THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Solving quadratic equations in dimension 5 or more without factoring

Pierre Castel

msp

THE OPEN BOOK SERIES **1** (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.213

msp

Solving quadratic equations in dimension 5 or more without factoring

Pierre Castel

Let Q be a 5×5 symmetric matrix with integral entries and with $\det Q \neq 0$, but neither positive nor negative definite. We describe a probabilistic algorithm which solves the equation ${}^t xQx = 0$ over $\mathbb{Z}$ without factoring $\det Q$. The method can easily be generalized to forms of higher dimensions by reduction to a suitable subspace.

1. Introduction

Solving quadratic equations in dimension 1 is trivial: Since the equation is $ax^2 = 0$, the only solution is $x = 0$. In two dimensions, the homogeneous equation is $ax^2 + bxy + cy^2 = 0$, and the solution is obtained by computing a square root. In dimension 3, the equation is

$$ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz = 0,$$

where the coefficients are integers. Since the polynomial becomes more complicated as the dimension increases, we use matrix notation instead. We define Q as the associated quadratic form. If we denote by $X = (x, y, z)$ the row vector containing the variables, the equation becomes

$${}^t X \begin{bmatrix} a & d & e \\ d & b & f \\ e & f & c \end{bmatrix} X = 0.$$

MSC2010: primary 11E20; secondary 11D09.
Keywords: general quadratic forms, factorization, general quadratic equations, isotropic spaces, algorithmic number theory, Cebotarev density theorem.

If the equation has a solution, several algorithms exist for finding solutions, for instance see Simon [11] or Cremona [3]. In dimension 3 it is known that finding a (nontrivial) isotropic vector is equivalent to factoring the determinant of the form.

The situation is almost the same in dimension 4 when the determinant is a square: Solutions may not exist, and if a solution exists, finding one is equivalent to factoring the determinant.

The situation is quite different in dimensions greater than or equal to 5. The Hasse-Minkowski theorem [9] asserts that in such dimensions a nontrivial solution always exists. It is easy to see that one just needs the result in dimension 5, since larger dimensions can handled by restricting the form to a subspace of dimension 5 where the form has a suitable signature. This is why we will focus on quadratic forms in dimension 5. As in dimensions 3 and 4, there exist algorithms such as the ones given in [10], but since they are generalizations of algorithms in smaller dimensions, they still need the factorization of the determinant, which rapidly becomes prohibitive. Thus, if we know the factorization of the determinant we can easily find a solution, so the question is whether it is possible to find a solution (in polynomial time) without factorizing the determinant. The goal of this paper is to show that this is indeed possible; in other words, we will give an algorithm which finds a (nontrivial) isotropic vector for a 5-dimensional quadratic form which does not require the factorization of the determinant.

As already mentioned, this algorithm can also be used for forms of higher dimensions by restricting the form to a dimension 5 subspace where the restricted form has a suitable signature. The solution is found over the integers, but since the equation is homogeneous, this is equivalent to finding a rational solution.

The first part of this paper gives the definitions needed to understand the algorithm, the second part explains how the algorithm works, and the last part gives some ideas of the complexity of the method. The full analysis of its complexity is not done here, since it requires a number of tools from analytic number theory and the Cebotarev density theorem [6]. I refer the interested reader to [1].

Basic definitions and notation

To begin, we give definitions and basic properties which we need.

We denote the set of integral quadratic forms as follows.

Definition 1.1. Let n be a nonzero positive integer. We denote by $\mathrm{Sym}(n,\mathbb{Z})$ the set of $n \times n$ symmetric matrices with nonzero determinant and integral entries.

We recall the definition of the Smith normal form of a matrix; for more details, see [2].

Definition 1.2 (Smith normal form). Let A be an $n \times n$ matrix with coefficients in $\mathbb{Z}$ and nonzero determinant. There exists a unique matrix in Smith normal form B such that $B = VAU$ with U and V elements of $\mathrm{GL}_n(\mathbb{Z})$. If we set $d_i = b_{i,i}$, the d_i are called the *elementary divisors* of the matrix A, and we have

$$A = U^{-1} \begin{bmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & d_n \end{bmatrix} V^{-1}$$

with $d_{i+1} \mid d_i$ for $1 \le i < n$.

Definition 1.3. For a matrix $M \in \mathcal{M}_n(\mathbb{Z})$ with nonzero determinant, we denote by $d_1(M), \dots, d_n(M)$ its elementary divisors (given by its Smith normal form). If there is no possible confusion, they will be denoted $d_1, \dots, d_n$.

We can now add a restriction to the set of quadratic forms.

Definition 1.4. Let n be a nonzero positive integer. We denote by $\mathrm{Sym}^*(n, \mathbb{Z})$ the set of $n \times n$ symmetric matrices with nonzero determinant and integral entries, such that their coefficient d_2 as defined above is equal to 1.

2. The algorithm

2A. ***The main idea.*** The key idea of the method is to increase by 1 the dimension of the form by adding a row and a column, then to use an efficient algorithm to find solutions to our new form, and finally to deduce a solution to the original form by considering intersections of hyperbolic spaces of suitable dimensions.

Since Simon's algorithm [10] is very efficient when the factorization of the determinant is known, we are going to build a new 6-dimensional quadratic form Q_6 starting from Q, whose determinant will be equal to $2p$ where p is an odd prime number. We will call this the *completion step*. To do this, we choose an integral vector $X = (x_1, \dots, x_5)$ of dimension 5 and an integer z and we complete Q in the following way:

$$Q_6 = \left[\begin{array}{ccc:c} & & & x_1 \\ & Q & & \vdots \\ & & & x_5 \\ \hdashline x_1 & \cdots & x_5 & z \end{array}\right]. \tag{1}$$

Lemma 2.1. *Let Q be a symmetric matrix with integral entries and with* $\det Q \neq 0$. *If we complete Q to the form Q_6 as described in* (1) *above, then we have*

$$\det Q_6 = z \det Q - {}^tX \operatorname{Co}(Q) X, \tag{2}$$

where $\mathrm{Co}(Q)$ *is the matrix of cofactors of the matrix* Q.

Proof. Simply use the formula involving the cofactors of Q_6 for computing its determinant, and expand it along the row and then the column containing the x_i. □

Some special cases may occur: There exist cases where all the values taken by $\det Q_6$ have a common factor. To avoid these cases we will have to do some minimizations of the form Q before completing it. In order to be able to do a complexity analysis of the algorithm we will need the determinant of Q_6 to be odd, so we will also have to perform a reduction of the even part of the determinant.

