i,j \le r}$ is full rank. A lattice vector $\mathbf{v}$ is then uniquely determined by its first r coordinates. Further, given the first r coordinates of a vector $\mathbf{v}$, we can check if there is a vector in $\mathcal{L}$ with the same initial block of r coordinates. Furthermore, we can produce such a lattice vector by solving the appropriate system of linear equations. Hence we can refine our exhaustive search by generating tuples $\langle \alpha_1, \cdots, \alpha_r \rangle$ with $|\alpha_i| \le \sqrt{d}$ and checking if there is a vector in $\mathcal{L}$ whose projection along the first r coordinates matches the tuple $\langle \alpha_1, \cdots, \alpha_r \rangle$ and also if it is of the correct norm. This yields a method to compute $\vartheta_{\mathcal{L}}(d)$ in time $2^{O(r \log d)}$ (ignoring factors that are polynomial in n). Summarizing, we have:

Theorem 4.1. *There is a deterministic algorithm that when given a lattice $\mathcal{L} \subseteq Q^n$ of rank r and an integer d in binary computes $\vartheta_{\mathcal{L}}(d)$ in time $2^{O(r \log d + \log n + \log s)}$, where s is the number of bits to encode the basis of $\mathcal{L}$.*

5. Review of Modular forms

In this section we review the relevant portion of the theory of modular forms as it applies to our discussion. For good introductions to this elegant and deep theory see [Gun62, Ogg69, La76, Kob93], the original work of Hecke [Hec83a] or the beautiful article by Zagier [Zag92].

Let $\mathfrak{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ be the Poincaré half-plane. Let Γ_1 be the group $\text{PSL}(2, \mathbb{Z})$ - the group of 2×2 matrices of determinant 1 with integer entries.

Definition 5.1. A holomorphic function $f : \mathfrak{H} \to \mathbb{C}$ is called a *modular form* (for Γ_1) of *weight* k (k is a non-negative integer) if the following conditions hold:

(1) $f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau + d)^k f(\tau)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1$.

(2) As $\tau \to \imath\infty$, $|f(\tau)|$ is bounded.

The set of all modular forms of a certain weight form a $\mathbb{C}$-vector space, and we denote this space by $M_k(\mathbb{C})$. Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1$, the transformation law (1) above says that $f(\tau) = f(\tau + 1)$. Thus any modular form is periodic in vertical strips of width 1 on the complex plane. Now $\mathfrak{H}/\{z \mapsto z + 1\}$ (essentially a cylinder) has a complex analytic isomorphism to the open punctured disc of radius 1, by the map $z \mapsto e^{2\pi\imath z}$. Holomorphic maps f on $\mathfrak{H} \cup \{i\infty\}$ such that $f(\tau) = f(\tau+1)$ when considered

as maps on the open disc have a Taylor expansion about the origin: $f(z) = \sum_{0 \le n} a_n z^n$. It is a fact that this expansion converges everywhere in the disc. Pulling this back via the isomorphism we get the expansion $f(\tau) = \sum_{n \in \mathbb{N}} a_n q^n$ where $q = e^{2\pi\imath\tau}$. The fact that f is a modular form, implies that $a_n = O(n^{k-1})$, where k is the weight. The subspace $S_k(\Gamma_1)$ of $M_k(\Gamma_1)$ of modular forms whose Fourier expansion has $a_0 = 0$ are the so-called *cusp forms* of weight k. Note that there are no non-zero modular forms of *odd* weight, since $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma_1$.

The most important fact about modular forms is that $M_k (= M_k(\Gamma_1))$ is a finite dimensional vector space, with an explicit basis.

Theorem 5.2 (see [La76]). *The dimension of the vector space M_k is given by (for* even *k)*

$$\dim M_k = \begin{cases} \lfloor \frac{k}{12} \rfloor + 1, & \text{if } k \ge 0, k \not\equiv 2 \mod 12 \\ \lfloor \frac{k}{12} \rfloor, & \text{if } k \ge 0, k \equiv 2 \mod 12 \\ 0, & \text{if } k < 0. \end{cases}$$

Our next task is to describe an explicit basis for M_k.

Let $k > 2$ be even, the **Eisenstein series** of weight k is $G_k(\tau) = \frac{-B_k}{2k} + \sum_{1 \le n} \sigma_{k-1}(n) q^n, \tau \in \mathfrak{H}, q = e^{2\pi\imath\tau}$, where B_k is the k-th Bernoulli number (the coefficient of $\frac{x^k}{k!}$ in the Taylor expansion of $\frac{x}{e^x - 1}$) and $\sigma_{k-1}(n) = \sum_{r \mid n} r^{k-1}$. The **Discriminant function** Δ is defined by $\Delta(\tau) = q \prod_{1 \le r} (1 - q^r)^{24}, \tau \in \mathfrak{H}, q = e^{2\pi\imath\tau}$. It is a fact that $G_k(\tau)$ is a modular form of weight k, and Δ is a cusp form of weight 12. Now given an arbitrary modular form in M_k we can subtract a suitable multiple of G_k to get a cusp form. This gives us a direct sum decomposition of this space M_k as $\langle G_k \rangle \oplus S_k$. Also S_k is isomorphic to M_{k-12}. These facts lead to the following theorem:

