SOLVING QUADRATIC FORMS OVER THE RATIONALS

ABSTRACT. The scope of this essay is to examine the solubility of quadratic forms $Q(x_1, x_2, ...x_n)$ over $\mathbb{Q}$ and give explicit algorithms which construct such a solution if it exists. The essay consists mainly of two parts. In the first part we develop the theoretical background behind the quadratic forms with our goal to prove the Hasse-Minkowski theorem which states that a quadratic form is soluble over $\mathbb{Q}$ if and only if it is soluble over any p-adic field $\mathbb{Q}_p$ for any prime p and over $\mathbb{R}$. This turns out to be an essential tool as it provides a great link for passing from local to global as solubility locally is well understood. In the second part we concentrate on techniques mainly minimization methods and reduction algorithms which construct solutions in computationally reasonable time.We are dealing with the case of three and four variables and the main work is based on the papers **[Sim1]**,**[Sim2]** and **[Cr]**.

April 30, 2009

CONTENTS

1. Introduction 2
1.1. Quadratic Spaces over fields $\mathbb{K}$ and Isotropic Spaces 2
1.2. Isotropic Spaces 4
2. The p-adic fields $\mathbb{Q}_p$ 5
2.1. Introduction to p-adic fields 5
2.2. Hensel's lemma 6
2.3. Hilbert's Symbol 6
3. Quadratic Forms 8
3.1. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{R}$ 8
3.2. Dirichlet's theorem on primes in arithmetic progression 11
3.3. Hasse-Minkowski theorem 11
3.4. Quadratic Forms over $\mathbb{Q}$ 13
3.5. Classification of Quadratic Forms 13
4. A computational Approach 14
4.1. Introduction to the theory of algorithms 14
4.2. Legendre Reduction in case of conics 18
4.3. Lattice Methods 19
4.4. Minimization techniques for conics 22
4.5. Solving quadratics in four variables 26
References 32

1. Introduction

In the first section of the essay we examine quadratic forms $Q(x_1, x_2, ...x_n)$ over fields $\mathbb{K}$ of char$\mathbb{K} \neq 2$ and using basic theorems and results from Linear Algebra related to symmetric bilinear forms defined on finite dimensional vector spaces we can find out some interesting facts on that forms.
From now we denote as (V,Q) the pair , where V is a finite dimensional $\mathbb{K}$-vector space and $Q : V \to \mathbb{K}$ a function with the following properties:

[1] $Q(ax) = a^2Q(x)$ for all $a \in \mathbb{K}$, x $\in V$.
[2] The function $< x, y >:\to Q(x + y) - Q(x) - Q(y)$ is $\mathbb{K}$-bilinear.

Such a pair is called a quadratic vector space or a quadratic module if we take as V a module over a commutative ring A according to **[Ser,Ch IV,p.27]**.
Setting $Q(x, y) =< x, y >=(Q(x + y) - Q(x) - Q(y))/2$ we can see that the map (x,y) $\to$ Q(x,y) is a symmetric bilinear form on V,(the scalar product associated with Q).
Actually as we will see there is a bijective correspondece between this quadratic spaces (V,Q) and the quadratic forms.

1.1. **Quadratic Spaces over fields $\mathbb{K}$ and Isotropic Spaces.** .

Suppose $e_1, e_2, ..., e_n$ is a basis of V where n=dimV and n is finite.
Then consider
$f(x_1, x_2, ..., x_n) = Q(\sum_{1\leq k\leq n} x_ke_k) = Q(\sum_{1\leq i\leq n} x_ie_i, \sum_{1\leq j\leq n} x_je_j)$
$= \sum_{1\leq i\leq n} \sum_{1\leq j\leq n} x_ix_jQ(e_i, e_j)$ where each $x_i \in \mathbb{K}$.This is a quadratic form.
From that we see that there is a correspondence between quadratic forms and the quadratic spaces (V,Q),as every form arises in this way and every quadratic form gives rise to a quadratic space by defining the corresponding symmetric bilinear form by $Q(e_i, e_j)$.
From now on instead of the quadratic form we work with the corresponding quadratic space and denote the determinant of a quadratic form **d(Q):=det**Q_{ij} where Q_{ij} the matrix given by $Q(e_i, e_j)$.
In case d(Q)=0 the form is called non-singular otherwise singular and the latter is what we are interested in.Notice that since we are deal up with homogeneous polynomials we are particularly interested for solutions (x,y,z) in the projective space $\mathbb{P}^n(\mathbb{Q})$ each of which has a primitive representation with x,y,z $\in \mathbb{Z}$ and hcf(x,y,z)=1.

1.1.1. ***Definition.*** For the quadratic form $\sum_{1\leq i,j\leq n} f_{ij}x_ix_j$ where $f_{ij} = f_{ji}$ we call the matrix with entries f_{ij} the **representation matrix** of *f*.

1.1.2. ***Definition.*** (Equivalence of quadratic forms)Two forms f and g are said to be equivalent if there exists an invertible matrix R such that $F = R^TGR$ where F,G the representation matrices of f and g respectively.

Taking determinants on both sides in the definition above we see that d(f) is uniquely determined up to multiplication by $(\mathbb{K}^*)^2$ as we have $d(f) = det(R)^2 d(g)$,so the determinant is an invariant in $\mathbb{K}^*/(\mathbb{K}^*)^2$ which is one of the invariants which are needed for the classification of quadratic forms as we will prove in the next sections.

1.1.3. ***Definition.*** Let $f(x_1, x_2, ..., x_n)$ and $g(x_1, x_2, ..., x_m)$ be two quadratic forms with F,G be there representation matrix respectively.
Then we denote the orthogonal sum $f \oplus g$ as $f(x_1, x_2, ..., x_n) + g(x_{n+1}, x_{n+2}, ..., x_{n+m})$ and $F \oplus G$ be the matrix with the matrices F and G on the diagonal.

The above definitions are useful for passing from quadratic forms to quadratic spaces (V,Q). In addition two elements x,y of V are said to be orthogonal if $< x, y >= 0$.With an easy check we see that quadratic spaces admits always an orthogonal basis so it is reasonable to work with diagonal forms as we will do repeatedly for proving the main theorems.

1.1.4. ***Definition.*** Two orthogonal basis $(e_i)_{1 \le i \le n}$ and $(e'_i)_{1 \le i \le n}$ of a quadratic space (V,Q)are said to be **contiguous** if there exists a sequence of orthogonal basis $A_r : a_{r,1}$, $a_{r,2}....a_{r,n}$ for $1 \le r \le N$such that:
[1] $A_1 = (e_i)_{1 \le i \le n}$ and $A_N = (e'_i)_{1 \le i \le n}$
[2] $\forall r$ the basis A_r, A_{r+1} have at least n-2 elements in common.

Remark: It is true that any pair of orthogonal basis of a quadratic space (V,Q) are contiguous. For proving this it is just a simple matter of Linear Algebra so we avoid it and for more details one can see **[Ca,Ch II,p.16]**.

1.1.5. ***Witt's Theorem.*** Suppose (V_1, Q_1) and (V_2, Q_2) are two isomorphic and non-degenerate quadratic vector spaces.If U is a subspace of V then every injective metric morphism $\phi : U \to V_2$ can be extended to a metric isomorphism of V_1 onto V_2.

Proof: The proof is ommited for more details see **[Ser,Ch IV,p.30]**

1.1.6. ***Remark:*** The previous lemma is very useful as it gives as the cancellation theorem which states that if $f_1 = g_1 + h_1$ and $f_2 = g_2 + h_2$ are two non-degenerate quadratic forms where f_1 equivalent to f_2 and h_1 equivalent to h_2 then g_1 equivalent to g_2.
Using Witt's lemma we observe that two subspaces of a non-degenerate quadratic vector space which are isomorphic they have isomorphic orthogonal complements since the isomorphism of the two subspaces induces an automorphism on the whole space and then taking restrictions to the orhogonal complements we are done.Thus we can easily deduce that if f is nongenerate then f can be written as $h_1 + h_2 + ... + h_n + g$ where each h_i is hyperbolic and g doesn't represent zero.

1.2. **Isotropic Spaces.**

1.2.1. ***Definition.*** A quadratic space (V,Q) is said to be **isotropic** if it satisfies Q(x)=0 for a non trivial vector x,otherwise it said to be **anisotropic**.Also it is said that it represents zero.

Example: The simplest most useful example for our interest is the Hyperbolic Plane denoted as $\mathbb{H}$ as we will prove below.

1.2.2. ***Definition.*** Hyperbolic Plane ($\mathbb{H}$) is a 2-dimensional quadratic space with basis satisfying $Q(e_1) = Q(e_2) = 0$ and $Q(e_1, e_2) = 1$.

1.2.3. ***Lemma.*** All non-singular isotropic quadratic spaces contain a copy $\mathbb{H}$ and so decomposes as $U = \mathbb{H} \oplus \mathbb{H}^{\perp}$.

Proof:
Since the quadratic space is well defined pick a non-zero element x such that $Q(x) =$ and without loss of generality let y be a vector such that $Q(x, y) = 1$.
Then taking $x' = y - xQ(y)/2$ we see that the elements x, x' span a subspace of V isomorphic to $\mathbb{H}$.So we can decompose the space V by considering the complement of the hyperbolic plane with respect to the given scalar product.

1.2.4. ***Corollary.*** Any form in n variables that vanishes on a non zero vector is equivalent to $f_1 + h$ where h hyperbolic and f_1 a quadratic form in n-2 variables.

Remark: The above remark is very useful for our computations in the last section since we can decompore any isotropic quadratic space as the direct sum of copies of the hyperbolic plane and of a definite space of smaller dimension which makes the problem of finding a solution easier in the computational point of view.
Below we present an algorithm for finding an isotropic subspace of maximal dimension in a unimodular quadratic space. The assumption that the quadratic space is unimodular is reasonable as we will prove that there exists algorithm for reducing a quadratic form to a unimodular quadratic form .This is very useful for the study of quadratic forms in higher dimensions as it can be used as an inductive tool for reducing the dimension to dimension which are easier to study since we can decompose the spave V as $E \oplus R$ where E is totally isotropic of maximal dimension and R is a positive or negative definite quadratic space.
We use this algorithm widely as we will see in the last section of the essay for solving quadratics in four variables.

1.2.5. ***Algorithm:*** Let Q $\in M_n(\mathbb{Z})$ a unimodular symmetric matrix of signature (r,s).Then do the following steps

[1] If r=0 or s=0.Output : D=Q

[2]Solve $X_1^T Q X_1 = 0$ and extend to a basis $X_1, X_2, ..., X_n$

[3]Find a new basis such that $Q = H \oplus Q'$ where H the matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ *or* $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

($detQ' = -detQ$ and Q' has signature (r-1,s-1) and dimension n-2).

[4]Return $H \oplus R$ where R is the output of this algorithm applied on Q'.

Remark: This algorithm can be applied to indefinite unimodular quadratic form , to find a new basis in which Q decomposes as $\mathbb{H}^{min(r,s)} \oplus D$ where is D is positive or negative definite.

2. THE P-ADIC FIELDS $\mathbb{Q}_p$

2.1. **Introduction to p-adic fields.** The p-adics were first introduced by Kurt Hensel and the purpose were to construct number systems in such a way that they can use powerful theorems from analysis in number theory.The exact construction of these fields is described below.

By Ostrowski's theorem which states that any non-trivial absolute value on $\mathbb{Q}$ is equivalent either to the real absolute value or the p-adic absolute value defined as $|x|_p = p^{-n}$ by writing x as $p^n a/b$ with (a,b)=1 and neither a or b is divisible by p.(Note that we set 0 to have infinite valuation for this to be consistent).The completion with respect to this norm gives the construction of $\mathbb{Q}_p$.For more details related to this construction see [**Ca,Ch 3,p35**].