2B. ***Minimizations.*** The values taken by the determinant of the form Q_6 will follow from the next result.

Theorem 2.2. *Let* $Q \in \mathrm{Sym}(5, \mathbb{Z})$ *and* $\Delta = \det Q$. *Then for all* $X \in \mathbb{Z}^5$ *and for all* $z \in \mathbb{Z}$ *we have that* $d_2(Q)$ *divides* $\det Q_6$, *where* Q_6 *is defined by* (1).

Proof. Consider the Smith normal form of Q: There exist three matrices D, U, and V with integer entries such that D is diagonal with the elementary divisors on the diagonal, U and V have determinant ± 1, and $D = UQV$. Because of the relation (2), let us consider the values of $-{}^tX\,\mathrm{Co}(Q)X \pmod{\Delta}$. We have

$$\begin{aligned}\mathrm{Co}(Q) &= \mathrm{Co}(V^{-1})\,\mathrm{Co}(D)\,\mathrm{Co}(U^{-1})\\ &= (\det V)(\det U)\,{}^tV\,\mathrm{Co}(D)\,{}^tU\\ &= \pm{}^t\big(U\,{}^t\mathrm{Co}(D)V\big)\\ &= \pm{}^t(U\,\mathrm{Co}(D)V).\end{aligned}$$

Since D is the diagonal matrix of elementary divisors, it follows that $\mathrm{Co}(D)$ is also diagonal and that every coefficient is divisible by $d_2(Q)$. We thus have

$$\begin{aligned}{}^tX\,\mathrm{Co}(Q)X &= \pm{}^tX\,{}^t(U\,\mathrm{Co}(D)V)X\\ &\equiv 0 \pmod{d_2(Q)}.\end{aligned}$$

Combining this congruence with the formula (2) proves the result. □

Remark. If $d_1(Q) \neq \det Q$ it will not be possible to have $\det Q_6$ equal to a prime or twice an odd prime number, so we will first need to minimize Q so as to obtain an equivalent form Q' such that $d_2(Q') = 1$.

Remark 2.3. If we perform a change of basis using the matrix V of the previous result with $d_i(Q) \neq 1$ and $d_{i+1}(Q) = 1$, the first i columns and rows will be divisible by $d_i(Q)$.

We are now going to explain what to do in order to avoid the case $d_2(Q) \neq 1$.

Case $d_5 \neq 1$.

Proposition 2.4. *Let* $Q \in \mathrm{Sym}(5, \mathbb{Z})$ *such that* $d_5(Q) \neq 1$. *There exist two* 5×5 *matrices with integral entries* G *and* Q_f *such that*

$$d_5 Q_f = {}^t G Q G,$$
$$\det Q_f = \frac{1}{d_5^5} \det Q.$$

The proof is given by the following algorithm.

Algorithm 2.5 (Minimization 5).

Input: $Q \in \mathrm{Sym}(5, \mathbb{Z})$ such that $d_5(Q) \neq 1$ and $m \neq 1 \in \mathbb{Z}$ dividing $d_5(Q)$.

Output: Q_f: a form equivalent to Q such that $\det Q_f = (1/m^5) \det Q$;
G : the corresponding change of basis such that $d_5 Q_f = {}^t G Q G$.

1. Set $G := \mathrm{Id}_5$.
2. Set $Q_f := (1/m)Q$.
3. Return Q_f, G.

When the coefficient d_5 of the Smith normal form of Q is different from 1, the whole matrix Q is divisible by d_5, so the minimization simply consists in dividing the matrix by d_5 and the corresponding change of basis G is equal to Id_5.

Case $d_4 \neq 1$ *and* $d_5 = 1$.

Proposition 2.6. *Let* $Q \in \mathrm{Sym}(5, \mathbb{Z})$ *such that* $d_4(Q) \neq 1$ *and* $d_5(Q) = 1$. *There exist two* 5×5 *matrices with integral entries* G *and* Q_f *such that*

$$d_4 Q_f = {}^t G Q G,$$
$$\det Q_f = \frac{1}{d_4^3} \det Q.$$

The proof is given by the following algorithm.

Algorithm 2.7 (Minimization 4).

Input: $Q \in \mathrm{Sym}(5, \mathbb{Z})$ such that $d_4(Q) \neq 1$ and $d_5(Q) = 1$, $m \neq 1 \in \mathbb{Z}$ dividing $d_4(Q)$.

Output: Q_f: a form equivalent to Q such that $\det Q_f = (1/m^3) \det Q$;
G : the corresponding change of basis such that $m Q_f = {}^t G Q G$.

1. Let V be the V matrix given by the SNF of Q.
2. Let H be the diagonal matrix such that for $1 \leq i \leq 4$, $H_{i,i} = 1$ and $H_{5,5} = m$.
3. Set $G := V \times H$; $Q' := (1/m)\, {}^t G Q G$.

4. Apply the LLL algorithm for indefinite forms to Q' (see [11] for more details). Let Q_f be the returned form and G' the corresponding change of basis.
5. Set $G := G \times G'$.
6. Return Q_f, G.

As stated in Remark 2.3, after the change of basis in step 1, the first four columns and rows are divisible by d_4. Thus we apply this change of basis, multiply the last row and column by d_4, and divide the whole matrix by d_4.

Remark. The notion of equivalence between quadratic forms used here simply means that both corresponding quadratic equations have the same solutions up to a change of basis.

Case $d_3 \neq 1$ and $d_4 = 1$.

Proposition 2.8. *Let $Q \in \mathrm{Sym}(5, \mathbb{Z})$ such that $d_3(Q) \neq 1$ and $d_4(Q) = 1$. There exist two 5×5 matrices with integer entries G and Q_f such that*

$$d_3 Q_f = {}^t G Q G,$$
$$\det Q_f = \frac{1}{d_3} \det Q.$$

The proof is given by the following algorithm:

Algorithm 2.9 (Minimization 3).

Input: $Q \in \mathrm{Sym}(5, \mathbb{Z})$ such that $d_3(Q) \neq 1$ and $d_4(Q) = 1$, $m \neq 1 \in \mathbb{Z}$ dividing $d_3(Q)$.

Output: Q_f: a form equivalent to Q such that $\det Q_f = (1/m) \det Q$;
G : the corresponding change of basis such that $m Q_f = {}^t G Q G$.

