Quaternions, Arithmetic and Diophantine Equations

Jorge Costa
Mestrado em Matemática
Departamento de Matemática

2023

Orientador
António Machiavelo, Professor Auxiliar
Faculdade de Ciências da Universidade do Porto

U.PORTO

FC FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

MSc

Acknowledgments

There are some people who were fundamental in making this thesis happen, and I cannot help but acknowledge them and shower them with my gratitude. I will start expressing my deepest gratitude to my supervising professor, António Machiavelo, thanking him not only for accepting me as his student before I even entered my master's, but also for his presence and insight all the way through, enduring my millions of questions and my insistence in continuing on with my research before having everything written down.

To my lovely family, the present and the unfortunately gone, who for the past 23 years were as supportive of me as one could dream of, and that made me the man and mathematician I am today.

To Leonor, who heard me ramble about mathematics more than I thought humanly possible, without a single complaint, who was by my side throughout all the process, delighted in the highs and a beacon of positivity in the lows.

To Afonso and Rita, for being the most wonderful people that I met along this journey.

To all my friends who were still there for me despite me being unavailable most of the year, and to a certain group chat that consistently, and jokingly I hope, insist that they are being neglected, no matter what I did.

To all the students I tutored, who keep my love for math ever burning.

I also cannot forget to thank professor Luís Roçadas and Adriana, for their continuous help backed by their expertise.

And finally to my institution, FCUP, for the great master's I had the pleasure of partaking in, and for providing this experience.

Abstract

The set of quaternions is more than just an abstract algebra object, it can, and was, used as an important tool to prove results outside its domain. One such result was the conjecture 1-3-5, which states that for every $m \in \mathbb{N}$, there exists $x, y, z, t \in \mathbb{N}$, such that $m = x^2 + y^2 + z^2 + t^2$ and $x + 3y + 5z$ is a perfect square. In this thesis we will start by introducing the basic quaternion arithmetics, seeing how they are defined, what properties they have and other related results. Then we will observe their usefulness in proving the aforementioned conjecture, giving a sketch of how the proof came to be, and follow that up with applying the methods used beforehand to problems of a similar nature. In the end we will branch out, and use a different approach, in order to completely describe the values of m for which there exists $x, y, z, t \in \mathbb{N}$ such that $m = x^2 + y^2 + z^2 + t^2$ and ax is a perfect square, where a is a natural number.

Keywords: Quaternions, Lipschitz integers, Hurwitz integers, Diophantine systems, 1-3-5 conjecture.

Resumo

O conjunto formado pelos quaterniões é mais do que apenas um objeto de álgebra abstrata, pode, e foi, usado como uma ferramenta importante para provar resultados fora do seu domínio. Um tal resultado foi a conjetura 1-3-5, que afirma que para todo $m \in \mathbb{N}$, existem $x, y, z, t \in \mathbb{N}$, tais que $m = x^2 + y^2 + z^2 + t^2$ e $x + 3y + 5z$ é um quadrado perfeito. Nesta tese começaremos por introduzir a aritmética básica dos quaterniões, vendo como são definidos, que propriedades têm e outros resultados relacionados. Depois observaremos a sua utilidade na prova da conjetura antes mencionada, mostrando um esboço de como a prova foi concebida, sendo que de seguida aplicaremos métodos análogos em problemas de natureza similar. Por fim, seguiremos outro caminho, e usaremos uma abordagem diferente, de forma a descrever completamente os valores de m para os quais existem $x, y, z, t \in \mathbb{N}$ tais que $m = x^2 + y^2 + z^2 + t^2$ e ax é um quadrado perfeito, onde a é um número natural.

Palavras-chave: Quaterniões, Inteiros de Lipschitz, Inteiros de Hurwitz, sistemas Diofantinos, conjetura 1-3-5.

Contents

Introduction

While quaternions and Number Theory are not subjects usually associated together, there are connecting bridges between both of them, such as Lagrange's Four Square Theorem and the fact that the norm of a quaternion is the sum of the squares of its four coordinates.

The 1-3-5 conjecture, the inspiration to this thesis, first conjectured in 2017 by Zhi-Wei Sun, in [10], and later proved by António Machiavelo and Nikolaos Tsopanidis, in [8], was a number theory problem that had quaternions playing a fundamental part in the proof. The conjecture is easy to explain to everyone equipped with basic mathematical knowledge: if we take a natural number m, can we find a way of writing it as the sum of four squares x^2, y^2, z^2 and t^2, where $x + 3y + 5z$ is itself a square. This can be translated to finding the solutions of a system of Diophantine equations.

Working on certain subrings of the quaternions, namely the Lipschitz and Hurwitz integers, the goal was to inspect the arguments used in the proof of that conjecture, and then tackle other problems of the same genre using the same techniques.

The initial questions, which would later become the goals of this research, were the following:

1. Why only this specific and seemingly arbitrary combination of coefficients, $1, 3, 5$?

2. Were there more?

3. If so, which ones?

4. If not, for which values of m does the system of equations not have solutions?

In the first chapter of this thesis, we will present the necessary results to get situated with all the nuances and inner workings of different types of quaternions and their properties, before delving into bigger problems.

Afterwards, in chapter 2, there will be an overview of the 1-3-5 conjecture and we shall show a sketch of the proof, providing all the general ideas that went into it.

Later, chapter 3 looks into cases similar to the 1-3-5 case, leading us into numbers that can be written in exactly two ways as a sum of four squares, a characteristic present in 35, which is equal to $1^2+3^2+5^2$ and $1^2+3^2+3^2+4^2$. The importance of this property is explained in chapter 2. We will then be applying the techniques that helped solve the 1-3-5 conjecture, to tackle these similar problems.

Lastly, in chapter 4, we focused on systems with a specific configuration, where we wanted to find x, y, z, t such that $m = x^2+y^2+z^2+t^2$ and ax was a square. We managed a full description of the behavior of every system of this form, finding out exactly for what values of m there is a natural solution.

Every single attempt and every hour spent researching leads me to believe that there is still a lot to be found in these "unexplored waters" of mathematics, and I sincerely hope that this thesis may invoke, in whoever reads it, a fraction of the curiosity and passion I now hold for this field.

Note that throughout this thesis, whenever the natural numbers are mentioned, the number 0 is being included. [1]

[1] Necessary in order to avoid dozens of mentions of "every positive integer" or the use of $\mathbb{N}_0$.

Chapter 1

Some Basic Notions on Quaternions

To get started we need to define what a quaternion is. Sir William Rowan Hamilton first introduced the concept in 1843, in which he represented a quaternion in the form $a+bi+cj+dk$, where a,b,c,d are real numbers and i, j and k are the basis elements that satisfy the Hamilton equations:

$$
\begin{gathered}
ij = k, \qquad jk = i, \qquad ki = j, \\
ji = -k, \qquad kj = -i, \qquad ik = -j, \\
i^2 = j^2 = k^2 = -1.
\end{gathered}
$$

These relations between i, j and k, in conjunction with the distributive property define the product between quaternions, which is not commutative. One can easily check that:

$$
\begin{aligned}
(u_0 + u_1 i + &u_2 j + u_3 k)(v_0 + v_1 i + v_2 j + v_3 k) = \\
&(u_0v_0 - u_1v_1 - u_2v_2 - u_3v_3) + (u_0v_1 + u_1v_0 + u_2v_3 - u_3v_2)i + \\
&(u_0v_2 - u_1v_3 + u_2v_0 + u_3v_1)j + (u_0v_3 + u_1v_2 - u_2v_1 + u_3v_0)k.
\end{aligned}
$$

Definition 1. *Considering $h = a + bi + cj + dk$, we define:*

i) $Re(h) := a$, the real (or scalar) part of h,

ii) $\tilde{h} := bi + cj + dk$, the imaginary (or vector) part of h,

ii) $\overline{h} = a - bi - cj - dk$, the conjugate of h.

We can see from the explicit expression of the product that, for $x, y \in \mathbb{H}$, $Re(xy) = x \cdot \overline{y}$, where the dot represents the usual inner product in $\mathbb{R}^4$, and then obtain $x \cdot y = Re(x\overline{y})$.

With coordinate by coordinate summation, the ring of quaternions is a non-commutative algebra over the real numbers. The quaternion ring also has the particular property of every non-zero quaternion having a multiplicative inverse, and therefore is a division algebra.

The results in this thesis will mainly focus not on the quaternions, but on certain subsets that are more interesting as far as Number Theory is concerned.

Definition 2. *The set:*

$$\mathcal{L} = \{a + bi + cj + dk \in \mathbb{H} : a, b, c, d \in \mathbb{Z}\}$$

is called the set of Lipschitz integers*.*

We will consider, for the majority of the situations, the following set:

Definition 3. *The set:*

$$\mathcal{H} = \left\{ \frac{a + bi + cj + dk}{2} : a \equiv b \equiv c \equiv d \pmod 2 \right\}$$

is called the set of Hurwitz integers*.*

In order to further characterize these sets, we shall introduce the following concepts:

Definition 4. *A non-zero ring A is called:*

i) a domain, if the product of any two non-zero elements is not 0.

ii) a principal ideal ring, if every left and every right ideal is principal, that is, if you take a right (left) ideal I of A, there exists an element $a \in I$ such that $I = aA$ $(I = Aa)$.

iii) a right (left) euclidean ring, if there exists a function λ from $A \setminus \{0\}$ to $\mathbb{N}$ satisfying the following property: if $(a, b) \in A \times A \setminus \{0\}$, then there exists q and r in A such that $a = bq + r$ $(a = qb + r)$ and either $r = 0$ or $\lambda(r) < \lambda(b)$. If it is both a left and right euclidean ring, it will be called an euclidean ring.

The choice to work with the set of Hurwitz integers was made due to the fact that $\mathcal{L}$ is not a principal ideal ring (for example, $< 1+i, 1+j >$ is not principal) and $\mathcal{H}$ is an euclidean ring, for the norm ([11, Lemma 11.3.2]), which we will define next, as well as defining the trace of an element.

Definition 5. *The* norm *and* trace *of a quaternion* $h = a+bi+cj+dk$*, where* $\overline{h} = a-bi-cj-dk$ *is its conjugate, is defined in the following way:*

$$N(h) = h\overline{h} = a^2 + b^2 + c^2 + d^2,$$

$$Tr(h) = 2Re(h) = h + \overline{h} = 2a.$$

Note that, since $N(h) = h\overline{h}$, the inverse of h is equal to $\frac{\overline{h}}{N(h)}$.

It is immediate that the norm of a Lipschitz integer is always a natural number. That is also the case for a Hurwitz integer, but some calculations are necessary. Take $h \in \mathcal{H} \setminus \mathcal{L}$, then h is of the form $\frac{a+bi+cj+dk}{2}$ where $a \equiv b \equiv c \equiv d \equiv 1 \pmod 2$, which implies that $a^2 \equiv b^2 \equiv c^2 \equiv d^2 \equiv 1 \pmod 4$. Since $N(h) = \frac{a^2+b^2+c^2+d^2}{4}$ and $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod 4$, then $N(h)$ is always a natural number.

Proposition 1. *The norm is a multiplicative map, that is, for all* $h_1, h_2 \in \mathcal{H}$*, one has:*

$$N(h_1h_2) = N(h_1)N(h_2).$$

Proof. Let $h_1 = a + bi + cj + dk$ and $h_2 = x + yi + zj + tk$. It is fairly easy to check that $\overline{h_1h_2} = \overline{h_2}\ \overline{h_1}$, and so we have:

$$N(h_1h_2) = h_1h_2\overline{h_1h_2} = h_1(h_2\overline{h_2})\overline{h_1} = N(h_2)h_1\overline{h_1} = N(h_1)N(h_2).$$

□

Now that we have defined the norm, we can determine the units of $\mathcal{H}$. One element h is a *unit* in $\mathcal{H}$ if it is invertible in $\mathcal{H}$, in other words, there exists h' such that $hh' = 1$. We know then that $N(h)N(h') = N(hh') = N(1) = 1$, and since the norm of a quaternion in $\mathcal{H}$ is always a natural number, the only possible value for $N(h)$ is 1. Conversely, $N(h) = 1 \implies h\overline{h} = 1$, which implies that h is invertible in $\mathcal{H}$ since $\overline{h}$ is in $\mathcal{H}$. This means that the units of $\mathcal{H}$ are exactly the quaternions of norm 1, which are listed below:

$$U(\mathcal{H}) = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}.$$

The first 8 being the ones obtained from the basis elements, and the last 16 the ones we get when we make the jump to the Hurwitz integers: $N\left(\frac{\pm 1 \pm i \pm j \pm k}{2}\right) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$, while any other Hurwitz quaternion, that is not a Lipschitz one, even with the slighest modification (changing a 1 to a 3) will have a norm that surpasses 1, for example:

$$N\left(\frac{3+i+j+k}{2}\right)=\left(\frac{3}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2=\frac{9}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=\frac{12}{4}=3.$$

Other than the units, there are some other important elements to consider in $\mathcal{H}$, such as:

Definition 6. *A Hurwitz integer h is called*

i) irreducible *if it is neither a unit nor zero and it cannot be expressed as a product of non-units. This condition is equivalent to the norm of h being a prime number [11, Lemma 11.4.6].*

ii) primitive *if it cannot be written as $h = nq$, where $n \in \mathbb{Z} \setminus \{\pm 1\}$ and $q \in \mathcal{H}$.*

Irreducible quaternions are often called prime quaternions, but they are not primes in the regular sense, due to the non-commutativity of the ring $\mathcal{H}$. It is possible for an irreducible element h to divide ab, and not divide neither a nor b. But we will be calling them prime quaternions, since this is the standard in the existing literature.

Recall that two quaternion primes, p and q, are said to be *associate* if you can obtain p by multiplying q by an unit, and vice-versa.

We will now present two results that are the backbone to the connection between quaternions and Diophantine equations, these two being *Lagrange's Theorem of Four Squares*, following the proof presented in [2] and the *Unique Factorization in Hurwitz quaternions*, following the proof presented in [4].

Theorem 1 (Lagrange's Four Squares Theorem)**.** *Every natural number can be written as the sum of four natural square numbers.*

Proof. Writing n as a sum of four squares is the same as expressing it as the norm of a Lipschitz quaternion, since $n = x^2 + y^2 + z^2 + t^2 = N(x + yi + zj + tk)$, $x, y, z, t \in \mathbb{N}$. Because of the multiplicativity of the norm, if two numbers can be written as the sum of 4 squares, then their product also has the same property, which means that by proving the result for prime numbers, it then follows for composite numbers. For 0 and 1, the result is trivial. We start the proof with the following lemma:

Lemma 1. *Let $p \in \mathbb{N}$ be a prime for the natural numbers. There exists $u, v \in \mathbb{Z}$ such that*

$$1 + u^2 + v^2 \equiv 0 \pmod{p}.$$

Remark 1. *This implies that there always exists $h \in \mathcal{L}$ ($h = 1 + ui + vj$, for example) such that p does not divide h, but p divides the norm of h.*

Proof. We will prove this statement using the Pigeonhole Principle, which states that if you have more "pigeons" than "containers" where you will distribute the pigeons, then at least one container will contain more than one pigeon.

The result is trivial for $p = 2$, as you only need to consider $u = 1, v = 0$. So we may focus on odd primes. Working modulo p, we can easily prove that the following quadratic residues are all distinct:

$$0^2, 1^2, ..., \left(\frac{p-1}{2}\right)^2.$$

Imagine that they were not, then there would exist $i, j \in \left\{0, 1, ..., \frac{p-1}{2}\right\}$ distinct, such that $i^2 \equiv j^2 \pmod p$ which would imply $i^2 - j^2 = (i-j)(i+j) \equiv 0 \pmod p$. Since p is prime, p either divides $i + j$ or $i - j$, but $1 \leq i + j \leq p - 1$ and $1 \leq |i - j| \leq |i| + |j| \leq p - 1$ (remember that i and j are distinct), but there are no multiples of p in the interval $[1, p - 1]$.

We will use those representatives to form the following two lists, each one containing $\frac{p+1}{2}$ elements:

$$1 + 0^2, 1 + 1^2, ..., 1 + \left(\frac{p-1}{2}\right)^2,$$

$$0^2, -1^2, ..., -\left(\frac{p-1}{2}\right)^2.$$

Together, the two lists consist of $p + 1$ elements. Since there are only p residue classes, by the pigeon principle, there are two elements, one of each list (because both lists are composed of distinct elements), that coincide. So there exists $u, v \in \left\{0, 1, ..., \frac{p-1}{2}\right\}$ such that:

$$1 + u^2 \equiv -v^2 \pmod p,$$

which proves the claim. $\square$

Returning to the proof of Theorem 1, out of all of the primes we only need to look at the odd ones because $2 = 1^2 + 1^2 + 0^2 + 0^2$. Then, let p be such prime and let $h = 1 + ui + vj \in \mathcal{L}$ be in the conditions of the previous lemma, meaning that p divides $N(h)$. We now claim the following:

$$\mathcal{H}p \subsetneq \mathcal{H}p + \mathcal{H}h \subsetneq \mathcal{H}.$$

If we assume this to be true, then, since $\mathcal{H}$ is a principal ideal ring, we have $\mathcal{H}p + \mathcal{H}h = \mathcal{H}b$ for some $b \in \mathcal{H}$ where the norm of b is different than 1, otherwise the sum of the two ideals would be the entire set. Due to $\mathcal{H}p \subsetneq \mathcal{H}b$, we have that $p = mb$ for some $m \in \mathcal{H}$ where, again,

$N(m) \neq 1$, otherwise both sets would be equal. We then have:

$$\begin{aligned} p = mb &\iff N(p) = N(mb) \\ &\iff p^2 = N(m)N(b) \\ &\implies p = N(m), \end{aligned}$$

as $N(m)$ and $N(b)$ can only be $1, p, p^2$, but none of them are 1, and so both are equal to p. Thus p, an odd prime, is the norm of a certain Hurwitz quaternion, almost what we are looking for, which is that p is the norm of a Lipschitz quaternion. Let us now prove what we claimed, that $\mathcal{H}p \subsetneq \mathcal{H}p + \mathcal{H}h \subsetneq \mathcal{H}$.

The first inclusion is trivial, so we need to check that it is proper. If $h \in \mathcal{H}p$, then $2h$ would belong to $\mathcal{L}p$, and so p would divide $2h = 2 + 2ui + 2vj$, implying that p divides 2, which is absurd and therefore the containment is proper. The second inclusion is also trivial, and therefore we only need to check that it is indeed proper. To show that, it is sufficient to prove that $1 \notin \mathcal{H}p + \mathcal{H}h$.

Suppose it was, and so $1 = ap + bh$, for some $a, b \in \mathcal{H}$. Since

$$N(ap + bh) = (ap + bh)(\overline{a}p + \overline{bh}) = N(a)p^2 + (a\overline{bh} + \overline{a}bh)p + N(b)N(h)$$

is divisible by p, we have an contradiction, thus proving the claim.

We already know that for any odd prime p, $p = N(h)$ for some $h \in \mathcal{H}$. If $h \in \mathcal{L}$ then p can be written as the sum of four squares, those being the coefficients of h. The problem is when $h \in \mathcal{H} \setminus \mathcal{L}$, which we will solve with the following lemma.

Lemma 2. *For any $h \in \mathcal{H} \setminus \mathcal{L}$, it is possible to find δ of the form $\frac{\pm 1 \pm i \pm j \pm k}{2}$ such that $h\delta \in \mathcal{L}$*

Proof. Since $h \in \mathcal{H} \setminus \mathcal{L}$, then h is of the form $\frac{a+bi+cj+dk}{2}$ where $a \equiv b \equiv c \equiv d \equiv 1 \pmod 2$, meaning we can write them as follows:

$$a = 4a_1 + \epsilon_1, b = 4b_1 + \epsilon_2, c = 4c_1 + \epsilon_3, d = 4d_1 + \epsilon_4,$$

where $\epsilon_i = \pm 1$ for $i = 1, 2, 3, 4$. Then:

$$h = 2(a_1 + b_1 i + c_1 j + d_1 k) + \frac{\epsilon_1 + \epsilon_2 i + \epsilon_3 j + \epsilon_4 k}{2},$$

and if we consider $\gamma = \frac{\epsilon_1+\epsilon_2 i+\epsilon_3 j+\epsilon_4 k}{2}$, we have:

$$\begin{aligned}
h\overline{\gamma} &= (2(a_1 + b_1 i + c_1 j + d_1 k) + \gamma)\overline{\gamma} \\
&= 2(a_1 + b_1 i + c_1 j + d_1 k)\frac{1}{2}(\epsilon_1 - \epsilon_2 i - \epsilon_3 j - \epsilon_4 k) + \gamma\overline{\gamma} \\
&= (a_1 + b_1 i + c_1 j + d_1 k)(\epsilon_1 - \epsilon_2 i - \epsilon_3 j - \epsilon_4 k) + N(\gamma),
\end{aligned}$$

where the first part is the product of two Lipschitz quaternions, and therefore itself a Lipschitz quaternion; and $N(\gamma) = 1$, thus $h\overline{\gamma}$ is a Lipschitz quaternion. □

We thus complete the proof. If $p = N(h)$ for some $h \in \mathcal{H} \setminus \mathcal{L}$, then there always exists $\delta \in U(\mathcal{H} \setminus \mathcal{L})$ such that $N(h) = N(h\delta)$ and $h\delta \in \mathcal{L}$, thus proving that p can be written as the sum of four natural squares. □

The second result, central in quaternion arithmetic, is the following:

Theorem 2 (Unique factorization in Hurwitz quaternions)**.** *Let $h \in \mathcal{H}$ be primitive, and let $N(h) = p_1 \cdots p_n$ be a fixed prime factorization of $N(h)$, where the order of the p_i's matters.*

Then h can be factored as $h = P_1 \cdots P_n$ such that $N(P_i) = p_i$. Moreover, any other factorization of h, modelled on the same fixed prime factorization of $N(h)$, has the form $h = P_1U_1 \cdot U_1^{-1}P_2U_2 \cdots U_{n-1}P_n$, for $U_1, \dots, U_{n-1}$ units of $\mathcal{H}$. It is therefore said that the factorization on a given model is unique up to unit-migration.

Proof. Due to $\mathcal{H}$ being an principal ideal domain, the ideal $p_1\mathcal{H} + h\mathcal{H}$ must be equal to $P_1\mathcal{H}$, for some $P_1 \in \mathcal{H}$.

The norm of P_1 must divide $N(p_1) = p_1^2$, so it can only be either $1, p$ or p^2. Suppose $N(P_1) = 1$, then $p_1\mathcal{H} + h\mathcal{H}$ would be equal to $\mathcal{H}$. Considering an element of $p_1\mathcal{H} + h\mathcal{H}$, it is of the form $p_1 a + hb$, for $a, b \in \mathcal{H}$ and has the norm:

$$N(p_1 a + hb) = (p_1 a + hb)(p_1\overline{a} + \overline{hb}) = p_1^2 N(a) + p_1(a\overline{hb} + hb\overline{a}) + N(h)N(b),$$

and considering that $N(h) = p_1 \cdots p_n$, we have that p_1 divides the norm of every element of the ideal, a contradiction.

If $N(P_1) = p^2$, then we have $p_1 = P_1 U$, where U is an unit, because P_1 divides p_1 and they have the same norm. On the other hand, $P_1 = p_1 U^{-1}$ divides h, and so p_1 does too, a contradiction due to the fact that h is primitive. We can then conclude that $N(P_1) = p_1$, meaning that P_1 is Hurwitz prime that divides h, and so $h = P_1 h_1$, where $N(h_1) = p_2 \cdots p_n$ and P_1 is unique up to right multiplication by a unit.

We can now take h_1 and repeat the process, which gives us $h_1 = P_2 h_2 ...$ By doing this n times, we obtain $h = P_1 \cdots P_n$, such that $N(P_i) = p_i$, where p_i are primes, a factorization of h as the product of Hurwitz primes unique up to unit migration. $\square$

Finally, another result that will be very prevalent throughout the thesis is the following:

Theorem 3. *If $m \in \mathbb{N}$ is not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$, then m can be written as the sum of 3 squares.*

This theorem is known as Legendre's three-square theorem, as it was first proved by Adrien-Marie Legendre in the later stages of the 18th century. You can see [5] for the original proof and see [1] for a more modern one.

Chapter 2

1-3-5 Conjecture

One of the main motivators for this work was the conjecture of Zhi-Wei Sun (see [10, Conjecture 4.3]) that, in 2021, Machiavelo and Tsopanidis solved (see [8]), and which is now presented as a theorem:

Theorem 4 (1-3-5 conjecture)**.** *For any $m \in \mathbb{N}$ there are $x, y, z, t \in \mathbb{N}$ such that $m = x^2 + y^2 + z^2 + t^2$ where x+3y+5z is itself a square number.*

It is important to note, before moving forward, that during the writing of this thesis, the author, Jorge Costa, found a mistake in the original proof which will be covered toward the end of this chapter.

Before giving an idea of the proof, let us introduce a notation that will be useful throughout the rest of the thesis. Consider the following system, where $m, n, a, b, c, d \in \mathbb{N}$ are fixed,

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

This system will be denoted by $S_{m,n}(a, b, c, d)$, and so, one way to reformulate the 1-3-5 conjecture is by saying that, for any $m \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that $S_{m,n}(1, 3, 5, 0)$ has a solution in the natural numbers.

By setting $\zeta = a + bi + cj + dk \in \mathcal{L}$, with a, b, c, d all greater than 0, solving these equations is equivalent to finding $\gamma = x + yi + zj + tk \in \mathcal{L}$, such that $N(\gamma) = m$ and $\gamma \cdot \zeta = Re(\overline{\gamma}\zeta) = n^2$. Consider we have such γ, and set $\delta = \overline{\gamma}\zeta$. Since $Re(\delta) = n^2$, then $\delta = n^2 + Ai + Bj + Ck$, for some $A, B, C \in \mathbb{Z}$, and taking the norm on both sides yields:

$$mN(\zeta) - n^4 = A^2 + B^2 + C^2,$$

which is equivalent to $mN(\zeta) - n^4$ being non-negative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$, by Legendre's three-square Theorem.

By starting with $mN(\zeta) - n^4$ being able to be written as the sum of three squares, and applying the same process backwards one can obtain $\gamma, \xi \in \mathcal{L}$, such that $N(\gamma) = m$ and $\gamma \cdot \xi = Re(\overline{\gamma}\xi) = n^2$.

This results in the following theorem, that will work as a basis for the rest of the thesis:

Theorem 5. *Let $m, n, \ell \in \mathbb{N}$ be such that $m\ell - n^4 \geq 0$ and not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$. Then, for some $a, b, c, d \in \mathbb{N}$ with $N(a + bi + cj + dk) = \ell$, the system $S_{m,n}(a, b, c, d)$ has integer solutions x, y, z and t.*

This innocuous looking theorem actually gives us a lot of information. Note that it only gives us integer solutions, and later on we will focus on improving them into natural ones. Let us take, for example, $\ell = 18$, which can be written as the sum of three squares in exactly three ways:

$$18 = 1^2 + 1^2 + 4^2 = 1^2 + 2^2 + 2^2 + 3^2 = 3^2 + 3^2.$$

We can conclude that, if $m, n \in \mathbb{N}$ are such that $18m - n^4 \geq 0$, and not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$, then at least one of the systems $S_{m,n}(1, 1, 4, 0)$, $S_{m,n}(1, 2, 2, 3)$ and $S_{m,n}(3, 3, 0, 0)$ has an integer solution.

Another thing we can conclude is that if $\ell \in \mathbb{N}$ can only be written as the sum of four squares in one way, then we know that the corresponding system has integer solutions under the restrictions of theorem 5. In other words:

Corollary 1. *Consider $\ell \in \mathbb{N}$, such that ℓ can only be written as the sum of four squares in exactly one ordered way, that is, $\ell = a^2 + b^2 + c^2 + d^2$, for $a, b, c, d \in \mathbb{N}$ with $a \leq b \leq c \leq d$. Let $m, n \in \mathbb{N}$ be such that $m\ell - n^4 \geq 0$ and not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$. Then the system $S_{m,n}(a, b, c, d)$ has integer solutions x, y, z and t.*

The extensive list of the values of ℓ for which there is only one ordered way of writing it as the sum of four squares is (see [6, Theorem 1]):

$$\ell = \begin{cases} 1, 3, 5, 7, 11, 15, 23 \\ \quad 2^g, 3 \cdot 2^g, 7 \cdot 2^g \end{cases}$$

where g is odd and positive.

To see what Theorem 5 gives us in the context of the conjecture, we need to consider ℓ to be the sum of the squares of $1, 3$ and 5 which is 35, that can be written as the sum of four squares in exactly two ways:

$$35 = 1^2 + 3^2 + 5^2 = 1^2 + 3^2 + 3^2 + 4^2,$$

and so, if the conditions stated on the theorem are verified, that is, if, for fixed $m, n \in \mathbb{N}$, $35m - n^4$ is non-negative, and not of the form $4^r(8s + 7)$ for any $r, s \in \mathbb{N}$, then at least one of the following systems will have integer solutions:

$$\begin{cases} x^2 + y^2 + z^2 + t^2 = m \\ x + 3y + 5z = n^2, \end{cases} \qquad \begin{cases} x^2 + y^2 + z^2 + t^2 = m \\ x + 3y + 3z + 4t = n^2. \end{cases}$$

While far from the objective, it is still a great step in order to prove the conjecture. For m, n that verify the conditions of the theorem 5, if we have an integer solution for $S_{m,n}(1, 3, 5, 0)$, then we are done; if not, then we have an integer solution for $S_{m,n}(1, 3, 3, 4)$, and we can try to modify this solution, using quaternion arithmetic, into a solution of the previous system. The next section focuses on this process, and later, the proof focuses on extending the result to natural solutions.

First, we need to introduce the following concept: α and $\alpha' \in \mathcal{L}$ are said to be *comorphic* if you can obtain one by reordering and changing the signs of the coordinates of the other one, which we will write as $\alpha \sim \alpha'$.

From now on, we set $\alpha = 1+3i+5j$ and $\beta = 1+3i+3j+4k$, as we will reference them many times. In order to apply theorem 5, we will assume that $m, n \in \mathbb{N}$ are such that $35m - n^4 \geq 0$ and not of the form $4^r(8s + 7)$, for any $r, s \in \mathbb{N}$, which implies, by the Theorem of Three Squares, that there exists $A, B, C \in \mathbb{Z}$ such that $35m - n^4 = A^2 + B^2 + C^2$. This then implies that $35m = N(n^2 + Ai + Bj + Ck)$, and so there exists a quaternion $\delta = n^2 + Ai + Bj + Ck \in \mathcal{L}$ such that $N(\delta) = 35m$. By the unique factorization in quaternions, there exist $\zeta, \gamma \in \mathcal{L}$ such that $N(\zeta) = 35$, $N(\gamma) = m$, and $\delta = \gamma\zeta$.

Since $N(\zeta) = 35$, there are only two non-comorphic options for ζ: either $\zeta \sim \alpha$ or $\zeta \sim \beta$. If $\zeta \sim \alpha$, we can obtain γ' by changing the sign and order of the coefficients of γ, such that $Re(\gamma'\alpha) = Re(\gamma\zeta) = n^2$, and therefore have an integer solution for $S_{m,n}(1, 3, 5, 0)$. If $\zeta \sim \beta$, again from γ, we can obtain γ', such that $Re(\gamma'\beta) = Re(\gamma\zeta) = n^2$, and thus we can assume that $\zeta = \beta$, without loss of generality.

The remark that follows is the main idea that enables what will be done in the following stages of the proof.

Remark 2. *Suppose we have a solution for $S_{m,n}(1, 3, 3, 4)$, i.e. that we have γ such that $Re(\gamma\beta) = n^2$ and $N(\gamma) = m$. Since for any $\rho \in \mathcal{H} \setminus \{0\}$, one has $Re(\rho^{-1}\delta\rho) = Re(\delta)$,*

$N(\rho^{-1}\gamma\rho) = N(\gamma)$, and for any $\sigma \in \mathcal{L} \setminus \{0\}$, one has :

$$\rho^{-1}(\gamma\beta)\rho = \rho^{-1}\gamma\sigma\sigma^{-1}\beta\rho,$$

if one can find $\rho, \sigma \in \mathcal{H}$ with $N(\rho) = N(\sigma)$, such that $\rho^{-1}\gamma\sigma \in \mathcal{L}$ and $\sigma^{-1}\beta\rho = \alpha' \sim \alpha$, then we would have:

$$N(\rho^{-1}\gamma\sigma) = N(\gamma) = m$$
$$Re((\rho^{-1}\gamma\sigma)\alpha') = Re(\gamma\beta) = n^2,$$

and therefore would have an integer solution for $S_{m,n}(1,3,5,0)$ created from a solution of $S_{m,n}(1,3,3,4)$.