There is also a more useful notation for these fields which is refered in [**Ser,ChII,p.11**] by considering the surjective homomorphisms (projections)

$$\phi_n : \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathrm{Z/p}^{n-1}\mathbb{Z} \text{ with } ker(\phi_n) = p^{n-1}\mathbb{Z}$$

and then taking the projective limit of the projective system defined by the sequence

$$.... \rightarrow \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^{n-1}\mathbb{Z} \rightarrow ..... \rightarrow \mathbb{Z}/p\mathbb{Z}$$

This gives us the ring $\mathbb{Z}_p$ and then by localization we get the field $\mathbb{Q}_p$.

Below we state some elementary properties of the p-adic fields which are very useful and the proofs are ommited .

[**1**] The sequence $0 \rightarrow \mathbb{Z}_p \overset{p^n}{\rightarrow} \mathbb{Z}_p \overset{pr_n}{\rightarrow} \mathbb{Z}/p^n\mathbb{Z} \rightarrow 0$ is exact where pr_n the projection to $\mathbb{Z}/p^n\mathbb{Z}$.

[**2**] a $\in \mathbb{Z}_p$ is invertible $\Leftrightarrow pr_1(a) \neq 0$.

[**3**]$\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ has order 8 and generated by $< 2, -1, 5 >$.

[**4**]$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ $(p \neq 2)$ has order 4 and generated by $< p, r >$ where r is a quadratic non-residue.

2.2. **Hensel's lemma.** This is the p-adic analoque of Newton's method , starting with an approximate root we can refine it to a better.

2.2.1. ***Lemma.*** (Hensel's lemma)Suppose $f \in \mathbb{Z}_p[X]$ is a monic polynomial and suppose $\exists$ x $\in \mathbb{Z}/p^n\mathbb{Z}$ for $n \geq 1$ with $f(x) = 0, f'(x) mod p \neq 0$.
Then $\exists! y \in \mathbb{Z}_p$ such that $y mod p^n \equiv x$ and $f(y) = 0$.

Proof: Let x represent some $x' \in \mathbb{Z}_p$.
Then $f(x') \equiv 0 mod p^n$ and using Taylor's expansion of f we get
$f(x' + p^n z) = f(x') + p^n z f'(x') + p^{2n} z^2 A \equiv (f(x') + p^n z f'(x')) mod p^{n+1}$ for some A.
Then $f(x' + p^n z) \equiv 0 mod p^{n+1}$if and only if $z = -f(x')/p^n f'(x')$.
Therefore taking $y' = x + p^n z$ with z given as above we lift the solution to a solution in $\mathbb{Z}/p^{n+1}\mathbb{Z}$.
Succesively find $x_n = x, x_{n+1} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$,x_{n+2}... such that $x_{k+1} \equiv x_k mod p^k$ for all $k \geq n$ and $f(x_k) = 0$ in $\mathbb{Z}/p^k\mathbb{Z}$.
So simply take $y = (x_k)$ $\forall$ k and the lemma follows.

In othe words this lemma states that if there exists a solution in $\mathbb{Z}/p\mathbb{Z}$ then this solution can be lifted to a solution in $\mathbb{Z}_p$.As our machinery is builted up we will really understand how strong and helpful is this result since it enables us to check if a quadratic form is soluble over $\mathbb{Z}_p$ by just checking solubility in $\mathbb{Z}/p\mathbb{Z}$ which is very simple to check and then using Hasse-Minkowski as we will see later we can extract results for solubility over $\mathbb{Q}$.

2.3. **Hilbert's Symbol.** In this paragraph we let $\mathbb{K}$ to be $\mathbb{R}$ or $\mathbb{Q}_p$ with multiplicative group $\mathbb{K}^*$.

2.3.1. ***Definition.*** (Hilbert Symbol) Hilbert Symbol or Norm Residue Symbol is an algebraic construction , a function from $\mathbb{K}^*/(\mathbb{K}^*)^2 \times \mathbb{K}^*/(\mathbb{K}^*)^2$ into $< -1, +1 >$ defined as :
[1] $(a, b) = 1$ if $z^2 = ax^2 + by^2$ has a non-trivial solution in $(\mathbb{K}^*)^3$
[2] -1 otherwise.

The following lemma is crucial for understanding the properties of this symbol.

2.3.2. ***Lemma.*** Let $a, b \in \mathbb{K}^*$ and consider the field extension $L = \mathbb{K}(\sqrt{b})$.Then a necessary and sufficient condition for $(a, b) = 1$ is that $a \in N(L^*)$.

Proof: Firstly if $\sqrt{b} \in \mathbb{K}$ then $(x, y, z) = (0, 1, \sqrt{b})$ is a non trivial solution of $z^2 = ax^2 + by^2$.
So now suppose that $\sqrt{b} \notin \mathbb{K}$, if $w \in L$ then $w = a_1 + a_2\sqrt{b}$ with $a_1, a_2 \in \mathbb{K}$ and it is very easy to spot that any element of the norm subgroup is of the form $x^2 - by^2$ so $N(w) = {a_1}^2 - b{a_2}^2$.
Thus if $a \in N(L^*)$ then $\exists$y,z $\in \mathbb{K}$ such that $a = N(y + \sqrt{b}z) = y^2 - bz^2$ so $(a, b) = 1$.
Converesly if $(a, b) = 1$ then let (x, y, z) be a non trivial solution.Then $x \neq 0$ for the extension L to be non trivial and thus a is the norm of $z/x + \sqrt{b}y/x$.

2.3.3. ***Lemma.*** (Symbol's Properties)
[1]$(a,b) = (b,a)$ and $(a,c^2) = 1\ \forall a,b,c \in \mathbb{K}$.
[2]$(a,-a) = 1, (a, 1-a) = 1\ \forall a \in \mathbb{K}$.
[3]$(a_1a_2, b) = (a_1,b)(a_2,b)\ \forall a_1, a_2, b \in \mathbb{K}$.
[4]$(a, b_1b_2) = (a,b_1)(a,b_2)\ \forall b_1, b_2, a \in \mathbb{K}$.
[5]If $p \neq 2$or ∞ and$|a|_p = |b|_p = 1$ then $(a,b) = 1$.

Proof:
[1] If (x,y,z) a non-trivial solution for $ax^2 + by^2 = z^2$ then (y,x,z) a non-trivial solution for $bx^2 + ay^2 = z^2$.
For second part $ax^2 + c^2y^2 = z^2$ has the non-trivial solution (0,1,c).

[2] The conic $ax^2 - ay^2 = z^2$ has the solution (1,1,0) so (a,-a)=1
For second part $ax^2 + (1-a)y^2 = z^2$ has the solution (1,1,1) so (a,1-a)=1

[3]To prove this let b be fixed then we need to prove that a's such that (a,b)=1 form a multiplicative subgroup of $\mathbb{Q}_p$ which is either the whole $\mathbb{Q}_p$ or of index 2.
To show it is multiplicative let $a = z_1^2 - by_1^2$ and $a' = z_2^2 - by_2^2$
Then we have $aa' = (z_1z_2 + by_1y_2)^2 - b(z_1y_2 + z_2y_1)^2$
Thus it is a group under multiplication
To prove it is either $\mathbb{Q}_p$ or a subgroup of index 2 we have to use the structure of the groups $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ given in the previous section.
Leting a and b running through the generators we can easily prove that by simply considering all the possible cases.
For more details about these tables see **[Ca,Ch 3,p.43]**

[4]This follows immediately using the first part of [1] and [3] 0.1cm
[5]This is equivalent to proving that for $f_1x^2 + f_2y^2 + f_3z^2 = 0$ where all f_i have same valuation is always soluble.
Without loss of generality by multiplying the given equation with an appropriate power of p we can assume $|f_i|_p = 1$ for all f_i.
Reducing the equation modp we have to show $f_1x_1^2 + f_2x_2^2 = -f_3$modp and so using Hensel's Lemma we can lift it a solution in $\mathbb{Z}_p$ and so the result follows.
The solubility of that form is proved as follows.
Claim: For p≠ 2 , the form $f(x) = f_1x_1^2 + f_2x_2^2 + f_3x_3^2$ where $|f_i| = 1$ for all i is isotropic.

Proof: Firstly we are going to prove the existence of a solution over $\mathbb{F}_p$ and then using Hensel's Lemma we lift the solution over $\mathbb{Q}_p$.
Have $f_1x_1^2 + f_2x_2^2 + f_3x_3^2 \equiv 0 mod p \Leftrightarrow f_1y_1^2 \equiv -f_3 - f_2y_2^2 mod p$ for some $y_1, y_2 \in \mathbb{F}_p$
But the possible values of the left handside as y_1 runs through the elements of $\mathbb{F}_p$ is (p+1)/2 and same for the right hand side as y_2 runs through all elements of $\mathbb{F}_p$.
Thus there exists a solution (u_1, u_2, u_3) to the equation with $u_3 \equiv 1 mod p$

Using the claim now if we consider diagonal form $\sum_{1\le i\le n} f_ix_i^2$ we can use substitutions of the form $x_i - > r_ix_i$ with $c_i \in \mathbb{Q}_p^*$ so that at least three of $|f_i|$ (wlog say f_1,f_2,f_3) are 1 and hence we can find a solution for $f(x) = f_1x_1^2 + f_2x_2^2 + f_3x_3^2 = 0$ and set the other variables zero.

2.3.4. ***Lemma.*** (Product Formula)
Let a,b $\in \mathbb{Q}^*$ .Then (a,b)=1 for almost all p and $\prod_{\forall p,\infty}(a,b)_p = 1$

Proof:(sketch)
Using property [5] of the Hilbert's Symbol since we have $|a|_p = |b|_p = 1$ for almost all primes we see that $(a,b)_p = 1$.
This can be easily deduced as a number can be written as a product of finitely many primes.
Let h(a,b)=$\prod_{\forall p,\infty}(a,b)_p$, then by property [3] of Hilbert's Symbol we have $h(a_1a_2,b) = h(a_1,b)h(a_2,b)$.
Thus it is enough to prove $h(a,b) = 1$ for a,b running through generators $< -1, 2, p' >$ of $\mathbb{Q}^*$ where p' prime.
This is easily deduced from the quadratic reciprocity law .For more details for this part see [**Ca,Ch 4,p.23**].

3. Quadratic Forms

3.1. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{R}$.

In this section after understanding the machinery we have so far we are going to study the quadratic forms over $\mathbb{Q}_p$ in detail.For the theoretical point of view it is much easier to consider the diagonal forms $\sum f_i {x_i}^2$ where $f_i \in \mathbb{Q}_p^*$ letting also p to be ∞,but this is not very useful for a computational point of view as we will see in the last chapter.
We are going to introduce some invariants for the quadratic forms over these fields which will help us to classify them.So far we proved that the determinant is an invariant.

3.1.1. ***Definition.*** Hasse-Minkowski symbol is denoted as $c(f) = \prod_{i<j}(f_i, f_j)$.

3.1.2. ***Theorem.*** $c(f)$ is an invariant of (V,Q) where V a quadratic $\mathbb{Q}_p$-vector space.

Proof:
Pick two orthogonal basis of the quadratic space (V,Q) say $(e_i)_{1\leq n}$ and $(e'_i)_{\leq 1 i \leq n}$ and These basis gives rise to two diagonal forms of the form f say $\sum_{1\leq n} < e_i, e_i > x_i^2$ and $\sum_{1\leq n} < e'_i, e'_i > x_i^2$.
So our aim is to prove that:
$c_p(f) = \prod_{i<j}(< e_i, e_i >, < e_j, e_j >) = \prod_{i<j}(< e'_i, e'_i >, < e'_j, e'_j >)$
For the case of a two dimensional quadratic space:
$c_p(f) = 1 \Leftrightarrow (< e_1, e_1 >, < e_2, e_2 >) = 1$
which is clearly independent of choosing other orthonormal basis as this means that the equation $< e_1, e_1 > x_1^2 + < e_2, e_2 > x_2^2 = 1$ is solvable.
For higher dimensions we will use induction on the dimension and use the theory of contiguous basis developed in the introduction.Since Hilbert's Symbols is symmetric

permuting one element of the basis the symbol remains unchanged so it is enough to prove the claim for two contiguous basis say $(e_i)_{1\leq 1i\leq n}$ and $(e'_i)_{1\leq 1i\leq n}$ with $e_1 = e'_1$.
Thus we have $\prod_{i<j}(< e_i, e_i >, < e_j, e_j >)$
$= (< e_1, e_1 >, < e_2, e_2 > ... < e_n, e_n >) \prod_{2\leq i<j}(< e_i, e_i >, < e_j, e_j >)$
$= (< e_1, e_1 >, < e_1, e_1 > d(f)) \prod_{2\leq i<j}(< e_i, e_i >, < e_j, e_j >)$
$= (< e'_1, e'_1 >, < e'_1, e'_1 > d(f)) \prod_{2\leq i<j}(< e'_i, e'_i >, < e'_j, e'_j >)$
As we proved d(f) is invariant and using induction on the complement of $< e_1 >$ we may assume the product is the same.
Thus Hasse-Minkowski symbol is independent of the basis chosen so it is an invariant of (V,Q). Now we are going to prove how we can check solubility for a quadratic form over $\mathbb{Q}_p$.This will turn out to be easy as a finite set of instructions will be enough to check solubility over these fields.Then by Hasse-Minkowski theorem we know that we can check solubility of forms globally.

3.1.3. ***Theorem.*** For a quadratic form over $\mathbb{Q}_p$ of n variables to vanish on some isotropic vector a necessary and sufficient condition is:
[1] n=2 and d(f)=-1 as an element of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$
[2] n=3 and $(-1, -d(f))c(f) = 1$
[3] n=4 and either d(f)≠1 or d(f) =1 and c(f)=(-1,-1)
[4] n $\geq$ 5

Proof:
Case n=2:
Consider the diagonal form $f = f_1x_1^2 + f_2x_2^2$ where $f_i \in \mathbb{Q}_p^*$. As f has a non trivial solution $\Rightarrow \exists$ non zero vector $(a, b) \in \mathbb{Q}_p^* \times \mathbb{Q}_p^*$ on which f vanishes.
$\Rightarrow f_1a^2 + f_2b^2 = 0 \Rightarrow f_1f_2^{-1} = -(b/a)^2$
Then for f to be soluble we need the above condition and so $d(f) = f_1f_2 = -(f_1a/b)^2$
Thus d(f)=-1 (in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$).

Case n=3:
Let $f = f_1x_1^2 + f_2x_2^2 + f_3x_3^2$ where $f_i \in \mathbb{Q}_p^*$ and suppose (a,b,c) is a non-trivial vector on which f vanishes.
Clearly if f vanishes on some vector then $-f_3f$ vanishes on the same vector.
$\Rightarrow -f_3f_1x_1^2 - f_3f_2x_2^2 - x_3^2 = 0$
$\Leftrightarrow (-f_3f_1, -f_3f_2)_p = 1$
Then using the properties of Hilbert Symbol's as above we have
$(-1, -d(f))_pc_p(f) = (-1, -1)_p(-1, f_1f_2f_3)_p(f_1, f_2)_p(f_1, f_3)_p(f_2, f_3)_p$
$= (-1, -1)_p(-1, f_1)_p(-1, f_2)_p(f_3, f_2)_p(f_1, f_2)_p(f_1, f_3)_p(f_2, f_3)_p$
$= (-f_3f_1, -f_3f_2)_p$
$= 1$ as we have $(f_3, f_2) = (-1, f_3)$

Case n=4:
Consider again the diagonal form .
This form is isotropic if and only if there exists $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ such that $f_1x_1^2 + f_2x_2^2 = a$ and $f_3x_3^2 + f_4x_4^2 = -a$.
Have $f_1x_1^2 + f_2x_2^2 = a \Leftrightarrow (a, -f_1f_2) = (f_3, f_4)$

and $f_3x_1^2+f_4x_4^2=-a \Leftrightarrow (a,-f_3f_4)=(-f_3,-f_4)$
Consider the sets A and B for which the elements of these are the elements satisfying condition 1 and 2 respectively.Then for a solution not to exist we need the intersection of this sets to be empty.Clearly the sets are non-empty as f_1 and $-f_3$ are in A and B respectively.
So have $A\cap B$ non empty$\Leftrightarrow$ $f_1f_2=f_3f_4$ and $(f_1,f_2)=-(-f_3,-f_4)$.
So for f to be insoluble we need to have empty intersection (i.e the following conditions).
$f_1f_2=f_3f_4 \Rightarrow d(f)=1$.
$(f_1,f_2)=-(-f_3,-f_4) \Rightarrow c_p(f)=(-1,-1)$ which can be simply obtained by expaning out and using Hilbert's Symbol properties.

Case $n\geq 5$:
Using the property [5] of Hilbert's Symbol we see that this is enough if p is not 2.

For proving also the statement for p=2 we just consider again the diagonal form of five variables say $\sum_{1\leq i\leq 5} f_ix_i^2$.
It is enough to prove the existence of an element r $\in \mathbb{Q}_p^*$ such that $f_1u_1^2+f_2u_2^2+f_3u_3^2=r$ and $f_4u_4^2+f_5u_5^2=-r$ for some u_i.Assuming that $p\neq\infty$ we can easily deduce that the form in three variables represents all except possibly one class of $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ and the quadratic at least the half classes so there must exist an element with the appropriate property.

3.1.4. ***Lemma.*** In case of conics $ax^2+by^2+cz^2$ over $\mathbb{Q}$ we have to check solubility over $\mathbb{Q}_p$ for only finitely many primes.

Proof: Firstly suppose that all a,b,c are coprime(this can be done as the equation is homogeneous), and then consider the equation over $\mathbb{F}_p$ where p a prime which doesn't divide any of the three.Reducing the equation modp have $ax^2+by^2+cz^2\equiv 0 mod p$. Then by rearanging and noting that inverses of all a,b,c exist this is equivalent to solve $a_1x^2+a_2y^2\equiv a_3 mod p$ which is always solvable as rewriting this as $a_1x^2\equiv a_3-a_2y^2 mod p$ this is solvable as LHS takes (p+1)/2 values while x runs through $\mathbb{F}_p$ and so does the RHS.Then by applying Hensel's Lemma lift the solution to $\mathbb{Z}_p$.
Now let p dividing abc.Wlog say p divides a, then reducing modp we have $by^2+cz^2\equiv 0 mod p \Leftrightarrow (yz^{-1})^2\equiv -cb^{-1} mod p \Leftrightarrow -cb$ is a square modp. Thus by considering all the possible primes dividing abc we can determine if it is solvable modp. Then by applying Hensel's Lemma we know that this solution lifts to $\mathbb{Z}_p$.

example: Find for which primes p the form $5x^2-y^2-3z^2$ is isotropic over $\mathbb{Q}_p$: First note that abc=15 so for all primes not 3 or 5 previous lemma quarantees solubility.In case of p=3, reducing the equation mod3 have $2x^2-y^2\equiv 0 mod 3 \Leftrightarrow 2$ is a square mod3 which is not.For the case p=5 reducing mod5 we have $y^2-3z^2\equiv 0 mod 5 \Leftrightarrow 3$ is a square mod5 which is not.So this is isotropic for all primes except 3 and 5.

Quadratic Forms over $\mathbb{R}$

Consider now a real quadratic form , then considering its representation matrix over $\mathbb{R}$ and using Silvester's Law of Inertia we have that f is equivalent to a form

$$\sum_{i\leq r} x_i^2\text{-}\sum_{r+1\leq i\leq n} x_i^2$$

where $r \geq 0$ and the pair (r,n-r) is the signature of f.
Then if r=0 or n=r the form can't vanish anywhere else except of the origin.In case r,s and are non-zero then simply $(x_1, x_2, ..., x_r, y_1, ...y_s)$ where any min(r,s) of $x_i's$ and of $y'is$ are 1 and the rest zero is a non-zero vector on which the quadratic form vanishes. Thus checking solubility over $\mathbb{R}$ is straightforward considering the diagonal form of the form over the reals.
In the next section our aim is to prove Hasse-Minowski theorem.For proving this we need the theorem of Dirichlet's on primes in arithmetic progression so a sketch of the proof of the statement is presented below.

3.2. **Dirichlet's theorem on primes in arithmetic progression.**

3.2.1. ***Theorem.*** (Dirichlet's theorem on primes in arithmetic progressions)
Let m≥1 and a such that $hcf(a, m) = 1$.Then there are infinitely many primes of the form $a + nm$ for n integer.

Comment on the proof: For more details one can see [**Ser,Ch 6,p.61**]which actualy uses theory from L-series and Dirichlet characters to prove it.Below we give a rough idea how this arises.
Discussion on proof: Let P be the set of primes and P_k be a subset.Then one can show that $\sum_{p\in P}(1/p^s)/log(1/(s-1)) \to 1$ as s→ 1 and then we define the density of P_k as the limit of $\sum_{p\in P_k}(1/p^s)/log(1/(s-1))$ as $s \to 1$.
Then if we denote as P_a the set of primes given by the theorem we can prove that this set has density $1/\phi(m)$ and so this set is actually infinite.
For a rough idea about how to prove the last , we consider the Dirichlet character χ on $(\mathbb{Z}/m\mathbb{Z})^*$ and by considering $f_\chi(s) = \sum_{pnot/m} \chi(p)/p^s$ which is convergent for $s > 1$.
For $\chi = 1$ then this tends to log(1/(s-1)) as s → 1.So for the other case to show is still bounded consider for $Re(s) > 1$ $logL(s, \chi) = \sum log(1/(1-\chi(p)p^{-s})) = \sum_{n,p} \chi(p)^n/np^{ns} = f_\chi(s) + \sum_{p,n\geq 2} \chi(p)^n/np^{ns}$ and as the first and third sums can be proved that are bounded then the claim follows.
Then using that $\sum_\chi \chi(a^{-1}p) = \phi(m)$ if $a^{-1}p \equiv 1 mod m$ and 0 otherwise we can easily see that $\sum_\chi \chi(a)^{-1} f_\chi(s)/\phi(m) = \sum_{p\in P_a} 1/p^s$ and the theorem follows.

3.3. **Hasse-Minkowski theorem.**

3.3.1. ***Theorem.*** (Hasse-Minkowski)
A quadratic form is isotropic over $\mathbb{Q}$ (or globally) if and only if it is isotropic over $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime p (or locally).

This is the classical local-global principle.

Proof: The necessity is trivial as $\mathbb{Q}$ injects into $\mathbb{Q}_p$ and R so we just need to prove that this is sufficent.
Use as usual the equivalent diagonal form $\sum_{1\leq i\leq n} f_i {x_i}^2$.
We split the prove in four parts for n=2,n=3,n=4, and n $\geq$ 5 and suppose that this form is always solvable over the reals and over every p-adic field.

Case n=2:
Let $f = f_1{x_1}^2 + f_2{x_2}^2$ where $f_i \in \mathbb{Q}^*$.
For that form to be solvable over $\mathbb{R}$ we need that $f_1 f_2 < 0$ so we may consider the form $f = {x_1}^2 - a{x_2}^2$ where $a > 0$ to check solubility.Then for any prime p and by denoting $u_p(a)$ the usual p-adic valuation we can write a in the form $\prod_p p^{u_p(a)}$, and for a fixed p' prime $u_p(a) = 0$ for all $p \neq p'$ and $u'_p(a)$ has to be even as solubility over $\mathbb{Q}_{p'}$ implies a is a square in $\mathbb{Q}_{p'}$. Thus a is a square over $\mathbb{Q}$.