1. Let V be the V matrix given by the SNF of Q.
2. Let H be the diagonal matrix such that for $1 \leq i \leq 3$, $H_{i,i} = 1$ and $H_{4,4} = H_{5,5} = m$.
3. Set $G := V \times H$; $Q' := (1/m)\, {}^t G Q G$.
4. Apply the LLL algorithm to Q'. Let Q_f be the returned form and G' the corresponding change of basis.
5. Set $G := G \times G'$.
6. Return Q_f, G.

The minimizing method for this case is essentially the same as for the previous one.

Case $d_2 \neq 1$ and $d_3 = 1$. This case is much more complicated than the previous ones. If we try to do it in the same way, we will multiply the determinant by some factor which is of course not what we want. The idea is first to perform a change of basis thanks to the matrix V given by the SNF of Q, and then to work on the 3×3 block that remains which may not be divisible by $d_2(Q)$. What we need to do in order to be able to apply the same method is to be in the case where the upper-left coefficient of this block is already divisible by $d_2(Q)$. We are thus going to do a special change of basis in order to succeed. The method is given by the following result.

Proposition 2.10. *Let $Q \in \mathrm{Sym}(5, \mathbb{Z})$ such that $d_2(Q) \neq 1$ and $d_3 = 1$. Let m be an integer such that $m \neq 1$ and $m \mid d_2(Q)$. There exist two 5×5 matrices with integral entries G and Q_f, with G unimodular, and such that*

$$mQ_f = {}^tGQG,$$
$$\det Q_f = \frac{1}{m} \det Q.$$

Proof. We first compute the SNF of Q, so that $D = UQV$ where D, U, V have integral entries and U and V are unimodular. We apply the change of basis given by the matrix V. The quadratic form $Q' = {}^tVQV$ is equivalent to the form Q and its first two rows and columns are divisible by m. Denote by Q_3 the restriction of Q' to the space spanned by the last three columns of the matrix V. This corresponds to the submatrix $(Q_3)_{i,j} = (Q')_{i,j}$ with $3 \leq i \leq 5$, $3 \leq j \leq 5$. We now want to have $Q_{3\,1,1} \equiv 0 \pmod m$. We apply a Gram-Schmidt orthogonalization process to the matrix Q_3 modulo m. If we find a noninvertible element modulo m, this means that we have found a factor of m. In that case we start the process again by replacing m by its divisor. During the process, if we find a vector whose norm is 0 modulo m, we just have to skip this step since this vector is exactly the one we need. Otherwise the process ends and gives us a change of basis such that in this new basis, the form $Q_3 \pmod m$ has the shape

$$\begin{bmatrix} a & & 0 \\ & b & \\ 0 & & c \end{bmatrix} \pmod m.$$

We must now solve the following quadratic equation:

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod m. \tag{3}$$

Since we do not want to factor m, we have to use a method which does not use its factorization. Such a method is described in [8]: If the coefficient a is not invertible modulo m we have found a factor of m, so we can continue the process with both factors, obtain the solution for each of them and combine them using the Chinese

remainder theorem and Hensel lifting if needed. We are thus reduced to the case where a is invertible modulo m. Solving (3) is equivalent to solving the equation

$$x^2 + ba^{-1}y^2 \equiv -ca^{-1}z^2 \pmod{m}. \tag{4}$$

If we take the arbitrary choice $z = 1$, we have exactly the type of equation that is solved in [8]. We thus use this method to obtain a solution S of (3). We complete the single vector family $\{S\}$ to a unimodular matrix G, and we extend the matrix G to a matrix G' of dimension 5 by taking the identity matrix Id_5 and replacing the 3×3 lower-right block by G. We now apply G' to Q' and obtain Q'' which has the form

$${}^tG'Q'G' = Q'' = \left[\begin{array}{c|ccc} mM_{2,2} & \multicolumn{3}{c}{mM_{2,3}} \\ \hline & m* & * & * \\ mM_{3,2} & * & * & * \\ & * & * & * \end{array}\right],$$

where the $*$ are integers. It is now possible to use the same methods explained in the previous cases: We multiply the last rows and columns by m and divide the whole matrix by m. □

Remark. The case where we find a factor of m practically never happens. The reason is simply that the forms used to test the algorithm always have a determinant which is very hard to factor. So finding a factor in such a way is quite hopeless.

The corresponding algorithm is the following.

Algorithm 2.11 (Minimization 2).

Input: $Q \in \mathrm{Sym}(5, \mathbb{Z})$ such that $d_2(Q) \neq 1$ and $d_3(Q) = 1$, $m \neq 1 \in \mathbb{Z}$ dividing $d_2(Q)$.

Output: Q_f: a form equivalent form to Q;
G : the corresponding change of basis such that $m'Q_f = {}^tGQG$ with $1 < m' \mid m$.

1. Compute the SNF of Q with the algorithm described in [5].
2. Set $G := V$ and $Q := {}^tGQG$.
3. Let Q_3 be the 3×3 bottom-right submatrix of Q.
4. Apply a modified Gram-Schmidt orthogonalization process (see below) to Q_3 and m.
5. If the Gram-Schmidt process returns a vector, store it in S and go to step 10. If it returns an integer m', go back to step 4 with $m = m'$.
6. Denote by D_3 the returned matrix and by G_3 the corresponding change of basis.

7. Let $d = \gcd(D_3[1,1], m)$. If $d \neq 1$, go back to step 5 with $m = d$.
8. Use the Pollard-Schnorr algorithm [8] to solve

$$X^2 + \frac{D_3[2,2]}{D_3[1,1]} Y^2 \equiv -\frac{D_3[3,3]}{D_3[1,1]} \pmod{m}.$$

   Let S be a solution.
9. Set $S := [S, 1]$.
10. Let H be a 3×3 matrix whose first column is equal to S and whose columns form a $\mathbb{Z}^3$ basis. This can be done using the Hermite normal form algorithm.
11. Set $G_3 := G_3 \times H$.
12. Let $\widetilde{G}$ be the block-diagonal 5×5 matrix such that the 2×2 upper-left block is the identity and the 3×3 bottom-right block is equal to G_3.
13. Set $G := G \times \widetilde{G}$ and $Q' := (1/m)\, {}^tGQG$.
14. Apply the LLL algorithm to reduce Q', and denote by Q_f the returned form and by G' the corresponding change of basis.
15. Set $G := G \times G'$.
16. Return Q_f, G.

