Extended Lagrange's four-square theorem ⋆

J. Lacalle [1] L.N. Gatti [2]

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

Abstract

We prove the following extension of Lagrange's theorem: given a prime number p and $v_1, \ldots, v_k \in \mathbb{Z}^4$, $1 \leq k \leq 3$, 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 $p \geq 1$.

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 [5] proved the square case of the Fermat polygonal number theorem in 1770, also solving Bachet's conjecture.

⋆ This work is an extended abstract containing only the statement of our results. The full article, with proofs, is under consideration in *Commun Number Theory.*

[1] Email: `jlacalle@etsisi.upm.es`

[2] Email: `ln.gatti@alumnos.upm.es`

Gauss [2] 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 [7]. 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 [6], 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 [9] has proposed some refinements of the Lagrange's theorem such as, for example: $n \in \mathbb{N}$ 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 [4]. We study the simplest version of this problem, which was already presented as a conjecture at a conference by the authors [3].

The outline of the article is as follows: In section 2 we set up notations and discuss some basic properties. In section 3 we give some ideas about the proof of 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 $\{e_1, e_2, e_3, e_4\}$.

Given a set of linearly independent vectors $v_1, \ldots, v_k \in \mathbb{R}^4$, they generate the *lattice* $\Lambda = \{ b_1 v_1 + \cdots + b_k v_k \mid b_1, \ldots, b_k \in \mathbb{Z} \}$ [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 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 $v_1, \ldots, v_k \in \mathbb{Z}^4$ such that $N(v_i) = p$ for all $1 \le i \le k$ and $\langle v_i | v_j \rangle = 0$ for all $1 \le i < j \le k$, we will say that $S = \{ v_1, \ldots, v_k \}$ is a $p-$*orthonormal system* and, if $k = 4$, that S is a $p-$*orthonormal base*. The *support of* S is $supp(S) = \{ k \mid \exists j$ such that the $k-$coordinate of $v_j \neq 0 \}$.

However, we are not interested in Λ, but rather in its *orthogonal lattice* $\Lambda^\perp = \{ v \in \mathbb{Z}^4 \mid \langle v_i | v \rangle = 0 \text{ for all } 1 \le i \le k \}$. The resolution method of systems of linear Diophantine equations computes a base of $\Lambda^\perp$ with $4-k$ vectors. Then the dimension of $\Lambda^\perp$ 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* [8] of V and its *invariant factors* $\alpha_1, \ldots, \alpha_k$:

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

Lemma 2.1 *Given a number $p \ge 1$ and a $p-$orthonormal system $S = \{ v_1, \ldots, v_k \}$, $1 \le k \le 3$, 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 $\Lambda^\perp$.*

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

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* $S = \{ v_1, v_2 \}$, $v_1 = (x_1, \ldots, x_4)$ *and* $v_2 = (y_1, \ldots, y_4)$, *with* $|supp(S)| > 2$, *then* $gcd(x_1, \ldots, x_4) = gcd(y_1, \ldots, y_4) = 1$ *and the invariant factors of* V *also verify* $\alpha_1 = \alpha_2 = 1$.

Proof. Suppose, by contradiction, that $\gcd(x_1, \ldots, x_4) = g > 1$. Then $N(v_1) = g^2(x_1'^2 + \cdots + x_4'^2) = p$, where $x_i' = \dfrac{x_i}{g}$ for all $1 \le i \le 4$, and this fact contradicts the primality of p. So, we have that $\gcd(x_1, \ldots, x_4) = 1$ and in the same way we conclude that $\gcd(y_1, \ldots, y_4) = 1$. 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:

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

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

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

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

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 $N(v_{k+1}) = p$.

Analyzing the problem we find four cases. The first two are trivial: S has a single vector and S has two vectors with $|\text{supp}(S)| = 2$. The third one, S has three vectors, can be easily proved using the exterior product of the vectors.

The last one, S has two vectors with $|\text{supp}(S)| > 2$, requires a detailed study of the lattice $\Lambda^\perp$ and its associated Gram matrix G. As a result of this analysis, we have that $p \,|\, G$. So, $v^t G v = p$ if and only if $v^t G' v = 1$, where $G' = G/p$ is a unimodular matrix. Finally, the existence of v is deduced from the theorem 2.3. In this way, the proof of the following result is concluded.

Theorem 3.1 *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 verified (exhaustively) the result of the theorem 3.1 for every $1 \leq p \leq 10000$. Hence, 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?*

The answer for $n = 2$ is true (trivial). The case $n = 4$ has already been studied and, in the case $n = 8$, we have checked the result for $1 \leq p \leq 36$.

We try to find counterexamples, in order to understand the problem. Given $p \geq 1$, we consider the $p-$orthonormal base in $\mathbb{Z}^4$ $S_1 = \{v_1, v_2, v_3, v_4\}$ and the matrix A, which is obtained by placing these vectors by rows,

$$\begin{array}{ll} v_1 = (x_1, x_2, x_3, x_4) & v_3 = (-x_3, x_4, x_1, -x_2) \\ v_2 = (-x_2, x_1, -x_4, x_3) & v_4 = (x_4, x_3, -x_2, -x_1) \end{array} \quad \text{where} \quad p = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

If p is the 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, which is again obtained by placing these vectors by rows: $u_1 = (y_1, y_2)$ and $v_2 = (-y_2, y_1)$. 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, $n = 1 \bmod 4$ and $n \neq 1$.

(ii) C_2 if p cannot be written as a sum of two squares, $n = 2 \bmod 4$ and $n \neq 2$.

(iii) C_3 if p is not a square and can be written as a sum of two squares and $n = 3 \bmod 4$.

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

These facts make us think that conjecture 4.1 should be generalized as follows.

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

References

[1] Cassels, J.W.S.: An Introduction to the Geometry of Numbers. Springer (1997)

[2] Gauss, C.F.: Disquisitiones Arithmeticae. Yale University Press (1966)

[3] 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)

[4] Gatti, L.N., Lacalle, J.: A model of discrete quantum computation. Quantum Information Processing, (submitted)

[5] Lagrange, J.L.: Oeuvres **3**, 189—201 (1869)

[6] Mordell, L.J.: A new Waring's problem with squares of linear forms. Quart. J. Math. Oxford **1**, 276—288 (1930)

[7] 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)

[8] Smith, H.J.S.: On systems of linear indeterminate equations and congruences. Phil.Trans. London **151**, 293—326 (1861)

[9] Sun, Z.-W.: Refining Lagrange's four-square theorem. J. Number Theory **175**, 167—190 (2017)