Case n=3:
Let $f = f_1{x_1}^2 + f_2{x_2}^2 + f_3{x_3}^2$ where $f_i \in \mathbb{Q}^*$.
Again solubility over $\mathbb{R}$ implies that not all the signs of the coefficients are the same and so it is enough to consider the form $f = {x_1}^2 - a{x_2}^2 - b{x_3}^2$ where a,b$\in \mathbb{Z}$ and square free.
We assume that $|b| \geq |a|$ and then use induction on $k = |a| + |b|$.
If k=2 then a,b have to be 1 or -1 and using inequality for coefficients we see that it is solvable over $\mathbb{Q}$.
Factorise b=$p_1 p_2 .. p_r$, and let p be such a prime. Since the equation is solvable over $\mathbb{Q}_p$ we pick a primitive solution say (r_1, r_2, r_3) then reducing modp:
$\Rightarrow$r$_1^2 - a{r_2}^2 \equiv 0 modp$
From this we deduce that $r_2 \neq 0 modp$ since if it was true then $r_1 \equiv modp$ and then $b{r_3}^2$ is divisible by p^2 which implies $r_3 \equiv 0 modp$ contradicting primitivity and so $x^2 \equiv amodp$ is solvable for any such prime p. Then by Chinese Remainder theorem it follows that $x^2 \equiv amodb$ is solvable.
$\Rightarrow$t$^2 = a + bl$ for some t,l $\in \mathbb{Z}$ with $|t| \leq |b|/2$ so that $|l| \leq |b|$.Now using Lemma 2.3.2 we see that initial form vanishes if and only if the form $f = {x_1}^2 - a{x_2}^2 - l{x_3}^2$.But by removing any square factor of l we get an equivalent form with k reduced and so by induction we are done.

Case n=4:
For this we will need the following corollary arising from Dirichlet's theorem .
Claim: Suppose A is a finite set of primes which may includes ∞.Then for $p \in A$ associate an element $a_p \in {\mathbb{Q}_p}^*$.Then $\exists\ a \in \mathbb{Q}^*$ with the property that $a \in a_p \mathbb{Q}_p^{*2}\ \forall p \in A$ and $|a|_p = 1$ for all p $\notin$ A and not ∞ ,except possibly for one p=p_0.

Proof of claim:
For $p \in A$, not ∞ write $a_p = p^{u_p(a_p)} u$ where u is a unit in $\mathbb{Q}_p$.Then pick a such that $|a| = p_0 \prod_{p \in A, p \neq \infty} p^{u_p(a_p)}$ where $p_0 \notin A$.Now pick this prime p_0 such that $p^{-u_p(a_p)} a \equiv umod8$ for p=2 and $\equiv umodp$ for the other cases.This can be done by applying Dirichlet's theorem.

Assuming now the claim let A be the set of primes dividing $2f_1f_2f_3f_4$ and allowing ∞. Then we can find $k_1, k_2, k_3, k_4, a_p \in \mathbb{Q}_p$ not all zero such that:
$f_1k_1^2 + f_2k_2^2 = a_p$
and $f_3k_3^2 + f_4k_4^2 = -a_p$. Then by the claim these become $f_1x_1^2 + f_2x_2^2 - am_1^2 = 0$ and $f_3k_3^2 + f_4k_4^2 + am_2^2 = 0$
and as all the valuations are 1 we proved that they are soluble and so we are done proving solubility over $\mathbb{Q}$.
(note that for primes not in this set we proved solubility is immediate)

Case n $\geq$ 5:
As in previous case pick $a_p \in \mathbb{Q}_p^*$ such that $f_1x_1^2 + f_2x_2^2 - a_pm_1^2$ and $f_3x_3^2 + f_4x_4^2 + ... + f_nx_n^2 + a_pm_2^2$ are isotropic over $\mathbb{Q}_p$.
Let $a_p = f_1k_1^2 + f_2k_2^2$ with $k_1, k_2 \in \mathbb{Q}_p$ then we can easily prove that we can find $b_1, b_2 \in \mathbb{Q}$ such that $a = f_1b_1^2 + f_2b_2^2$ satisfying $a \in a_p\mathbb{Q}_p^{*2}$ so $f_3x_3^2 + f_4x_4^2 + ... + f_nx_n^2 + au^2$ is isotropic for $p \in P$ and for other primes not in this set again the valuations are all one hence have again solubility.So we are done by induction on the number of variables as n$\geq$ 5.

3.4. **Quadratic Forms over $\mathbb{Q}$.**

So far we studied the quadratic forms over p-adic fields and over $\mathbb{R}$ and using Hasse-Minkowski theorem we are able now to pass to global fields.In this section we consider diagonal quadratic forms over $\mathbb{Q}$ of n variables and we denote its invariants as d(f) ,its signature (r,s) and for any prime p we consider $c_p(f)$ since the injection of $\mathbb{Q} \to \mathbb{Q}_p$ allows to look of the image of rational in the p-adic fields.
By Hasse-Minkowski we simply observe that any two quadratic forms are equivalent over $\mathbb{Q}$ if and only if they are equivalent over $\mathbb{Q}_p$ for any prime p and over $\mathbb{R}$.
We note also that a quadratic form over $\mathbb{Q}$ with $n \geq 5$ vanishes on an isotropic vector if and only if it vanishes over $\mathbb{R}$ since as we saw in section 3 solvability in these case over $\mathbb{Q}_p$ is immediate.

3.5. **Classification of Quadratic Forms.**

So far we proved the Hasse-Minkowski Theorem which is a great link between quadratic forms over $\mathbb{Q}$ and over $\mathbb{Q}_p$.In this section we are going to classify the quadratic forms over the p-adic fields and then classify them over the rationals using this powerful theorem.

3.5.1. ***Theorem.*** Two quadratic forms f,f' over $\mathbb{Q}_p$ are equivalent iff and only the following properties are satisfied:
[i] n(f)=n(f')
[ii] d(f)=d(f')
[iii] $c_p(f) = c_p(f')$ $\forall$ p prime

Proof: This is consequence of the theorem 3.1.3 and can be proved easily using induction on the dimension of the quadratic space.
Using theorem 3.1.3 we see that two forms f and f' represent the same elements of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.
Pick an element a $\in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ we see that f and f' are equivalent to $ar^2 + f_1$ and $ar^2 + f_1'$ where f_1, f_1' are of dimension n-1 and so we are done by induction.
For the case that two quadratic forms if they are equivalent they fullfil these conditions it is trivial and was proved before.

Corollary 1: For two quadratic forms f,f' over $\mathbb{Q}$ to be equivalent over $\mathbb{Q}$ a necessary and sufficient condition is that they are equivalent over $\mathbb{Q}_p$ for all primes p.

Corollary 2: For f,f' to be equivalent over $\mathbb{Q}$ the following conditions are necessary and sufficient:
[i] Equivalent over $\mathbb{Q}_p$ $\forall$ p prime.
[ii] They have the same signature.

4. A computational Approach

4.1. **Introduction to the theory of algorithms.**

After being equiped with the appropriate machinery we are going to study in detail some algorithms for constructing a solution in case of quadratic forms of three variables (conics) and in case of four variables.In theoretical computer science after building an algorithm the next concern is to check how efficient or fast is the algorithm and these are the computational questions we are going to deal with.

4.1.1. ***Definition:*** Polynomial algorithm is the algorithm in which the number of computation steps an abstract machine needs to perform in order to get a result is bounded above by a polynomial in the size of the input of the algorithm

In simple words a polynomial algorithm is synonymous to being feasible or fast so our aim is our algorithms to be of polynomial time.
The main drawback in the algorithms in number theory is factorizing large numbers , so our main effort is to avoid as many as possible steps involving factorizations.In all cases we need to know the factorisation of detQ as solubility over $\mathbb{Q}_p$ for any p not dividing the determinant is immediate,so as soon as the factorisation is known we provide efficient way to proof existence of a nontrivial global solution.

The types of the algorithms we will use mainly now on are:

[**1**]Minimization algorithms

[**2**]Reduction Algorithms based on the Reduction of Lattices

The central idea of these algorithms is that at each step we reduce the given quadratic form to a new form with its determinant as small as possible so that a solution of the latter can be deduced easily.At each stage we keep in mind a transformation so that a

linear back-substitution will help us to find a solution to the original problem.
At this stage we are going to present and analyze some algorithms which will help us in the next sections for constructing solutions for quadratic forms.

Below we present an algorithm which given a a basis $e_1, e_2, ...e_n$ for $\mathbb{R}^n$ enhanced with a scalar product , has as output an orthogonal basis $e_1^*, e_2^*, ...e_n^*$ where $e_i^* = e_i - \sum_{1\leq j\leq n-1}\mu_{i,j}e_j^*$ where $\mu_{i,j} = (e_i, e_i^*)/(e_j^*, e_j^*)$.

4.1.2. ***Algorithm***. (Gram Schmidt)

```
For $i = 1, ...n$ do
set $e_i^* = e_i$
for $j = 1, .., i-1$ set $\mu_{i,j} = (e_i, e_i^*)/(e_j^*, e_j^*)$ and $e_i^* = e_i^* - \mu_{i,j}e_j^*$
```

Note: detQ=$\prod_{1\leq i\leq n}(e_i^*)^2$

The algorithm above is entirely elementary and we use it as input to the algorithms we are going to use for constructing new basis which are more suitable in a computational point of view for our aim which is to find a solution to a quadratic form.
The next algorithm is an algorithm which is used to find in a 2-dimensional lattice enhanced with a norm the vector which minimizes the norm.We will use this for constructing later algorithms for finding solutions in conices which do not involve factorisations of integers.

4.1.3. ***Algorithm***. (Gaussian 2-dimensional Lattice Reduction)

```
Start with a basis $e_1, e_2$ of $\mathbb{R}^2$ and let $\mu_{2,1} = (e_1, e_2)/(e_1, e_1)$.
[1]If $|\mu_{2,1}| > 1/2$ let $e_2 = e_2 - r.e_1$ where r denotes the integer closest to $\mu_{2,1}$.
[2]if $(e_1, e_1) > (e_2, e_2)$ then interchange $e_1$ with $e_2$.
Output: $e_1$.
```

Remark: This can also be found in bibliography as the algorithm of 'finding **short vectors**'. The role of this algorithm is very useful for finding if a quadratic form in 2 variables is isotropic and then we can generalize as we will see below in higher dimensions.We can simply consider a quadratic $f_1x_1^2 + f_2x_2^2$ and taking as norm of vector (u,v) to be $||(u, v)||^2 = |f_1|u^2 + |f_2|v^2$ if the form is isotropic then the short vector related to this form will help us as we will see to find a non-trivial solution for the form.

Now we are going to develop a general lattice reduction algorithm, the LLL algorithm.This is a polynomial time lattice reduction algorithm which has as input lattice basis vectors with integer entries and gives as output an LLL-reduced basis ,i.e a basis where the vectors are as short as possible.The positive definite form considered in diagonal forms is $||x||^2 = \sum_{1\leq i\leq n}|f_i|x_i^2$ .This is reasonable as the original form is bounded by this form but they have the same determinant up to sign.Hence a reduced basis for the latter form is also a reduced basis for the original.The exact definition is presented below.

4.1.4. ***Definition***. (LLL-reduced basis)
A basis of $\mathbb{Z}^n$ is said to be reduced if the following properties are established:
[1]If $(e_{k-1}^*, e_{k-1}^*) < \nu(e_k^*, e_k^*)$ for $1 < k \leq n$ where $\nu > 4/3$.
[2]$(e_1, e_1)^n \leq \nu^{n(n-1)/2}det(Q)$

The algorithm for constructing such a set of basis is given below.As we will see in the next sections this algorithm is widely used for finding a solution in case of unimodular quadratic forms.Combining this algorithm with the minimization methods we are going to develop later we will be able to construct an algorithm for building a nontrivial global solution.

4.1.5. ***Algorithm.*** (LLL)
Let $1/4 < r < 1$ and $e_1, e_2, .., e_n$ be a basis for $\mathbb{Z}^n$, then the following algorithm gives an LLL-reduced set of basis.
[1]Let k=2.
[2]Compute the new orthogonal basis using Gram Schmidt algorithm.
[3]For i=n,...,1 for j=1,...,i-1 set $q = [\mu_{i,j}]$, $e_i = e_i - qb_j$ and $\mu_{i,j} = \mu_{i,j} - q$ where q the closest integer to $\mu_{i,j}$.
[4]If $(e^*_k, e^*_k)+\mu^2_{k,k-1}(e^*_{k-1}, e^*_{k-1}) < r(e^*_{k-1}, e^*_{k-1})$, exchange e_k and e_{k-1} ,and set k=max(k-1,2).Otherwise k++.
[5]if $k \leq n$ go to step 2,else terminate return the basis e_i.

Remark: In case of an indefinite quadratic form we just take absolute values to the fourth step and the outcome is the same.The case of the application of the algorithm to indefinite quadratic form is more useful since we can define the scalar product to be $(x, y) = (Q(x+y) - Q(x) - Q(y))/2$ and this is related immediately with our problem.

Output:The given algorithm either finds a non-trivial solution solution of $x^TQx = 0$ or it gives a set of reduced basis.
Below we present some examples of LLL algorithm on different some quadratic forms.In all cases we give initially to the algorithm the standard basis of $\mathbb{R}^3$ and consider the norm $< x, x >= x^TQx$ where Q the representation matrix of the ternary quadratic form q.

Example 1:

Let $q(x, y, z) = 36907x^2 + 57575417y^2 + 2915432xy - 4yz - 158zy$
Output: (0,0,1) is a solution

Example 2:

Let $q(x, y, z) = 5934x^2 + 985y^2 + 987z^2 + 3346xy + 3344yz + 1972zy$
Output: (0,-1,1) is a solution

Example 3:

Let $q(x, y, z) = 47x^2 + 51y^2 - 33z^2 + 42xy + 30yz - 66zy$
Output: (1,0,0) , (0,1,0) , (0,-1,1) is a reduced basis

Now we are going to prove that this algorithm is suitable for using it since it efficient.

4.1.6. ***Lemma.*** LLL-algorithm is a polynomial-time algorithm.

Proof: Suppose that no solution is found,then we have to show that it terminates after a number of steps bounded by a polynomial.
Consider $d_k = \prod_{1 \leq i \leq k} |(e_i^*, e_i^*)|$ which is the determinant of the minor of the matrix Q given by the first k rows and k coloumns of the matrix.As the matrix has integral entries then each d_i is integral.
Clearly at step [4] d_k diminishes by at least $1/r$ and other d_j do not change size so we are done.

Now we are going to use the LLL-algorithm so that we have as an output a solution in case of $x^T Qx = 0$ where Q is a unimodular symmetric matrix $\in M_n(\mathbb{Z})$ for $n \leq 9$.For simplicity of the algorithm we assume that neither r or s is zero and that the original LLL-algorithm do not find a solution.

4.1.7. ***Algorithm.*** [1] Use Gram-Schidt algorithm to calculate a basis.
[2]For $k = 1, ..., n$ find the subdeterminants $d_k = det(Q_{i,j})_{1 \leq i,j \leq k}$ and $d_0 = 1$
[3]If $d_i/d_{i-1} = -d_j/d_{j-1}$ for $i \neq j$ .Output : $e_i^* + e_j^*$

Remark: So far we proved that using LLL-algorithm we can find a solution when $d_k = 0$ for some k and that the Gram-Schimdt basis can be determined if all these subdeterminants are nonzero.Having in mind that $Q(e_k^*) = d_k/d_{k-1}$ we see that the output given in [3] is valid.According to **[Sim1,p.3]** we see that this is correct for $n \leq 9$

The next lemma is very crucial for the lattice methods whice we are going to develop in the next section for solving conic equations.As we will see the knowledge of the shortest vector in a lattice helps us to find a solution.

4.1.8. ***Lemma.*** If e_1, e_2, e_3 is an LLL-reduced basis of a 3-dimensional lattice then the short vector has the form $n_1 e_1 + n_2 e_2 + n_3 e_3$ where $n_i \in < -1, 0, 1 >$.

Proof: Let e_1^*, e_2^*, e_3^* be an orthonormal basis for $\mathbb{R}^3$
such that $e_1 = e_1^*$, $e_2 = e_2^* + \mu_{2,1} e_1^*$, $e_3 = e_3^* + \mu_{3,1} e_1^* + \mu_{3,2} e_2^*$
Using the definition of LLL-reduced basis we have that $|\mu_{i,j}| \leq 1/2$ for $1 \leq j < i \leq 3$ and
$|e_i^*|^2 \geq (3/4 - \mu_{i,i-1}^2)|e_{i-1}^*|^2 \geq |e_{i-1}^*|^2/2$ for i =2,3
Thus $|e_1^*|^2 \leq 2|e_2^*|^2 \leq 4|e_3^*|^2$
Then for any x $\in \ell$ with integral coefficients say x_i
$\Rightarrow |x|^2 = (x_1 + \mu_{2,1} x_2 + \mu_{3,1} x_3)^2 |e_1^*|^2 + (x_2 + \mu_{3,2} x_3)^2 |e_2^*|^2 + x_3^2 |e_3^*|^2$
Suppose $|x| < |e_1|$.
From the inequality $x_3^2 |e_3^*|^2 \leq |x|^2 < |e_1^*|^2 \leq 4|e_3^*|^2$ we see that $|x_3| \leq 1$
Then considering the cases $x_3 = 0$ and x_3 =1 or -1 with $|\mu_{i,j}| < 1/2$ we conclude that $|x_i| \leq 1$ for all i and so the lemma follows.

4.2. **Legendre Reduction in case of conics.**

In this section we prove the existence of an algorithm for finding a solution in case of conics $ax^2 + by^2 + cz^2$.This algorithm actually puts this equation into the norm form $x^2 - az^2 = by^2$ and our aim is to express b as norm from the number field $\mathbb{Q}(\sqrt{a})$ if it is possible.
For solubility over $\mathbb{R}$ we need that not both a and b are negative so we suppose that this case doesn't happen for the simplicity of the algorithm.The basic idea of the algorithm is that at each step we reduce the value of b and we have to solve an equivalent form with smaller b , we proceed in this way until a solution can be easily deduced and then using backward substitutions we can build a solution to the original problem.The exact algorithm is presented below.

4.2.1. ***Algorithm.*** (Legendre-type reduction or Fermat's Descent)
There exists an algorithm which has as input the coefficients of a conic equation in norm form and as output a non trivial solution given as follow:
[**1**]If $|a| > |b|$ interchange a and b and swap the solution (x,y,z) to (x,z,y)
[**2**]If a=1 or b=1. Output : (1,0,1) or (1,1,0) respectively
[**3**]If b=-a: Output : (0,1,1)
[**4**]If b=-1.Output: There is no non trivial solution
[**5**]If b=a and (x_0, y_0, z_0) a solution of $X^2 + Z^2 = aY^2$. Output: (ay_0, x_0, z_0)
[**6**]Let w be a solution of $X^2 \equiv a mod b$ with $|w| \leq |b|/2$ and let $(x_0, z_0) = (w, 1)$ solving $x_0^2 - az_0^2 \equiv 0 mod b$
[**7**]Using Gaussian 2-dimensional Reduction solve $x_0^2 - az_0^2 \equiv 0 mod b$ with $x_0^2 + |a|z_0^2$ as small as possible.
[**8**]Let $t = (x_0^2 - az_0^2)/b = t_1 t_2^2$ where t_1 square free
[**9**]If (x_1, y_1, z_1) solving $x^2 - az^2 = t_1 y^2$. Output: $(x_0x_1 + az_0z_1, t_1t_2y_1, z_0x_1 + x_0z_1)$

The Legendre's Reduction algorithm described above is an algorithm which looks for a non trivial solution of the norm form and detects if no such solution exists.It is actually a method of descent since as we observe in the above algorithm our aim is to reduce the initial norm form to a new norm form with the coefficient b smaller so that this is easier to solve and less time consuming and then can find a solution to the original equation.

Further Discussion of the algorithm: The steps [1]-[5] are made in order to ensure that the coefficients of the norm form $x^2 - az^2 = by^2$ satisfy $|b| > |a|$ and $a \neq 1$ and spot the cases where a solution is trivial to find. So our main purpose is to reduce the given norm form to one of these included in the first six steps so we can easily deduce solubility.
In step [6] we solve the congruence $x^2 \equiv a mod b$ which is very time consuming since includes factorization of b , solving the congrunce for each prime factor p of b and then lift the solution modb using Chinese Remainder Theorem.
This is in fact the most inefficient part of the algorithm as it involves factorisations of integers.
Then we consider the 2-tuple (w,1) where w satisfy the quadratic congruence above with $|w| \leq |b|/2$.

Then we consider the inner product $(e_1, e_2) = (ux_1 + by_1)(ux_2 + by_2) + |a|x_1x_2$ defined on $\mathbb{Z}^2$ which gives rise to the norm $||e_i||^2 = (ux_i + by_i)^2 + |a|x_i^2$.
Then using the Gaussian Algorithm given above we compute the shortest vector with respect to this norm say (x_0, y_0).Then setting $(x_0, y_0) = (x_0w + by_0, y_0)$ we simply verify that it satisfies the congruence given initially.
This is done since the shortest vector minimizes the $x^2 + |a|z^2$ and thus t as given in the algotirhm decreases faster.
Step [9] splits t to the square factor $t_2$and to the square-free factor t_1 and then consider the equation $x^2 - az^2 = t_1y^2$.In the stage of solving the congrunce we chose u such that $|u| \leq |b|/2$ so that $|t| = |(x_0^2 - az_0^2)/b| = |(u^2 - a)/b| \leq |u^2/b| + |a/b| \leq |b|/4 + 1$.This makes the algorithm more efficient as the coefficent b is significantly reduced.
The final stage just make a substitution to find a solution to the initial norm form using a solution of the reduced form. So substituding $(x_0x_1 + az_0z_1, t_1t_2y_1, z_0x_1 + x_0z_1)$ on the initial equation we get $(x_0x_1 + az_0z_1)^2 - a(z_0x_1 + x_0z_1)^2 = b(t_1t_2y_1)^2)$ which is equivalent by expanding out,using substitution for t and assuming (x_1, y_1, z_1) satisfies reduced form to the reduced form.

4.3. **Lattice Methods.**

So far Fermat's descent algorithm quarantees to deliver a non trivial solution for a given conic but it involves factorisation of integers which is a great drawback making the whole procedure to be inefficient in case of large numbers.Thus we develop and present two algorithms which avoid integer factorisations based on the theory of the Lattice's Reductions.In order to undestand the theory behind the reduction of lattices we have to establish the appropriate notation given below.

4.3.1. ***Definition.*** An integral triple (k_1, k_2, k_3) is called **solubility certificate** if it solves the following congruences:

$$[\mathbf{1}]k_1^2 \equiv -bcmoda$$
$$[\mathbf{2}]k_2^2 \equiv -camodb$$
$$[\mathbf{3}]k_3^2 \equiv -abmodc$$

4.3.2. ***Notation.*** .
ℓ(a,b,c;k$_1, k_2, k_3) =< (x, y, z) \in \mathbb{Z}^3 | by \equiv k_1zmoda, cz \equiv k_2xmodb, ax \equiv k_3ymodc >$.
With an easy check we see that this is actually a lattice of $\mathbb{Z}^3$ of index $|abc|$ and any element of the lattice satisfies $ax^2 + by^2 + cz^2 \equiv 0mod|abc|$.In the algorithms described below we are going to construct solutions lying in the above lattices.The main idea roughly is to reduce the conic equation or the equivalent lattice to another conic equation with the coefficients being as small as possible so we are able to deduce easily solutions in the latter case and then associate these solutions to solutions of the original one.
The first algorithm is based on the 2-dimensional Gaussian Reduction and the second to the 3-dimensional reduction using LLL algorithm.

4.3.3. ***Algorithm.*** There exists an algorithm based on Gaussian Reduction in which given (a, b, c) and a solubility certificate has as output (a', b', c') and a linear transformation mapping solution of the reduced problem to solutions of the original.

Remark: This is an algorithm based on 2-dimensional Gaussian reduction which involves no other factorisations except of the coefficients of the conic.

Discusion of the algorithm:
The main idea of this algorithm is given a solubility certificate (k_1, k_2, k_3) for a conic form of coefficients (a, b, c) construct a new solubility certificate for a reduced problems with new coefficients and a linear tranformation which maps solutions of the latter problem to the original one.This procedure is repeated until we built a reduced problem where a non-trivial solution can be deduced directly.
We assume that the coefficients a,b,c are pairwise coprime but not necessarily square-free.
Firstly we remove any square factor of any of the coefficients.This can be done easily since if p^2/a and as (bc,a)=1 then p is invertible modbc with inverse say p'.
Thus considering the reduced conic $(a/p^2)x^2 + by^2 + cz^2$ with a solubility certificate $(k_1, p'k_2, p'k_3)$ any solution of this (x_0, y_0, z_0) gives the solution $(x_0, p'y_0, p'z_0)$ of the original one.So from now we remove any square factor using this procedure.
Now we are going to give a sketch of the idea of the proof given in [**Cr,p.10-15**], the proof is very technical so we just present the parts of the proof which are enough to understand how to adapt an algorithm to get the result we need.We divide the proof in five steps.

[1]2-Dimensional Gaussian Reduction
Consider the sublattice of $\mathbb{Z}^2$ generated by the basis (1,w) and (0,a) where $w \equiv -c^{-1}k_1 \equiv -bk_1^{-1}\ moda$.
Turn this space into a normed space under the norm $||(x,y)||^2 = |b|x^2 + |c|y^2$.
Use Gaussian Reduction to get the short vector (w_1, w_2) of this norm.
We can easily show that $bw_1^2 + cw_2^2 = at$ and that $hcf(hcf(w_1, w_2), bc) = 1$.

[2]Constructing the reduced coefficients (a', b', c')
To prove this we need the following lemma.
Lemma: Let a_i be nonzero integers where $1 \leq i \leq n$ .Then we can find $b_i \in \mathbb{Z}$ for $1 \leq i \leq n$ which are pairwise coprime and integers c_I where I nonempty subsets of the set of naturals less than n such that we have $a_i = b_i^2 \prod_{I, i\in I} c_I$.
Proof: For more details see [**Cr**]

Using the lemma above decompose bc,a,and t as:
$bc = \alpha^2 b'c'$, $a = \beta^2 n_1 n_3$ and $t = \gamma^2 n_2 n_3 c'$ where n_1, n_2, n_3, b', c' are pairwise coprime.
Observing that $\alpha = \beta = 1$ since if not then we can find non-trivial square divisors of b and c and this leads to the simplification
$bc = b'c'$, $a = n_1 n_3$ and $t = \gamma^2 n_2 n_3 c'$.
We can easily show that (a',b',c') is a triple of integers pairwise coprime non of the same sign and $t > 0$.

[3]Further Conditions
In this step we provide some congruence conditions satisfied by some paramaters but we avoid to provide a lot of details.
Let $d_1 = hcf(c, c')$ and $d_2 = hcf(b, c')$
Then we can prove that we can arange the signs of each of d_i such that $c' = d_1 d_2$ and also we have the following hold:

[i] d_i/w_i for $i = 1, 2$

$$\textbf{[ii]}\ hcf(\beta,\gamma) = hcf(\gamma, c) = 1$$
$$\textbf{[iii]}\ hcf(w_1, n_2) = hcf(w_2, n_2) = 1$$
$$\textbf{[iv]}\ hcf(d_2, w_1) = hcf(d_1, w_2) = 1$$

[4]Constructing the new certificate (k'_1, k'_2, k'_3)

The following parameters give the new certificate for the new reduced problem with coefficients as found in step 2.

$$\textbf{[i]}\ k'_1 = -bw_1w_2^{-1}\ mod n_2 {=} {-k_1}\ mod n_3$$
$$\textbf{[ii]}\ k'_2 = (\alpha\gamma)^{-1}k_3w_1\ mod(c/d_1) {=} (\alpha\gamma)^{-1}k_2w_2\ mod(b/d_2)$$
$$\textbf{[iii]}\ k'_3 = k_2a'\gamma w_1^{-1} {=}\ mod d_2 {=} {-k_3}a'\gamma w_2^{-1}\ mod d_1$$

[5]Constructing the Linear Transformation

We just present the map for more details about the validity and the construction see **[Cr]**.

Let ℓ and ℓ' be two 3-dimensional lattices with paramaters $(a, b, c; k_1, k_2, k_3)$ and $(a', b', c'; k'_1, k'_2, k'_3)$ respectively.

Then there exists a well defined map $\theta : \ell' \to \ell$ with $\theta(x', y', z') = (x, y, z)$ defined as:

$$\textbf{[i]}x = -x'(\gamma n_3)$$
$$\textbf{[ii]}y = (cw_2y'/d_1d_2 + w_1z')/n_2$$
$$\textbf{[iii]}z = (bw_1y'/d_2d_1 - w_2z')/n_2$$

It can be proved that this is linear transformation mapping solutions of the reduced conic to the original one.Thus we presented an algorithm which involves 2-dimensional reduction and avoids integer factorisations.The next algorithm we are going to develop is based on 3-dimensional reduction (LLL-algorithm).

4.3.4. ***Algorithm.*** LLL algorithm quarantees to deliver a non-trivial solution of a given conic.

Discussion of the statement

In this case we consider the sublattice of index 2 ℓ' of ℓ generated by the elements of ℓ satisfying $ax^2 + by^2 + cz^2 \equiv mod2|abc|$.Using theorem of Gauss (see **[Ca]**) based on the Geometry of Numbers we know there exists a point lying in the lattice ℓ' with $|ax^2 + by^2 + cz^2| < 2|abc|$ which also solves the conic equation.

We proved that the LLL algorithm has as output a set of reduced basis with respect to an associated norm.In this case the associate norm taken is $||(x, y, z)||^2 = |a|x^2 + |b|y^2 + |c|z^2$.The shortest vector with respect to can be found easily as we proved before.

Firstly we have to find a basis for ℓ' and this can be done if we find a basis for ℓ and a surjective map between the two lattices.

After finding a basis for ℓ' we can use LLL algorithm to find the solution

Using Euclidean Algorithm we can find u,v,m,n such that ub+vc=1 and am+bcn=1.

Then consider the conqruences:

$l_1 \equiv nck_1\ moda$

$l_2 \equiv umbk_3 modbc$

and $l_3 \equiv vmck_2\ modbc$

Then the lattice of $\mathbb{Z}^3$ generated by $< (bc, 0, 0), (al_2, a, 0), (l_1l_2 + l_3, l_1, 1) >$ .Using conqrunces we see that by construction these elements lie in the lattice ℓ since they all

satisfy $ax^2 + by^2 + cz^2 \equiv \bmod abc$ and since they are linearly independent then it has to be ℓ.
Thus this is actually a basis for the lattice ℓ.
Our next goal is to use this basis to construct a basis for ℓ'.This is achieved by considering the additive surjective homomorphism
$\phi : \ell \to \mathbb{Z}/2\mathbb{Z}$.
$(x, y, z)- > f(x, y, z)/abc$ mod2.
Then let u_i be a vector of the original lattice satisfying $\phi(u_i) = 1$ and define w_j to be:
[1] $2u_i$ if j=i.
[2] $u_i - u_j$ if j≠i and $\phi(u_j) = 1$
[3] u_j if j≠i and $\phi(u_j) = 0$
Thus this is a basis for ℓ'.So now simply use this basis and apply LLL-algorithm to get a reduced basis $< e_1, e_2, e_3 >$ and check which of the vectors of the form $n_1e_1+n_2e_2+n_3e_3$ where n_i is 1 or 0 or -1 is the shortest vector in the associated norm as we proved before.
The output of the algorithm is this vector which solves the conic equation.

4.4. Minimization techniques for conics.

In this part we are going to develop an algorithm for solving the ternary quadratic forms based on minimization techniques.Our aim is to build another quadratic form equivalent to the original form but with determinant +1 or -1 such that a solution of the original equation can be deduced from a solution of the new form.
As we will prove in the next theorem, the LLL-algorithm quarantees to find a solution in case of unimodular quadratic forms in polynomial time so trying to minimize a quadratic form to a unimodular quadratic form is reasonable.

4.4.1. ***Theorem:*** Let $n \leq 5$ and q be a unimodular integral quadratic form with matrix representation Q $\in M_n(\mathbb{Z})$ such that $|detQ| = 1$.Then running the LLL algorithm with $1/4 + 2^{-2/(n-1)} < r < 1$ and suppose it does not find a non-trivial solution.Then the corresponding Gram matrix of the reduced forms has diagonal elements -1 or 1.

Proof: Using LLL algorithm we obtain an LLL-reduced basis satisfying
$|(e^*_{i-1}, (e^*_{i-1})| \leq \gamma||(e^*_i, e^*_i)||$ for $1 < i \leq n$
Hence we have $1 \leq |(e^*_1, e^*_1)|^n \leq \gamma^{n(n-1)/2}|detQ|$
Using the bound for r as in the theorem and setting $\gamma = 1/(r-1/4)$ we have $|(e^*_1, e^*_1)| = 1$ as it is an integral vector.
Now considering the coefficients $\mu_{i,j}$ used in the algorithm we know that for a reduced basis $|\mu_{i,j}| \leq 1/2$.
Since $|\mu_{j,1}| = |(e^*_j, e^*_1)|$ the above bound implies $\mu_{j,1} = 0$ and so we established that all other basis is orthonogonal to e^*_1.Hence by induction on the complement of $< e^*_1 >$ we have that the basis are pairwise orthogonal satisfying $|(e^*_j, e^*_j)| = 1$.
Thus the matrix representation of Q with respect to this basis is diagonal with diagonal entries being 1 or -1.

Remark: Since the matrix representation of the form with respect to this reduced basis is diagonal with entries being +1 or -1 it is very easy for us to find a solution in this case and then using the base-change transformation find the corresponding solutions for the original unimodular form.

Remark: According to **[Sim1,Thm1.8,p1535]** this algorithm can be extended in case of unimodular indefinite quadratic forms up to dimension 6 by running the LLL-algorithm using $1/4 + 2^{-2/(n-1)}(3/4)^{1/(n^2-n)} < r < 1$.The extension to dimension 6 will be proved very helpful when we proving the existence of an algorithm for solving quadratic forms in dimension 4 as we will see that we will need to know how to find solutions to specific 6 dimensional unimodular quadratic forms.

So far we proved that we can find solutions to a unimodular quadratic form so now we are going to study the minimization techniques for a general form .Through our algorithms we assume that the factorisation of the determinant is known.The next theorem is what we want to prove and we are proving it considering all possible cases for the rank of the matrix Q over a finite field $\mathbb{F}_p$.
Roughly speaking at each step we are going to build a new form equivalent to the original form but with the difference that the determinant of the new form differs to that of the original form to at least one prime factor.Repeating this argument we can remove all the prime factors until to get a unimodular form.The precise statement of what we are going to prove is the following theorem.