The minimization algorithm. We can now give the complete algorithm that minimizes an integral quadratic form of dimension 5.

Algorithm 2.12 (Minimization).

Input: $Q \in \mathrm{Sym}(5, \mathbb{Z})$.

Output: $Q_t \in \mathrm{Sym}^*(5, \mathbb{Z})$ equivalent to Q;
B : the corresponding change of basis.

1. Set $Q_t := Q$.
2. Compute the SNF D of Q.
3. If $d_1 = \det Q$, go to step 8.
4. If $d_5 \neq 1$ set $i := 5$.
5. Let $i \leq 5$ be such that $d_i \neq 1$ and $d_{i+1} = 1$ or $d_i = d_5$ if $d_5 \neq 1$.
6. Set $B := \mathrm{Id}_5$.
7. While $d_1 \neq \det Q_t$:
   (a) Switch according to i:
   Case $i = 5$: apply Algorithm 2.5 to Q_t and d_i.
   Case $i = 4$: apply Algorithm 2.7 to Q_t and d_i.
   Case $i = 3$: apply Algorithm 2.9 to Q_t and d_i.

Case $i = 2$: apply Algorithm 2.11 to Q_t and d_i.

(b) Let Q_f and G be the returned matrices.

(c) Set $Q_t := Q_f$ and $B := B \times G$.

(d) Compute the SNF D of Q_t.

(e) Let d_i be the diagonal coefficient of the SNF of Q_t such that $d_i \neq 1$ with $d_{i+1} = 1$ and $d_i = d_5$ if $d_5 \neq 1$.

8. Return Q_t, B.

Remark. This algorithm computes the Smith normal form at any step. To do this, it is strongly recommended to use the method described in [5] which is optimized and also gives the corresponding matrices U and V.

Remark. In this algorithm, we do not use a divisor m of d_i, but d_i itself. Using a divisor would force the algorithm to use factorization.

Remark. Algorithms 2.7, 2.9, and 2.11 include a reduction step using an LLL algorithm for indefinite quadratic forms given in [11]. This reduction is done to have concrete bounds for the size of the coefficients at the end of the algorithm.

2C. ***Reducing the even part of the determinant.*** After performing the *minimization step*, we get a form whose coefficient d_2 is equal to 1. We now need to have an equivalent form whose determinant is odd. This is performed by what we call the *reducing the even part step*.

Lemma 2.13. *Let $Q \in \mathrm{Sym}^*(5, \mathbb{Z})$ be indefinite. Let v be the quotient in the Euclidean division of the 2-adic valuation of* $\det Q$ *by 2. There exist two matrices Q' and G such that*

$$\begin{aligned} \det G &= \frac{1}{2^v}, \\ Q' &= {}^tGQG, \\ v_2(\det Q') &= 0 \text{ or } 1, \\ Q' &\in \mathrm{Sym}^*(5, \mathbb{Z}). \end{aligned}$$

Proof. If $\det Q$ is odd, we simply take $G = \mathrm{Id}_5$ and $Q' = Q$. Thus assume that $v_2(\det Q) \neq 0$. We compute the SNF of Q and obtain unimodular integer matrices U, V and a diagonal matrix D such that $D = UQV$, and $d_{1,1} = |\det Q|$. Since $d_2(Q) = 1$ the other diagonal coefficients of D are all equal to 1. We apply to Q the change of basis given by the matrix V. The first row and the first column of $Q'' = {}^tVQV$ are divisible by $2^{v_2(\det Q)}$. Let v be the quotient in the Euclidean division of the 2-adic valuation of $\det Q$ by 2, F be the diagonal matrix whose upper-left entry is equal to $1/2^v$ and the others equal to 1. If $v_2(\det Q)$ is even, the determinant of ${}^tFQ''F = Q'$ is odd. Otherwise the determinant of Q'

is divisible by 2 but not by 4. So we take $G = V \times F$. It remains to show that $Q' \in \mathrm{Sym}^*(5, \mathbb{Z})$. We know that $Q \in \mathrm{Sym}^*(5, \mathbb{Z})$. Since the change of basis given by the SNF is unimodular the invariant factors have not changed during the process. The last operation is done on the first column and only with a power of 2, so it also does not change the invariant factors, and so we have $Q' \in \mathrm{Sym}^*(5, \mathbb{Z})$. □

The corresponding algorithm is as follows.

Algorithm 2.14 (Reduction of the even part — I).

Input: $Q \in \mathrm{Sym}^*(5, \mathbb{Z})$ indefinite, of dimension 5, of determinant Δ.

Output: $Q' \in \mathrm{Sym}^*(5, \mathbb{Z})$ indefinite, of determinant $2^k n$ with n odd and $k \equiv v_2(\det Q) \pmod 2$, Q' equivalent to Q;
G the corresponding change of basis.

1. If $\Delta \equiv 1 \pmod 2$, return Q, Id_5.
2. Set $G := \mathrm{Id}_5$.
3. Let v_2 be the 2-adic valuation of Δ.
4. Let v be the quotient in the Euclidean division of v_2 by 2.
5. Let U, V and D be the matrices given by the SNF of Q such that $D = UQV$.
6. Set $Q' := {}^tVQV$ and $G := G \times V$.
7. Let H be the diagonal matrix such that $H_{1,1} = 1/2^v$ and $H_{i,i} = 1$ otherwise.
8. Set $Q' := {}^tHQ'H$ and $G := G \times H$.
9. Return Q', G.

Lemma 2.15. *Let $Q \in \mathrm{Sym}^*(5, \mathbb{Z})$ indefinite and such that $\det Q = 2k$, $k \in \mathbb{Z}$, odd. There exist two matrices Q' and G such that*

$$\begin{aligned} \det G &= \frac{1}{2^3}, \\ Q' &= 2 \times {}^tGQG, \\ \det Q' &\equiv k \pmod 2. \end{aligned}$$

Proof. As in proof of the previous lemma, we begin by computing the Smith normal form of Q to obtain integer matrices U, V unimodular and D diagonal such that $D = UQV$ and $d_{1,1} = |\det Q|$. We apply to Q the change of basis given by the matrix V and obtain Q' which has the following form:

$$Q' = {}^tVQV = \begin{bmatrix} 2* & 2* & & \\ & Q_1 & * & * \\ 2* & & * & * \\ & & * & * \\ & & * & * \end{bmatrix}.$$

