

Extended Lagrange's four-square theorem

Jesús Lacalle

Laura N. Gatti

Abstract

Lagrange's four-square theorem states that every natural number n can be represented as the sum of four integer squares: $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Ramanujan generalized Lagrange's result by providing, up to equivalence, all 54 quadratic forms $ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ that represent all positive integers. In this article, we prove the following extension of Lagrange's theorem: given a prime number p and $v_1 \in \mathbb{Z}^4$, \dots , $v_k \in \mathbb{Z}^4$, $1 \leq k \leq 3$, such that $\|v_i\|^2 = p$ for all $1 \leq i \leq k$ and $\langle v_i | v_j \rangle = 0$ for all $1 \leq i < j \leq k$, then there exists $v = (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ such that $\langle v_i | v \rangle = 0$ for all $1 \leq i \leq k$ and

$$\|v\|^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$$

This means that, in \mathbb{Z}^4 , any system of orthogonal vectors of norm p can be completed to a base. We conjecture that the result holds for every norm $p \geq 1$. The problem comes up from the study of a discrete quantum computing model in which the qubits have Gaussian integers as coordinates, except for a normalization factor $\sqrt{2^{-k}}$.

Keywords. Lagrange's four-square theorem, p -orthonormal base extension theorem, systems of p -orthonormal vectors, orthogonal lattices

1 Introduction

Long before Lagrange proved his theorem, Diophantus had asked whether every positive integer could be represented as the sum of four perfect squares greater than or equal to zero. This question later became known as Bachet's conjecture, after the 1621 translation of Diophantus by Bachet. In parallel, Fermat proposed the problem of representing every positive integer as a sum of at most n n -gonal numbers. Lagrange [7] proved the square

J. Lacalle: Dep. de Matemática Aplicada a las Tecnologías de la Información y las Comunicaciones, ETSI de Sistemas Informáticos, Universidad Politécnica de Madrid, C/ Alan Turing s/n, 28031, Madrid, Spain; e-mail: jlacalle@etsisi.upm.es

L.N. Gatti: Dep. de Matemática Aplicada a las Tecnologías de la Información y las Comunicaciones, ETSI de Sistemas Informáticos, Universidad Politécnica de Madrid, C/ Alan Turing s/n, 28031, Madrid, Spain; e-mail: ln.gatti@alumnos.upm.es

Mathematics Subject Classification (2010): Primary 11D09; Secondary 11H06

case of the Fermat polygonal number theorem in 1770, also solving Bachet's conjecture. Gauss [3] proved the triangular case in 1796 and the full polygonal number theorem was not solved until it was finally proven by Cauchy in 1813. Later, in 1834, Jacobi discovered a simple formula for the number of representations of an integer as the sum of four integer squares.

The same year in which Lagrange proved his theorem, Waring asked whether each natural number k has an associated positive integer s such that every natural number is the sum of at most s natural numbers to the power of k . For example, every natural number is the sum of at most 4 squares, 9 cubes, or 19 fourth powers. The affirmative answer to the Waring's problem, known as the Hilbert–Waring theorem, was provided by Hilbert in 1909.

A possible generalization of Lagrange's problem is the following: given natural numbers a, b, c and d , can we solve

$$n = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$$

for all positive integers n in integers x_1, x_2, x_3 and x_4 ? Lagrange's four-square theorem answered in the positive the case $a = b = c = d = 1$ and the general solution was given by Ramanujan [9]. He proved that if we assume, without loss of generality, that $a \leq b \leq c \leq d$ then there are exactly 54 possible choices for a, b, c and d such that the problem is solvable in integers x_1, x_2, x_3 and x_4 for all $n \in \mathbb{N}$.

Another possible generalization, due to Mordel [8], tries to represent positive definite integral binary quadratic forms instead of positive integers. He proved that the quadratic form $x^2 + y^2 + z^2 + u^2 + v^2$ represents all positive definite integral binary quadratic forms.

Sun [11] has proposed some refinements of the Lagrange's theorem such as, for example, the following: $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{Z}$ such that $x + y + z$ (or $x + 2y$, or $x + y + 2z$) is a square (or a cube).

The extension of the Lagrange's four-square theorem proposed in this article comes up from the study of the model of discrete quantum computation introduced by the authors [5]. In this model, the discrete quantum states (qubits) have Gaussian integers as coordinates, except for a normalization factor $\sqrt{2^{-k}}$. The model is constructed from two elementary quantum gates, H and G . The Hadamard gate H is one of the most relevant quantum gates that allows superposition, and therefore entanglement and parallelism.

The other gate, G , is a three qubit gate in which the first two are control qubits, while the third is the target. If the control qubits are in state $|1\rangle$ then the gate V is applied to the third qubit.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

These quantum gates allow the construction of all discrete states (states with integer real and imaginary parts, i.e. Gaussian integers, as coordinates). It is because of this fact

that the authors call the second gate G (for Gauss).

The model was designed to generate all discrete quantum states from the computational base. For this reason the proof of this fact was relatively simple. The defined discrete quantum gates in the model have discrete quantum states as columns (and as rows). As a matter of fact, the authors did not expect that the elementary quantum gates H and G could generate all discrete quantum gates, because this means simultaneously generating as many discrete quantum states as gate columns. But, surprisingly, this could be done and indicated to the authors that it might be true that an orthonormal system of discrete quantum states can always be completed to a base. In this article we include the simplest version of this problem, which was already presented as a conjecture at a conference by the authors [4].

The outline of the article is as follows: In section 2 we set up notations and discuss some basic properties. In section 3 we prove the main result. Finally, in section 4 we expose several generalizations and conjectures related to the proposed problem.

2 Notations and basic properties

We consider \mathbb{Z}^4 as a part of the vector space \mathbb{R}^4 provided with the inner product $\langle v|w \rangle = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$, where $v = (x_1, x_2, x_3, x_4)$ and $w = (y_1, y_2, y_3, y_4)$ are vectors of \mathbb{R}^4 , and with the canonical base $\{e_1, \dots, e_4\}$.

Given a set of linearly independent vectors $v_1, \dots, v_k \in \mathbb{R}^4$, they generate the *lattice* $\Lambda = \{b_1v_1 + \dots + b_kv_k \mid b_1, \dots, b_k \in \mathbb{Z}\}$ [1] and constitute a *base of* Λ , B . So the *dimension of* Λ will be k . From now on we will only consider bases whose vectors belong to \mathbb{Z}^4 , i.e. Λ will always be an *integral lattice*.

Given a point $v \in \Lambda$, described by its coordinates in B , $v = (b_i)_B$, the number $N(v) = \|v\|^2 = \langle v|v \rangle$ is called the *norm of* v and can be calculated by the expression $N(v) = b^t G b$, where G is the *Gram matrix* of the vectors of B . The determinant of G , $\det(G)$, is an invariant of Λ whose square root is denoted by $\det(\Lambda)$. So $\det(\Lambda) = \sqrt{\det(G)}$ and, geometrically, it is interpreted as the volume of the fundamental parallelepiped of Λ . The matrix G is symmetric and positive definite and is associated to a quadratic form that collects the main properties of Λ .