Theorem 5.3 (see [Zag92]). *The space M_k of modular forms of weight k has a basis given by the set of forms $\Delta^l G_{k-12l}$ for $0 \le l \le \frac{k-4}{12}$, and if k is divisible by* 12 *the function $\Delta^{k/12}$ is also in the basis.*

6. The Approach for Unimodular Lattices

In this section we describe our method for counting the number of lattice vectors in a restricted class of lattices. In §8 we remove the restrictions we place here.

Let $\mathcal{L} \subseteq \mathbb{Q}^d$ be a rank r lattice. Choosing a basis for $\mathcal{L}$ we can form an isomorphism to $\mathbb{Z}^r$, this isomorphism is given by a linear transformation. Under the isomorphism the square of the norm function for $\mathcal{L}$ transforms into a positive definite quadratic form $Q_{\mathcal{L}}$ on $\mathbb{Q}^r$. The *theta series* associated to the lattice $\mathcal{L}$ is given by

$$\begin{aligned} \Theta_{\mathcal{L}}(\tau) &= \sum_{\mathbf{v} \in \mathcal{L}} q^{\|\mathbf{v}\|^2} \\ &= \sum_{\mathbf{x} \in \mathbf{Z}^r} q^{Q_{\mathcal{L}}(\mathbf{x})}, q = e^{2\pi\imath\tau}. \end{aligned}$$

The quadratic form $Q_{\mathcal{L}}(\mathbf{x})$ can be written as $\frac{1}{2}\mathbf{x}^t A \mathbf{x}$ for an *even symmetric matrix* A (i.e., $A = (a_{ij}) \in \mathbb{Z}^{r \times r}, A = A^t$ and a_{ii} are even integers). The lattice $\mathcal{L}$ is said to be *unimodular* if $\det A = 1$.

The following astonishing fact (and some of its generalizations) was proved by Schoeneberg [Sch39], see also [Hec83b].

Theorem 6.1. *Let $\mathcal{L}$ be a lattice of even rank r, such that the matrix A associated to the quadratic form $Q_{\mathcal{L}}$ of the lattice is unimodular. Then the theta series $\Theta_{\mathcal{L}}$ of the lattice is a modular form of weight $\frac{r}{2}$ for the full modular group.*

This suggests the following algorithm. Given a lattice $\mathcal{L}$ of rank r, we know that the theta series of the lattice $\Theta_{\mathcal{L}}$ lives in the finite dimensional space $M_{r/2}$. By definition $\Theta_{\mathcal{L}}(\tau) = \sum_{0 \leq n} a_n q^n$ ($q = e^{2\pi\imath\tau}$), where $a_n = |\{\mathbf{v} \in \mathcal{L} \ : \ \|\mathbf{v}\|^2 = n\}|$, so our task is to compute the Fourier coefficients of $\Theta_{\mathcal{L}}$. Furthermore, we know an explicit basis for this space (say) $\{f_1, \cdots, f_D\}$, where D is the dimension of $M_{r/2}$. Suppose we can also find $\alpha_1, \cdots, \alpha_D$ such that $\Theta_{\mathcal{L}} = \alpha_1 f_1 + \cdots + \alpha_D f_D$. Then we can find the Fourier coefficients of $\Theta_{\mathcal{L}}$ by combining the appropriate Fourier coefficients of the f_i according to the linear relation we found for $\Theta_{\mathcal{L}}$. If we can compute the Fourier coefficients of f_i asymptotically faster than the running time of the algorithm in §4 then we get a faster algorithm for computing $\Theta_{\mathcal{L}}$.

6.1. **Computing the Basis of M_k.** Here we show that computing the m-th Fourier coefficient of the basis elements of M_k can be done in $2^{O(\log m)}$ time.

Theorem 6.2. *There is a deterministic algorithm that when given m in binary computes the m-th Fourier coefficient of G_k in $2^{O(\log m + \log\log k)}$ time if $m \geq 1$ and in $2^{O(\log k)}$ time if $m = 0$.*

Proof : If $m = 0$, we need to compute the k-th Bernoulli number. This can be done in $k^{O(1)}$ time using the Akiyama-Tanigawa algorithm [Knk00]. If $m > 1$, then the m-th Fourier coefficient of G_k is $\sigma_{k-1}(m) = \sum_{d|m} d^{k-1}$. One simple way of computing this is to factor m completely and then to evaluate the sum by running over all the divisors of m. Factoring the number m, can clearly be done in $2^{O(\log m)}$ time, even by simple trial division. As every divisor of m is $\leq m$ the number of divisors is $O(m)$. Computing the term d^{k-1} can be done in $O(\log k \log d)$ time. Thus the sum can be evaluated by this procedure in $\log k \times 2^{O(\log m)}$ as claimed. □