We are now interested in the form Q_1 which is the restriction of the form Q to the subspace generated by the second and third vectors of the basis. Denote this form by the following matrix: $\left[\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right]$. We are looking for a change of basis such that the coefficient a in the new basis will be even. This means that we want a pair (x, y) such that $ax^2 + cy^2 \equiv 0 \pmod 2$. We solve this equation, apply the corresponding change of basis to Q_1, and we multiply the whole matrix by 2. The determinant of the form is now divisible by 2^6 but not by 2^7. We rescale the first two vectors by a factor 2. The determinant is now divisible by 2^2. We then compute the SNF of this matrix and apply the change of basis according to the matrix V. Since the determinant is divisible by 4, we have two possibilities: If the kernel modulo 2 has dimension 1, the first row and the first column are divisible by 2 and the upper left coefficient is divisible by 4. In this case, we rescale the first vector by 2. Otherwise, the kernel has dimension 2. In this case, the first two rows and columns are divisible by 2. Consider the upper-left 2×2 block of the matrix. This corresponds to the restriction of the form to the subspace generated by the first two vectors of the basis. We are going to apply a change of basis such that the upper-left coefficient will be divisible by 4. This corresponds to solving the equation $ax^2 + cy^2 \equiv 0 \pmod 2$ which can be done as explained above. Once the change of basis is done, we simply rescale the first vector by 2. In such a basis, the determinant of the form is now odd. It remains to show that this form belongs to $\mathrm{Sym}^*(5, \mathbb{Z})$. Indeed, since the determinants of the changes of basis that we have applied are all equal to a power of 2 they are invertible modulo the odd primes factors of the determinant of the form, and it follows that the rank of the form is unchanged, so we have $Q' \in \mathrm{Sym}^*(5, \mathbb{Z})$. □

The corresponding algorithm is as follows.

Algorithm 2.16 (Reduction of the even part — II).

Input: $Q \in \mathrm{Sym}^*(n, \mathbb{Z})$ indefinite, with $\det Q = \Delta = 2^k n$ with n odd and $k = 0$ or 1.

Output: Q', a form in $\mathrm{Sym}^*(5, \mathbb{Z})$ with odd determinant and same solutions as Q up to a change of basis;
G the corresponding change of basis.

1. If $\Delta \equiv 1 \pmod 2$ return Q, Id_5.
2. Set $G := \mathrm{Id}_5$.
3. Let v be the 2-adic valuation of Δ.
4. Let U, V and D be the matrices given by the SNF of Q such that $D = UQV$.
5. Set $Q' := {}^tVQV$ and $G := G \times V$.
6. If $(q'_{2,2}, q'_{3,3}) \equiv (1, 1) \pmod 2$,

(a) set $H := \mathrm{Id}_5$ and $H[3,2] := 1$,
(b) set $Q' := {}^tHQ'H$ and $G := G \times H$.

7. If $(q'_{2,2}, q'_{3,3}) \equiv (1,0) \pmod 2$,
   (a) set $H := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$,
   (b) set $Q' := {}^tHQ'H$ and $G := G \times H$.
8. Set $Q' := 2 \times Q'$.
9. Set $P := \mathrm{Id}_5$ and $P[2,2] := 1/2$.
10. Set $Q' := {}^tPQ'P$ and $G := G \times P$.
11. Let U', V' and D' be the matrices given by the SNF of Q' such that $D = UQ'V$.
12. Set $Q' := {}^tV'Q'V'$ and $G := G \times V'$.
13. If $q'_{1,1} \equiv 0 \pmod 4$,
    (a) set $R := \mathrm{Id}_5$ and $R[1,1] := 1/2$,
    (b) set $Q' := {}^tRQ'R$ and $G := G \times R$,
    (c) return Q', G.
14. Repeat steps 6 to 2 with $(q'_{1,1}, q'_{2,2})$.
15. Set $R := \mathrm{Id}_5$ and $R[1,1] := 1/2$.
16. Set $Q' := {}^tRQ'R$ and $G := G \times R$.
17. Return Q', G.

2D. ***Completion.*** We now explain how to complete the form to a form of dimension 6 in the way announced in Section 2A, and in particular how to choose the value of z. Controlling this value will allow us to change the signature of the completed form Q_6.

Lemma 2.17. *Let $Q \in \mathrm{Sym}(5,\mathbb{Z})$ be an indefinite form with signature (r,s) and determinant Δ. Let X be a 5-dimensional column vector with integral entries and $\overline{\beta}$ be a coset representative of the coset of ${}^tX\,\mathrm{Co}(Q)X$ modulo Δ. Let*

$$z := \frac{{}^tX\,\mathrm{Co}(Q)X - \overline{\beta}}{\Delta}$$

and

$$Q_6 = \begin{bmatrix} Q & X \\ {}^tX & z \end{bmatrix}.$$

The signature of Q_6 is determined by the signs of $\overline{\beta}$ and $\det Q$ *as follows*:

$$\text{signature of } Q_6 = \begin{cases} (r, s+1) & \text{if } \overline{\beta} \det Q > 0; \\ (r+1, s) & \text{if } \overline{\beta} \det Q < 0. \end{cases}$$

Moreover we have $\overline{\beta} = -\det Q_6$.

Proof. As seen in Section 2A, the formula (2) gives us the determinant of the form Q_6:

$$\det Q_6 = z \det Q - {}^tX \operatorname{Co}(Q) X.$$

We also have defined the quantities: $\beta = {}^tX \operatorname{Co}(Q)X$ and $\overline{\beta}$ a coset representative of the coset of β modulo Δ which is also equal to $\beta - z\Delta = -\det Q_6$. Since the link between Q and Q_6 is the addition of a row and a column, if we consider the restriction of Q to the subspace generated by the first 5 vectors of the basis, we get back exactly the form Q. Thus if we add a row and a column, we do not change its signature on this subspace. It follows that we can deduce the signature of Q_6 from the signature of Q by simply considering the sign of their determinant. Indeed, we know that $\operatorname{sgn}(\det Q) = (-1)^s$. If $\det Q > 0$, we have $s \equiv 0 \pmod 2$. We take $\overline{\beta} > 0$ and have $\det Q_6 < 0$. We have changed the sign of the determinant, so the signature of Q_6 is $(r, s+1)$. The others cases are done in the same way, and combining them gives the formula for the signature given in the lemma. □

In order to be able to compute a solution, we need the signature (u, v) of Q_6 to satisfy $u \geq 2$ and $v \geq 2$. The following algorithm will choose the value of $\overline{\beta}$ so that this is satisfied. The algorithm for completing the form and controlling the signature is the following.

