Solving Restricted Sums of Four Squares using Quaternions

António Leite antonio.leite@fc.up.pt
Joint work in progress with: António Machiavelo and Luís Roçadas

Centro de Matemática da Universidade do Porto, Departamento de Matemática,
Faculdade de Ciências da Universidade do Porto, rua do Campo Alegre s/n, 4169–007 Porto, Portugal

U.PORTO
FACULDADE DE CIÊNCIAS UNIVERSIDADE DO PORTO
CENTRO DE MATEMÁTICA UNIVERSIDADE DO PORTO

Introduction

In 1770, Lagrange established the four-square theorem which states that any $m \in \mathbb{N}$ can be written as the sum of four integer squares. In 2017, Zhi-Wei Sun [6] made the following conjecture:

Sun's 1-3-5 Conjecture. Any $m \in \mathbb{N}$ can be written as a sum of four squares, $m = x^2+y^2+z^2+t^2$, with $x, y, z, t \in \mathbb{N}$, in such a way that $x+3y+5z$ is a perfect square.

This conjecture was proved by A. Machiavelo and N. Tsopanidis [3] using the arithmetic of quaternions. The main goal of our work is to explore the connection between the arithmetic of quaternions and number theory, by establishing some general results that come from variations of this conjecture. In particular, if a, b, c, d are non-negative integers, we want to study the solvability, in $\mathbb{Z}$, for any positive integer m of the system, which we call $(a-b-c-d)$,

$$\begin{cases} m = x^2+y^2+z^2+t^2 \\ n^2 = ax+by+cz+dt. \end{cases}$$

Remark: A solution of $(b-a-c-d)$ easily gives a solution of $(a-b-c-d)$, just by changing x and y! Hence, given a, b, c, d we can fix the system $(a-b-c-d)$.

Quaternions and Integers

While the previous attemps to attack the 1-3-5 conjecture used the theory of quadratic forms, in [3] the arithmetic of quaternions was used. In particular, one uses a subring of Hamilton quaternions known as **Lipschitz Integers** $\mathcal{L} = \mathbb{Z}+\mathbb{Z}i+\mathbb{Z}j+\mathbb{Z}k$, where $i^2=j^2=k^2=ijk=-1$. However, it happens that this ring is not a PID ... as opposed to the ring of **Hurwitz Integers**: $\mathcal{H} = \mathcal{L} \cup (\omega + \mathcal{L})$, where $\omega = \frac{1+i+j+k}{2}$.

Due to the lack of commutativity in $\mathcal{H}$, there is no unique factorization as we know it from $\mathbb{Z}$. Instead, one has the following:

Theorem (Conway and Smith 2003). Let $\gamma \in \mathcal{H}$ be primitive with norm $N(\gamma) = m$. For each factorization of its norm into a product of primes $p_0 p_1 \cdots p_k$, where the order matters, we have a factorization of γ,

$$\gamma = \pi_0 \pi_1 \cdots \pi_k, \qquad \text{where } N(\pi_i) = p_i.$$

modeled on that factorization of m, i.e., $\mathrm{N}(\pi_i) = p_i$. This factorization is unique up to unit-migration.

It follows from [1,4] that in $\mathcal{L}$ one can only guarantee the existence of this factorization modeled on the norm.

General setting

Putting $\gamma = x+yi+zk+tk$, and $\zeta = a+bi+cj+dk \in \mathcal{L}$, the system $(a-b-c-d)$ is equivalent to

$$\begin{cases} \mathrm{N}(\gamma) = m \\ \gamma \cdot \zeta = \mathrm{Re}(\bar{\gamma}\zeta) = n^2, \end{cases} \tag{1}$$

where the dot denotes the usual inner product on $\mathbb{R}^4$. Let $\bar{\gamma}\zeta = n^2 + Ai + Bj + Ck$, for some $A, B, C \in \mathbb{Z}$, and $\mathrm{N}(\zeta) = \ell$. It follows, that $m\ell - n^4 = A^2+B^2+C^2$, and so by Legendre's three square theorem, a necessary condition for the solvability of the system is that

$$n \leq \sqrt[4]{m\ell} \text{ and } m\ell - n^4 \text{ is not of the form } 4^r(8s+7), \text{ for any } r, s \in \mathbb{N}. \tag{2}$$

Conversely, if (2) is satisfied for some m, n and ℓ, it follows from the existence of factorizations modeled on factorizations of the norm in $\mathcal{L}$ that the system (1) is satisfied for some γ', and ξ with $\mathrm{N}(\xi) = \ell$.

Theorem (Machiavelo and Tsopanidis, 2021). Let $m, n, \ell \in \mathbb{N}$ be such that $n \leq \sqrt[4]{m\ell}$, and assume that $m\ell - n^4$ is not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$. Then, for some $a', b', c', d' \in \mathbb{N}$ such that $\mathrm{N}(a'+b'i+c'j+d'k) = \ell$ the system $(a'-b'-c'-d')$ has integer solutions.

Remark: The theorem only proves the existence of solution for ℓ! Therefore, a', b', c', d' may be different from the original a, b, c, d. For example, when $\ell = 35$, one can have $(1-3-5-0)$ or $(1-3-3-4)$.

However, if a natural number ℓ has precisely one partition into sums of four squares of nonnegative numbers, the theorem has a direct consequence:

Theorem (Machiavelo and Tsopanidis, 2021). Let $\zeta \in \mathcal{L}$ and $m, n \in \mathbb{N}$ be such that $\mathrm{N}(\zeta)m - n^4$ is nonnegative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. If $\zeta = a+bi+cj+dk \in \mathcal{L}$, then the system $(a-b-c-d)$, has integer solutions whenever $\mathrm{N}(\zeta) \in \{1,3,5,7,11,15,23\} \cup \{2^g\} \cup \{3 \cdot 2^g\} \cup \{7 \cdot 2^g\}$, where g is odd and positive.

From 1-3-5-0 to variations

As 35 has precisely two partitions into sums of four squares of nonnegative numbers, we see that there exist two possibly systems $(1-3-5-0)$ and $(1-3-3-4)$.

In $\mathcal{L}$ there exist two different quaternions with norm 35, up to the signs and the order of the coeficients, $\alpha = 1+3i+5j$ and $\beta = 1+3i+3j+4k$. To prove that the system $(1-3-5-0)$ always has solution for every $m \in \mathbb{N}$, we seek quaternionic conditions to transform a solution of the $(1-3-3-4)$ into a solutions of the $(1-3-5-0)$. This is done using the following technique, which we call **metaconjugation**.

Noticing that, for any $\rho \in \mathcal{L}\backslash\{0\}$, one has $\mathrm{Re}\left(\rho^{-1}\bar{\gamma}\beta\rho\right) = \mathrm{Re}(\bar{\gamma}\beta)$ and $\mathrm{N}\left(\rho^{-1}\bar{\gamma}\beta\rho\right) = \mathrm{N}(\gamma\beta)$, and for any $\sigma \in \mathcal{L}\backslash\{0\}$, one has that $\rho^{-1}\bar{\gamma}\beta\rho = \rho^{-1}\bar{\gamma}\sigma\sigma^{-1}\beta\rho$, if we find $\rho, \sigma \in \mathcal{L}\backslash\{0\}$ such that $\sigma^{-1}\beta\rho = \alpha'$, where α' can be obtained from α by permuting and changing the sign of its coordinates, and $\rho^{-1}\bar{\gamma}\sigma \in \mathcal{L}$, with $\mathrm{N}(\rho) = \mathrm{N}(\sigma)$, then from a solution of $(1-3-3-4)$ one can obtain a solution of $(1-3-5-0)$. In this case, it was enough to use primes ρ with norm $3, 5$ and 7.

As a generalization, we now consider numbers that, similarly to 35, can be written as sums of four integer squares in precisely two different ways (up to the signs and the order of the coeficients). They can be described as

$$\{9,13,17,19,21,29,30,31,35,39,46,47,71\}, 5 \times 2^n, \;\; 11 \times 2^n \text{ and } \{1,3,30,46\} \times 4^n \text{ where } n > 0.$$

For some of these numbers, we already know that at least one of the system is always possible (see [2,3,5]), and so the following conjecture came naturally:

Conjecture. If ℓ can be represented as a sum of four squares in precisely two different ways, then at least one of the possible systems has integer solutions for every $m \in \mathbb{N}$.

We were able to reduce the proof to a finite number of cases, and prove it for $\ell \in \{4,9,12,20,30,40,44,46,71,88\}$.

Another interesting example is the case where $\ell = 18$, since there exist precisely three ways of writting it as a sum of four squares. This leads to the quaternions: $\alpha = 1+2i+2j+3k$, $\beta = 1+1i+4j+0k$, $\omega = 3+3i$. Using primes of norm 7 and primes of norm 3, we find conditions that allow us to see the following:

Proposition. For $m \in \mathbb{N}$, any solution of $(1-1-4-0)$ gives origin to a solution of $(1-2-2-3)$, and any solution of $(3-3-0-0)$ gives origin to a solution of $(1-2-2-3)$ or a solution of $(1-1-4-0)$.

Theorem. Any $m \in \mathbb{N}$ can be represented as $x^2+y^2+z^2+t^2$ with $x, y, z, t \in \mathbb{Z}$ such that $x+2y+2z+3t$ is a square.

References

[1] J. H. Conway and D. A Smith. "On Quaternions and Octonions". AK Peters/CRC Press, 2003.

[2] Jorge Costa. "Quaternions, Arithmetic and Diophantine Equations". Master Thesis Universidade do Porto, 2023.

[3] António Machiavelo and Nikolaos Tsopanidis. "Zhi-Wei Sun's 1-3-5 Conjecture and Variations". Journal of Number Theory 222,2021.

[4] Gordon Pall. "On The Arithmetic Of Quaternions". Transactions of the American Mathematical Society 47, 1940.

[5] Yue-Feng She and Guang-Liang Zhou. "Numbers Represented By Restricted Sums Of Four Squares". Rocky Mountain Journal of Mathematics 54, 2024.

[6] Zhi-Wei Sun. "Refining Lagrange's four-square theorem". Journal of Number Theory 175, 2017.

PORTUGAL 2030 — UNIÃO EUROPEIA Fundo Social Europeu

The author was supported by the FCT doctoral scholarship with reference 2025.01855.BD, and partially supported by CMUP, member of LASI, which is financed by national funds through FCT - Fundação para a Ciência e a Tecnologia, I.P., under the project with reference UID/00144/2025 and associated DOI given by https://doi.org/10.54499/UID/00144/2025.

fct Fundação para a Ciência e a Tecnologia