Sampling a Uniform Solution of a Quadratic Equation Modulo a Prime Power*

Chandan Dubey and Thomas Holenstein

Institute for Theoretical Computer Science, ETH Zürich
{chandan.dubey,thomas.holenstein}@inf.ethz.ch

Abstract

An n-ary integral quadratic form is a formal expression $Q(x_1, \cdots, x_n) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j$ in n variables $x_1, \cdots, x_n$, where $a_{ij} = a_{ji} \in \mathbb{Z}$. We present a randomized polynomial time algorithm that given a quadratic form $Q(x_1, \cdots, x_n)$, a prime p, a positive integer k and an integer t, samples a uniform solution of $Q(x_1, \cdots, x_n) \equiv t \bmod p^k$.

1998 ACM Subject Classification F.2.1 Numerical Algorithms and Problems

Keywords and phrases Quadratic Forms, Lattices, Modular, p-adic

Digital Object Identifier 10.4230/LIPIcs.APPROX-RANDOM.2014.643

1 Introduction

Let R be a commutative ring with unity and $\mathrm{R}^\times$ be the set of units (i.e., invertible elements) of R. A quadratic form over the ring R in n-formal variables $x_1, \cdots, x_n$ in an expression $\sum_{1 \le i,j \le n} a_{ij} x_i x_j$, where $a_{ij} = a_{ji} \in \mathrm{R}$. A quadratic form can equivalently be represented by a symmetric matrix $\mathtt{Q}^n = (a_{ij})$ such that $Q(x_1, \cdots, x_n) = (x_1, \cdots, x_n)'\mathtt{Q}(x_1, \cdots, x_n)$. The quadratic form is called integral if $\mathrm{R} = \mathbb{Z}$ and the determinant of the quadratic form Q is defined as $\det(\mathtt{Q})$.

Quadratic forms are central to various branches of Mathematics, including number theory, linear algebra, group theory, and Lie theory. They also appear in several areas of Computer Science like Cryptography and Lattices. Several modern factorization algorithms, including Dixon's algorithm [6], the continued fractions method, and the quadratic sieve; try to solve $x^2 \equiv t \bmod n$, where n is the number being factorized. They also arise naturally as the ℓ_2 norm of lattice vectors.

It is not surprising that the study of quadratic forms predates Gauss, who gave the law of quadratic reciprocity and contributed a great deal in the study of quadratic forms, including a complete classification of binary quadratic forms (i.e., $n = 2$). Another giant leap was made by Minkowski in his "Geometry of Numbers" [11], which proposed a geometric method to solve problems in number theory. Minkowski also gave explicit formulae to calculate the number of solutions $\mathbf{x} = (x_1, \cdots, x_n) \in (\mathbb{Z}/p^k\mathbb{Z})^n$ to the equation $\mathbf{x}'\mathtt{Q}\mathbf{x} \equiv t \bmod p^k$. Several alternatives are available for counting. We refer to [17, 12, 19, 10, 5, 7, 9], and note that many of these papers (also) solve much more general problems. As an example, [17] gives an ingenious Gaussian sum technique to count solutions in case p does not divide $2t \det(\mathtt{Q})$.

The case of the prime $p = 2$ is tricky and needs careful analysis. Pall [13] pointed out that the work of Minkowski omits many details, resulting in errors for the case of prime 2. Later, Watson [18] found errors in the fixes suggested by Pall. It is believed by the community that the work by Watson does not contain any errors.

* This research was supported by the Swiss National Science Foundation, grant no. 200021–132508.

17th Int'l Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX'14) / 18th Int'l Workshop on Randomization and Computation (RANDOM'14).
Editors: Klaus Jansen, José Rolim, Nikhil Devanur, and Cristopher Moore; pp. 643–653

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

We remark that typically mathematicians are mainly interested in counting the number of solutions if k is "large enough".[1] One reason for this is that once k is large enough, increasing k by 1 simply multiplies the number of solutions by p^{n-1}. Another reason is that the corresponding normalized quantity (the local density, which is the number of solutions divided by $p^{k(n-1)}$ for k large enough) seems to be the "mathematically natural quantity". It arises in many places, for example in (some forms of) the celebrated Siegel mass formula [17].

On the question of finding any solution (in contrast to sampling one uniformly at random), we are aware of two relevant results. The first [1, 15] solves $x^2 - ky^2 \equiv m \pmod{n}$ for composite n, when the factorization of n is unknown. The second and more relevant is the work done by Hartung [8]. For odd p, he gives a correct polynomial time algorithm to find one solution of $Q \equiv t \bmod p^k$ (thought it seems to be safe to say that the possibility of this was folklore before). Unfortunately, his construction seems to contain errors for the case $p = 2$ (e. g., he divides by 2 in the proof of the relevant Lemma 3.3.1 pp. 47–48).

Our Contribution

Apart from the difficulty of giving correct formulae for $p = 2$, the method of Minkowski (and others, including the Gaussian sum method) for counting the number of solutions of $\mathbf{x}'\mathtt{Q}\mathbf{x} \equiv t \bmod p^k$ has another drawback. It is not constructive in the sense that it does not provide a way to sample uniform solutions to the equation. In this work, we give an alternate way of counting solutions, and thus by the above remarks, and alternate way to compute the local density. Our algorithm also yields a Las Vegas algorithm that, given an integral quadratic form $\mathtt{Q}$, a prime p, a positive integer k and an integer $t \in \mathbb{Z}/p^k\mathbb{Z}$, runs in time $\mathrm{poly}(n, k, \log p)$ and samples a uniform random solution of $\mathbf{x}'\mathtt{Q}\mathbf{x} \equiv t \bmod p^k$.

2 Preliminaries

Integers and ring elements are denoted by lowercase letters, vectors by bold lowercase letters and matrices by typewriter uppercase letters. The i'th component of a vector $\mathbf{v}$ is denoted by v_i. We use the notation $(v_1, \cdots, v_n)$ for a column vector and the transpose of matrix $\mathtt{A}$ is denoted by $\mathtt{A}'$. The matrix $\mathtt{A}^n$ will denote a $n \times n$ square matrix. If $\mathtt{Q}_1^n, \mathtt{Q}_2^m$ are matrices, then the *direct product* of $\mathtt{Q}_1$ and $\mathtt{Q}_2$ is denoted by $\mathtt{Q}_1 \oplus \mathtt{Q}_2$ and is defined as $\mathrm{diag}(\mathtt{Q}_1, \mathtt{Q}_2) = \begin{pmatrix} \mathtt{Q}_1 & 0 \\ 0 & \mathtt{Q}_2 \end{pmatrix}$. Given two matrices $\mathtt{Q}_1$ and $\mathtt{Q}_2$ with the same number of rows, $[\mathtt{Q}_1, \mathtt{Q}_2]$ is the matrix which is obtained by concatenating the two matrices columnwise. A matrix is called unimodular if it is an integer $n \times n$ matrix with determinant 1.