Algorithm 2.18 (Completion).

Input: Q: an indefinite, nondegenerate dimension 5 integral quadratic form; $k \geq 1$ an integer.

Output: Q_6: an indefinite, nondegenerate dimension 6 integral quadratic form with signature (r, s) such that $r \geq 2$ and $s \geq 2$, of the form: $\begin{bmatrix} Q & X \\ {}^tX & z \end{bmatrix}$, and such that $|\det Q_6| < k|\det Q|$.

1. Compute the signature (r, s) of Q.
2. Choose an integer vector X whose coordinates are nonnegative integers less than $|\det Q|^5$.
3. Set $\beta := {}^tX \operatorname{Co}(Q)X$ and $\overline{\beta} := \beta \pmod{\det Q}$ with $0 \leq \overline{\beta} < |\det Q|$.
4. If $r = 1$ and $\det Q > 0$, set $\overline{\beta} := \overline{\beta} - |\det Q|$.
5. If $s = 1$, set $\overline{\beta} := \overline{\beta} - \det Q$.
6. Set $z := \dfrac{\beta - \overline{\beta}}{\det Q}$.

7. Add a random multiple of $|\det Q|$ to $\bar{\beta}$ so that $|\det Q_6| < k\,|\det Q|$ while respecting the signature condition, and update the value of z.
8. Return $Q_6 = \begin{bmatrix} Q & X \\ {}^tX & z \end{bmatrix}$.

Remark. The bounds on X in step 2 are chosen in this way since everything is then reduced modulo $\det Q$. Changing the bounds would not change the complexity of the whole algorithm.

Remark. At the end of the algorithm, the determinant of Q_6 is always equal to $\bar{\beta}$. This is a consequence of the choice of the value of z.

Remark. We will use this algorithm until we obtain a $\bar{\beta}$ of the form $2 \times p$ with p an odd prime number. This choice will be explained in Section 2E.

2E. ***Computing a solution.*** The complete algorithm for finding a nonzero isotropic vector for a quadratic form dimension 5 without factoring the determinant is as follows.

Algorithm 2.19 (Solving).

Input: Q, an integral indefinite, nondegenerate quadratic form of dimension 5.

Output: X, a nonzero integral isotropic vector for Q.

1. Apply the minimization Algorithm 2.12 to Q.
2. Apply Algorithms 2.14 and 2.16 to the result of step 1.
3. Apply the completion Algorithm 2.18 to the result of step 2 until the determinant of the returned form Q_6 is equal to $\pm 2p$ where p is an odd prime number.
4. Solve the equation ${}^tXQ_6X = 0$.
5. Write $Q_6 = H \oplus Q_4$ where H is a hyperbolic plane.
6. Solve the equation ${}^tXQ_4X = 0$.
7. Write $Q_4 = H' \oplus Q_2$ where H' is a hyperbolic plane.
8. Deduce from the previous steps a solution S to the equation ${}^tXQX = 0$.
9. Return S.

Theorem 2.20. *Let Q be an integral indefinite, nondegenerate quadratic form of dimension 5. Then Algorithm 2.19, applied to Q, outputs a nonzero integral vector S that is a solution to the equation ${}^tXQX = 0$ without factorizing any integer.*

Remark. The above algorithm is based on the fact that the method developed by Simon in [11] is very efficient as soon as the factorization of the determinant of the form is known. This theorem shows that there exists an efficient algorithm even when the factorization is not known or when it is not possible to factor the determinant in a reasonable amount of time.

Proof. This proof follows the steps of the algorithm. We are going to divide the proof in the same way as the algorithm is divided:

1: Minimizations

2: Reducing the even part

3: Choice of the signature and completion of Q while imposing the form of the determinant

4: Computing a solution for Q_6

5: Decomposition in a sum with a hyperbolic plane

6: Computing a solution for Q_4

7: Decomposition in a sum with a hyperbolic plane

8: Computing a solution for Q

Step 1: We apply Algorithm 2.12 to Q. At the end of this step, we have a form $Q^{(2)} \in \mathrm{Sym}^*(5, \mathbb{Z})$ equivalent to Q, an invertible matrix G_2, and a nonzero rational number $\lambda^{(2)}$ such that $Q^{(2)} = \lambda^{(2)}\, {}^tG_2 Q G_2$.

Step 2: We successively apply Algorithms 2.14 and 2.16 to $Q^{(2)}$ in order to have a form with an odd determinant. At the end of this step, we obtain a form $Q^{(3)} \in \mathrm{Sym}^*(5, \mathbb{Z})$ equivalent to Q, an invertible matrix G_3, and a nonzero rational number $\lambda^{(3)}$ such that $Q^{(3)} = \lambda^{(3)}\, {}^tG_3 Q^{(2)} G_3$ and the determinant Δ of $Q^{(3)}$ is odd.

Step 3: We apply Algorithm 2.18 and choose $k = 10^6$ (the value of k will be detailed in a further paper) until the determinant of the returned form is equal to $\pm 2p$ with p an odd prime number; the condition $2 \times p$ is necessary because of some conditions on local solubility at 2. It is possible to show that a vector X verifying these conditions can always be found efficiently by using an effective version of the Cebotarev density theorem [6]. At the end of this step, we have a form Q_6 whose restriction to the subspace generated by the first 5 vectors of the basis is equal to $Q^{(3)}$, whose determinant is equal to $\pm 2p$ with p an odd prime number, and whose signature (r, s) is such that $r \geq 2$ and $s \geq 2$.

Step 4: We use the algorithm described in [11], and obtain a nonzero integral vector T such that ${}^tTQ_6T = 0$. We divide T by the GCD of its coordinates in order to have T primitive.