Let us consider the *coordinate matrix* V , formed by the vectors of the base B of Λ placed by rows. If V is a square matrix, we can compute the determinant of Λ from V , $\det(\Lambda) = |\det(V)|$, and it holds that $\det^2(V) = \det(G)$.

Given a set of vectors $v_1, \dots, v_k \in \mathbb{Z}^4$ such that $N(v_i) = p$ for all $1 \leq i \leq k$ and $\langle v_i|v_j \rangle = 0$ for all $1 \leq i < j \leq k$, we will say that $S = \{v_1, \dots, v_k\}$ is a *p-orthonormal system* and, if $k = 4$, that S is a *p-orthonormal base*. The *support of* S is $\text{supp}(S) = \{i \mid \exists j \text{ such that the } i\text{-coordinate of } v_j \neq 0\}$.

However, we are not interested in Λ , but rather in its *orthogonal lattice*

$$\Lambda^\perp = \{ v \in \mathbb{Z}^4 \mid \langle v_i | v \rangle = 0 \text{ for all } 1 \leq i \leq k \}$$

The resolution method of systems of linear Diophantine equations [2] computes a base of Λ^\perp with $4 - k$ vectors. Then the dimension of Λ^\perp will be $k^\perp = 4 - k$. In order to do this we have to solve the linear system $VX = 0$, computing the *Smith normal form* [10] of V and its *invariant factors* $\alpha_1, \dots, \alpha_k$:

$$LVR = \begin{pmatrix} \alpha_1 & & & \\ & \ddots & & \\ & & & \alpha_k \end{pmatrix} = N \quad \text{such that} \quad \begin{array}{l} L \in GL_k(\mathbb{Z}) \\ R \in GL_4(\mathbb{Z}) \\ 0 < \alpha_1, \dots, \alpha_k \\ \alpha_1 | \alpha_2, \dots, \alpha_{k-1} | \alpha_k \end{array}$$

Lemma 2.1. *Given a number $p \geq 1$ and a p -orthonormal system $S = \{ v_1, \dots, v_k \}$, $1 \leq k \leq 3$, with associated lattice Λ , then the last $4 - k$ columns of the matrix R , in the Smith normal form of V , constitute a base of Λ^\perp .*

Proof. It holds that $VX = 0 \Leftrightarrow LVR R^{-1}X = L0 = 0$ and, considering $Y = R^{-1}X$, we have that $VX = 0 \Leftrightarrow NY = 0 \Leftrightarrow y_1 = \dots = y_k = 0$. So, the base that generates the solutions of $VX = 0$ is $B^\perp = \{ R e_{k+1}, \dots, R e_4 \}$, i.e. the set with the last $4 - k$ columns of R . \square

Throughout the article we will use identities among polynomials in many variables whose demonstration only requires the polynomial expansion of the difference of both members of the equalities. We will call this type of proof *polynomial checking*.

Proposition 2.2. *Given a prime number p and a p -orthonormal system $S = \{ v_1, v_2 \}$, $v_1 = (x_1, \dots, x_4)$ and $v_2 = (y_1, \dots, y_4)$, with $|\text{supp}(S)| > 2$, then $\gcd(x_1, \dots, x_4) = \gcd(y_1, \dots, y_4) = 1$ and the invariant factors of V also verify $\alpha_1 = \alpha_2 = 1$.*

Proof. Suppose, by contradiction, that $\gcd(x_1, \dots, x_4) = g > 1$. Then $N(v_1) = g^2(x_1'^2 + \dots + x_4'^2) = p$, where $x_i' = \frac{x_i}{g}$ for all $1 \leq i \leq 4$, and this fact contradicts the primality of p . So, we have that $\gcd(x_1, \dots, x_4) = 1$ and in the same way we conclude that $\gcd(y_1, \dots, y_4) = 1$. Applying these results, together with the property of the first invariant factor, we get $\alpha_1 = 1$.

In order to obtain the value of α_2 we will use the following identity, that can be proved by polynomial checking:

$$N(v_1)N(v_2) - \langle v_1 | v_2 \rangle^2 = \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}^2 + \begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix}^2 + \dots + \begin{vmatrix} x_3 & x_4 \\ y_3 & y_4 \end{vmatrix}^2$$

By hypothesis, $N(v_1)N(v_2) - \langle v_1 | v_2 \rangle^2 = p^2$. Suppose, again by contradiction, that $g = \gcd(m_{12}, \dots, m_{34}) > 1$, where

$$m_{ij} = \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} \quad \text{and} \quad m'_{ij} = \frac{m_{ij}}{g}$$

Then $p^2 = g^2(m'_{12}{}^2 + \dots + m'_{34}{}^2)$ and there are, at least, two minors different from 0 because $|\text{supp}(S)| > 2$. These facts contradict the primality of p . So, we have that $\gcd(m_{12}, \dots, m_{34}) = 1$ and, since this value matches the second invariant factor, we get $\alpha_2 = 1$. \square

Finally, we introduce the fundamental result of the branch of number theory called the geometry of numbers, proved by Minkowski in 1889.

Theorem 2.3 (Minkowski [1]). *Let K be a convex set in \mathbb{R}^n which is symmetric with respect to the origin. If the volume of K is greater than 2^n times the volume of the fundamental domain (parallelepiped) of a lattice Λ , then K contains a non-zero lattice point.*

3 Extended Lagrange's four-square theorem

We are dealing with the following problem: given a prime number p and a p -orthonormal system $S = \{v_1, \dots, v_k\}$, $1 \leq k \leq 3$, with associated lattice Λ , prove that there exists $v_{k+1} \in \Lambda^\perp$ with norm $N(v_{k+1}) = p$.

Remark 3.1. If the p -orthonormal system S has a single vector $v_1 = (x_1, x_2, x_3, x_4)$, the solution (valid for all $p \geq 1$) is trivial: $v_2 = (x_2, -x_1, x_4, -x_3)$.

Remark 3.2. If the p -orthonormal system S has two vectors and $|\text{supp}(S)| = 2$, the solution (also valid for all $p \geq 1$) is as well trivial. Suppose, without loss of generality, that $\text{supp}(S) = \{1, 2\}$ and that $v_1 = (x_1, x_2, 0, 0)$. Then, the required vector is, for example, $v_3 = (0, 0, x_1, x_2)$.

3.1 Three vectors p -orthonormal systems

If the p -orthonormal system has three vectors, their exterior product allows us to obtain the required vector.

Proposition 3.3. *Given a number $p \geq 1$ and a p -orthonormal system $S = \{v_1, v_2, v_3\}$, with associated lattice Λ , there exists $v_4 \in \Lambda^\perp$ such that $N(v_4) = p$.*

Proof. Given the coordinates of the three vectors of S , $v_1 = (x_1, x_2, x_3, x_4)$, $v_2 = (y_1, y_2, y_3, y_4)$ and $v_3 = (z_1, z_2, z_3, z_4)$, we consider the exterior product $t = (t_1, t_2, t_3, t_4)$ where

$$t_1 = - \begin{vmatrix} x_2 & x_3 & x_4 \\ y_2 & y_3 & y_4 \\ z_2 & z_3 & z_4 \end{vmatrix} \quad \dots \quad t_4 = \begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix}$$

It can be proved that $t \in \Lambda^\perp$, by polynomial checking of $\langle v_i | t \rangle = 0$, $1 \leq i \leq 3$, and that $t_i^2 = p^2(p - x_i^2 - y_i^2 - z_i^2)$, $1 \leq i \leq 4$. In order to check the last equality, for example for $i = 4$, it is enough to verify, by polynomial checking, that

$$t_4^2 = N(x)N(y)N(z) + 2\langle x|y\rangle\langle x|z\rangle\langle y|z\rangle - N(x)\langle y|z\rangle^2 - N(y)\langle x|z\rangle^2 - N(z)\langle x|y\rangle^2,$$

where $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$ and $z = (z_1, z_2, z_3)$, to replace the following values

$$\begin{aligned} N(x) &= p - x_4^2 & \langle x|y \rangle &= -x_4 y_4 \\ N(y) &= p - y_4^2 & \langle x|z \rangle &= -x_4 z_4 \\ N(z) &= p - z_4^2 & \langle y|z \rangle &= -y_4 z_4 \end{aligned}$$

and to test the expression obtained by replacing t_4^2 with $p^2(p - x_4^2 - y_4^2 - z_4^2)$ by polynomial checking. Finally, $v_4 = \frac{t}{p}$ has the required properties: $v_4 \in \Lambda^\perp$ and $N(v_4) = p$. \square

3.2 A two vectors p -orthonormal system S with $|\text{supp}(S)| > 2$

First of all, let us get a base of Λ^\perp , B^\perp , by computing a Smith quasi-normal form in which $L \in GL_k(\mathbb{Q})$. Note that in this case lemma 2.1 also holds. Let V be the coordinate matrix of the p -orthonormal system $S = \{v_1, v_2\}$ with $|\text{supp}(S)| > 2$, $v_1 = (x_1, x_2, x_3, x_4)$, $v_2 = (y_1, y_2, y_3, y_4)$ and $p \geq 1$. Suppose, rearranging the coordinates of v_1 and v_2 if necessary, that

$$x_1 \neq 0, \quad \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \neq 0 \quad \text{and} \quad 4 \in \text{supp}(S), \text{ i.e. } x_4 \neq 0 \text{ or } y_4 \neq 0$$

The Smith quasi-normal form of S is:

$$LVR = \begin{pmatrix} c & 0 & 0 & 0 \\ 0 & cd & 0 & 0 \end{pmatrix} \quad \text{such that} \quad \begin{aligned} L &\in GL_k(\mathbb{Q}) \\ R &\in GL_4(\mathbb{Z}) \\ 0 &< c, d \\ R &= R_1 R_2 R_3 R_4 R_5 \end{aligned}$$

where the matrices L and R_i , $1 \leq i \leq 5$, and the parameters c and d are those that appear in table 1.

Lemma 3.4. *Given a number $p \geq 1$ and a p -orthonormal system $S = \{v_1, v_2\}$ with associated lattice Λ , then $B^\perp = \{w_1, w_2\}$ is a base of Λ^\perp , where*

$$\begin{aligned} w_1 &= \left(\frac{x_2 y'_3}{c_1 d_1} - \frac{x_3 y'_2 \sigma_1}{c_2 d_1}, -\frac{x_1 y'_3}{c_1 d_1} - \frac{x_3 y'_2 \tau_1}{c_2 d_1}, \frac{c_1 y'_2}{c_2 d_1}, 0 \right) \\ w_2 &= \left(\frac{y'_4(c_1 x_3 \sigma_1 \tau_4 + c_2 x_2 \sigma_4)}{c_1 c_2 d} - \frac{d_1 x_4 \sigma_1 \sigma_2}{c d}, \right. \\ &\quad \left. \frac{y'_4(c_1 x_3 \tau_1 \tau_4 - c_2 x_1 \sigma_4)}{c_1 c_2 d} - \frac{d_1 x_4 \sigma_2 \tau_1}{c d}, -\frac{d_1 x_4 \tau_2}{c d} - \frac{c_1 y'_4 \tau_4}{c_2 d}, \frac{c_2 d_1}{c d} \right) \end{aligned}$$

$R_1 = \begin{pmatrix} \sigma_1 & \frac{-x_2}{c_1} & 0 & 0 \\ \tau_1 & \frac{x_1}{c_1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{aligned} x_1\sigma_1 + x_2\tau_1 &= c_1 = \gcd(x_1, x_2) \\ y'_1 &= \sigma_1 y_1 + \tau_1 y_2 \\ y'_2 &= \frac{-x_2}{c_1} y_1 + \frac{x_1}{c_1} y_2 \end{aligned}$
$R_2 = \begin{pmatrix} \sigma_2 & 0 & \frac{-x_3}{c_2} & 0 \\ 0 & 1 & 0 & 0 \\ \tau_2 & 0 & \frac{c_1}{c_2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{aligned} c_1\sigma_2 + x_3\tau_2 &= c_2 = \gcd(c_1, x_3) \\ y''_1 &= \sigma_2 y'_1 + \tau_2 y_3 = \sigma_2\sigma_1 y_1 + \sigma_2\tau_1 y_2 + \tau_2 y_3 \\ y'_3 &= \frac{-x_3}{c_2} y'_1 + \frac{c_1}{c_2} y_3 = \frac{-x_3}{c_2} \sigma_1 y_1 + \frac{-x_3}{c_2} \tau_1 y_2 + \frac{c_1}{c_2} y_3 \end{aligned}$
$R_3 = \begin{pmatrix} \sigma_3 & 0 & 0 & \frac{-x_4}{c} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \tau_3 & 0 & 0 & \frac{c_2}{c} \end{pmatrix}$	$\begin{aligned} c_2\sigma_3 + x_4\tau_3 &= c = \gcd(c_2, x_4) \\ y'''_1 &= \sigma_3 y''_1 + \tau_3 y_4 = \sigma_3\sigma_2\sigma_1 y_1 + \sigma_3\sigma_2\tau_1 y_2 + \sigma_3\tau_2 y_3 + \tau_3 y_4 \\ y'_4 &= \frac{-x_4}{c} y''_1 + \frac{c_2}{c} y_4 = \frac{-x_4}{c} \sigma_2\sigma_1 y_1 + \frac{-x_4}{c} \sigma_2\tau_1 y_2 + \frac{-x_4}{c} \tau_2 y_3 + \frac{c_2}{c} y_4 \end{aligned}$
$L = \begin{pmatrix} 1 & 0 \\ -y'''_1 & c \end{pmatrix}$	
$R_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sigma_4 & \frac{-y'_3}{d_1} & 0 \\ 0 & \tau_4 & \frac{y'_2}{d_1} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$y'_2\sigma_4 + y'_3\tau_4 = d_1 = \gcd(y'_2, y'_3)$
$R_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sigma_5 & 0 & \frac{-y'_4}{d} \\ 0 & 0 & 1 & 0 \\ 0 & \tau_5 & 0 & \frac{d_1}{d} \end{pmatrix}$	$d_1\sigma_5 + y'_4\tau_5 = d = \gcd(d_1, y'_4)$

Table 1: Smith quasi-normal form data.

Proof. We obtain the result just by multiplying the matrices R_1, R_2, R_3, R_4 and R_5 and applying lemma 2.1 to the Smith quasi-normal form of S . \square

Remark 3.5. Let V and G_V be the coordinate matrix and the Gram matrix, respectively, of the set of vectors $B \cup B^\perp$ and let G be the Gram matrix of the set of vectors B^\perp . Then, $\det^2(V) = \det(G_V) = p^2 \det(G)$ and, since $\det^2(\Lambda^\perp) = \det(G)$, we concluded that $\det(\Lambda^\perp) = \frac{|\det(V)|}{p}$.

We can use remark 3.5 to compute $\det(\Lambda^\perp)$ and, indirectly, to study the matrix G , considered as a symmetric positive definite quadratic form.

Proposition 3.6. Given a number $p \geq 1$ and a p -orthonormal system $S = \{v_1, v_2\}$, with associated lattice Λ , then $\det(\Lambda^\perp) = \frac{p}{cd}$, where c and d are the parameters that appear in table 1.

Proof. To obtain the result we only have to compute $\det(V)$, by remark 3.5. Developing the expression of the determinant of V , where w_1 and w_2 are the vectors obtained in

1		$c_1 c_2 x_1^2 y_2^2$	2		$c_1 c_2 x_1^2 y_3^2$	3		$c_1 c_2 x_1^2 y_4^2$
4		$-2c_1 c_2 x_1 x_2 y_1 y_2$	5	×	$-c_1 c_2 x_1 x_3 y_1 y_3$	6	×	$-c_1 c_2 x_1 x_4 y_1 y_4$
7		$c_1 c_2 x_2^2 y_1^2$	8		$c_1 c_2 x_2^2 y_3^2$	9		$c_1 c_2 x_2^2 y_4^2$
10	×	$-c_1 c_2 x_2 x_3 y_2 y_3$	11	×	$-c_1 c_2 x_2 x_4 y_2 y_4$	12		$c_1 c_2 x_3^2 y_4^2$
13	×	$-c_1 c_2 x_3 x_4 y_3 y_4$	14	×	$-c_1 x_1^2 x_4 y_1 y_4 \sigma_1 \sigma_2$	15	×	$-c_1 x_1 x_2 x_4 y_1 y_4 \sigma_2 \tau_1$
16	×	$-c_1 x_1 x_2 x_4 y_2 y_4 \sigma_1 \sigma_2$	17	×	$-c_1 x_1 x_3 x_4 y_3 y_4 \sigma_1 \sigma_2$	18	×	$c_1 x_1 x_4^2 y_1^2 \sigma_1 \sigma_2$
19	×	$c_1 x_1 x_4^2 y_2^2 \sigma_1 \sigma_2$	20	×	$c_1 x_1 x_4^2 y_3^2 \sigma_1 \sigma_2$	21	×	$-c_1 x_2^2 x_4 y_2 y_4 \sigma_2 \tau_1$
22	×	$-c_1 x_2 x_3 x_4 y_3 y_4 \sigma_2 \tau_1$	23	×	$c_1 x_2 x_4^2 y_1^2 \sigma_2 \tau_1$	24	×	$c_1 x_2 x_4^2 y_2^2 \sigma_2 \tau_1$
25	×	$c_1 x_2 x_4^2 y_3^2 \sigma_2 \tau_1$	26	×	$-c_1 x_3^2 x_4 y_1 y_4 \sigma_1 \sigma_2$	27	×	$-c_1 x_3^2 x_4 y_2 y_4 \sigma_2 \tau_1$
28	×	$-c_1 x_3^2 x_4 y_3 y_4 \tau_2$	29	×	$c_1 x_3 x_4^2 y_1 y_3 \sigma_1 \sigma_2$	30	×	$c_1 x_3 x_4^2 y_2 y_3 \sigma_2 \tau_1$
31	×	$c_1 x_3 x_4^2 y_3^2 \tau_2$	32	×	$-c_2 x_1^2 x_3 y_1 y_3 \sigma_1$	33	×	$-c_2 x_1 x_2 x_3 y_1 y_3 \tau_1$
34	×	$-c_2 x_1 x_2 x_3 y_2 y_3 \sigma_1$	35	×	$c_2 x_1 x_3^2 y_1^2 \sigma_1$	36	×	$c_2 x_1 x_3^2 y_2^2 \sigma_1$
37	×	$-c_2 x_2^2 x_3 y_2 y_3 \tau_1$	38	×	$c_2 x_2 x_3^2 y_1^2 \tau_1$	39	×	$c_2 x_2 x_3^2 y_2^2 \tau_1$
40	×	$-x_1^2 x_3 x_4 y_1 y_4 \sigma_1 \tau_2$	41	×	$-x_1 x_2 x_3 x_4 y_1 y_4 \tau_1 \tau_2$	42	×	$-x_1 x_2 x_3 x_4 y_2 y_4 \sigma_1 \tau_2$
43	×	$x_1 x_3^2 x_4 y_1 y_4 \sigma_1^2 \sigma_2$	44	×	$x_1 x_3^2 x_4 y_2 y_4 \sigma_1 \sigma_2 \tau_1$	45	×	$x_1 x_3 x_4^2 y_1^2 \sigma_1 \tau_2$
46	×	$-x_1 x_3 x_4^2 y_1 y_3 \sigma_1^2 \sigma_2$	47	×	$x_1 x_3 x_4^2 y_2^2 \sigma_1 \tau_2$	48	×	$-x_1 x_3 x_4^2 y_2 y_3 \sigma_1 \sigma_2 \tau_1$
49	×	$-x_2^2 x_3 x_4 y_2 y_4 \tau_1 \tau_2$	50	×	$x_2 x_3^2 x_4 y_1 y_4 \sigma_1 \sigma_2 \tau_1$	51	×	$x_2 x_3^2 x_4 y_2 y_4 \sigma_2 \tau_1^2$
52	×	$x_2 x_3 x_4^2 y_1^2 \tau_1 \tau_2$	53	×	$-x_2 x_3 x_4^2 y_1 y_3 \sigma_1 \sigma_2 \tau_1$	54	×	$x_2 x_3 x_4^2 y_2^2 \tau_1 \tau_2$
55	×	$-x_2 x_3 x_4^2 y_2 y_3 \sigma_2 \tau_1^2$						

Table 2: Monomials of $\det(V)c_1 c_2 c d$.

lemma 3.4, we obtain:

$$\begin{aligned}
\det(V)c_1 c_2 d_1 c d &= c y_4' (c_1 (x_1^2 y_4 - x_1 x_4 y_1 + x_2 (x_2 y_4 - x_4 y_2)) + \\
&\quad x_3 (\underline{x_1 \sigma_1 + x_2 \tau_1}) (x_3 y_4 - x_4 y_3)) (y_2' \sigma_4 + y_3' \tau_4) + \\
&\quad d_1 (c_1^2 y_2' (c_2 (x_1 y_2 - x_2 y_1) + x_1 x_4 y_4 \sigma_2 \tau_1 - \\
&\quad x_4 \sigma_2 (x_2 y_4 \sigma_1 + x_4 (y_1 \tau_1 - y_2 \sigma_1))) + \\
&\quad c_1 x_3 y_2' (c_2 (x_1 y_3 \tau_1 - x_2 y_3 \sigma_1 + x_3 (y_2 \sigma_1 - y_1 \tau_1)) + \\
&\quad x_4 \tau_2 (x_1 y_4 \tau_1 - x_2 y_4 \sigma_1 + x_4 (y_2 \sigma_1 - y_1 \tau_1))) + \\
&\quad c_2 y_3' (c_2 (x_1^2 y_3 - x_1 x_3 y_1 + x_2 (x_2 y_3 - x_3 y_2)) + \\
&\quad x_4 (x_1^2 y_4 \tau_2 - x_1 (x_3 y_4 \sigma_1 \sigma_2 + x_4 (y_1 \tau_2 - y_3 \sigma_1 \sigma_2)) + \\
&\quad x_2 (x_2 y_4 \tau_2 - x_3 y_4 \sigma_2 \tau_1 + x_4 (y_3 \sigma_2 \tau_1 - y_2 \tau_2))))))
\end{aligned}$$

where all the parameters appear in table 1.

Throughout the proof we will replace expressions by applying equalities from table 1.

Substituting the underlined expressions by c_1 and d_1 respectively, all occurrences of d_1 are canceled. Similarly, substituting $c_1 y_2'$, $c_2 y_3'$ and $c y_4'$ for the expressions

$$\begin{aligned}
&x_1 y_2 - x_2 y_1, \\
&c_1 y_3 - x_3 (\sigma_1 y_1 + \tau_1 y_2) \text{ and} \\
&c_2 y_4 - x_4 (\sigma_2 \sigma_1 y_1 + \sigma_2 \tau_1 y_2 + \tau_2 y_3)
\end{aligned}$$

respectively, the parameter c disappears from the second equality member.

The expression $\det(V)c_1 c_2 c d$ is a homogeneous polynomial of total degree 6 in the variables $c_1, c_2, x_1, x_2, x_3, x_4, y_1, y_2, y_3$ and y_4 , in which only the parameters $\sigma_1, \tau_1, \sigma_2$

14	×	15	$-c_1^2 x_1 x_4 y_1 y_4 \sigma_2$	16	×	21	$-c_1^2 x_2 x_4 y_2 y_4 \sigma_2$
17	×	22	$-c_1^2 x_3 x_4 y_3 y_4 \sigma_2$	18	×	23	$c_1^2 x_4^2 y_1^2 \sigma_2$
19	×	24	$c_1^2 x_4^2 y_2^2 \sigma_2$	20	×	25	$c_1^2 x_4^2 y_3^2 \sigma_2$
32	×	33	$-c_1 c_2 x_1 x_3 y_1 y_3$	34	×	37	$-c_1 c_2 x_2 x_3 y_2 y_3$
35		38	$c_1 c_2 x_3^2 y_1^2$	36		39	$c_1 c_2 x_3^2 y_2^2$
40	×	41	$-c_1 x_1 x_3 x_4 y_1 y_4 \tau_2$	42	×	49	$-c_1 x_2 x_3 x_4 y_2 y_4 \tau_2$
43	×	50	$c_1 x_3^2 x_4 y_1 y_4 \sigma_1 \sigma_2$	44	×	51	$c_1 x_3^2 x_4 y_2 y_4 \sigma_2 \tau_1$
45	×	52	$c_1 x_3 x_4^2 y_1^2 \tau_2$	46	×	53	$-c_1 x_3 x_4^2 y_1 y_3 \sigma_1 \sigma_2$
47	×	54	$c_1 x_3 x_4^2 y_2^2 \tau_2$	48	×	55	$-c_1 x_3 x_4^2 y_2 y_3 \sigma_2 \tau_1$
14	×	40	$-c_1 c_2 x_1 x_4 y_1 y_4$	16	×	42	$-c_1 c_2 x_2 x_4 y_2 y_4$
17	×	28	$-c_1 c_2 x_3 x_4 y_3 y_4$	18		45	$c_1 c_2 x_4^2 y_1^2$
19		47	$c_1 c_2 x_4^2 y_2^2$	20		31	$c_1 c_2 x_4^2 y_3^2$
26	×	43	0	27	×	44	0
29	×	46	0	30	×	48	0
5		32	$-2c_1 c_2 x_1 x_3 y_1 y_3$	6		14	$-2c_1 c_2 x_1 x_4 y_1 y_4$
10		34	$-2c_1 c_2 x_2 x_3 y_2 y_3$	11		16	$-2c_1 c_2 x_2 x_4 y_2 y_4$
13		17	$-2c_1 c_2 x_3 x_4 y_3 y_4$				

Table 3: Monomials resulting from operations.

and τ_2 appear. The monomials of the aforementioned polynomial are included in table 2 and are identified by indexes placed in the first cells of the corresponding rows.

In order to eliminate the parameters σ_1 , τ_1 , σ_2 and τ_2 , we group the monomials of the table 2 in pairs to apply the following operations:

- (1) Substitute $x_1 \sigma_1 + x_2 \tau_1$ by c_1 .
- (2) Substitute $c_1 \sigma_2 + x_3 \tau_2$ by c_2 .
- (3) Cancel opposite monomials.
- (4) Add equal monomials.

Applied operations are detailed in table 3, where the resulting monomials are identified by the indexes of the first monomials that are operated on. Each time an operation is applied, the monomials involved are marked with a \times to the right of the index that identifies the monomial, so as not to use them again. The operations are done iteratively on monomials of tables 2 and 3 that are not marked, until no operation can be further applied.

All the resulting monomials have the factor $c_1 c_2$. Therefore, by simplifying this factor the next equality is obtained:

$$\begin{aligned}
 \det(V)cd &= x_1^2 y_2^2 + x_1^2 y_3^2 + x_1^2 y_4^2 - 2x_1 x_2 y_1 y_2 - 2x_1 x_3 y_1 y_3 - 2x_1 x_4 y_1 y_4 \\
 &\quad x_2^2 y_1^2 + x_2^2 y_3^2 + x_2^2 y_4^2 - 2x_2 x_3 y_2 y_3 - 2x_2 x_4 y_2 y_4 + x_3^2 y_4^2 \\
 &\quad - 2x_3 x_4 y_3 y_4 + x_4^2 y_1^2 + x_4^2 y_2^2 + x_4^2 y_3^2 + x_3^2 y_1^2 + x_3^2 y_2^2
 \end{aligned}$$

$c_1^2 x_1^2 y_2^2$	$-2c_1 x_1^2 x_3 y_1 y_3 \sigma_1$	$-2c_1^2 x_1 x_3 y_1 y_3$	$-2c_1 x_1 x_2 x_3 y_2 y_3 \sigma_1$	$-2c_1^2 x_2 x_3 y_2 y_3$
$c_1^2 x_1^2 y_3^2$	$-2c_1 x_1 x_2 x_3 y_1 y_3 \tau_1$		$-2c_1 x_2^2 x_3 y_2 y_3 \tau_1$	
$-2c_1^2 x_1 x_2 y_1 y_2$	$x_1^2 x_3^2 y_1^2 \sigma_1^2$	$c_1^2 x_3^2 y_1^2$	$x_1^2 x_3^2 y_2^2 \sigma_1^2$	$c_1^2 x_3^2 y_2^2$
$c_1^2 x_2^2 y_1^2$	$x_2^2 x_3^2 y_1^2 \tau_1^2$		$x_2^2 x_3^2 y_2^2 \tau_1^2$	
$c_1^2 x_2^2 y_3^2$	$2x_1 x_2 x_3^2 y_1^2 \sigma_1 \tau_1$		$2x_1 x_2 x_3^2 y_2^2 \sigma_1 \tau_1$	

Table 4: Monomials of $N(w_1)c_1^2 c_2^2 d_1^2$.

By polynomial checking, it is easy to verify the next equality:

$$\det(V)cd = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) - (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2$$

By hypothesis, the second member of the previous equality is equal to p^2 . Therefore, by applying remark 3.5, we conclude that:

$$\det(\Lambda^\perp) = \frac{p}{cd} \quad \square$$

Lemma 3.7. *Given a number $p \geq 1$, a p -orthonormal system $S = \{v_1, v_2\}$ and w_1 the first vector of the base B^\perp of the orthogonal lattice Λ^\perp , then $N(w_1) = \frac{p(p - x_4^2 - y_4^2)}{c_2^2 d_1^2}$, where c_2 and d_1 are the parameters in table 1.*

Proof. The proof is similar to that of proposition 3.6. Considering the vector w_1 obtained in lemma 3.4 and calculating $N(w_1)$, the following equality is obtained:

$$N(w_1)c_1^2 c_2^2 d_1^2 = c_1^4 y_2'^2 + c_1^2 x_3^2 y_2'^2 (\sigma_1^2 + \tau_1^2) + 2c_1 c_2 x_3 y_2' y_3' (x_1 \tau_1 - x_2 \sigma_1) + c_2^2 y_3'^2 (x_1^2 + x_2^2)$$

Substituting in the second member of equality $c_1 y_2'$ by $-x_2 y_1 + x_1 y_2$ and $c_2 y_3'$ by $-x_3 \sigma_1 y_1 - x_3 \tau_1 y_2 + c_1 y_3$, a homogeneous polynomial of total grade 6 in the variables c_1 , x_1 , x_2 , x_3 , y_1 , y_2 and y_3 is obtained, in which only the parameters σ_1 and τ_1 appear.

The monomials of the aforementioned polynomial are listed in table 4. The results of the following substitution are also included in the table: replace $x_1 \sigma_1 + x_2 \tau_1$ by c_1 .

All the remaining monomials are multiplied by the factor c_1^2 . Therefore, simplifying this factor, we obtain:

$$\begin{aligned} N(w_1)c_2^2 d_1^2 &= x_1^2 y_2^2 + x_1^2 y_3^2 - 2x_1 x_2 y_1 y_2 + x_2^2 y_1^2 + x_2^2 y_3^2 \\ &\quad - 2x_1 x_3 y_1 y_3 - 2x_2 x_3 y_2 y_3 + x_3^2 y_1^2 + x_3^2 y_2^2 \end{aligned}$$

By polynomial checking, it is easy to verify the next equality:

$$\begin{aligned} N(w_1)c_2^2 d_1^2 &= (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &\quad - (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2 - x_4^2 (y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &\quad - y_4^2 (x_1^2 + x_2^2 + x_3^2 + x_4^2) + 2x_4 y_4 (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4) \end{aligned}$$

By hypothesis, the second member of the previous equality is equal to $p^2 - px_4^2 - py_4^2$. Therefore, we conclude that:

$$N(w_1) = \frac{p(p - x_4^2 - y_4^2)}{c_2^2 d_1^2} \quad \square$$

Lemma 3.8. *Given a prime number p and a p -orthonormal system $S = \{v_1, v_2\}$ with $|\text{supp}(S)| > 2$, associated to the lattice Λ , then $c = d = 1$, where c and d are the parameters that appear in table 1.*

Proof. According to table 1 it holds that $c = \gcd(x_1, x_2, x_3, x_4)$ and, by proposition 2.2, we conclude that $c = 1$. This result implies that the Smith quasi-normal form described in table 1 is actually a normal form, because in this case $L \in GL_k(\mathbb{Z})$, and consequently d is the second invariant factor of V . Considering once more proposition 2.2 we conclude that $d = 1$. \square

Proposition 3.9. *Given a prime number p , a p -orthonormal system $S = \{v_1, v_2\}$ with $|\text{supp}(S)| > 2$ and the Gram matrix G of the base $B^\perp = \{w_1, w_2\}$ of the orthogonal lattice Λ^\perp , then it holds that $p \mid G$.*

Proof. Suppose that the Gram matrix $G = \begin{pmatrix} \mu & \lambda \\ \lambda & \nu \end{pmatrix}$.