Theorem 6.3. *There is a deterministic algorithm that when given m in binary, computes the m-th Fourier coefficient of Δ^l in $2^{O(\log m + \log\log l)}$ time.*

Proof : Now $\Delta^l = q^l \prod_{1 \leq r} (1 - q^r)^{24l}$. We just need to compute this product upto the $r = O(m/l)$ term. Each term of the product requires $(\log l)^{O(1)}$ multiplications (by repeated squaring), we need to compute $O(m)$ such products, and this can be done in $2^{O(\log m + \log\log l)}$ time. □

Given these two theorems it is easy to see that the m-th coefficient of the basis for M_k can be computed in $2^{O(\log m + \log k)}$ time.

Remark 6.4. Let $D = \dim M_k$, and $f_1, \cdots, f_D$ be the basis for the vector space M_k given in Theorem 5.3. Let the q-expansion of the f_i's be given by

$$f_i(\tau) = \sum_{0 \leq j} a_{ij} q^j, \text{ for } 1 \leq i \leq D.$$

Then the matrix $(a_{ij})_{1 \leq i \leq D, 0 \leq j < D}$ has full rank. This is easily seen directly, since the matrix we get is an upper triangular matrix with non-zero entries along the diagonal.

6.2. **The algorithm for unimodular lattices.**

Theorem 6.5. *Let $\mathcal{L}$ be a lattice in $\mathbb{Q}^n$ of rank r, such that the matrix associated to the quadratic form $Q_{\mathcal{L}}$ is unimodular. Then there is a deterministic algorithm that when given inputs $\mathcal{L}$ (encoded as a sequence of basis vectors, requiring s bits) and d in binary, computes $\vartheta_{\mathcal{L}}(d)$ in time $2^{O(r \log r + \log d + \log s)}$.*

Proof : By Theorem 6.1 the theta series of the lattice $\Theta_{\mathcal{L}}$ is a modular form of weight $r/2$. Let $D = \dim M_{r/2}$ and let $f_1, \cdots, f_D$ be the basis for $M_{r/2}$ as given in Theorem 5.3. Our aim is to find $\gamma_1, \cdots, \gamma_D \in \mathbb{C}$ such that $\Theta_{\mathcal{L}} = \gamma_1 f_1 + \cdots + \gamma_D f_D$. The γ_i are in fact in $\mathbb{Q}$ since the Fourier coefficients of $\Theta_{\mathcal{L}}$ are integers and those of the f_i are rational numbers.

To find the γ_i we compute D Fourier coefficients $a_1, \cdots, a_D$ of $\Theta_{\mathcal{L}} = \sum_{l \in \mathbb{N}} a_l q^l$ using the algorithm in §4. Next we compute the corresponding D Fourier coefficients of basis elements f_i. This yields linear equations for the γ_i. By remark 6.4 this system of linear equations has full rank. Thus we can solve for the γ_i in $r^{O(1)}$ time.

To find the a_i for $1 \leq i \leq D$ (and noting that $D = O(r)$) we need $2^{O(r \log r + \log s)}$ time using the algorithm in §4. Now to compute the d-th Fourier coefficient of $\Theta_{\mathcal{L}}$ we need to compute the d-th Fourier coefficients of the basis elements which can be computed in $2^{O(\log d + \log r)}$ time. This proves the theorem. □

Remark 6.6. One might wonder how restrictive the condition of unimodularity is on the quadratic form associated to a lattice. It turns out that if $\mathcal{L}$ is a unimodular lattice then the dimension is a multiple of 8 (see for instance [Gun62] (§23) Theorem 2). One can find some examples in [Ogg69, Hec40, Hec83b] and [Sch39]. If the dimension is a multiple of 8 then there are unimodular lattices of that dimension see [Cha85] Chapter 10, this fact is used in §7.

7. Reductions to Integer Factorization

In view of Theorem 3.1 we can consider various relaxations of the original problem of counting lattice vectors. In this section we show that two natural restrictions of the problem are at least as hard as integer factorization.

7.1. **Fixed rank lattices.**

In the L_1-norm the problem of counting the number of lattice vectors for fixed rank lattices is in P [DyK97]. It is natural to ask if the same is true for L_2-norm. The following theorem shows that this is unlikely.

Theorem 7.1. *There is a randomized polynomial time reduction from integer factorization to counting lattice vectors in lattices of fixed rank $r \geq 8$.*

Proof : There is a lattice $\mathcal{E}_8$ with the following properties[1]:

(1) The rank of $\mathcal{E}_8$ is 8;
(2) $\mathcal{E}_8$ is unimodular,

see [Ser70] Chapter V, example 1.4.3 and Chapter VII, example 6.6.(i). By Theorem 6.1 $\Theta_{\mathcal{E}_8} \in M_4$. But M_4 is one dimensional with basis G_4. Thus $\Theta_{\mathcal{E}_8} = cG_4$, a quick computation (using the fact that any lattice has only one vector of norm 0) shows that $c = 240$. Thus $\vartheta_{\mathcal{E}_8}(d) = 240\sigma_3(d)$ for $d \geq 1$. It is known that there is a randomized polynomial time reduction from integer factorization to computing $\sigma_k(n)$ for any fixed k [BMS86]. Now to get a reduction from integer factorization to computing $\vartheta_{\mathcal{L}}$ where $\text{rank}(\mathcal{L}) = r > 8$ we can boost the rank of $\mathcal{E}_8$ to r. More precisely, let $\mathbf{v}_i = \langle v_{ij} \rangle$ for $1 \leq i, j \leq 8$ be the basis for $\mathcal{E}_8$. We construct a lattice $\mathcal{E}_8^r \subseteq \mathbb{Q}^r$ given by the following

[1]The notation reflects the fact that $\mathcal{E}_8$ is the root lattice associated to the exceptional Lie algebra $\mathfrak{e}_8$.

basis vectors:

$$\begin{aligned}
\mathbf{v}_1 &= \langle v_{11}, \cdots, v_{18}, \underbrace{0, \cdots, 0}_{r-8} \rangle \\
\mathbf{v}_2 &= \langle v_{21}, \cdots, v_{28}, 0, \cdots, 0 \rangle \\
&\vdots \\
\mathbf{v}_8 &= \langle v_{81}, \cdots, v_{88}, 0, \cdots, 0 \rangle \\
\mathbf{v}_9 &= \langle \underbrace{0, \cdots, 0}_{8}, d, 0, \cdots, 0 \rangle \\
&\vdots \\
\mathbf{v}_r &= \langle 0, \cdots, 0, 0, 0, \cdots, d \rangle.
\end{aligned}$$

One can see that $\vartheta_{\mathcal{E}_8^r}(d) = \vartheta_{\mathcal{E}_8}(d)$ and so we get a reduction from factoring to computing $\vartheta_{\mathcal{L}}$ where $\text{rank}(\mathcal{L}) > 8$. □

It is likely that one could show a result analogous to Theorem 7.1 even for lattices of rank $r < 8$. In particular, note that for the lattice of dimension 2 (say) $\mathcal{Z}^2$, generated by $\langle 0, 1 \rangle, \langle 1, 0 \rangle$ we have $\vartheta_{\mathcal{Z}^2}(d) = r_2(d)$—the number of representations of d as a sum of two squares. It is a classical fact that $r_2(n) = 4(d_1(n) - d_3(n))$ where $d_i(n)$ is the number of divisors of n of the form $4k + i$. It seems that computing $r_2(n)$ is hard without a knowledge of the factorization of n.

7.2. **Lattices with bounded norm basis vectors.** The reduction in Theorem 3.1 has the feature that the lattice produced has a basis of vectors that have *large* norms. We can consider a variant of the counting problem, where we restrict the lattices to have a basis of vectors all of whose norms are bounded. With regard to this question, we can show the following theorem:

Theorem 7.2. *There is a reduction from integer factorization to computing $\vartheta_{\mathcal{L}}$ for lattices with a basis of bounded norm vectors.*

We need some preliminary results before we prove Theorem 7.2.

Definition 7.3. Let $\mathcal{L} \subseteq \mathbb{Q}^{m_1}$ be a lattice of rank n_1 given by basis $\mathbf{u}_i = \langle u_{ij} \rangle$ for $1 \leq i \leq n_1$, $1 \leq j \leq m_1$ and let $\mathcal{M} \subseteq \mathbb{Q}^{m_2}$ be another lattice of rank n_2 given by basis $\mathbf{v}_k = \langle v_{kl} \rangle$ for $1 \leq k \leq n_2$, $1 \leq l \leq m_2$. Then define $\mathcal{L} \oplus \mathcal{M} \subseteq \mathbb{Q}^{m_1+m_2}$ to be the lattice generated by the basis

$$\begin{aligned}
\mathbf{w}_1 &= \langle u_{11}, \cdots, u_{1m_1}, \underbrace{0, \cdots, 0}_{m_2} \rangle \\
&\vdots \\
\mathbf{w}_{n_1} &= \langle u_{n_1 1}, \cdots, u_{n_1 m_1}, 0, \cdots, 0 \rangle \\
\mathbf{w}_{n_1+1} &= \langle \underbrace{0, \cdots, 0}_{m_1}, v_{11}, \cdots, v_{1m_2} \rangle \\
&\vdots \\
\mathbf{w}_{n_1+n_2} &= \langle 0, \cdots, 0, v_{n_2 1}, \cdots, v_{n_2 m_2} \rangle.
\end{aligned}$$

The following lemma is immediate from the definition.

Lemma 7.4. *If $\mathcal{L}$ and $\mathcal{M}$ are two lattices then $\Theta_{\mathcal{L} \oplus \mathcal{M}} = \Theta_{\mathcal{L}} \Theta_{\mathcal{M}}$.*

Let $d \geq 3$ be an integer. Consider the lattice $\mathcal{L}_d \subseteq \mathbb{Q}^d$ of rank $d-1$ generated by the basis vectors

$$\begin{aligned}
\mathbf{v}_1 &= \langle \underbrace{1, -1, 0, \cdots, 0}_{d} \rangle \\
\mathbf{v}_2 &= \langle 0, 1, -1, 0, \cdots, 0 \rangle \\
&\vdots \\
\mathbf{v}_{d-1} &= \langle 0, \cdots, 0, 1, -1 \rangle.
\end{aligned}$$

The following lemma is evident from the definition of $\mathcal{L}_d$.

Lemma 7.5. *Suppose* $\mathbf{w} = \langle w_0, w_1, \cdots, w_{d-1} \rangle \in \mathcal{L}_d$, *then* $\mathbf{w}^{\oslash} = \langle w_{d-1}, w_0, \cdots, w_{d-2} \rangle \in \mathcal{L}_d$.

Proposition 7.6. *Let* $\mathbf{w} \in \mathcal{L}_p$ *where* p *is an odd prime. If* $\mathbf{w} \neq \mathbf{0}$ *then* $\mathbf{w}, \mathbf{w}^{\oslash}, \mathbf{w}^{\oslash^2}, \cdots, \mathbf{w}^{\oslash^{p-1}}$ *are all distinct.*

Proof : Suppose $\mathbf{w}^{\oslash^i} = \mathbf{w}^{\oslash^j}$ for $0 \leq i \neq j \leq p-1$. Then $\mathbf{w}^{\oslash^{(i-j)}} = \mathbf{w} = \mathbf{w}^{\oslash^p}$, which implies that $\mathbf{w}^{\oslash^{\gcd(i-j,p)}} = \mathbf{w}$. Thus $\mathbf{w}^{\oslash} = \mathbf{w}$, but this means that all the coordinates of $\mathbf{w}$ are equal. But all vectors of $\mathcal{L}_p$ have coordinates summing to 0. Thus $\mathbf{w}$ must be the zero vector contradicting the hypothesis of the proposition. □

Corollary 7.7. *If* p *is an odd prime then* $\Theta_{\mathcal{L}_p} \equiv 1 \mod p$.

Proof : Group all non-zero vectors in $\mathcal{L}_p$ by their orbits via the action $\mathbf{w} \mapsto \mathbf{w}^{\oslash}$. Each such orbit is of size p by Proposition 7.6. Further, noting that $\|\mathbf{w}\| = \|\mathbf{w}^{\oslash}\|$ we see that $\Theta_{\mathcal{L}_p} \equiv 1 \mod p$. □

Proof :(of Theorem 7.2) Suppose $\mathcal{A}$ is an algorithm that can compute $\vartheta_{\mathcal{L}}$ for lattices generated by a basis of bounded norm vectors. Then we show that $\mathcal{A}$ can be used to compute the function $\sigma_3(n)$, which will prove the theorem in view of [BMS86].

We first pick small primes p_i for $1 \leq i \leq k$ such that $\prod_{1 \leq i \leq k} p_i > n^4 > \sigma_3(n)$. Then we use $\mathcal{A}$ to compute $\vartheta_{\mathcal{E}_8 \oplus \mathcal{L}_{p_i}}(n)$ for each p_i. By Corollary 7.7 and Lemma 7.4, we have that $\vartheta_{\mathcal{E}_8 \oplus \mathcal{L}_{p_i}}(n) \equiv \vartheta_{\mathcal{E}_8}(n) \mod p_i$. Now applying the Chinese remainder theorem we can find $\vartheta_{\mathcal{E}_8}(n)$. By the prime number theorem it suffices to take the first $k = O(\log n)$ primes for the p_i. The theorem now follows. □

8. The General Case

In the general case the theta series of the lattice is no longer a modular form for the full modular group, but for a congruence subgroup. We first describe the space of modular forms for congruence subgroups. Let

$$\begin{aligned}
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1 \;\middle|\; c \equiv 0 \mod N \right\} \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \;\middle|\; a \equiv 1 \mod N \right\}.
\end{aligned}$$

The space $M_k(\Gamma_1(N))$ are those functions $f(z)$ that are holomorphic on $\mathfrak{H}$ such that for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N), (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) = f(z)$ and for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1$ the function $(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$ has a Fourier expansion $\sum_n a_n q^n$ such that $a_n = 0$ for all $n < 0$. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$ be a Dirichlet

character modulo N (i.e., χ is a homomorphism of multiplicative groups extended so that $\chi(n) = 0$ if $\gcd(n, N) \neq 1$). We define

$$M_k(N, \chi) = \left\{ f \in M_k(\Gamma_1(N)) \;\middle|\; (cz+d)^{-k} f\left(\frac{az+d}{cz+d}\right) = \chi(d) f(z), \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\}.$$

Now in the general case for lattices that are not necessarily unimodular we have:

Theorem 8.1. *Let $\mathcal{L}$ be a lattice of rank r (r even). Let $Q_{\mathcal{L}}$ be the associated quadratic form, and A be the even summetric matrix with integer entries such that $Q_{\mathcal{L}} = \frac{1}{2}\mathbf{x}^t A \mathbf{x}$. Let N be the smallest positive integer such that NA^{-1} is again even symmetric with integer entries. Let $D = (-1)^{\frac{r}{2}} \det A$. Then the theta series of the lattice $\mathcal{L}$ is a modular form of level N, weight $\frac{r}{2}$ and character $\chi = \left(\frac{D}{d}\right)$ (the Kronecker symbol), i.e., $\Theta_{\mathcal{L}} \in M_{\frac{r}{2}}(N, \chi)$.*

Remark 8.2. In our situation the basis vectors have integer entries so N is always a divisor of $\det A$, so that χ is indeed a character modulo N, even though it need not be a primitive character modulo N. The fact that the matrix A is invertible follows from the theory of bilinear forms and that $Q_{\mathcal{L}}$ arose from an inner product (see [MiH73] Lemma I.§2.2). See Ogg's book [Ogg69] Chapter 6, or Zagier's article [Zag92] for more background on this theorem.

The space $M_k(\Gamma_1(N))$ decomposes as $\oplus_\chi M_k(N, \chi)$ where the sum is over all Dirichlet characters modulo N. Further, the space $M_k(\Gamma_1(N))$ splits up into a part generated by generalized Eisenstein series and a part made up of cusp forms which in turn decomposes into a sum $\oplus_\chi S_k(N, \chi)$. The following theorem shows that we can compute a basis of forms for the space $M_k(\Gamma_1(N))$. The algorithm is the result of the cumulative work of many individuals, see [AtL70, Cre97, Kob93, Li75, Man72, Mer94, Ste00].

Theorem 8.3. *There is a basis for $M_k(\Gamma_1(N))$ composed of forms each of whose n-th Fourier coefficient can be computed in $\dim M_k(\Gamma_1(N)) \times 2^{O(\log n)}$ time.*

We only sketch the ideas behind the method for computing the Fourier coefficients of the basis elements since the details are available in other sources. The basis for the space generated by the generalized Eisenstein series can be explicitly worked out (see for instance [Kob93] III.§3, Proposition 22.) The Fourier coefficients of these elements can also be computed though they are no longer rational but involve roots of unity. Computing the space of cusp forms is much more involved. In this case there is an algebra of operators the *Hecke operators* on this space $\mathbb{T} : S_k(N, \chi) \to S_k(N, \chi)$. A beautiful theorem of Hecke says that there is a basis for the space $S_k(N, \chi)$ composed of eigenforms for this algebra [Hec83a]. More importantly, the eigenvalues *are the Fourier coefficients* of the eigenform. The situation is not as straightforward as described, and one needs the full power of the Atkin-Lehner theory [AtL70, Li75] to understand these spaces. Since we do not have a basis for the cusp forms it seems that it is impossible to determine the eigenvectors for the operators—seemingly a circular problem. The idea is to use the space of *modular symbols* for which a concrete presentation is available by an idea of Manin [Man72], the space modular forms embeds (actually as a dual) into the space of modular symbols by the Eichler-Shimura theory. The Hecke algebra acts on the space of modular symbols, and the eigenvectors for this action are then translated to the space of modular forms. The details of this method have been worked out in exhaustive detail in [Mer94], [Cre97] chapter 2, and in [Ste00] chapters 2 and 3. The Fourier coefficients are algebraic and the number field containing *all* the coefficients of the basis is a finite extension but the degree can be very large (as big as $(\dim S_k(N)^2)!$), since we need to construct the splitting field of the characteristic polynomials of the Hecke operators. For our purposes it suffices to get good approximations to these coefficients, which we do indeed get from the algorithm.

Now our previous algorithm for computing $\vartheta_{\mathcal{L}}$ generalizes readily to this situation. The space $S_k(N,\chi)$ has dimension $O(kN^2)$ [CoO77, Ste00]. The key step in the algorithm is to find the coordinates of the theta series $\Theta_{\mathcal{L}}$ in the space $M_{r/2}(\Gamma_1(N))$. To do this we must accumulate enough linear relations among the Fourier coefficients of the basis for the space and $\Theta_{\mathcal{L}}$. For the case discussed in the previous section this was easy since the matrix formed by the first $\dim M_k$ coefficients of the basis forms has full rank. In our case, we do not have an explicit basis to work with so we must argue indirectly. We make use of a result (Proposition 2.16 in [Shi71]) that says if $F \in M_k(\Gamma)$ for Γ any congruence subgroup (actually this result holds in more generality) then if Z is the number of zeros of the function F counting multiplicty in $\mathfrak{H}$ then $Z = \Theta(\dim(M_k(\Gamma)))$. Let $D = \dim M_{r/2}\Gamma_1(N)$, and let $f_1, \cdots, f_D$ be a basis for $M_{r/2}(\Gamma_1(N))$. Suppose we had scalars $\alpha_1, \cdots, \alpha_D$ such that $\alpha_1 f_1 + \cdots + \alpha_D f_D = c_m q^m + c_{m+1}q^{m+1} + \cdots$, with $c_m \neq 0$ (i.e., the α_i cancel out all Fourier coefficients below m) then the function $F(z) = \alpha_1 f_1 + \cdots + \alpha_D f_D$ vanishes to order m at $i\infty$. Thus in particular if $m > Z$ then $F(z)$ is identically zero by the above result. This implies that $\alpha_i = 0$ since the f_i form a basis. Thus among the first $\Theta(D)$ Fourier coefficients of the basis elements, we arrive at a matrix of full rank. One can also derive this bound directly from a theorem of Sturm [Stu87], but we do not need the full strength of Sturm's theorem.

Suppose we have an algorithm that counts the number of points in a lattice $\mathcal{L}$ (of level N) of rank r of norm square d in time $T(r,d)$ then in time $T(r,D)^{O(1)}$ ($D = \dim M_{r/2}(\Gamma_1(N))$) we can find the coordinates of the theta series $\Theta_{\mathcal{L}}$ in the space $M_{r/2}(\Gamma_1(N))$ by solving the linear system gathered from the coefficients. Then the number of points of norm square d can be found in time $T(r, rN^2)^{O(1)}2^{O(\log r + \log N + \log d)}$ by combining the Fourier coefficients. This yields the following theorem:

Theorem 8.4. *Let $\mathcal{L}$ be a lattice in $\mathbb{Q}^n$ of rank r (all of whose basis vectors have integer entries and r is even), with $Q_{\mathcal{L}}$ as the associated quadratic form and A the even symmetric matrix of the quadratic form. Let N be the smallest integer such that NA^{-1} is integral and even symmetric. Suppose that there is an algorithm B that can compute the number of lattice vectors of norm square at most d in time $T(r,d)$, then there is a deterministic algorithm to do the same in time $T(r, rN^2)^{O(1)}2^{O(\log r + \log N + \log d)}$.*

Clearly, the above theorem is not useful if the existing algorithm B is very efficient, but it can be used to boost the performance of an algorithm that does not perform well for large values of the distance d. For example, using the algorithm presented in section 4 and observing that if the lattice is encoded by vectors using s bits then $N \leq \det A \leq 2^{O(s)}$ we get:

Theorem 8.5. *Let $\mathcal{L}$ be a lattice of rank r (r even) in $\mathbb{Q}^n$, such that the basis vectors can be encoded using s bits. Then the number of lattice vectors of norm square d can be computed deterministically in time $2^{O(rs + \log d)}$.*

8.1. **Odd rank lattices.** We can reduce the case of odd rank lattices to that of the even rank case as follows.

The idea is to use the "rank boosting" method in section (7.) Let $\mathcal{L} \subseteq \mathbb{Q}^n$ be an odd rank lattice. Set $\mathcal{M}_d \subseteq \mathbb{Q}$ be the rank 1 lattice generated by the vector $\langle 2d \rangle$. Now the lattice $\mathcal{M}_d \oplus \mathcal{L}$ is an even rank lattice, which satisfies $\vartheta_{\mathcal{M}_d \oplus \mathcal{L}}(d) = \vartheta_{\mathcal{L}}(d)$. We can apply our algorithm to $\mathcal{M}_d \oplus \mathcal{L}$ to count the vectors of norm square d and we note that the reduction does not change the asymptotic running time of the algorithm.

9. Concluding Remarks

In this article we have displayed a family of modular forms (not of fixed weight or level), whose Fourier coefficients are hard to compute ($\sharp\mathsf{P}$-complete). It is natural to ask in view of Theorem 8.5: How hard is it to compute a basis of modular forms? Since many number theoretically interesting sequences of integers appear as Fourier coefficients of modular forms this is an important question to ask. The belief seems to be that there can be no *general* algorithm that can compute these Fourier coefficients *efficiently*. For example, factoring integers of the form $n = pq$ (RSA moduli) reduces to computing the Ramanujan Tau function which gives the Fourier coefficients of Δ a cusp form [BaC05]. It is not clear at all whether computing $\tau(n)$ is only as hard as factoring. Another avenue of research is to look at the problem of *approximating* $\vartheta_{\mathcal{L}}(d)$ or computing $\vartheta_{\mathcal{L}}(d)$ modulo a fixed prime p.

Acknowledgements: I would like to thank Eric Bach, Jin-Yi Cai, Rohit Chatterjee, Rajasekar Krishnamurthy, Bill McGraw, Dieter van Melkebeek and William Stein for extremely useful discussions. The author is especially grateful to William Stein for pointing out several references and for responding to several queries on the basis computation for $S_k(\Gamma_0(N), \chi)$.

References

[Aj97] Ajtai, M.; *The Shortest Vector problem in L_2 is* NP*-hard for Randomized reductions*, ACM STOC-1998, pages 10-19, 1998.

[AtL70] Atkin, A. O. L.; Lehner, J.; *Hecke operators on $\Gamma_0(n)$*, Math. Ann. **185**, 134-160, 1970.

[BMS86] Bach, E.; Miller, G.; Shallit, J.; *Sums of Divisors, Perfect numbers, and Factoring*, SIAM Journal on Computing **15**, 1143-1154, 1986.

[BaC05] Bach, Eric; Charles, Denis; *The hardness of computing a Hecke Eigenform*, under preparation, 2005.

[Cai99] Cai, Jin-Yi; *Some Recent Progress on the Complexity of Lattice problems*, in the Proceedings of The 14th Annual IEEE conference on Computational Complexity, 158-177, 1999.

[Cha85] Chandrasekharan, K.; *Elliptic Functions*, Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, 1985.

[CoO77] Cohen, H.; Oesterlé, J.; *Dimensions des espaces de formes modulaires*, Lecture Notes in Mathematics, Vol. **627**, 69-78, Springer-Verlag, 1977.

[Cre97] Cremona, J., E.; *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997.

[DyK97] Dyer, M., E.; Kannan, R.; *On Barvinok's algorithm for counting lattice points*, Mathematics of Operations Research, Vol. 22, 545-549, 1997.

[Gun62] Gunning, R., C.; *Lectures on Modular Forms*, Annals of Mathematics Studies, Number 48, Princeton University Press, 1962.

[Hec40] Hecke, Erich; *Analytische Arithmetik der positiven quadratischen Formen*. Kgl. Danske Videnskabernes Selskab. Mathematisk-fysike Meddelelser, **XVII**, 12, (1940).

[Hec83a] Hecke, Erich; *Mathematische Werke*, Third Edition, Vandenhoeck & Ruprecht, Göttingen, 1983.

[Hec83b] Hecke, Erich; *Lectures on Dirichlet Series, modular functions and quadratic forms.*, Vandenhoeck & Ruprecht, Göttingen, 1983.

[Kan87] Kannan, Ravi; *Algorithmic Geometry of Numbers*, Ann. Rev. Comput. Sci., **2**, 231-267, 1987.

[Knk00] Kaneko, Masanobu; *The Akiyama-Tanigawa algorithm for Bernoulli numbers*, Electronic Journal of Integer Sequences, Vol. **(3)**, article 00.2.9, 2000.

[Kob93] Koblitz, Neal; *Introduction to Elliptic Curves and Modular Forms*, 2nd Ed., Graduate Texts in Mathematics, Vol 97, Springer-Verlag, 1993.

[La76] Lang, Serge; *Introduction to Modular forms*, Grundlehren der mathematischen Wissenschaften, Vol. 222, Springer-Verlag, 1976.

[Li75] Li, Wen-Ching Winnie; *Newforms and functional equations*, Math. Ann., **212**, 285-315, 1975.

[Man72] Manin, Yu., I., *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36**, 19-66, 1972.

[Mer94] Merel, L.; *Universal Fourier Expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations, Lectures Notes in Math., Vol. 1585, Springer-Verlag, 1994.

[MiH73] Milnor, J.; Husemoller, D.; *Symmetric Bilinear forms*, Ergebnisse Der Mathematik und Ihrer Grenzgebiete, Vol. 73, 1973.

[Ogg69] Ogg, Andrew; *Modular forms and Dirichlet Series*, W. A. Benjamin Inc., 1969.
[Pap94] Papdimitriou, Christos; *Computational Complexity*, Addison-Wesley, 1994.
[RS01] Ravi Kumar, S.; Sivakumar, D.; *On the uniqueness of the shortest lattice vector problem*, Theoretical Computer Science, **255** (1-2), 641 - 648, 2001.
[Sch39] Schoeneberg, Bruno; *Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen*, Math. Annalen, **116**, 511-523, 1939.
[Ser70] Serre, Jean-Pierre; *A Course in Arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag, 1970.
[Shi71] Shimura, Goro; *Introduction to the Arithmetic Theory of Automorphic functions*, Princeton University Press, 1971.
[Ste00] Stein, William; *Explicit approaches to modular abelian varieties*, University of California, Berkeley, Ph. D. Thesis, 2000.
[Stu87] Sturm, Jacob; *On the congruence of modular forms.* , Number Theory, Lecture Notes in Math., 1240, Springer-Verlag, 275-280, 1987.
[Val79] Valiant, L. G.; *The complexity of computing the permanent*, TCS **(8)**, 189-201, 1979.
[Zag92] Zagier, D.; *Introduction to Modular forms*, in From Number Theory to Physics, edited by Waldschmidt, M.; Moussa, P.; Luck, J.-M.; Itzykson C.; Springer-Verlag , 1992.

Department of Computer Science, University of Wisconsin-Madison, Madison WI - 53706.
E-mail address: cdx@cs.wisc.edu