Step 5: This step consists in finding a hyperbolic plane containing the vector T. The existence of such a plane is given by the result in [9, p.55, Proposition 3.]. We first write the form Q_6 in a unimodular basis whose first vector is the vector T (the basis can be found by using the HNF of a primitive vector), we denote by G_4 such a change of basis. We then have $Q_6^{(1)} = {}^tG_4 Q_6 G_4$ and the upper-left coefficient is 0. Let $R = \big(Q_6^{(1)}[1,2], Q_6^{(1)}[1,3], Q_6^{(1)}[1,4], Q_6^{(1)}[1,5], Q_6^{(1)}[1,6]\big)$, and let G_5

be a unimodular matrix such that $RG_5 = (a, 0, 0, 0, 0)$, where a is the GCD of the coefficients of the vector R. Since a divides the first row and the first column of the matrix $Q_6^{(1)}$ we have $a^2 \mid \det Q_6^{(1)}$, but since $\det Q_6^{(1)} = \pm 2p$ with p prime, we must therefore have $a = 1$. Such a G_5 matrix is given by the HNF of the vector R. We can now set $G_6 = \begin{bmatrix} 1 & 0 \\ 0 & G_5 \end{bmatrix}$, and we then have

$$Q_6^{(2)} = {}^tG_6 Q_6^{(1)} G_6 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & b_2 & b_3 & b_4 & b_5 & b_6 \\ 0 & b_3 & * & * & * & * \\ 0 & b_4 & * & * & * & * \\ 0 & b_5 & * & * & * & * \\ 0 & b_6 & * & * & * & * \end{bmatrix}.$$

Now let G_7 be the following matrix:

$$G_7 = \begin{bmatrix} 1 & \left[\frac{-b_2}{2}\right] & -b_3 & -b_4 & -b_5 & -b_6 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

We have $\det G_7 = 1$, and

$$Q_6^{(3)} = {}^tG_7 Q_6^{(2)} G_7 = \left[\begin{array}{cc:cccc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & \multicolumn{4}{c}{\multirow{4}{*}{Q_4}} \\ 0 & 0 & & & & \\ 0 & 0 & & & & \\ 0 & 0 & & & & \end{array}\right],$$

where $Q_4 \in \mathrm{Sym}(4, \mathbb{Z})$. We also have $\det Q_4 = -\det Q_6$. The coefficient in this matrix is either 0 or 1 according to the parity of the coefficient b_2, but it will not change anything in the rest of the algorithm. We regroup all the changes of basis and set $G_8 = G_4 \times G_6 \times G_7$. We then have $Q_6^{(3)} = {}^tG_8 Q_6 G_8$. This step ends with the computation of the matrices $Q_6^{(3)}$ and G_8.

Step 6: We now work on the quadratic form Q_4 defined above. Its determinant is $-\det Q_6$, which is still equal to $\mp 2p$ with p a prime number. We are going to show that the equation ${}^tXQ_4X = 0$ has a nontrivial solution: We know that Q_4 is indefinite; indeed, the form $Q^{(3)}$ has been completed in order to have $r \geq 2$ and $s \geq 2$. We have decomposed this form into the sum of a hyperbolic plane and a dimension 4 quadratic form Q_4, but the signature of a quadratic form on a

hyperbolic plane is $(1,1)$, and $Q_6^{(3)}$ has the same signature as Q_6, so the signature Q_4 is $(r-1,s-1)$ and we have $r-1\geq 1$, $s-1\geq 1$, showing that Q_4 is indefinite hence that there exists real solutions. We now need to show the existence of a solution over $\mathbb{Q}_\ell$ for every prime number ℓ. If ℓ is an odd prime number not dividing $\det Q_4$, the consideration of Hilbert symbols shows that solutions always exist. Two cases remain: $\ell=2$ and $\ell \mid \det Q_4$. We know that $\det Q_4 = \pm 2p$ is not a square neither in $\mathbb{Q}_2$ nor in $\mathbb{Q}_p$ since the valuations are odd and $p\neq 2$, so there exist local solutions, and using the local-global principle allows us to conclude. Since solutions exist, we can now use Simon's algorithm to compute such a solution, and since the determinant is equal to $\pm 2p$ with p prime, we do not need to use any factorization. We denote by R a primitive solution.

Step 7: This step is the same as the step 5, but the work is done over the form $Q_4^{(1)}$. Let B be the corresponding change of basis.

Step 8: We have to recall the changes of basis done on the matrix Q_4. We set

$$G_9 = \left[\begin{array}{cc|cccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & \multicolumn{4}{c}{\multirow{3}{*}{B}} \\ 0 & 0 & & & & \\ 0 & 0 & & & & \\ 0 & 0 & & & & \end{array}\right]$$

and

$$P = G_8 \times G_9.$$

We thus have a matrix P such that

$${}^tPQ_6P = \left[\begin{array}{cc|cc|c} 0 & 1 & & & \\ 1 & \alpha & \multicolumn{2}{c|}{0} & 0 \\ \hline & & 0 & 1 & \\ \multicolumn{2}{c|}{0} & 1 & \beta & 0 \\ \hline & & & & \\ 0 & & 0 & & Q_2 \end{array}\right]$$

with $\alpha,\beta = 0$ or 1. We note that the first and the third columns of P are solutions of the equation ${}^tXQ_6X=0$. But they also are orthogonal vectors for Q_6. It follows that every linear combination of these vectors still is a solution for Q_6. We now consider a combination such that the last coordinate is 0, denote it by J. We then have

$$J = \begin{bmatrix} U \\ \hline 0 \end{bmatrix} \quad \text{with } U \in \mathbb{Z}^5.$$

We know that ${}^tJQ_6J = 0$, but we give the computation in detail:

$$\begin{aligned} {}^tJQ_6J &= \begin{bmatrix} {}^tU & 0 \end{bmatrix} \left[\begin{array}{c|c} Q^{(3)} & X \\ \hline {}^tX & z \end{array}\right] \begin{bmatrix} U \\ \hline 0 \end{bmatrix} \\ &= {}^tUQ^{(3)}U \\ &= 0. \end{aligned}$$

Thus U is a nonzero solution to the equation ${}^tXQ^{(3)}X = 0$. We then set $S = G_2G_3U$, and we have ${}^tSQS = 0$. We are finally done. □

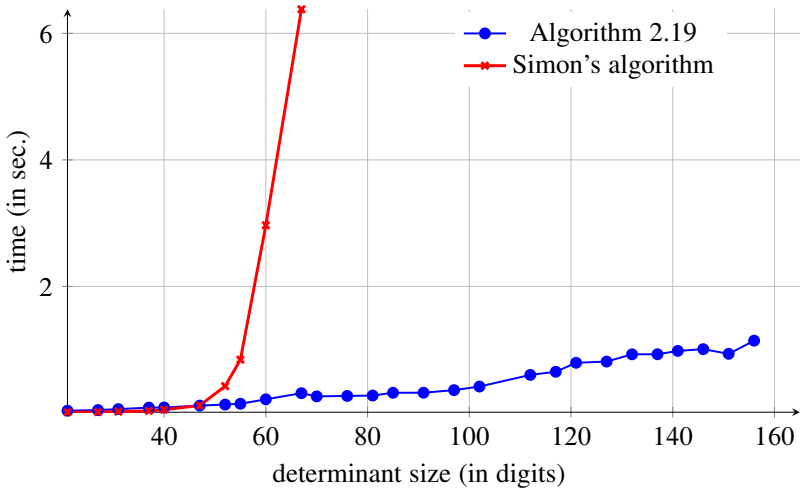
Remark. The condition of having the determinant equal to $\pm 2 \times p$ with p an odd prime is necessary due to the condition of local solubility over $\mathbb{Q}_2$. The 2 can be replaced by 2^{2k+1} with $k \in \mathbb{N}$, but the analysis is much more complicated in this case and it practically does not affect the running time of the algorithm.