Let us consider the value of $\mu = N(w_1)$ obtained in lemma 3.7. The prime factorization of $p(p - x_4^2 - y_4^2)$ contains only one factor p , because p is prime and $-p < p - x_4^2 - y_4^2 < p$ (remember that we are assuming that $x_4 \neq 0$ or $y_4 \neq 0$). Then, the prime factorization of $c_2^2 d_1^2$ does not contain p , because the number of times it contains each prime factor is even. Consequently $c_2^2 d_1^2 \mid (p - x_4^2 - y_4^2)$ and this implies that $p \mid \mu$, i.e. $\mu = p\mu'$. Moreover, $|\mu'| < p$.

Applying proposition 3.6, lemma 3.8 and the property $\det^2(\Lambda^\perp) = \det(G)$, we get $p^2 = p\mu'\nu - \lambda^2$. This implies $p \mid \lambda^2$ and, keeping in mind that p is a prime, we have that $p \mid \lambda$, i.e. $\lambda = p\lambda'$.

Reconsidering the previous equality, and canceling a factor p , we obtain $p = \mu'\nu - p\lambda'^2$. This implies again that $p \mid \mu'\nu$ and, considering that p is prime and $|\mu'| < p$, we get $p \mid \nu$, i.e. $\nu = p\nu'$.

We arrive to the final conclusion that $G = p \begin{pmatrix} \mu' & \lambda' \\ \lambda' & \nu' \end{pmatrix}$, i.e. $p \mid G$. \square

Theorem 3.10. *Given a prime number p , a p -orthonormal system $S = \{v_1, v_2\}$ with $|\text{supp}(S)| > 2$ and associated lattices Λ and Λ^\perp , there exists $v_3 \in \Lambda^\perp$ such that it verifies $N(v_3) = p$.*

Proof. Let G be the Gram matrix of the base B^\perp of the associated lattice Λ^\perp .

Proposition 3.6, lemma 3.8 and property $\det^2(\Lambda^\perp) = \det(G)$ allow us to conclude that $\det(G) = p^2$. Applying now proposition 3.9 we obtain that $G' = \frac{G}{p}$ is an unimodular matrix, i.e. $G' \in GL_2(\mathbb{Z})$, and that, given a vector $v_3 \in \Lambda^\perp$, $N(v_3) = b^t G b = p$ if and only if $b^t G' b = 1$, b being the coordinate vector of v_3 in the base B^\perp .

Let $K = \{x \in \mathbb{R}^2 \mid x^t G' x \leq 1\}$ and $\{u_1, u_2\}$ be an orthonormal base of eigenvectors of G' with eigenvalues λ_1 and λ_2 respectively. Note that λ_1 and λ_2 are real, since G' is symmetric, positive, because G' is definite positive, and verify $\lambda_1 \lambda_2 = \det(G') = 1$. Then K is the ellipse $\lambda_1 x^2 + \lambda_2 y^2 \leq 1$, with respect to the reference system determined by u_1 and u_2 , and has volume $\pi \frac{1}{\sqrt{\lambda_1}} \frac{1}{\sqrt{\lambda_2}} = \pi$.

Given a $0 < \epsilon < 1$, let be E_ϵ the ellipse K scaled by a factor $f_\epsilon = \frac{2}{\sqrt{\pi}} + \epsilon$. The ellipse E_ϵ has volume $\pi f_\epsilon^2 > \pi \frac{2^2}{\pi} = 2^2$. Then, for the Theorem 2.3, there exists a point b in the lattice \mathbb{Z}^2 (with volume of the fundamental domain 1) such that $b \neq 0$ and $b \in E_\epsilon$. Since the set of points of \mathbb{Z}^2 that belong to any of the ellipses E_ϵ is finite, it is shown that there is a point b in the lattice \mathbb{Z}^2 such that $b \neq 0$ and $b \in K$.

The point b defines a vector $v_3 \in \Lambda^\perp$ that verifies $0 < b^t G' b \leq 1$. Then, it holds $b^t G' b = 1$, since $b^t G' b$ is integer, and, at last, is the wanted vector of Λ^\perp , because $N(v_3) = b^t G b = p$. \square

3.3 Extensions of p -orthonormal systems

Putting together remark 3.1, remark 3.2, proposition 3.3 and theorem 3.10, we obtain the following theorem.

Theorem 3.11. *Given a prime number p and a p -orthonormal system in \mathbb{Z}^4 , S , then S can be extended to a p -orthonormal base.*

4 Generalizations and conjectures

We have proved that every p -orthonormal system of vectors in \mathbb{Z}^4 can be extended to a p -orthonormal base if p is a prime number. Besides, we have verified the result for every $1 \leq p \leq 10000$. In this section, all verifications for given values of p and n have been made by exhaustive checking of all p -orthonormal systems in \mathbb{Z}^n . From the previous results we conjecture that the following result holds.

Conjecture 4.1. *Given an integer number $p \geq 1$ and a p -orthonormal system in \mathbb{Z}^4 , S , then S can be extended to a p -orthonormal base.*

The most natural generalization of the problem is to consider it in any dimension $n \geq 1$, i.e. to study the problem in \mathbb{Z}^n .

Problem 4.2. *Given an integer number $p \geq 1$ and a p -orthonormal system in \mathbb{Z}^n , S , can S be extended to a p -orthonormal base?*

This problem arose from the study of discrete quantum states [5], for quantum computing. Because the dimension of the vector space of these states (m -qubits) is 2^m , it would be expected that the result would be fulfilled for these dimensions.

An analogous construction to that given in remark 3.1 shows the result for $n = 2$. Note that if p cannot be written as a sum of two squares [6] (the prime decomposition of p contains a prime congruent to 3 mod 4 raised to an odd power), there are no p -orthonormal systems in \mathbb{Z}^2 . The case of dimension 4 has already been studied and, in the case $n = 8$, we have checked the result for $1 \leq p \leq 36$.

To analyze the problem in other dimensions we try to find counterexamples that help us to understand in which cases the problem has a positive answer. If p is not a square and there exists a p -orthonormal base in \mathbb{Z}^n then there are counterexamples for p in dimension $n + 1$. Indeed, let $\{v_1 \dots, v_n\}$ be a p -orthonormal base in dimension n . Then $\{w_1 \dots, w_n\}$ is a p -orthonormal system in dimension $n + 1$ that cannot be extended to a p -orthonormal base, being:

$$w_j = (v_{j,1}, \dots, v_{j,n}, 0) \quad 1 \leq j \leq n$$

This construction allows us to find counterexamples for any dimension $n \not\equiv 0 \pmod{4}$, $n \not\equiv 1$ and $n \not\equiv 2$. Given an integer $p \geq 1$, we consider the p -orthonormal base in \mathbb{Z}^4 $S_1 = \{v_1, v_2, v_3, v_4\}$ and the matrix A ,

$$\begin{aligned} v_1 &= (x_1, x_2, x_3, x_4) \\ v_2 &= (-x_2, x_1, -x_4, x_3) \\ v_3 &= (-x_3, x_4, x_1, -x_2) \\ v_4 &= (x_4, x_3, -x_2, -x_1) \end{aligned} \quad \text{and} \quad A = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & -x_4 & x_3 \\ -x_3 & x_4 & x_1 & -x_2 \\ x_4 & x_3 & -x_2 & -x_1 \end{pmatrix},$$

where $p = x_1^2 + x_2^2 + x_3^2 + x_4^2$. If p can be written as a sum of two squares, $p = y_1^2 + y_2^2$, we define the p -orthonormal base in \mathbb{Z}^2 $S_2 = \{u_1, u_2\}$ and the matrix B ,

$$\begin{aligned} u_1 &= (y_1, y_2) \\ u_2 &= (-y_2, y_1) \end{aligned} \quad \text{and} \quad B = \begin{pmatrix} y_1 & y_2 \\ -y_2 & y_1 \end{pmatrix}.$$

Then, the rows of the matrices C_1, C_2 y C_3 define non-extensible p -orthonormal systems.