4.4.2. ***Theorem:*** Let Q $\in M_3(\mathbb{Z})$ be a symmetric matrix with non-zero determinant such that $x^TQx = 0$ has a non trivial solution in $\mathbb{Q}_p$ for any prime p.Then there exists a matrix V $\in M_3(\mathbb{Z})$ with the following properties:
[1]$detV = |detQ|$
[2]Q'=$V^TQV/detQ \in M_3(\mathbb{Z})$
[3]$|detQ'| = 1$
From now on let $\overline{Q}$ to be the reduction modp of the matrix Q and that the equation $x^TQx = 0$ is solvable over $\mathbb{Q}_p$ for all primes p.
The possible cases for the dimension of the kernel of $\overline{Q}$ are 1 and 2 and we consider each case separately below:

Case [1]: $u_p(detQ) = 1$ (i.e the kernel of $\overline{Q}$ is one dimensional)

Since the kernel of the reduction of the matrix is one dimensional hence we can find a basis-change matrix U such that

$$Q'=U^TQU=\begin{bmatrix} p* & p* & p* \\ p* & \text{Q'}_{2,2} & \text{Q'}_{2,3} \\ p* & \text{Q'}_{3,2} & \text{Q'}_{3,3} \end{bmatrix}$$

So now our aim it to find a transformation R such that $R^TQ'R$ has all its entries divisible by p.

If $p/Q'_{2,2}$ then consider R to be $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p \end{bmatrix}$

we have Q'= $\begin{bmatrix} p* & p* & p* \\ p* & p* & p* \\ p* & p* & p* \end{bmatrix}$

So now assume that p does not divide $Q'_{2,2}$

In this case take R to be $\begin{bmatrix} 1 & 0 & 0 \\ 0 & p & x \\ 1 & 0 & 1 \end{bmatrix}$ and then we have $R^TQ'R = \begin{bmatrix} p* & p* & p* \\ p* & p* & p* \\ p* & p* & l \end{bmatrix}$
where l=$x^2{Q'_{2,2}}^2 + xQ'_{2,3} + xQ'_{3,2} + Q'_{3,3}$
Now our aim is to pick x such that this entry is divisible by p
Let $u \equiv {Q'_{2,2}}^{-1} modp$ and r be such that $r^2 \equiv ({Q'_{3,2}}^2 - Q'_{2,2}Q'_{3,3}) modp$ and let $x = u(r - Q'_{2,3})$
Then substituding on l and expanding out we see that this choice for x works and the entry is divisible by p.
Then the matrix $(UR)^TQ(UR)$ has determinant differing from the original by p^{-1} as required.

Case [2]: $u_p(detQ) \geq 2$ and $dim_{\mathbb{F}_p}(ker\overline{Q}) = 1$

In this case we want to built a form equivalent to the first but with determinant differing from the original by p^{-2}.
Again as in previous case let U be the base change transformation such that the first coloumn of U is the vector of the kernel of $\overline{Q}$ and let R to be $\begin{bmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{bmatrix}$
Then we have by expanding out that
$Q' = (RU)^TQRU = \begin{bmatrix} \text{Q'}_{1,1} & \text{pQ'}_{1,2} & \text{pQ'}_{1,3} \\ \text{pQ'}_{2,1} & \text{p}^2* & \text{p}^2* \\ \text{pQ'}_{3,1} & \text{p}^2* & \text{p}^2* \end{bmatrix}$
But we have that $Q'_{1,1}$ is divisible by p^2 and $Q'_{1,2}$ and $Q'_{1,3}$ by p.
So we managed to built the required form.

Case [2]: $u_p(detQ) \geq 2$ and $dim_{\mathbb{F}_p}(ker\overline{Q}) = 2$

Let again U to be the change basis matrix such that
$Q' = U^TQU = \begin{bmatrix} p* & p* & p* \\ p* & p* & p* \\ p* & p* & \text{Q'}_{3,3} \end{bmatrix}$ and taking R $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p \end{bmatrix}$
we have $(UR)^TQUR$ has all the entries divisible by p and so we are done.

Examples of minimization:

Below we present some examples of conics and their corresponding minimized matrix.The program was implemented on C language to perform the operations above until get to a unimodular matrix.We run the program in the special case of conics.

Example 1:

$$\begin{bmatrix} 97 & 0 & 0 \\ 0 & -221 & 0 \\ 0 & 0 & -167 \end{bmatrix} \overset{minimization}{\longrightarrow} \begin{bmatrix} 36907 & 1457716 & -2 \\ 1457716 & 57575417 & -79 \\ -2 & -79 & 0 \end{bmatrix}$$

Example 2:

$$\begin{bmatrix} 589 & 0 & 0 \\ 0 & -151 & 0 \\ 0 & 0 & -5 \end{bmatrix} \overset{minimization}{\rightarrow} \begin{bmatrix} 755 & -177878 & -83726 \\ -177878 & 41907939 & 19725783 \\ -83726 & 19725783 & 9284792 \end{bmatrix}$$

Example 3:

$$\begin{bmatrix} 211 & 0 & 0 \\ 0 & -337 & 0 \\ 0 & 0 & -3 \end{bmatrix} \overset{minimization}{\rightarrow} \begin{bmatrix} 1011 & -71107 & -4433 \\ -71107 & 5001122 & 311766 \\ -4433 & 311766 & 19431 \end{bmatrix}$$

Worked Example for conics:

We consider the ternary quadratic form $97x^2 - 221y^2 - 167z^2 = 0$
Running the minimization algorithm in this case we have

$$\begin{bmatrix} 97 & 0 & 0 \\ 0 & -221 & 0 \\ 0 & 0 & -167 \end{bmatrix} \overset{minimization}{\rightarrow} \begin{bmatrix} 36907 & 1457716 & -2 \\ 1457716 & 57575417 & -79 \\ -2 & -79 & 0 \end{bmatrix}$$

Minimization quarantees that the second matrix is unimodular
As we proved in the begining of the section running LLL-algorithm we get a solution or a set of Reduced Basis such that with respect to these basis the matrix is diagonal with +1 or -1 on the diagonal.

In this case the output of the LLL-algorithm is the vector $(0, 0, 1)$
The matrix U such that $(detQ)Q' = U^T QU$ is given by

$$\text{U=} \begin{bmatrix} 36907 & 1457716 & -2 \\ 0 & 97 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Thus the solution to the original problem is given by $U(1, 0, 0)^T$ which is (-2,1,1) and clearly solves the problem.

4.5. **Solving quadratics in four variables.**

In this section we are going to develop and analyze algorithms for solving quadratic forms in four variables.Trying to adapt the classical proof of Hasse-Minkowski theorem in case of dimension four to construct an algorithm for checking solubility or finding a solution we see that this becomes very inefficient.This is due to the fact that we have to use the theorem of Dirichlet's on primes in arithmetic progressions which in the computational point of view is very inefficient.

In the previous section we examined algorithms for finding a solution in case of three variables which were based on minimizing the ternary quadratic form to an equivalent unimodular quadratic form and then using the LLL-algorithm we were able to find such a solution since we proved that a ternary unimodular quadratic form is diagonal with diagonal entries +1 or -1 with respect to the LLL-reduced basis.

Unfortunately in dimension 4 the minimization of the form can't be easily achieved and so we have to move in higher dimensions.Actually we are trying to turn a proof which doesn't use the Dirichlet's theorem based on the theory of binary quadratic forms into an algorithm.We actually use Cassels trick (see **[Ca,Ch14]**) which asserts that there exists a binary quadratic form Q_2 such that $Q \oplus Q_2$ is minimizable and equivalent to $\mathbb{H} \oplus \mathbb{H} \oplus \mathbb{H}$ .We will show that we construct this form the local invariants of the form q and knowing the 2-Sylow subgroup of Cl($\sqrt{detQ}$). Assuming that the factorization of the determinant of the representrom ation matrix is known the algorithm consists mainly of two parts.

[1] Minimization Step:

[**i**]Remove as many prime factors in dimension 4

[**ii**]Increase the dimension by 1 to remove the square factors of detQ

[**iii**]Increase the dimension by 2 to remove the remaining factors

[2] Reduction Step: In this step we just apply the LLL-algorithm given in the previous section to obtain a reduced basis in which the form is diagonal.

Through the rest of this chapter we examine each step separately.

Minimization Step

In this part we consider a general quadratic form of n variables q(x) with the corresponding reprentation matrix Q.Our aim is to apply linear transformations over $\mathbb{Q}$ to the matrix Q in such a way that the the quadratic form with respect to this matrix has integral coefficients and the determinant becomes smaller.

We are handling the general case where Q $\in M_n(\mathbb{Z})$ since as we will see later the algorithm developed for solving quadratic forms in four variables needs to know how to minimize a quadratic form in 6 variables.Again as usual to avoid factorisations we assume the factorization of detQ is known and we work separately for any divisor p of detQ.

Let $\overline{Q}$ be the reduction modp of the matrix Q , $d = dim_{\mathbb{F}_p} ker(\overline{Q})$ and u_p be the valuation of detQ with respect to a prime divisor.

After chosing a suitable basis we can assume that matrix Q has the form

$$\begin{bmatrix} pQ' & p* \\ p* & W \end{bmatrix}$$

where Q'= $(Q_{ij}/p)_{1\leq i,j\leq d}$ and W $\in M_{n-d}(\mathbb{Z})$ invertible modp.
The logic behind the transformations is the same as the logic used in case of conics , i.e we are trying to construct the appropriate transformation U such that the form U^TQU lies in $M_n(\mathbb{Z})$ and the determinant is reduced.The idea is again simple since if x is a solution to $(Ux)^TQ(Ux) = 0$ then Ux is the solution to the original equation.Now we are going to handle different cases separately.

Case 1:$dim_{\mathbb{F}_p}(\overline{Q}) = n$

In this case as the dimension of $\overline{Q}$ is the same as the dimension of the space then we can find a new basis such that all the entries of Q are divisible by p.Hence we can divide each entry by p and work with the matrix Q/p which has determinant $(detQ)/p^n$

Case 2:$dim_{\mathbb{F}_p}(\overline{Q}) < u_p$

In this case since $d < u$ then expanding out the determinant of Q in the given form we observe that the matrix $Q'modp$ doesn't have trivial kernel so let r to be its dimension. Then find a new basis such that with respect to this basis the matrix Q' has its first r coloumns divisible by p.Then if we use same basis to represent matrix Q we see that the entries $(Q'_{ij})_{1\leq i,j\leq r}$ are divisible by p^2.
Then take U diagonal to have the first r entries 1/p and the rest one and consider the matrix U^TQU.
Then this matrix lies in $M_4(\mathbb{Z})$ and has determinant reduced by a factor p^{-2r}.

Case 3:n odd, d=$u_p \geq 2$

Take U diagonal to have the first d entries 1 and the rest p.
Then the matrix U^TQU/p has determinant $p^{n-2d}detQ$

Case 4:d=$u_p \geq 3$

Take U diagonal with first entry 1/p and the rest 1.
Then the matrix $U^TQU \in M_n(\mathbb{Z})$ and has determinant $p^{-2}detQ$

Case 5:$d = u_p = 2$ **and** $-detQ' \equiv a^2$**modp is soluble**

Use same transformation as previous case.

Case 6:d=u_p**=1 and n odd or d=**u_p**=2 and n even .Furthemore min(r,s)=(n-d)/2**

Taking U diagonal with the first d+(n-d)/2 entries 1 and other p we have that the form $U^TQU/p \in M_n(\mathbb{Z})$ and has determinant $p^{-u_p}detQ$

Since most cases involve just simple linear algebra we avoided details in some cases and for more details see **[Sim2,page 6]**

Now when we have a matrix Q we check in which category falls and we use the corresponding transformation to minimize.So far we have the appropriate machinery for minimizing quadratic forms and our next is concern is to construct solutions.

Solving a form with square determinant

Now we assume that Q is symmetric matrix $\in M_4(\mathbb{Z})$ with determinant D^2 or $-D^2$.We are going to develop an algorithm for checking unsolvability of $x^TQx = 0$ or finding a nontrivial solution.For simplicity we assume that the factorization of the determinant

is known and neither r or s is zero where (r,s) the signature of the matrix.
In previous part where we studied the minimization methods of quadratic forms we proved that if we have a form with determinant as stated before then we are able to find a new basis such that with respect to this basis the new matrix has determinant with all the prime divisors removed.Thus minimization in this case leads to a unimodular matrix.
Then by simply applying LLL-algorithm we can find a solution of the last form and then find a solution corresponding to the original form.

The full algorithm runs as below :

4.5.1. ***Algorithm:*** .
[**1**] Find (r,s).If r or s is zero. Output: There is no solution
[**2**]Minimize Q and let Q' be the new matrix with determinant D'
[**3**]If some prime p/D'. Output : There is no solution
[**4**]Run LLL-algorithm and find a solution for $x^TQ'x = 0$ and then deduce for $y^TQy = 0$

Solving a form with non-square determinant

So far we established techniques for minimizing a form and we proved that solubility in case of square determinant is easy.From now on we deal up with the case of a quadratic form in four variables of the form $x^TQx = 0$ with Q $\in M_4(\mathbb{Z})$ symmetric,sign(r,s) be its signature and detQ non-square.Furthermore we assume $x^TQx = 0$ has a nontrivial solution in $\mathbb{Q}^4$ since as we will see we can easily check unsolvability.
The following two lemmas are very crucial for understanding the algorithm we are going to develop.

4.5.2. ***Lemma:*** Let Q be a matrix satisfying the conditions given above.Then there exists a matrix U $\in SL_4(\mathbb{Z})$ such that:

$$U^TQU = \begin{bmatrix} H & 0 \\ 0 & \mathrm{Q}_2 \end{bmatrix}$$

where H is the hyperbolic plane and Q_2 a binary quadratic form with the following properties:
[**i**]$detQ_2 = -detQ$
[**ii**]$sign(Q_2) = (r-1, s-1)$
[**iii**]$c_p(Q_2) = c_p(Q)(-1, -detQ)_p$

Proof: Since $x^TQx = 0$ has a nontrivial solution in $\mathbb{Q}^4$ and the equation is homogeneous let x be such a solution with the entries not be divisible by a common prime.
Let A $\in SL_4(\mathbb{Z})$ be a matrix with the first coloumn x.
Then by expanding out we see that the matrix $Q' = A^TQA$ has the first diagonal entry zero.
Now our aim is to construct another matrix B such that $B^TQ'B$ has the form

$$\begin{bmatrix} 0 & r & 0 & 0 \\ r & \mathrm{k}_2 & \mathrm{k}_3 & \mathrm{k}_4 \\ 0 & \mathrm{k}_3 & * & * \\ 0 & \mathrm{k}_4 & * & * \end{bmatrix} \text{ for some non zero r}$$

We can easily construct B in the following way
Let Q $\in SL_3(\mathbb{Z})$ such that $(Q'_{1,2}, Q'_{1,3}, Q'_{1,3})Q = (r, 0, 0)$ then taking B to be $\begin{bmatrix} 1 & 0 \\ 0 & W \end{bmatrix}$ and expanding out we see that this works.
So far we have that $B^T A^T QAB$ has the required form.
Taking determinants in both sides then we have that r is 1 or -1 as detQ is squarefree. Then by simply multiplying by -1 the second and third coloumn of B we can have r=1. At final step we want to construct a matrix C such that $C^T B^T A^T QABC$ has the form as stated in the lemma.Letting

$$\mathrm{C}=\begin{bmatrix} 1 & -[\mathrm{k}_2/2] & \text{-k}_3 & -\mathrm{k}_4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

we see that this works.
The properties for Q_2 are trivial to prove it by considering the given matrix with respect to the new basis.

Remark: So far we proved existence of Q_2 but we do not how to find it.The construction will be shown during in the algorithm latter and is based on the theory of the class group of binary quadratic forms.At the moment we use its existence.

Now with the following lemma we are going to show how to adapt the trick of moving to dimension 6 where the associated quadratic form of 6 variables can be easily reduced to a unimodular form and since the latter can be solved we will be able to solve the original form .

4.5.3. ***Lemma:*** Let $Q'_2 \in M_2(\mathbb{Z})$ symmetric with the following properties:
[i]$detQ'_2 = -detQ$
[ii]$sign(Q'_2) = (r-1, s-1)$
[iii]$c_p(Q'_2) = c_p(Q)(-1, -detQ)_p$ for all primes $p/2detQ$
Then considering $Q \oplus -Q'_2$ this has determinant $-(detQ)^2$ and signature(3,3) .
Also there exists a matrix U $\in M_6(\mathbb{Q})$ such that $U^T(Q \oplus -Q'_2)U$ is a quadratic form in 6 variables of determinant -1 and of integral entries.

Proof: The proof is avoided since it is just application of minimization techniques and computations.
For more details see **[Sim2,Prop 13]**.

The full Algorithm:
As we have understood theoretically how we can find a solution in case of four variables moving to the case of dimension 6 now we are going to establish the full algorithm. The algorithm seems to be long but it consists mainly of the three following steps:
[**1**]Checking for unsolvability conditions
[**2**]Building the binary quadratic form Q'_2 with the required properties
[**3**]Minimization of the form corresponding to $Q \oplus -Q'_2$

4.5.4. ***Algorithm:*** Performing the following steps we either prove unsolvability of $x^TQx = 0$ or construct a solution.
[**1**]Checking Unsolvability
[**i**]Compute (r,s).if r or s is zero.Output : No solution
If $r < s$ Make the change Q to -Q and r to s.
[**ii**]Minimize the form Q and let Q' be the new matrix with determinant D'
[**iii**]If D' has a square factor. Output: There is no solution
[**iv**]Set $\delta = 4D'$ and compute $c_p(Q')$ for all p/δ.If D'≡1mod8 and $c_2(Q') = 1$.
Output: There is no solution
[**2**]Building the form Q'_2
[**i**]Find the generators $g_1, g_2, ..., g_r$ of the 2-Sylow subgroup of the class of primitive quadratic forms of discriminant δ
[**ii**]Compute $c_p(g_i)$ for p/δ.Find a g=$\prod_i g_i^{a_i}$ with invariants either $c_p(g) = c_p(Q')(-1, -\delta)_p$ or $c_p(g) = c_p(Q')(-1, -\delta)_p(2, \delta)_p$.
[**iii**]If the form builted has the first invariant then write g=(a,2b,c) and take Q'_2= $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$
In the second case let g be one of (a,b,c),(c,-2b,a) or (a+2b+c,2b+2c,c) whose first coefficient is even and write g=(2a',2b,c) let Q'_2= $\begin{bmatrix} a' & b \\ b & 2c \end{bmatrix}$
[**3**]Minimizing the new 6-dimensional form $R = Q \oplus -Q'_2$
[**i**]Minimize R and let R' be the new matrix with determinant -1.
[**ii**]Apply LLL-algorithm for dimension 6.Let be a subspace $\mathbb{Q}^4$ of $\mathbb{Q}^6$ with respect to this decomposition and F a subspace of dimension totally isotropic for R.

Discussion on the Algorithm: The steps [1] and [3] are clear since they are consequences of the lemmas stated before.
The only thing to note is that the LLL-algorithm gives us the equivalence between Q_2 and $\mathbb{H} \oplus \mathbb{H} \oplus \mathbb{H}$ so a vector in the 3-dimensional subspace of the latter with a a four dimensional subspace of Q_2 gives a solution to $x^TRx = 0$.
The only part left to explain in detail is the second part which involves the construction of the binary quadratic form Q'_2.
Fistly for computing the 2-Sylow Class group we use the Algorithm given in [**BoSt**] which is proved to be of polynomial time.We don't present the algorithm analytically since we are only interested in the construction of the binary quadratic form of the given properties.
We want to construct a binary quadratic form Q'_2 with same invariants as Q_2.Since at the first step we ensure that $r > s$ then Q_2 has signature either (1,1) or (2,0).
So let $Q_2 = ax^2 + 2bxy + cy^2$ of $disc(Q_2) = 4D'$ and the corresponding representation

matrix having determinant -4D'.From this we see that multiplication by 4 is evident as we make in this way δ to be a discriminant.

Now we consider the possible cases whether $D' \equiv 1 mod 4$ or not.

In the latter case since the discriminant of the form is fundamental then we know that we can build the required form inside the class group as it is equivalent to a form contained in the class group.This is beacause multiplying two quadratics in the obvious way we get another quadratic form , and as we proved the existence of such a binary quadratic with the properties we want this has to be a product in the generators of the Class group.

As all the forms which have odd order have trivial invariants then we can restrict inside the 2-Sylow subgroup of the class group to build the form .We do this as it is more efficient in a compuational point of view.

In first case no we have a problem since the discriminant of the form Q_2 is not fundamental.

Then there are two possible representations for Q_2

[i] The coefficients of Q_2 are not divisible by a common prime and has discriminant δ

[ii] Q_2=2A with A be primitive of discriminant $\delta/4$.

In case [i] The case 1 of the step [2ii] of the algorithm will build such a form.

In case [ii] let A=(a,b,c) then we have to prove that it is equivalent to another form with first coefficient being odd.

Using the matrices I,S,T where I the identity acting on the coefficients (a, b, c),

$$\text{S}=\begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{T}=\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$$

then the form is equivalent to the images of this matrices as they are unimodular matrices.

As b^2-4ac is odd then at least one of the first coefficient is odd and so the form (a,2b,4c) is primitive of discriminant δ with the required properties.

Now we want to build Q_2'.We know that the discriminant of the product given in the algorithm is 4δ thus we can write g in the form (a,2b,c).

In first case Q_2' has the required properties but in second case we have to consider 2g which has the required properties.Let g=(2a',2b,c) then the form (a',2b,2c) over $\mathbb{Q}$ is equivalent to 2g thus they have the same local invariants.

Thus we managed to construct a form Q_2' with same invariants as Q_2.

Conclusion: Summarizing ,we proved initially the Hasse-Minkowsi theorem which is actually our main tool used for constructing the algorithms for solving rational quadratic forms.This is a great result as in practice and computationally it is easy to construct algorithms for checking solubility of a given quadratic form over the fields $\mathbb{Q}_p$ and over $\mathbb{R}$ as using Hensel's lemma for the first case it is enough to check solubility over a finite field $\mathbb{F}_p$ where p a prime. In the second half of the essay we constructed and analyzed algorithms for solving quadratic forms over the Rationals in three and four variables. In both cases we tried to give algorithms running in polynomial time and to avoid as possible steps involving factorisations.

References

[Ca] J.W.S Cassels,‘Rational Quadratic Forms’,Dover Publications 2008

[Coh] H.Cohen,’A course in computational number theory’,Graduate Texts in Mathematics,Springer 1996.

[Ser] Jean-Pierre Serre ‘A Course in Arithmetic’,Graduate Texts in Mathematics ,Springer 1973

[BoSt] ’On the computation of quadratic 2-class groups’,J,Theor,Nombres Bordeaux 8 (1996),no 2,283-313

[Cr] J.E. Cremona, D.Rusin, ‘Efficient solution of rational conics’, Math. Comp. 72 (2003), no. 243, 14171441

[Sim1] D. Simon, ‘Solving quadratic equations using reduced unimodular quadratic forms’, Math. Comp. 74 (2005), no. 251, 15311543.

[Sim2] D. Simon, ‘Quadratic equations in dimensions 4, 5 and more’. Preprint, 2005. http://www.math.unicaen.fr/simon/maths/dim4.html