Remark. The complexity of the algorithm is not done here, but the number of vectors X that we need to try in step 3 until we have a determinant of the desired shape is $\mathcal{O}(\log|\det Q|)$.

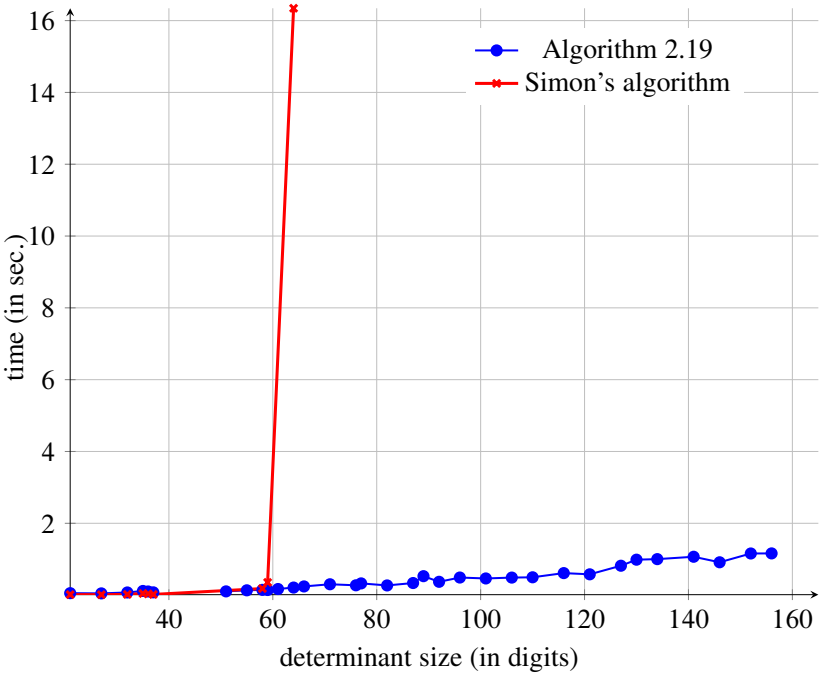
2F. ***Generalization to higher dimensions.*** The algorithm given above is for quadratic forms of dimension 5. It is easy to generalize it to higher dimensions: Indeed, since the algorithm needs a form of dimension 5 as an input, if the given form has a larger dimension, we simply need to restrict the form to a subspace of dimension 5. The only condition required is that the restriction of the form must have a signature (r, s) that verifies $r \geq 1$ and $s \geq 1$ so that the decomposition as the sum of two hyperbolic planes is possible. When a solution to the restriction is found, we simply lift the solution to the original space by setting the remaining coordinates to 0.

3. Overview of performance

This algorithm has been implemented in the PARI/GP language, see [7]. Since the proof of the complexity of this algorithm requires a considerable amount of additional work it will not be detailed here, but will be explained in a further work. However, we give an overview of the global performances of the algorithm with the two following figures. The comparisons are made with the method given by Simon in [11] and [10]. These algorithms have also been implemented in the PARI/GP language and can downloaded from the author's webpage (http://www.math.unicaen.fr/~simon).



These values have been computed by averaging over 100 random forms for each point. The forms are the same for each algorithm. We can clearly observe the fact that the factorization of the determinant makes Simon's algorithm very slow for determinants with size larger than 50 digits. The graph below shows the same comparison, but this time, the method used for building the forms is made in such a way that the algorithm often needs to do minimizations. We still can see the "wall" due to the factorization of the determinant in Simon's method.



Acknowledgments

I thank Henri Cohen for his help with translation and the anonymous reviewers for their helpful comments.

References

[1] Pierre Castel, *Un algorithme de résolution des équations quadratiques en dimension* 5 *sans factorisation*, Ph.D. thesis, Laboratoire de Mathématiques Nicolas Oresme, 2011. http://www.math.unicaen.fr/~castel/production/these_castel.pdf

[2] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, no. 138, Springer, Berlin, 1993. MR 94i:11105

[3] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441. MR 2004a:11137

[4] A. Fröhlich (ed.), *Algebraic number fields*: *L-functions and Galois properties*: *Proceedings of a Symposium held at the University of Durham*, *Sept.* $2--12$, 1975, Academic Press, London, 1977. MR 55 #10416

[5] Costas S. Iliopoulos, *Worst-case complexity bounds on algorithms for computing the canonical structure of finite abelian groups and the Hermite and Smith normal forms of an integer matrix*, SIAM J. Comput. **18** (1989), no. 4, 658–669. MR 91a:20065

[6] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in Fröhlich [4], 1977, pp. 409–464. MR 56 #5506

[7] PARI Group, Bordeaux, France, *PARI/GP (version* 2.5.0*)*, 2011. http://pari.math.u-bordeaux.fr/

[8] John M. Pollard and Claus-P. Schnorr, *An efficient solution of the congruence* $x^2 + ky^2 = m \pmod n$, IEEE Trans. Inform. Theory **33** (1987), no. 5, 702–709. MR 89e:11080

[9] Jean-Pierre Serre, *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1988.

[10] Denis Simon, *Quadratic equations in dimension* 4*,* 5 *and more*, preprint, 2005. http://www.math.unicaen.fr/~simon/maths/Dim4.pdf

[11] ———, *Solving quadratic equations using reduced unimodular quadratic forms*, Math. Comp. **74** (2005), no. 251, 1531–1543. MR 2005k:11246

PIERRE CASTEL: pierre.castel@unicaen.fr
Laboratoire de Mathématiques Nicolas Oresme, Université de Caen Basse-Normandie, UMR CNRS 6139, 14032 Caen, France

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS