# Algorithms for solving rational quadratic forms *

Josef Schicho, RICAM, Austrian Academy of Sciences, Linz
Jana Pílniková, RISC, Johannes Kepler University, Linz

**Abstract**

We present algorithms for solving quadratic forms over rational numbers based on constructive proofs of the Hasse principle for these forms.

## 1 Introduction

In this document we describe algorithms for finding a nontrivial rational solution of a given quadratic form with any number of variables.

Quadratic forms (i.e. homogenous quadratic polynomials) over rationals belong to the class of polynomials where the so-called Hasse principle holds. Namely, there exists a rational solution to the form if and only if there exists a solution in every local field containing $\mathbb{Q}$, it means any field complete with respect to some valuation defined on $\mathbb{Q}$.

In the case of quadratic forms there is even a stronger result: we can construct a global (means rational) solution of a given quadratic form by combining local solutions (means solutions in local fields).

For developing the algorithms we mainly follow [2]. After implementing the algorithm for solving ternary quadratic forms we learned that meanwhile there was another algorithm developed (cf. [3]), which avoids the expensive LLL reduction a is therefore faster. So in the last version of the package we replaced our version by that one. However, algorithms for solving forms with more variables are new.

It is worth to mention that the most interesting cases for solving quadratic forms are those with three and four variables. The reason is, that a form of 5 and more variables has a solution in every local field except possibly the field of real numbers (see Lemma 16). So, by the Hasse principle, if we want to test whether there is a rational solution, it is enough to test the solvability in $\mathbb{R}$, which is very easy.

We implemented all algorithms in Magma ([1]). They should appear in one of next versions of the system.

*Supported by SFB Grant F1303 of the Austrian FWF.

## 2 The field of $p$-adic numbers

**Definition 1.** *Let $k$ be any field. The function $|.| : k \to \mathbb{R}$ is called a* valuation *if it satisfies the following conditions:*

*(i)* $|a| \geq 0 \ \forall a \in k,$ *and* $|a| = 0$ *iff* $a = 0.$

*(ii)* $|ab| = |a||b| \ \forall a, b \in k.$

*(iii)* $|a + b| \leq |a| + |b| \ \forall a, b \in k$ *(triangle inequality).*

Here we consider only valuations defined for the field of rational numbers. We have the following possibilities how to define a non-trivial valuation:

- absolute value,
- *$p$-adic valuation*: For a fixed prime $p$ let

$$r = p^{\rho} u/v; \quad u, v \in \mathbb{Z}, \ p \nmid uv.$$

Then we define a non-archimedean valuation

$$|r|_p = p^{-\rho}.$$

Usually the standard absolute value is called *valuation at infinity* and denoted by $|.|_{\infty}$.

**Theorem 2. (Ostrowski)** *Every non-trivial valuation on $\mathbb{Q}$ is equivalent to one of the valuations $|.|_p$, where either $p$ is a prime number or $p = \infty$.*

Every valuation gives rise to a topology on $\mathbb{Q}$. And like the field $\mathbb{R}$ of real numbers is constructed as the completion of the field $\mathbb{Q}$ w.r.t. the absolute value, we have also the following

**Definition 3.** *Let $|.|_p$ be a non-archimedean valuation on $\mathbb{Q}$.* The field of $p$-adic numbers $\mathbb{Q}_p$ *is the completion of $\mathbb{Q}$ with respect to the valuation $|.|_p$.*

Again, as in the case of absolute value, one often denotes $\mathbb{R}$ by $\mathbb{Q}_{\infty}$, since it is the completion of $\mathbb{Q}$ w.r.t. $|.|_{\infty}$. Traditionally, the field of rational numbers is referred to as the *global field*, and all its completions (i.e. all $p$-adic fields together with $\mathbb{R} = \mathbb{Q}_{\infty}$) are called *local fields*.

Since every local field $\mathbb{Q}_p$ ($p$ being prime or $\infty$) contains $\mathbb{Q}$ as its subset, it is clear, that if a polynomial equation with rational coefficients has a solution over $\mathbb{Q}$, then this is also the solution over any local field. So we can decide about unsolvability of the equation over $\mathbb{Q}$ by finding one local field, where it is not solvable.

It would be very nice, if also the converse holds, namely:

**Local-Global Principle.** *The existence or non-existence of solutions in* $\mathbb{Q}$ *(global solution) of a diophantine equation can be detected by studying the solutions of the equation in* $\mathbb{Q}_p$*,* $p$ *- prime or* $\infty$ *(local solutions).*

**Example.** Sometimes the Hasse Principle does not work:

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$$

is solvable locally everywhere, but is not solvable globally, i.e. it has no rational solution.

Although the Hasse principle is not valid for all polynomials, still there are important classes of equations, for which it holds. One of such classes are quadratic forms over $\mathbb{Q}$. For these polynomials we have even more: we are able not only to decide the existence of a rational solution, but we can also construct the rational solution from the local ones.

# 3 Rational quadratic forms

## 3.1 Basic notions

**Definition 4.** *Let* $k$ *be a field of characteristic different from* 2*. By* n-ary quadratic form over $k$ *we understand a homogeneous quadratic polynomial over* $k$ *with* $n$ *variables.*

Using a linear transformation of variables any quadratic form can be brought into a diagonal form:

$$f(\mathbf{x}) = a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2; \quad a_i \in k. \tag{1}$$

So from now on we suppose that the quadratic form is given as in (1).

**Definition 5.** *The form (1) is* regular*, if* $a_i \neq 0\ \forall i$*.*

*A regular quadratic form is said to be* isotropic*, if there are* $b_1, \ldots, b_n \in k$ *not all 0, such that* $a_1b_1^2 + \cdots + a_nb_n^2 = 0$*. The vector* $(b_1, \ldots, b_n)$ *is then called an* isotropic vector*.*

*The form (1)* represents $c \in k$*, if there are* $c_1, \ldots, c_n \in k$ *such that* $a_1c_1^2 + \cdots + a_nc_n^2 = c$*. The form over* $k$ *is* universal *if it represents every non-zero element of* $k$*.*

**Lemma 6.** *Let* $f(\mathbf{x}) = a_1x_1^2 + a_2x_2^2$ *be isotropic. Then it is universal.*

## 3.2 Hasse principle for ternary quadratic forms

Using a linear transformation of variables we can any ternary quadratic form bring into the shape

$$f(\mathbf{x}) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \quad \text{with } a_i \in \mathbb{Z} \text{ and } a_1a_2a_3 \text{ square-free.}$$

To use the Hasse principle for deciding solvability and solving the form over rational numbers, we first have to solve the problem for infinitely many local fields. But the Lemma 7 allows us to restrict the decision process to finitely many cases. Afterwards the Lemma 8 says us that solving the quadratic form in a local field is equivalent to solving the form modulo prime, resp. power of prime.

**Lemma 7.** *Let $p \neq 2, \infty$ and let*

$$f(\mathbf{x}) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \quad \text{with} \quad |a_1|_p = |a_2|_p = |a_3|_p.$$

*Then $f(\mathbf{x})$ is isotropic over $\mathbb{Q}_p$.*

So we have to test the solvability only in $\mathbb{R}, \mathbb{Q}_2$ and those $\mathbb{Q}_p$, where $p$ divides one of coefficients $a_1, a_2, a_3$.