Let R be a commutative ring with unity and $\mathrm{R}^\times$ be the set of units (i.e., invertible elements) of R. If $\mathtt{Q} \in \mathrm{R}^{n \times n}$ is a square matrix, the *adjugate* of $\mathtt{Q}$ is defined as the transpose of the cofactor matrix and is denoted by $\mathrm{adj}(\mathtt{Q})$. The matrix $\mathtt{Q}$ is invertible if and only if $\det(\mathtt{Q})$ is a unit of the R. In this case, $\mathrm{adj}(\mathtt{Q}) = \det(\mathtt{Q})\mathtt{Q}^{-1}$. The set of invertible $n \times n$ matrices over R is denoted by $\mathrm{GL}_n(\mathrm{R})$. The subset of matrices with determinant 1 will be denoted by $\mathrm{SL}_n(\mathrm{R})$. For every prime p and positive integer k, we define the ring $\mathbb{Z}/p^k\mathbb{Z} = \{0, \cdots, p^k - 1\}$, where product and addition is defined modulo p^k.

▶ **Fact 1.** *A matrix* $\mathtt{U}$ *is in* $\mathrm{GL}_n(\mathrm{R})$ *iff* $\det(\mathtt{U}) \in \mathrm{R}^\times$.

[1] If k is 1 larger than the largest power of p in $8 \cdot t \cdot \det(\mathtt{Q})$, the following holds.

For quadratic forms, the prime 2 is special and all primes except 2 will be called *odd primes*. Let p be a prime, and a be an integer. Then, $\mathrm{ord}_p(a)$ is the highest power of p such that $p^{\mathrm{ord}_p(a)}$ divides a. We let $\mathrm{ord}_p(0) = \infty$. The p-coprime part of a is then $\textsc{copr}_p(a) = \frac{a}{p^{\mathrm{ord}_p(a)}}$. Note that $\textsc{copr}_p(a)$ is by definition a unit of $\mathbb{Z}/p\mathbb{Z}$. For a positive integer q, one writes $a \equiv b \bmod q$, if q divides $a - b$. By $x := a \bmod q$, we mean that x is assigned the unique value $b \in \mathbb{Z}/q\mathbb{Z}$ such that $b \equiv a \bmod q$. An integer t is called a *quadratic residue* modulo q if $\gcd(t, q) = 1$ and $x^2 \equiv t \bmod q$ has a solution.

▶ **Definition 2.** Let p be an odd prime, and t be a positive integer. Then, the Legendre-symbol of t with respect to p is defined as follows.

$$\left(\frac{t}{p}\right) := t^{(p-1)/2} \bmod p = \begin{cases} 1 & \text{if } t \text{ is a quadratic residue modulo } p, \text{ and } t \not\equiv 0 \pmod p \\ 0 & \text{if } t \equiv 0 \pmod p, \\ -1 & \text{otherwise.} \end{cases}$$

For the prime 2, there is an extension of Legendre symbol called the Kronecker symbol. It is defined for odd integers t and $\left(\frac{t}{2}\right)$ equals 1 iff $t \equiv \pm 1 \bmod 8$, -1 if $t \equiv \pm 3 \bmod 8$, and 0 otherwise. The p-sign of t, denoted $\mathrm{sgn}_p(t)$, is defined as $\left(\frac{\textsc{copr}_p(t)}{p}\right)$ for odd primes p and $\textsc{copr}_2(t) \bmod 8$ otherwise.

▶ **Fact 3.** *Let p be an odd prime. Then, there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p.*

An integer t is a square modulo q if there exists an integer x such that $x^2 \equiv t \pmod q$. The integer x is called the *square root* of t modulo q. If no such x exists, then t is a non-square modulo q.

▶ **Definition 4.** Let q be a prime power. A vector $\mathbf{v} \in (\mathbb{Z}/q\mathbb{Z})^n$ is called primitive if there exists a component v_i, $i \in [n]$, of $\mathbf{v}$ such that $\gcd(v_i, q) = 1$. Otherwise, the vector $\mathbf{v}$ is non-primitive.

▶ **Definition 5.** Let p be a prime, k be a positive integer and x be an element of $\mathbb{Z}/p^k\mathbb{Z}$. The p-expansion of x is x written in base p i.e., $x = d_0(x) + d_1(x) \cdot p + \cdots + d_{k-1}(x) \cdot p^{k-1}$, where $d_i(x) \in \mathbb{Z}/p\mathbb{Z}$ for $i \in \{0, \cdots, k-1\}$, is called the i'th *digit* of x.

For two sets A and B, the symbol $A \leftrightarrow B$ means that there is bijection between A and B.

Quadratic Form

An n-ary quadratic form over a ring R is a symmetric matrix $\mathtt{Q} \in \mathrm{R}^{n \times n}$, interpreted as the following polynomial in n formal variables $x_1, \cdots, x_n$ of uniform degree 2.

$$\sum_{1 \le i,j \le n} \mathtt{Q}_{ij} x_i x_j = \mathtt{Q}_{11} x_1^2 + \mathtt{Q}_{12} x_1 x_2 + \cdots = \mathbf{x}' \mathtt{Q} \mathbf{x}$$

The quadratic form is called *integral* if it is defined over the ring $\mathbb{Z}$ and is also positive definite if for all non-zero column vector $\mathbf{x}$, $\mathbf{x}'\mathtt{Q}\mathbf{x} > 0$. This work deals with integral quadratic forms, henceforth called simply *quadratic forms*. The *determinant* of the quadratic form is defined as $\det(\mathtt{Q})$. A quadratic form is called *diagonal* if $\mathtt{Q}$ is a diagonal matrix.

Given a set of formal variables $\mathbf{x} = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix}'$ one can make a linear change of variables to $\mathbf{y} = \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix}'$ using a matrix $\mathtt{U} \in \mathrm{R}^{n \times n}$ by setting $\mathbf{y} = \mathtt{U}\mathbf{x}$. If additionally, $\mathtt{U}$ is invertible over R i.e., $\mathtt{U} \in \mathrm{GL_n(R)}$, then this change of variables is reversible over the ring. We now define the equivalence of quadratic forms over the ring R (compare with Lattice Isomorphism).

▶ **Definition 6.** Let $\mathtt{Q}_1^n, \mathtt{Q}_2^n$ be quadratic forms over a ring R. They are called R-*equivalent* if there exists a $\mathtt{U} \in \mathrm{GL_n(R)}$ such that $\mathtt{Q}_2 = \mathtt{U}'\mathtt{Q}_1\mathtt{U}$.

If $\mathrm{R} = \mathbb{Z}/q\mathbb{Z}$, for some positive integer q, then two integral quadratic forms $\mathtt{Q}_1^n$ and $\mathtt{Q}_2^n$ will be called q-equivalent (denoted, $\mathtt{Q}_1 \overset{q}{\sim} \mathtt{Q}_2$) if there exists a matrix $\mathtt{U} \in \mathrm{GL_n}(\mathbb{Z}/q\mathbb{Z})$ such that $\mathtt{Q}_2 \equiv \mathtt{U}'\mathtt{Q}_1\mathtt{U} \pmod q$.

Let $\mathtt{Q}^n$ be a n-ary integral quadratic form, and q, t be positive integers. If the equation $\mathbf{x}'\mathtt{Q}\mathbf{x} \equiv t \pmod q$ has a solution then we say that t has a q-representation in $\mathtt{Q}$ (or t has a representation in $\mathtt{Q}$ over $\mathbb{Z}/q\mathbb{Z}$). Solutions $\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n$ to the equation are called q-*representations* of t in $\mathtt{Q}$. We classify the representations into two categories: *primitive* and *non-primitive*, see definition 4. The set of non-primitive, primitive and all p^k-representations of t in $\mathtt{Q}$ is denoted by $\mathrm{A}_{\mathrm{p^k}}(\mathtt{Q}, t), \mathrm{B}_{\mathrm{p^k}}(\mathtt{Q}, t)$ and $\mathrm{C}_{\mathrm{p^k}}(\mathtt{Q}, t)$. Their respective sizes are denoted by $\mathfrak{A}_{\mathrm{p^k}}(\mathtt{Q}, t), \mathfrak{B}_{\mathrm{p^k}}(\mathtt{Q}, t)$ and $\mathfrak{C}_{\mathrm{p^k}}(\mathtt{Q}, t)$ respectively.

Randomized Algorithms

Our randomized algorithms are Las Vegas algorithms. They either fail and output nothing, or produce a correct answer. The probability of failure is bounded by a constant. Thus, for any $\delta > 0$, it is possible to repeat the algorithm $O(\log \frac{1}{\delta})$ times and succeed with probability at least $1 - \delta$. Henceforth, these algorithms will be called *randomized algorithms*.

Througout this paper, we will say that an algorithm runs in polynomial time if it runs in time $\mathrm{poly}(n, k, \log(p))$.

3 Technical Overview

Given a quadratic form over a ring R, one can classify them according to the following equivalence. Two quadratic forms are equivalent over R if one can be obtained from the other by an invertible linear change of variables over R. For example, x^2 and $2y^2$ are equivalent over the field of reals $\mathbb{R}$ because the transformations $x \to \sqrt{2}y$ and $y \to \frac{1}{\sqrt{2}}x$ are inverse of each other in $\mathbb{R}$, are linear and transform x^2 to $2y^2$ and $2y^2$ to x^2 respectively. Thus, over $\mathbb{R}$ instead of trying to solve both x^2 and $2y^2$ separately, one can instead solve x^2 and then use the invertible linear transformation to map the solutions of x^2 to the solutions of $2y^2$. It is well known that every quadratic form in n-variables over $\mathbb{R}$ is equivalent to $\sum_{i=1}^{a} x_i^2 - \sum_{i=a+1}^{n} x_i^2$, for some $a \in [n]$. This is known as the Sylvester's Law of inertia. The following lemma shows that for counting/finding solutions over a ring R, it suffices to do it for an equivalent quadratic form.

▶ **Lemma 7.** *Let p be a prime, k, t be positive integers, $\mathtt{Q}$ be an integral quadratic form, $\mathtt{U} \in \mathrm{GL_n}(\mathbb{Z}/p^k\mathbb{Z})$ and $\mathtt{S} = \mathtt{U}'\mathtt{Q}\mathtt{U} \bmod p^k$. Then, $\mathrm{A}_{\mathrm{p^k}}(\mathtt{Q}, t) \leftrightarrow \mathrm{A}_{\mathrm{p^k}}(\mathtt{S}, t)$, and $\mathrm{B}_{\mathrm{p^k}}(\mathtt{Q}, t) \leftrightarrow \mathrm{B}_{\mathrm{p^k}}(\mathtt{S}, t)$.*

Proof. The map $\mathbf{x} \to \mathtt{U}\mathbf{x}$ preserves the primitiveness of the vector $\mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^n$ and is bijective because $\mathtt{U}$ is an invertible matrix over $\mathbb{Z}/p^k\mathbb{Z}$. The lemma follows from the equality $(\mathtt{U}\mathbf{x})'\mathtt{Q}(\mathtt{U}\mathbf{x}) \equiv \mathbf{x}'\mathtt{S}\mathbf{x} \bmod p^k$. ◀

For the $\mathrm{R} = \mathbb{Z}/p^k\mathbb{Z}$ such that p is odd, there always exists an equivalent quadratic form which is also diagonal (see [5], Theorem 2, page 369). Additionally, one can explicitly find the invertible change of variables that turns it into a diagonal quadratic form. The situation is tricky over the ring $\mathbb{Z}/2^k\mathbb{Z}$. Here, it might not be possible to eliminate all mixed terms, i.e., terms of the form $a_{ij}x_ix_j$ with $i \neq j$. For example, consider the quadratic form xy over

$\mathbb{Z}/2^k\mathbb{Z}$, for some positive k. An invertible linear change of variables over $\mathbb{Z}/2^k\mathbb{Z}$ is of the following form.

$$\begin{array}{ll} x \to a_1x_1 + a_2x_2 & \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \text{ invertible over } \mathbb{Z}/2^k\mathbb{Z} \\ y \to b_1x_1 + b_2x_2 & \end{array}$$

The mixed term after this transformation is $a_1b_2 + a_2b_1$. As $a_1b_2 + a_2b_1 \bmod 2$ is the same as the determinant of the change of variables above i.e., $a_1b_2 - a_2b_1$ modulo 2; it is not possible for a transformation in $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ to eliminate the mixed term. Instead, one can show that over $\mathbb{Z}/2^k\mathbb{Z}$ it is possible to get an equivalent form where the mixed terms are disjoint i.e., both x_ix_j and x_ix_k do not appear, where $i \neq j \neq k$. One captures this form by the following definition.

▶ **Definition 8.** A matrix $\mathtt{D}^n$ over integers is in a block diagonal form if it is a direct sum of type I and type II forms; where type I form is an integer while type II is a matrix of the form $\begin{pmatrix} 2^{\ell+1}a & 2^\ell b \\ 2^\ell b & 2^{\ell+1}c \end{pmatrix}$ with b odd.

The following theorem is folklore and is also implicit in the proof of Theorem 2 on page 369 in [5].

▶ **Theorem 9.** *Let $\mathtt{Q}^n$ be an integral quadratic form, p be a prime, and k be a positive integer. Then, there is an algorithm that takes time $O(n^4k\log p)$ and produces a matrix $\mathtt{U} \in \mathrm{SL}_n(\mathbb{Z}/p^k\mathbb{Z})$ such that $\mathtt{U}'\mathtt{Q}\mathtt{U} \pmod{p^k}$, is a diagonal matrix for odd primes p and a block diagonal matrix (in the sense of Definition 8) for $p = 2$.*

The next simplification is achieved by the following Lemma.

▶ **Lemma 10.** *Let $\mathtt{Q}^n$ be a quadratic form, p be a prime, k be a positive integer and t, s be integers such that $\mathrm{ord}_p(t \bmod p^k) = \mathrm{ord}_p(s \bmod p^k)$ and $\mathrm{sgn}_p(s \bmod p^k) = \mathrm{sgn}_p(t \bmod p^k)$. Then, $\mathrm{A}_{\mathrm{p}^k}(\mathtt{Q}, t) \leftrightarrow \mathrm{A}_{\mathrm{p}^k}(\mathtt{Q}, s)$, and $\mathrm{B}_{\mathrm{p}^k}(\mathtt{Q}, t) \leftrightarrow \mathrm{B}_{\mathrm{p}^k}(\mathtt{Q}, s)$.*

The pair $(\mathrm{ord}_p(t \bmod p^k), \mathrm{sgn}_p(t \bmod p^k))$ is called the p^k-symbol of t and is denoted by $\mathrm{sym}_{p^k}(t)$. By Lemma 10, the count depends only on the p^k-symbol of t. For notational convenience, we define the following sets.

$$\textsc{ord} = \{\infty, 0, \cdots, k-1\} \quad \textsc{sgn} = \begin{cases} \{1, -1\} & p \text{ is an odd prime} \\ \{1, 3, 5, 7\} & \text{otherwise} \end{cases} \tag{1}$$

Note that, there are p^k different possibilities for t over $\mathbb{Z}/p^k\mathbb{Z}$ but only $(2k+1)$ possibilities for $\mathrm{sym}_{p^k}(t)$ for odd primes and $(4k+1)$ for 2 (the extra 1 is for 0). The following definition is useful in reducing the problem of counting representations in higher dimensions to the problem of counting representations for individual blocks in a block diagonal form.

▶ **Definition 11.** Let p be a prime, k be a positive integer, $t \in \mathbb{Z}/p^k\mathbb{Z}$ be an integer, and γ_1, γ_2 be symbols. Then, the (γ_1, γ_2)-split size of t over $\mathbb{Z}/p^k\mathbb{Z}$, denoted $\mathfrak{S}^{\mathrm{t}}_{\mathrm{p}^k}(\gamma_1, \gamma_2)$, is the size of the following set,

$$\mathrm{S}^{\mathrm{t}}_{\mathrm{p}^k}(\gamma_1, \gamma_2) = \left\{(a, b) \in (\mathbb{Z}/p^k\mathbb{Z})^2 \mid \mathrm{sym}_{p^k}(a) = \gamma_1, \mathrm{sym}_{p^k}(b) = \gamma_2, t \equiv a + b \bmod p^k\right\}$$

If $\mathfrak{A}_{\mathrm{p}^k}(\mathtt{Q}, \gamma)$ is defined as $\mathfrak{A}_{\mathrm{p}^k}(\mathtt{Q}, a)$ for any $a \in \{x \in \mathbb{Z}/p^k\mathbb{Z} \mid \mathrm{sym}_{p^k}(x) = \gamma\}$, and $\mathfrak{B}_{\mathrm{p}^k}(\mathtt{Q}, \gamma), \mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}, \gamma)$ are defined similarly, then the following Lemma gives us a way to reduce the problem of counting solutions from $\mathtt{D} = \mathtt{D}_1 \oplus \mathtt{D}_2$ to counting solutions for $\mathtt{D}_1$ and $\mathtt{D}_2$.

▶ **Lemma 12.** *Let* $\mathtt{Q} = \mathrm{diag}(\mathtt{Q}_1, \mathtt{Q}_2)$ *be an integral quadratic form,* p *be a prime,* k *be a positive integer and* $t \in \mathbb{Z}/p^k\mathbb{Z}$*. Then,*

$$\mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}, t) = \sum_{\gamma_1,\gamma_2 \in \mathrm{ORD} \times \mathrm{SGN}} \mathfrak{S}^{\mathrm{t}}_{\mathrm{p}^k}(\gamma_1, \gamma_2) \cdot \mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}_1, \gamma_1) \cdot \mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}_2, \gamma_2)$$

$$\mathfrak{A}_{\mathrm{p}^k}(\mathtt{Q}, t) = \sum_{\gamma_1,\gamma_2 \in \mathrm{ORD} \times \mathrm{SGN}} \mathfrak{S}^{\mathrm{t}}_{\mathrm{p}^k}(\gamma_1, \gamma_2) \cdot \mathfrak{A}_{\mathrm{p}^k}(\mathtt{Q}_1, \gamma_1) \cdot \mathfrak{A}_{\mathrm{p}^k}(\mathtt{Q}_2, \gamma_2)$$

Proof. The formula for the total number of representations of t by $\mathtt{Q}$ over $\mathbb{Z}/p^k\mathbb{Z}$ follows from the calculations below. The same calculation works for the number of non-primitive representations because an representation of t by $\mathtt{Q}$ is non-primitive iff every component of the representation is non-primitive.

$$\begin{aligned}
\mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}, t) &= \sum_{a \in \mathbb{Z}/p^k\mathbb{Z}} \mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}_1, a) \cdot \mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}_2, t-a) \\
&= \sum_{a \in \mathbb{Z}/p^k\mathbb{Z}} \mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}_1, \mathrm{sym}_{p^k}(a)) \cdot \mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}_2, \mathrm{sym}_{p^k}(t-a)) \\
&= \sum_{\gamma_1,\gamma_2 \in \mathrm{ORD} \times \mathrm{SGN}} \mathfrak{S}^{\mathrm{t}}_{\mathrm{p}^k}(\gamma_1, \gamma_2) \cdot \mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}_1, \gamma_1) \cdot \mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}_2, \gamma_2)
\end{aligned}$$

◀

Overview of the Algorithm

Given $(\mathtt{Q}^n, p, k, t)$ our counting algorithm for finding $\mathfrak{C}_{\mathrm{p}^k}(\mathtt{Q}, t)$ is as follows.

1. Block diagonalize $\mathtt{Q}$ over $\mathbb{Z}/p^k\mathbb{Z}$ using Theorem 9. Let $\mathtt{D}^n = \mathtt{D}_1 \oplus \cdots \oplus \mathtt{D}_m$ be the block diagonal form returned by the algorithm. Recall, each $\mathtt{D}_i$ is either Type I i.e., an integer, or Type II (only when $p = 2$).
2. For each symbol $\gamma \in \mathrm{ORD} \times \mathrm{SGN}$ and $i \in [m]$, calculate $\mathfrak{C}_{\mathrm{p}^k}(\mathtt{D}_i, \gamma)$. The case of prime 2 is handled separately and needs careful analysis for Type II blocks.
3. For each triple $\gamma, \gamma_1, \gamma_2 \in \mathrm{ORD} \times \mathrm{SGN}$ compute the size of split classes i.e., $\mathcal{S}^{\gamma}_{p^k}(\gamma_1, \gamma_2)$
4. Compute $\mathfrak{C}_{\mathrm{p}^k}(\mathtt{D}_1 \oplus \cdots \oplus \mathtt{D}_i, \gamma)$ for each $\gamma \in \mathrm{ORD} \times \mathrm{SGN}$ and $i \in [m]$, using Lemma 12.
5. Output $\mathfrak{C}_{\mathrm{p}^k}(\mathtt{D}, \mathrm{sym}_{p^k}(t))$.

Because of the remarks in the introduction in the paper, this algorithm can also be used to compute what mathematicians call the "local density". We defer the details to the full paper.

Furthermore, this algorithm can be generalized to sample uniform representations. However, also here we defer the description of the details of this to the full paper. Nevertheless, the following two theorems are the main contribution of this paper.

▶ **Theorem 13.** *Let* $\mathtt{Q}^n$ *be an integral quadratic form,* k *be a positive integer, and* t *be an element of* $\mathbb{Z}/2^k\mathbb{Z}$*. Then, there exists a polynomial time algorithm that samples a uniform (primitive/non-primitive) representation of* t *by* $\mathtt{Q}$ *over* $\mathbb{Z}/2^k\mathbb{Z}$*.*

In other words, the algorithm is able to output a uniform representation, a representation which is uniform among the primitive ones, and a representation which is uniform among the non-primitive ones.

▶ **Theorem 14.** *Let* $\mathtt{Q}^n$ *be an integral quadratic form,* p *be an odd prime,* k *be a positive integer,* t *be an element of* $\mathbb{Z}/p^k\mathbb{Z}$*. Then, there is a polynomial time algorithm that fails and outputs a special symbol* $\perp$ *with probability at most* $\frac{1}{3}$*. Otherwise, the algorithm outputs a uniform (primitive/non-primitive)* p^k*-representation of* t *by* $\mathtt{Q}$*.*

Obviously the algorithm in this theorem can be repeated $\log(1/\delta)$ times to make the error probability at most δ.

4 Counting Representations: A Brief Overview

In order to explain the main ideas of the paper, we sketch in more detail how we count the number of representations.

4.1 Counting for $n = 1$

Counting both the primitive and non-primitive solutions of $Qx^2 = t \bmod p^k$ is rather simple, and of course well known. Ignoring some corner cases (such as $t = 0 \bmod p^k$), we can see that writing $x = x_0 p^\alpha$ with $\gcd(x_0, p) = 1$ we need $x_0^2 Q p^{2\alpha} = t \bmod p^k$, so that we certainly need that $\operatorname{ord}_p Q \geq \operatorname{ord}_p(t)$ and $\operatorname{ord}_p Q - \operatorname{ord}_p t$ is even. Furthermore, in case p is odd the Legendre-symbols of Q and t need to be the same, and it is not hard to show that these are the exact conditions. In case $p = 2$, of course $\textsc{copr}_2(Q) = \textsc{copr}_2(t)$ is required.

4.2 Counting for Type II matrics

Recall Definition 8 of a type II quadratic form. In this section, we solve the representation problem for Type II matrices over $\mathbb{Z}/2^k\mathbb{Z}$. But first we define a scaled version of a type II matrix.

▶ **Definition 15.** A two-by-two matrix of the following form is called type II* matrix.

$$\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \qquad a, b, c \in \mathbb{Z}, b \text{ odd}$$

Additionally, in this section we will think of type II* as the following quadratic form in formal variables x_1, x_2 which take values in the ring $\mathbb{Z}/2^k\mathbb{Z}$.

$$ax_1^2 + bx_1x_2 + cx_2^2 \qquad a, b, c \in \mathbb{Z}, b \text{ odd} . \tag{2}$$

In order to count the number of representations, the following lemma is key.

▶ **Lemma 16.** *Let $\mathtt{Q}^* = (a, b, c)$, b odd be a type II* integral quadratic form, and t, k be positive integers. If $a_1, a_2 \in \mathbb{Z}/2\mathbb{Z}$ be such that (a_1, a_2) represent t over $\mathbb{Z}/2\mathbb{Z}$ and either a_1 or a_2 is odd then there are exactly 2^{k-1} distinct representations (x_1, x_2) of t over $\mathbb{Z}/2^k\mathbb{Z}$ such that $x_1 \equiv a_1 \pmod 2, x_2 \equiv a_2 \pmod 2$.*

Proof. We prove this by induction on k. We show that given an representation y_1, y_2 of t over the ring $\mathbb{Z}/2^i\mathbb{Z}$, for $i \geq 1$, such that at least one of y_1, y_2 is odd there are exactly two representations z_1, z_2 of t over the ring $\mathbb{Z}/2^{i+1}\mathbb{Z}$ such that $z_1 \equiv y_1 \pmod{2^i}, z_2 \equiv y_2 \pmod{2^i}$.

Let (y_1, y_2) be an representation of t by $\mathtt{Q}^*$ over $\mathbb{Z}/2^i\mathbb{Z}$. Then, the pair of integers (z_1, z_2) such that $(z_1, z_2) \equiv (y_1, y_2) \pmod{2^i}$ is an representation of t over $\mathbb{Z}/2^{i+1}\mathbb{Z}$ iff

$$\begin{array}{ll} z_1 \equiv y_1 + b_1 \cdot 2^i \pmod{2^{i+1}} & z_2 \equiv y_2 + b_2 \cdot 2^i \pmod{2^{i+1}} \\ b_1, b_2 \in \{0, 1\} & az_1^2 + bz_1z_2 + cz_2^2 \equiv t \pmod{2^{i+1}} \end{array} \tag{3}$$

Plugging in the values of z_1 and z_2 and re-arranging we get the following equation.

$$(bb_2y_1 + bb_1y_2)2^i \equiv t - (ay_1^2 + by_1y_2 + cy_2^2) \pmod{2^{i+1}} \tag{4}$$

As b is odd, b is invertible over $\mathbb{Z}/2^{i+1}\mathbb{Z}$. By assumption, y_1, y_2 represent t over $\mathbb{Z}/2^i\mathbb{Z}$ and hence 2^i divides $t - (ay_1^2 + by_1y_2 + cy_2^2)$. The equation 4 reduces to the following equation.

$$b_2y_1 + b_1y_2 \equiv \frac{t - (ay_1^2 + by_1y_2 + cy_2^2)}{2^i b} \pmod 2 \tag{5}$$

We now split the proof in two cases: i) when y_1 is odd, and ii) when y_1 is even and y_2 is odd.

y_1 odd. For each choice of $b_1 \in \{0,1\}$ there is a unique choice for b_2 because $y_1 \equiv 1 \pmod 2$.

$$b_1 \in \{0,1\} \qquad b_2 = \frac{t - (ay_1^2 + by_1y_2 + cy_2^2)}{2^i b} - b_1y_2 \pmod 2$$

y_1 even. In this case, $y_2 \equiv 1 \pmod 2$ and so b_2 can be chosen freely.

$$b_2 \in \{0,1\} \qquad b_1 = \frac{t - (ay_1^2 + by_1y_2 + cy_2^2)}{2^i b} \pmod 2$$

◀

Using this lemma, in order to count the number of representations of t modulo 2^k by a type II* matrix, we simply first check how many of the three pairs $(0,1)$, $(1,0)$, and $(1,1)$ represent t modulo 2. The remaining case (where both a_1 and a_2 are even) obviously requires that t is divisible by 4, and can be settled by a simple recursion (where one represents $t/4$ modulo 2^{k-2}). We defer a detailed description to the full version of the paper.

4.3 Calculating the Split Classes

Our next step is to calculate the split size i.e., $\mathfrak{S}^{\mathrm{t}}_{\mathrm{p^k}}(\gamma_1, \gamma_2)$.

Let p be a prime, k be a positive integer and $t \in \mathbb{Z}/p^k\mathbb{Z}$. In this section, we calculate the value $\mathfrak{S}^{\mathrm{t}}_{\mathrm{p^k}}(\gamma_1, \gamma_2)$ for all possible symbol pairs (γ_1, γ_2) over $\mathbb{Z}/p^k\mathbb{Z}$. We also show that $\mathfrak{S}^{\mathrm{t}}_{\mathrm{p^k}}(\gamma_1, \gamma_2)$ only depends on the p^k-symbol of t and can also be written as $\mathfrak{S}^{\gamma}_{\mathrm{p^k}}(\gamma_1, \gamma_2)$, where $\gamma = \mathrm{sym}_{p^k}(t)$.

For a p^k-symbol γ, suppose $\mathrm{S}_{\mathrm{p^k}}(\gamma) = \{x \in \mathbb{Z}/p^k\mathbb{Z} \mid \mathrm{sym}_{p^k}(x) = \gamma\}$ and $\mathfrak{S}_{\mathrm{p^k}}(\gamma)$ be the cardinality of $\mathrm{S}_{\mathrm{p^k}}(\gamma)$. Then, the following lemma calculates, for each $a \in \mathbb{Z}/p^k\mathbb{Z}$, the number of elements in $\mathbb{Z}/p^k\mathbb{Z}$ with the same p^k-symbol as a.

▶ **Lemma 17.** *Let p be a prime, k be a positive integer and $a \in \mathbb{Z}/p^k\mathbb{Z}$ be a non-zero integer. Then,*

$$\mathfrak{S}_{\mathrm{p^k}}(\mathrm{sym}_{p^k}(a)) = \begin{cases} \max\{2^{k-\mathrm{ord}_2(a)-3}, 1\} & \text{if } p = 2 \\ \frac{p-1}{2}p^{k-\mathrm{ord}_p(a)-1} & \text{otherwise.} \end{cases}$$

Proof. Let $x \in \mathbb{Z}/p^k\mathbb{Z}$ be an element with the same p-symbol as a. Then, $\mathrm{ord}_p(x) = \mathrm{ord}_p(a)$ and $\mathrm{sgn}_p(x) = \mathrm{sgn}_p(t)$. Recall the p-expansion of x i.e., definition 5. There are k digits in the p-expansion of x for $x \in \mathbb{Z}/p^k\mathbb{Z}$; first $\mathrm{ord}_p(a)$ of which must be identically 0.

For odd prime p, $\mathrm{sgn}_p(x) = \mathrm{sgn}_p(a)$ iff $\left(\frac{\mathrm{COPR}_p(x)\,\mathrm{COPR}_p(t)}{p}\right) = 1$. Thus, the $(\mathrm{ord}_p(a)+1)$'th digit of x must be a non-zero element of $\mathbb{Z}/p\mathbb{Z}$ with the same sign as $\left(\frac{\mathrm{COPR}_p(a)}{p}\right)$. By Fact 3, there are $\frac{p-1}{2}$ possibilities for the $(\mathrm{ord}_p(a)+1)$'th digit of x. The rest can be chosen freely from $\mathbb{Z}/p\mathbb{Z}$.

For the prime 2, $\mathrm{sgn}_2(x) = \mathrm{sgn}_2(a)$ iff $\mathrm{COPR}_2(x) \equiv \mathrm{COPR}_2(a) \bmod 8$. Thus, the digits $(\mathrm{ord}_p(a)+1), \cdots, (\mathrm{ord}_p(a)+2)$ of x must match those of a. The rest can be chosen freely from $\mathbb{Z}/2\mathbb{Z}$. ◀

The following two lemmas show that if $\mathrm{ord}_p(t) \neq \mathrm{ord}_p(a)$ then the symbol of $t-a \bmod p^k$ is the same for every element of $\mathbb{Z}/p^k\mathbb{Z}$ which has the same p^k-symbol as a.

▶ **Lemma 18.** *Let k be a positive integer and a, t be elements of the ring $\mathbb{Z}/2^k\mathbb{Z}$. Then, the 2^k-symbol of $t-a$ can be computed from $\mathrm{sym}_{2^k}(t)$ and $\mathrm{sym}_{2^k}(a)$.*

Proof. The 2^k-symbol of $s = (t-a) \bmod 2^k$ can be calculated as follows.

$$\mathrm{ord}_2(s) = \min\{\mathrm{ord}_2(t), \mathrm{ord}_2(a)\}$$

$$\mathrm{COPR}_2(t-a) = \begin{cases} 2^{\mathrm{ord}_2(t)-\mathrm{ord}_2(a)}\,\mathrm{COPR}_2(t) - \mathrm{COPR}_2(a) & \text{if } \mathrm{ord}_2(t) > \mathrm{ord}_2(a) \\ \mathrm{COPR}_2(t) - 2^{\mathrm{ord}_2(a)-\mathrm{ord}_2(t)}\,\mathrm{COPR}_2(a) & \text{otherwise.} \end{cases}$$

$$\mathrm{COPR}_2(s) = \begin{cases} \mathrm{COPR}_2(t-a) \bmod 2^{k-\mathrm{ord}_2(a)} & \text{if } \mathrm{ord}_2(t) > \mathrm{ord}_2(a) \\ \mathrm{COPR}_2(t-a) \bmod 2^{k-\mathrm{ord}_2(t)} & \text{otherwise.} \end{cases}$$

The quantity $\mathrm{COPR}_2(s) \bmod 8$ can be computed from $\mathrm{COPR}_2(t) \bmod 8, \mathrm{COPR}_2(a) \bmod 8$, $\mathrm{ord}_2(t)$ and $\mathrm{ord}_2(a)$. ◀

▶ **Lemma 19.** *Let p be an odd prime, k be a positive integer and a, t be elements of the ring $\mathbb{Z}/p^k\mathbb{Z}$ such that $\mathrm{ord}_p(t) \neq \mathrm{ord}_p(a)$. Then, the p^k-symbol of $t-a$ can be computed from $\mathrm{sym}_{p^k}(t)$ and $\mathrm{sym}_{p^k}(a)$.*

Proof. The p^k-symbol of $t-a$ can be calculated as follows.

$$\mathrm{ord}_p(t-a) = \min\{\mathrm{ord}_p(t), \mathrm{ord}_p(a)\}$$

$$\mathrm{COPR}_p(t-a) = \begin{cases} p^{\mathrm{ord}_p(t)-\mathrm{ord}_p(a)}\,\mathrm{COPR}_p(t) - \mathrm{COPR}_p(a) & \text{if } \mathrm{ord}_p(t) > \mathrm{ord}_p(a) \\ \mathrm{COPR}_p(t) - p^{\mathrm{ord}_p(a)-\mathrm{ord}_p(t)}\,\mathrm{COPR}_p(a) & \text{otherwise.} \end{cases}$$

$$\left(\frac{\mathrm{COPR}_p(t-a)}{p}\right) = \begin{cases} \left(\frac{-\mathrm{COPR}_p(a)}{p}\right) & \text{if } \mathrm{ord}_p(t) > \mathrm{ord}_p(a) \\ \left(\frac{\mathrm{COPR}_p(t)}{p}\right) & \text{otherwise.} \end{cases}$$

◀

The next lemma is from [14].

▶ **Lemma 20.** *For an odd prime p, and non-zero $a \in \mathbb{Z}/p\mathbb{Z}$ the number of tuples $(x, x+a) \in (\mathbb{Z}/p\mathbb{Z})^2$ such that $\left(\frac{x}{p}\right) = s_1$, $\left(\frac{x+a}{p}\right) = s_2$ and $s_1, s_2 \in \{-1, 1\}$ is given by the following formula.*

$$\frac{1}{4} \cdot \left\{ p - (p \bmod 4) - \left(\frac{-1}{p}\right) \cdot \left(1 + s_1 \left(\frac{a}{p}\right)\right) \cdot \left(1 + s_2 \left(\frac{-a}{p}\right)\right) \right\} \tag{6}$$

The following lemma gives the size of the $\mathfrak{S}^{\mathrm{t}}_{\mathrm{p^k}}(\gamma_1, \gamma_2)$ for all possible p^k-symbol pairs over the ring $\mathbb{Z}/p^k\mathbb{Z}$.

▶ **Lemma 21.** *Let $t \in \mathbb{Z}/p^k\mathbb{Z}$, p be a prime, and k be a positive integer. Then, the size of the $\mathfrak{S}^{\mathrm{t}}_{\mathrm{p^k}}(\gamma_1, \gamma_2)$ for all possible p-symbol pairs over the ring $\mathbb{Z}/p^k\mathbb{Z}$ can be computed as follows.*

1. *if $\mathrm{ord}_p(\gamma_1), \mathrm{ord}_p(\gamma_2) > \mathrm{ord}_p(t)$ then $\mathfrak{S}^{\mathrm{t}}_{\mathrm{p^k}}(\gamma_1, \gamma_2) = 0$.*
2. *if $\mathrm{ord}_p(\gamma_1) \neq \mathrm{ord}_p(t)$ then $\mathfrak{S}^{\mathrm{t}}_{\mathrm{p^k}}(\gamma_1, \gamma_2) = \mathfrak{S}_{\mathrm{p^k}}(\gamma_1)$, for exactly one γ_2 and is 0 otherwise.*
3. *if $\mathrm{ord}_p(\gamma_2) \neq \mathrm{ord}_p(t)$ then $\mathfrak{S}^{\mathrm{t}}_{\mathrm{p^k}}(\gamma_1, \gamma_2) = \mathfrak{S}_{\mathrm{p^k}}(\gamma_2)$, for exactly one γ_1 and is 0 otherwise.*
4. *if $\mathrm{ord}_p(\gamma_2) = \mathrm{ord}_p(\gamma_1) = \mathrm{ord}_p(t)$ then $\mathfrak{S}^{\mathrm{t}}_{\mathrm{p^k}}(\gamma_1, \gamma_2)$ is 0 for $p = 2$ and otherwise it is calculated by substituting $\left(\frac{a}{p}\right) = \mathrm{sgn}_p(\gamma_1)$, $s_1 = \mathrm{sgn}_p(\gamma_2)$ and $s_2 = \left(\frac{\mathrm{COPR}_p(t)}{p}\right)$ in equation 6 and multiplying the result by $p^{k-\mathrm{ord}_p(t)-1}$.*

Proof. The $\mathfrak{S}^{t}_{p^k}(\gamma_1, \gamma_2)$ is defined as follows.

$$\mathfrak{S}^{t}_{p^k}(\gamma_1, \gamma_2) = \left|\{(a, b) \in (\mathbb{Z}/p^k\mathbb{Z})^2 \mid \mathrm{sym}_{p^k}(a) = \gamma_1, \mathrm{sym}_{p^k}(b) = \gamma_2, \text{ and, } t \equiv a + b \bmod p^k\}\right|$$

If both $\mathrm{ord}_p(\gamma_1)$ and $\mathrm{ord}_p(\gamma_2)$ are larger than $\mathrm{ord}_p(t)$ then it is not possible for such a pair to add up to t modulo p^k. If $\mathrm{ord}_p(\gamma_1)$ or $\mathrm{ord}_p(\gamma_2)$ is different from $\mathrm{ord}_p(t)$ then the correctness follows from lemma 18, when $p = 2$ and lemma 19 otherwise. Otherwise, $\mathrm{ord}_p(t) = \mathrm{ord}_p(\gamma_1) = \mathrm{ord}_p(\gamma_2)$. This is not possible in case $p = 2$ because the sum of two numbers of the same 2-order is always a number of higher 2-order. For odd prime p, we are looking for number of solutions in $\mathbb{Z}/p^k\mathbb{Z}$ of the following equation.

$$\begin{aligned} & p^{\mathrm{ord}_p(t)}\,\mathrm{COPR}_p(a) + p^{\mathrm{ord}_p(t)}\,\mathrm{COPR}_p(b) \equiv p^{\mathrm{ord}_p(t)}\,\mathrm{COPR}_p(t) \bmod p^k \\ & \iff \mathrm{COPR}_p(a) + \mathrm{COPR}_p(b) \equiv \mathrm{COPR}_p(t) \bmod p^{k-\mathrm{ord}_p(t)} \end{aligned} \tag{7}$$

The number of solutions of equation 4.3 modulo p is given by Lemma 20. The other $(k - \mathrm{ord}_p(t) - 1)$ digits in the p-expansion of $\mathrm{COPR}_p(a)$ can be chosen freely. Thus, the number of possibilities multiply by $p^{k-\mathrm{ord}_p(t)-1}$. ◀

▶ **Lemma 22.** *Let p be a prime, k be a positive integer, $t \in \mathbb{Z}/p^k\mathbb{Z}$ and γ_1, γ_2 be two one dimensional symbols. Then, $\mathfrak{S}^{t}_{p^k}(\gamma_1, \gamma_2)$ only depends on the p-symbol of $t \bmod p^k$.*

Proof. The calculation of $\mathfrak{S}^{t}_{p^k}(\gamma_1, \gamma_2)$ in Lemma 21 only depends on $\mathrm{ord}_p(t \bmod p^k)$ and $\mathrm{sgn}_p(t \bmod p^k)$. ◀

Thus, we mean the same thing by $\mathfrak{S}^{t}_{p^k}(\gamma_1, \gamma_2)$ and $\mathfrak{S}_{p^k}{}^{\mathrm{sym}_{p^k}(t)}(\gamma_1, \gamma_2)$.

Acknowledgements. We thank the reviewers for plenty of extremely helpful comments. In particular, we would like the two reviewers who gave extremely detailed comments and suggestion for improvements. We will incorporate more of their suggestions in the full version. All omissions and remaining errors are the authors responsability.

References

1 Leonard M. Adleman, Dennis R. Estes, and Kevin S. McCurley. Solving bivariate quadratic congruences in random polynomial time. *Mathematics of Computation*, 48(177):17–28, 1987.

2 Zenon Ivanovich Borevich and Igor Rostislavovich Shafarevich. *Number theory*, volume 20. Academic Press, 1986.

3 Sungmun Cho. Group schemes and local densities of quadratic lattices in residue characteristic 2. *arXiv:1210.7625v2*, preprint.

4 John Conway and Neil J. A. Sloane. Low-dimensional lattices IV. The mass formula. *Proc. R. Soc. Lond. A*, 419:259–286, 1988.

5 John Conway and Neil J. A. Sloane. *Sphere packings, lattices and groups*, volume 290. Springer, 1999.

6 John D Dixon. Asymptotically fast factorization of integers. *Mathematics of computation*, 36(153):255–260, 1981.

7 Wee Teck Gan and Jiu-Kang Yu. Group schemes and local densities. *Duke mathematical journal*, 105(3), 497–524, 2000.

8 Rupert Hartung. *Computational problems of quadratic forms: complexity and cryptographic perspectives*. Ph. D. thesis, Goethe-Universität Frankfurt a. M., 2008, http://publikationen.ub.uni-frankfurt.de/volltexte/2008/5444/pdf/HartungRupert.pdf, 2008.

9 Jonathan Hanke. Local densities and explicit bounds for representability by a quadratic form. *Duke mathematical journal*, 124(2), 351–388, 2004.

10 Yoshiyuki Kitaoka. *Arithmetic of quadratic forms*, volume 106. Cambridge University Press, 1999.

11 Hermann Minkowski. *Geometrie der Zahlen*. Berlin, 1910.

12 Onorato Timothy O'Meara. *Introduction to quadratic forms*, volume 117. Springer, 1973.

13 Gordon Pall. The weight of a genus of positive n-ary quadratic forms. In *Proc. Sympos. Pure Math*, volume 8, pages 95–105, 1965.

14 Oskar Perron. Bemerkungen über die Verteilung der quadratischen Reste. *Mathematische Zeitschrift*, 56:122–130, 1952.

15 John M. Pollard, Claus-Peter Schnorr An efficient solution of the congruence $x^2 + ky^2 = m \pmod{n}$. *IEEE Transactions on Information Theory* 33(5):702–709.

16 Victor Shoup. *A computational introduction to number theory and algebra*. Cambridge University Press, 2009.

17 Carl Ludwig Siegel. Über die analytische Theorie der quadratischen Formen. *The Annals of Mathematics*, 36(3):527–606, 1935.

18 G. L. Watson. The 2-adic density of a quadratic form. *Mathematika*, 23(01):94–106, 1976.

19 Tonghai Yang. An Explicit Formula for Local Densities of Quadratic Forms. *Journal of Number Theory*, 72:309–256, 1998.