- (i) C_1 if p is not a square, $n = 1 \pmod{4}$ and $n \neq 1$.
- (ii) C_2 if p cannot be written as a sum of two squares, $n = 2 \pmod{4}$ and $n \neq 2$.
- (iii) C_3 if p is not a square and can be written as a sum of two squares and $n = 3 \pmod{4}$.

$$C_1 = \begin{pmatrix} A & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & A & 0 \end{pmatrix} \quad C_2 = \begin{pmatrix} A & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & A & 0 & 0 \end{pmatrix} \quad C_3 = \begin{pmatrix} A & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & A & 0 & 0 \\ 0 & \cdots & 0 & B & 0 \end{pmatrix}$$

The experimental verifications and the previous counterexamples make us think that the generalization of conjecture 4.1 should be the following.

Conjecture 4.3. Given numbers $n = 0 \pmod{4}$ ($n \geq 1$) and $p \geq 1$ and a p -orthonormal system in \mathbb{Z}^n , S , then S can be extended to a p -orthonormal base.

But, what happens if p is a square? We have verified the result for $n = 3, 5$ and $1^2 \leq p \leq 100^2$, $n = 6$ and $1^2 \leq p \leq 33^2$, $n = 7$ and $1^2 \leq p \leq 13^2$ and $n = 9$ and $1^2 \leq p \leq 2^2$. Nevertheless, we have found that the problem 4.2 has a negative answer if $n = 9$, $p = 9$ and $S = \{(1, \dots, 1)\}$. This counterexample can be generalized as follows: if $n = \bar{n}^2$ and $p = n\bar{p}^2$ are odd integers, then the set $S = \{v_1 = (\bar{p}, \dots, \bar{p})\}$ cannot be extended to a p -orthonormal base in \mathbb{Z}^n . Indeed, S cannot be extended with a vector v_2 because, on one hand, the number of odd components of v_2 must be odd because $N(v_2) = p$ is odd and, on the other hand, the number of odd components of v_2 must be even because $\langle v_1 | v_2 \rangle = 0$ is even. Hence, if p is a square, our conjecture is as follows.

Conjecture 4.4. Given numbers $n \geq 1$ and $p \geq 1$, so that either n is even or p is even or $n \nmid p$, and a p^2 -orthonormal system in \mathbb{Z}^n , S , then S can be extended to a p -orthonormal base.

4.1 Structural properties of the problem

Given the integer number k and the vectors $u = (x_1, \dots, x_n)$ and $v = (y_1, \dots, y_n)$ belonging to \mathbb{Z}^n , we denote the *parity of k* by $P(k) = k \pmod{2}$, the *parity of u* by $P(u) = (x_1 + \dots + x_n) \pmod{2}$ and the *parity of u and v* by $P(u, v) = \langle u | v \rangle \pmod{2}$. Note that $P(u) = P(N(u))$.

These definitions allow us to consider the conditions of p -orthonormality in terms of parities (module 2), proving the following result.

Proposition 4.5. *Given a p -orthonormal system in \mathbb{Z}^n , $S = \{v_1, \dots, v_k\}$, then it holds that $P(p) = P(v_j)$, $1 \leq j \leq k$, and $P(v_h, v_j) = 0$, $1 \leq h, j \leq k$.*

4.2 Orthogonal extensions

Given a set of vectors belonging to \mathbb{Z}^n , $S = \{v_1, \dots, v_k\}$, such that $\langle v_i | v_j \rangle = 0$ for all $1 \leq i < j \leq k$, we will say that S is an *orthogonal system* and, if $k = n$, that S is an *orthogonal base*.

The relaxation of the condition from p -orthonormality to orthogonality allows to extend any orthogonal system. Indeed, lemma 2.1 does not depend on the normalization of the vectors and can be applied in \mathbb{Z}^n , proving the following proposition.

Proposition 4.6. *Given an orthogonal system in \mathbb{Z}^n , S , then S can be extended to an orthogonal base.*

Given an orthogonal set in \mathbb{Z}^n , $S = \{v_1, \dots, v_k\}$ ($1 \leq k \leq n$), we denote the *norm* of S by $N(S) = \max\{N(v_j) \mid 1 \leq j \leq k\}$. So, an interesting problem, in view of proposition 4.6, is the following:

Problem 4.7. *Given an orthogonal system in \mathbb{Z}^n , S , determine the orthogonal base with the smaller norm that extends S .*

References

- [1] Cassels, J.W.S.: An Introduction to the Geometry of Numbers. Springer (1997)
- [2] Chou, T.-W.J., Collins, G.E.: Algorithms for the solution of systems of linear Diophantine equations. SIAM J. Computing **11**, 687—708 (1982)
- [3] Gauss, C.F.: Disquisitiones Arithmeticae. Yale University Press (1966)
- [4] Gatti, L.N., García-López, J.: Geometría de estados discretos en computación cuántica. In: 10th Andalusian Meeting on Discrete Mathematics (La Línea de la Concepción, Cádiz, Spain, 2017)
- [5] Gatti, L.N., Lacalle, J.: A model of discrete quantum computation. Quantum Information Processing, (submitted)
- [6] Jones, G.A., Jones, J.M.: Elementary Number Theory. Springer (1998)
- [7] Lagrange, J.L.: Oeuvres **3**, 189—201 (1869)
- [8] Mordell, L.J.: A new Waring's problem with squares of linear forms. Quart. J. Math. Oxford **1**, 276—288 (1930)
- [9] Ramanujan, S.: On the expression of a number in the form $ax^2 + by^2 + cz^2 + du^2$. Proc. Cambridge Phil. Soc. **19**, 11—21 (1917)
- [10] Smith, H.J.S.: On systems of linear indeterminate equations and congruences. Phil.Trans. London **151**, 293—326 (1861)
- [11] Sun, Z.-W.: Refining Lagrange's four-square theorem. J. Number Theory **175**, 167—190 (2017)