**Lemma 8.** *Let*

$$f(\boldsymbol{x}) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$$

*with $a_1, a_2, a_3 \in \mathbb{Z}$ and $a_1a_2a_3$ square-free.*

*(i) Let $p$ be an odd prime, $p \mid a_3$. The form $f(\mathbf{x})$ is isotropic in $\mathbb{Q}_p$ if and only if there is an $r \in \mathbb{Z}$ such that $a_1r^2 + a_2 \equiv 0 \pmod{p}$.*

*(ii) Let $2 \mid a_3$. The form $f(\mathbf{x})$ is isotropic in $\mathbb{Q}_2$ if and only if there is an $s = 0$ or $1$ such that*

$$a_1 + a_2 + a_3s^2 \equiv 0 \pmod{8}.$$

*(iii) Let $2 \nmid a_1a_2a_3$. The form $f(\mathbf{x})$ is isotropic in $\mathbb{Q}_2$ if and only if after suitable permuting the suffices $1, 2, 3$ we have*

$$a_1 + a_2 \equiv 0 \pmod{4}.$$

**Theorem 9. (Legendre)** *Let*

$$f(\mathbf{x}) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$$

*with $a_1, a_2, a_3 \in \mathbb{Z}$ and $a_1a_2a_3$ square-free. Suppose that the following conditions are satisfied*

*(i) if $p$ is an odd prime dividing $a_1a_2a_3$, say $p \mid a_3$, then there is an integer $r_p$ such that*

$$a_1r_p^2 + a_2 \equiv 0 \qquad \pmod{p}.$$

*(ii) if $2 \mid a_1a_2a_3$, say $2 \mid a_3$ then*

$$a_1 + a_2 + a_3s^2 \equiv 0 \qquad \pmod{8}$$

*where $s = 0$ or $1$.*

*(iii) if $2 \nmid a_1a_2a_3$ then, on permuting $a_1, a_2, a_3$, if need be,*

$$a_1 + a_2 \equiv 0 \pmod{4}.$$

*Then there are $b_1, b_2, b_3 \in \mathbb{Z}$, not all 0, such that*

$$a_1b_1^2 + a_2b_2^2 + a_3b_3^2 = 0.$$

*A sketch of proof:* The idea of the proof is, that the modular quadratic equation can be reformulated into a linear condition for the isotropic vector.

(i) Let $p$ be an odd prime, $p \mid a_3$. The condition from the Theorem can be written as the linear condition for the solution, namely

$$z_1 \equiv r_p z_2 \pmod{p}.$$

Then $f(\mathbf{z}) \equiv 0 \pmod{p}$.

(ii) Let $2 \mid a_3$. Then the linear conditions

$$\begin{aligned} z_1 &\equiv z_2 \pmod{4} \\ z_3 &\equiv s z_2 \pmod{2} \end{aligned}$$

imply that $f(\mathbf{z}) \equiv 0 \pmod{8}$.

(iii) Let $2 \nmid a_1a_2a_3$. Then the linear conditions

$$\begin{aligned} z_1 &\equiv z_2 \pmod{2} \\ z_3 &\equiv 0 \pmod{2} \end{aligned}$$

imply that $f(\mathbf{z}) \equiv 0 \pmod{4}$.

So we have a collection of linear modular conditions for the isotropic vector and using Chinese remainder theorem we combine them into one linear modular equation, such that every its solution $\mathbf{z}$ is also a solution to the modular quadratic equation

$$f(\mathbf{z}) \equiv 0 \pmod{4a_1a_2a_3}.$$

The solutions to the linear equation form a lattice in $\mathbb{Z}^3$. By the results from geometry of numbers we know, that among the points in the lattice there exists also a point, which is a solution to the quadratic form over rational numbers, for example the shortest vector in the lattice. Therefore we finally use LLL-reduction to find the solution. $\square$

**Remark.** There are two expensive actions in the algorithm: first one is the factorization of the coefficients, and the second one is the final LLL-reduction. After implementing the algorithm we learned, that there is already an algorithm avoiding the LLL-reduction implemented in Magma, see [3]. Therefore at the end we replaced our LLL-based algorithm by the more efficient one.

## 3.3 Hasse principle for quaternary quadratic forms

While solving ternary quadratic forms we could avoid the work with $p$-adic numbers. First, finding a $p$-adic solution was equivalent to finding a solution modulo $p$ for odd prime $p$, or modulo 4 or 8 for $p = 2$. And afterwards instead of combining particular $p$-adic solutions into one rational solution of the quadratic form, it was enough to combine modular solutions of linear equations via Chinese remainder theorem.

However, for solving quaternary forms, it is not possible anymore to escape from the local fields. For this, let's first have a closer look at the solvability of ternary quadratic forms over local fields.

For the multiplicative group $\mathbb{Q}_p^*$ of every local field, the subset $(\mathbb{Q}_p^*)^2$ is its subgroup. Therefore we can form a factor group $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. One can prove that $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ is always of finite order. For example, for $\mathbb{Q}_\infty^* = \mathbb{R}^*$ we have $(\mathbb{R}^*)^2 = \mathbb{R}^+$, the group of all positive real numbers. So $|\mathbb{R}^*/(\mathbb{R}^*)^2| = 2$. If $p$ is an odd prime, then $|\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2| = 4$ and for $p = 2$, we have $|\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2| = 8$.

**Definition 10.** Hilbert norm residue symbol *is defined for* $a, b \in \mathbb{Q}_p^*$ *as follows:* $(.,.) : \ \mathbb{Q}_p^* \times \mathbb{Q}_p^* \to \{1, -1\}$,

$$(a, b) = \binom{a, b}{p} = \begin{cases} 1 & \textit{if } ax^2 + by^2 - z^2 \textit{ is isotropic} \\ -1 & \textit{otherwise.} \end{cases}$$

The Hilbert norm residue symbol $(a, b)$ depends only on $a, b$ modulo squares: $(a, b) = (ac^2, bd^2)$ for any $c, d \in \mathbb{Q}_p^*$, since any $(x_0, y_0, z_0)$ is a solution to $ax^2 + by^2 - z^2$ if and only if $(x_0/c, y_0/d, z_0)$ is a solution to $(ac^2)x^2 + (bd^2)y^2 - z^2$. Therefore $(.,.)$ is well defined on quadratic residuum classes. It follows that when deciding solvability of a ternary quadratic form over a local field, we can reduce to finitely many cases. We just have to find the residuum classes of the coefficients of the quadratic form and then look up the value of the Norm residue symbol in the table.

**Theorem 11. (Product formula)** *Let* $a, b, \in \mathbb{Q}^*$. *Then* $\binom{a,b}{p} = 1$ *for almost all* $p$ *and*

$$\prod_{p \leq \infty} \binom{a, b}{p} = 1.$$

**Remark.** The form $f(\mathbf{x}) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ is isotropic over $\mathbb{Q}_p$ if

$$\binom{-a_1a_3, -a_2a_3}{p} = 1.$$

By the Product formula

$$\prod_{p \leq \infty} \binom{-a_1a_3, -a_2a_3}{p} = 1.$$

So while testing solvability over local fields, we can omit one of them. This also explains, why in the Legendre Theorem the solvability of the form over $\mathbb{R}$ need not to be tested.

For solving a quaternary quadratic form

$$f(\mathbf{x}) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \quad \text{with} \quad a_j \in \mathbb{Z},\ j = 1, \ldots, 4,$$

we will split it into two ternary forms as follows:

$$\begin{array}{c} a_1x_1^2 + a_2x_2^2 - ty_1^2 \\ a_3x_3^2 + a_4x_4^2 + ty_2^2 \end{array}$$

for suitable $t \in \mathbb{Z}^*$. If the two ternary forms are isotropic, then apparently also the quaternary form is isotropic and we can construct its isotropic vector from the ones of two ternary forms and vice versa: isotropy of the quaternary forms enables us to construct the two ternary isotropic forms. By Lemma 6 we can in this case always construct regular ternary forms, i.e. with $t \neq 0$. So in our algorithm we will reduce the problem of solving a quaternary form to the problem of constructing the $t \in \mathbb{Z}$. We will do it in two steps: first we construct such $t_p$ in every relevant local field $\mathbb{Q}_p$ and afterwards we combine the "local" $t_p$'s into a "global" $t \in \mathbb{Q}$. The following Lemmas explain how to find a $t_p$ in a local field.

**Lemma 12.** *Let $g(\mathbf{x}) = a_1x_1^2 + a_2x_2^2$ be a regular form over $Q_p$. Then $b \neq 0$ is represented by $g$ if and only if*

$$(b, -a_1a_2) = (a_1, a_2).$$

**Lemma 13.** *The quaternary form $f(\mathbf{x}) = a_1x_1^2+a_2x_2^2+a_3x_4^2+a_4x_4^2$ is anisotropic if and only if*

$$\begin{aligned} -a_1a_2(\mathbb{Q}_p^*)^2 &= -a_3a_4(\mathbb{Q}_p^*)^2 \quad \text{and} \\ (a_1, a_2) &= -(-a_3, -a_4). \end{aligned}$$

The Corollary of the following Theorem plays the same role in solving quaternary forms, as the Chinese remainder theorem in solving ternary forms: It combines local "solutions" ($t_p \in \mathbb{Q}_p$) into a global "solution" ($t \in \mathbb{Q}$).

**Theorem 14. (Dirichlet)** *Let $l > 0$ and $m$ be coprime pair of integers. There are infinitely many primes $p \equiv m \pmod{l}$.*

**Corollary 15.** *Let $P$ be finite set of primes $p$ (possibly also $\infty$). For each $p \in P$ let $t_p \in \mathbb{Q}_p^*$ be given. Then there is a $t \in \mathbb{Q}^*$ such that*

*(i)* $t \in t_p(\mathbb{Q}_p^*)^2$ *for all* $p \in P$,

*(ii)* $|t|_p = 1$ *for all* $p \notin P, p \neq \infty$ *except possibly for one* $p = p_0$.

*Proof:* $p \in P, p \neq \infty: \; t_p = p^{\alpha(p)} s_p, \; |s_p|_p = 1$. We look for $t$ in the form:

$$t = \pm p_0 \prod_{p \in P \setminus \{\infty\}} p^{\alpha(p)}, \quad p_0 \notin P \text{ prime.}$$

The sign is chosen according to $p_\infty$ (if $\infty \in P$).
According to the Dirichlet theorem we can choose prime $p_0 > 0$ such that $\forall p \in P, p \neq \infty$

$$p^{-\alpha(p)} t \equiv s_p \begin{cases} \mod p & p \neq 2 \\ \mod 8 & p = 2 \end{cases}$$

Then the $t$ satisfies the desired properties. $\Box$

Now we have constructed $t \in \mathbb{Q}$, such that the forms

$$a_1 x_1^2 + a_2 x_2^2 - t y_1^2, \qquad a_3 x_3^2 + a_4 x_4^2 + t y_2^2 \tag{2}$$

are isotropic over $\mathbb{Q}_p$, if the forms

$$a_1 x_1^2 + a_2 x_2^2 - t_p y_1^2, \qquad a_3 x_3^2 + a_4 x_4^2 + t_p y_2^2$$

were isotropic over $\mathbb{Q}_p$. This holds for $p = 2, \infty$ and every prime dividing one of coefficients of the quaternary form (follows from the part (i) of the Corollary) as well as any prime not involved in the coefficients (follows from the part (ii)), up to possibly one prime $p_0$. Therefore the two ternary forms (2) are isotropic over every $\mathbb{Q}_p, p \neq p_0$. From the product formula (Theorem 11) we have, that they are isotropic over $\mathbb{Q}_{p_0}$ too, and hence by the Hasse principle isotropic over $\mathbb{Q}$.

### 3.4 Quadratic forms with 5 and more variables

**Lemma 16.** *Let $n \geq 5$, $p < \infty$. A form in $n$ variables over $\mathbb{Q}_p$ is isotropic.*

Since the Hasse principle holds for all quadratic forms (see [2]), for forms with at least 5 variables we have a very easy criterion for solvability: A form is isotropic over $\mathbb{Q}$ if and only if it is isotropic over $\mathbb{R}$.

## 4 The Algorithms

### 4.1 Isotropic vector of ternary quadratic form [1]

FUNCTION **SolubilityCertificate**
INPUT: Integers $b_1, b_2, b_3$, where all $b$'s are square-free and pairwise coprime, and $b_3$ is odd.
OUTPUT: Integer $r$ such that $r^2 = -b_1/b_2 (\mathrm{mod}\ b_3)$ if exists.

[1]The algorithm for ternary forms is obsolete. Instead, the algorithm described in [3] is used.

1. for each prime $p$ dividing $b_3$
   if $-b_1/b_2 (\mathrm{mod}\ p)$ is a perfect square over $Z_p$
   then $r_p := \sqrt{-b_1/b_2} \quad (\text{in } Z_p)$
   else print "not solvable"; exit
   end if
   end for;

2. By Chinese reminder theorem combine $r_p$'s
   (i.e. the solutions of the system $r_p = \sqrt{-b_1/b_2} \quad (\text{in } Z_p)$)
   to $r$ (i.e. the solution of $r = \sqrt{-b_1/b_2} \quad (\text{in } Z_{b_3})$).

3. *return* $r$.

FUNCTION **IsIsotropic3**
INPUT: Coefficients $c_1, c_2, c_3$ of a diagonal form $c_1x_1^2 + c_2x_2^2 + c_3x_3^2$.
OUTPUT: `true` if and only if the form is isotropic, and if so, returns an isotropic vector.

1. Solve trivial case, when one of the coefficients is zero.

2. Simple test of solvability: coefficients should be not all of the same sign ( $\sim$ solvability over $R$).

3. Transform the form $c_1x_1^2 + c_2x_2^2 + c_3x_3^2$ to the form $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ so that $a_1a_2a_3$ is square-free and create the matrix $T$ transforming solutions of $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ to the solutions of $c_1x_1^2 + c_2x_2^2 + c_3x_3^2$.

4. Compute the solubility certificate (exclude prime 2):
   $r_3 :=$ *SolubilityCerificate*$(a_1, a_2, \tilde{a}_3)$;
   $r_1 :=$ *SolubilityCerificate*$(a_2, a_3, \tilde{a}_1)$;
   $r_2 :=$ *SolubilityCerificate*$(a_3, a_1, \tilde{a}_2)$;
   where $\tilde{a}_i$ equals $a_i$ if $a_i$ is odd, and $a_i/2$ otherwise.

5. By Chinese reminder theorem combine the three modular equations

$$\begin{array}{rrrl} r_3x_1 - & x_2 & & = 0 \quad (\mathrm{mod}\ \tilde{a}_3) \\ & r_1x_2 - & x_3 & = 0 \quad (\mathrm{mod}\ \tilde{a}_1) \\ -x_1 & & +r_2x_3 & = 0 \quad (\mathrm{mod}\ \tilde{a}_3) \end{array}$$

   into one equation

$$k_1x_1 + k_2x_2 + k_3x_3 = 0 \quad (\mathrm{mod}\ \tilde{a}_1\tilde{a}_2\tilde{a}_3).$$

6. Add two extra modular equations for prime 2 (mod 2,4).

7. Compute the solution lattice of the three equations (modulo $4a_1a_2a_3$).

8. Find the shortest vector in the lattice.

9. Using the matrix $T$ transform the solution of $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ to the solution of $c_1x_1^2 + c_2x_2^2 + c_3x_3^2$.

## 4.2 Isotropic vector of quaternary quadratic form

FUNCTION: **IsIsotropic4**
INPUT: Coefficients $a_1, a_2, a_3, a_4$ of a diagonal form $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$.
OUTPUT: `true` if and only if the form is isotropic, and if so, returns an isotropic vector.

The algorithm constructs such $t$ that there are $b_1, b_2, b_3, b_4$:

$$\begin{aligned} t &= a_1b_1^2 + a_2b_2^2, \\ t &= -a_3b_3^2 - a_4b_4^2. \end{aligned}$$

Afterwards, two ternary forms

$$\begin{aligned} a_1x_1^2 + a_2x_2^2 - tu^2 = 0 \\ a_3x_3^2 + a_4x_4^2 + tv^2 = 0 \end{aligned}$$

are solved.

1. Solve trivial case, when one of the coefficients is zero.

2. Create the set $P$ of all relevant primes; $P = \{p;\ p|2a_1a_2a_3a_4\} \cup \{\infty\}$.

3. For each prime $p$ in the set $P$ find $t_p$ (resp. its residue class in $Q_p^*|(Q_p^*)^2$) such that

$$\begin{aligned} t_p &= a_1b_{1p}^2 + a_2b_{2p}^2 \qquad \text{for some } b_{1p}, b_{2p} \in Q_p \\ t_p &= -a_3b_{3p}^2 - a_4b_{4p}^2 \qquad \text{for some } b_{3p}, b_{4p} \in Q_p. \end{aligned}$$

   Such $t_p$ exists iff (Lemma 13)

$$(a_1, a_2) = (-a_3, -a_4) \qquad \text{or} \qquad -a_1a_2(Q_p^*)^2 \neq -a_3a_4(Q_p^*)^2.$$

   Otherwise print "No solution" and stop. (Both, decision of existence and finding the residue class for $t_p$ is made by looking up in the table.)

4. Construct

$$q = \pm \prod_{p \in P \setminus \{\infty\}} p^{\beta(p)} \text{ with } \beta(p) = \begin{cases} 1 & \text{if in } |t_p|_p = p^{-\alpha(p)} \text{ is } \alpha(p) \text{ odd,} \\ 0 & \text{otherwise.} \end{cases}$$

   The sign is chosen according to $t_\infty$.
   (Note: This and the previous step are done simultaneously.)

5. Generate all primes $p_0$ starting from 2. For each $p_0$ test if for $t = p_0q$ are forms

$$\begin{aligned} a_1x_1^2 + a_2x_2^2 - tu^2 = 0 \\ a_3x_3^2 + a_4x_4^2 + tv^2 = 0 \end{aligned}$$

   isotropic, i.e. if for each prime $p \in P - \{\infty\}$

$$\begin{aligned} (t, -a_1a_2) &= (a_1, a_2) \\ (t, -a_3a_4) &= (-a_3, -a_4). \end{aligned}$$

6. Solve ternary forms

$$\begin{aligned} a_1x_1^2 + a_2x_2^2 - tu^2 &= 0 \\ a_3x_3^2 + a_4x_4^2 + tv^2 &= 0. \end{aligned}$$

7. Construct the solution of $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$ from the solutions of two ternary forms.

## 4.3 Isotropic vector of quadratic form with 5 variables

FUNCTION **IsIsotropic5**
INPUT: Coefficients $a_1, a_2, a_3, a_4, a_5$ of a diagonal form $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2$.
OUTPUT: `true` if and only if the form is isotropic, and if so, returns an isotropic vector.

Algorithm looks for $t$ such that

$$\begin{aligned} f_1(\mathbf{x}) &= a_1x_1^2 + a_2x_2^2 - tu^2 \quad \text{is isotropic and} \\ f_2(\mathbf{x}) &= a_3x_3^2 + a_4x_4^2 + a_5x_5^2 + tv^2 \quad \text{is isotropic.} \end{aligned}$$

1. Solve trivial case, when one of the coefficients is zero.
2. Test solvability: coefficients should be not all of the same sign ( $\sim$ solvability over $R$).
3. Systematically generate non-trivial pairs $(b_1, b_2)$ of integers. For each pair
   (a) Compute $t = a_1b_1^2 + a_2b_2^2$.
   (b) If $t = 0$ then $(b_1, b_2, 0, 0, 0)$ is isotropic vector.
   (c) Case $t \neq 0$: solve quaternary quadratic form $a_3x_3^2 + a_4x_4^2 + a_5x_5^2 + tv^2$. If it is isotropic, then construct isotropic vector of the original form from $b_1, b_2$ and isotropic vector of the quaternary form.

## 4.4 Isotropic vector of quadratic form with 6 or more variables

FUNCTION **IsIsotropic**
INPUT: Vector $(a_1, a_2, \ldots, a_n)$ of the coefficients of a diagonal form $a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2$.
OUTPUT: `true` if and only if the form is isotropic, and if so, returns an isotropic vector.

Algorithm looks for $t$ such that

$$\begin{aligned} f_1(\mathbf{x}) &= a_1x_1^2 + a_2x_2^2 - tu^2 \quad \text{is isotropic and} \\ f_2(\mathbf{x}) &= a_3x_3^2 + \cdots + a_nx_n^2 + tv^2 \quad \text{is isotropic.} \end{aligned}$$

1. Solve trivial case, when one of the coefficients is zero.
2. Test solvability: coefficients should be not all of the same sign ( $\sim$ solvability over $R$). Notice also, whether the coefficients $a_3, \ldots, a_n$ have the same sign - it will be helpful when generating $t$.
3. Systematically generate non-trivial pairs $(b_1, b_2)$ of integers. For each pair
   (a) Compute $t = a_1 b_1^2 + a_2 b_2^2$.
   (b) If signs of $t, a_3, \ldots, a_n$ are not all the same, then construct an isotropic vector.
   (If $t = 0$ then $(b_1, b_2, 0, 0, \ldots, 0)$ is isotropic vector. Otherwise solve quadratic form $a_3 x_3^2 + \cdots + a_n x_n^2 + tv^2$ and construct isotropic vector afterwards.)

# 5 Implementation

We implemented the algorithms in Magma. To be able to use it, you need following files:

```
Diophant.spec
QuadForm2.m
QuadForm3.m
nrs.m
QuadForm4.m
QuadForm5.m
```

In Magma, load the package by:

```
> AttachSpec("Diophant.spec");
```

To compute an isotropic vector of the form with integer coefficients $a_1, a_2, a_2$ (i.e. of the form $a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2$) type

```
> IsIsotropic3(a1,a2,a3);
```

Functions for the forms with different number of variables work similarly:

```
> IsIsotropic2(a1,a2);
> IsIsotropic4(a1,a2,a3,a4);
> IsIsotropic5(a1,a2,a3,a4,a5);
```

All these functions accept as their argument also a symmetric matrix of particular dimension, for example:

```
> IsIsotropic3(M);
```

where M is a symmetric 3 by 3 matrix over integers.

For computing an isotropic vector of the quadratic form with more than 5 variables, there is a function

```
> IsIsotropic(M);
> IsIsotropic(a);
```

accepting a symmetric matrix M or a list a of coefficients $a_1, a_2, \ldots a_n$ (in this case the form is of the shape $a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2$).

There is also a test file for the package which can be loaded by

```
> Attach("Test.m");
```

It contains functions

```
> TestForm2(max);
> TestForm3(max);
> TestForm4(max);
> TestForm5(max);
```

taking as an argument a positive integer max, producing random coefficients $a_1, \ldots a_n \in \{-\mathtt{max}, \ldots \mathtt{max}\}$ and solving the form $a_1x_1^2 + \cdots + a_nx_n^2$ for $n = 2, 3, 4, 5$ (according to the function). These functions after generating and solving each form stop and wait for an input. The input can be <Enter> (after that a new form is processed) or q <Enter> (after that the functions exit).

For testing the algorithm for the forms of more than 5 variables, there is a similar function

```
> TestForm(n, max);
```

where n is the number of variables and max determines the range for the coefficients.

For testing the algorithm for the forms given by symmetric matrix there are functions

```
> TestFormM2(max);
  ...
> TestFormM5(max);
```

# References


[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978.

[3] J. E. Cremona and D. Rusin. Efficient solution of rational conics. *Math. Comp.*, 72(243):1417–1441 (electronic), 2003.

[4] Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, 1993. An introduction.