Considering that, for a certain $m \in \mathbb{N}$, we have $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ as a solution for $S_{m,n}(1,3,3,4)$, for some $n \in \mathbb{N}$. By setting $\gamma_0 = x_0 - y_0 i - z_0 j - t_0 k$, we can try to create a solution for $S_{m,n}(1,3,5,0)$ from it, using remark 2.

Remark 2 will give us certain congruences on the coefficients of the solutions, depending on $\rho \in \mathcal{L}$. The original proof uses quaternions ρ of norm p, where p is an odd prime, with the goal of using them to construct a sort of lattice of congruences which covers all possible solutions of $S_{m,n}(1,3,3,4)$, converting them into solutions of $S_{m,n}(1,3,5,0)$. With primes of norm $3, 5$ and 7 it was possible to fully cover all solutions, and in this thesis we will cover in depth the process for the primes of norm 3.

There are 4 right non-associated prime quaternions of norm 3 (see [3, Corollary 2.3]), one of them being, for example, $\rho = 1 + i - j$. We need $\sigma, \alpha' \in \mathcal{L}$, in the conditions of Remark 2, such that $\rho^{-1}\gamma\sigma \in \mathcal{L}$ and $\sigma^{-1}\beta\rho = \alpha'$, or $\beta\rho = \sigma\alpha'$.

Using PariGP, a computer algebra system essential for complex operations in Number Theory, we obtained the following equations:

i) $\beta(1 + i - j) = (1 - i + k)(-3 + 5i + k)$

ii) $\beta(1 - i - j) = (1 + j + k)(3 - 5j + k)$

iii) $\beta(1 + i + j) = (1 - j + k)(-3 + 4i + j + 3k)$

iv) $\beta(1 - i + j) = (1 + i + k)(3 - i + 4j + 3k)$.

This was done by first calculating the right greatest common denominator between $\beta\rho$ and 35, which gives us a quaternion of norm 35 that is a right divisor of the product $\beta\rho$, our so called α'. Afterwards, we calculate the quotient on the right hand side between $\beta\rho$ and α', yielding σ. Note that sometimes, for example on equations *iii*) and *iv*), this quaternion of norm 35, comorphic to α, does not exist, leading us to continue the process for prime quaternions of higher norms.

The first equation gives us:

$$\begin{aligned}
\rho^{-1}\gamma_0\sigma \in \mathcal{L} &\iff (1+i-j)^{-1}(x_0 - y_0 i - z_0 j - t_0 k)(1-i+k) \in \mathcal{L} \\
&\iff \frac{1}{3}(1-i+j)(x_0 - y_0 i - z_0 j - t_0 k)(1-i+k) \in \mathcal{L} \\
&\iff \frac{1}{3}((-3y_0) + (-x_0 - 2z_0 - 2t_0)i + (2x_0 - 2z_0 + t_0)j + (2x_0 + z_0 - 2t_0)k) \in \mathcal{L} \\
&\iff x_0 + 2z_0 + 2t_0 \equiv 0 \pmod 3 \\
&\iff x_0 - z_0 - t_0 \equiv 0 \pmod 3.
\end{aligned}$$

So, considering we had a solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ for the system $S_{m,n}(1,3,3,4)$, Remark 2 tells us that, when this congruence holds, $\rho^{-1}\gamma_0\sigma$ is an integer solution of $S_{m,n}(1,3,5,0)$. And with the second equation we have:

$$\begin{aligned}
\rho^{-1}\gamma_0\sigma \in \mathcal{L} &\iff (1-i-j)^{-1}(x_0 - y_0 i - z_0 j - t_0 k)(1+j+k) \in \mathcal{L} \\
&\iff \frac{1}{3}(1+i+j)(x_0 - y_0 i - z_0 j - t_0 k)(1+j+k) \in \mathcal{L} \\
&\iff \frac{1}{3}(3z_0 + (2x_0 - 2y_0 + t_0)i + (x_0 + 2y_0 + 2t_0)j + (2x_0 + y_0 - 2t_0)k) \in \mathcal{L} \\
&\iff x_0 + 2y_0 + 2t_0 \equiv 0 \pmod 3 \\
&\iff x_0 - y_0 - t_0 \equiv 0 \pmod 3.
\end{aligned}$$

As of now, we can conclude the following:

Theorem 6. *Let $m, n \in \mathbb{N}$ be such that $35m - n^4 \geq 0$, and not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$. If we have a solution $(x_0, y_0, z_0, t_0) \in \mathbb{N}^4$ of $S_{m,n}(1,3,3,4)$, then if either of the following congruences hold:*

i) $x_0 - y_0 - t_0 \equiv 0 \pmod 3$

ii) $x_0 - z_0 - t_0 \equiv 0 \pmod 3$

we have a solution for $S_{m,n}(1,3,5,0)$.

The other two equations, *iii*) and *iv*), give us two congruences that transform a solution of $S_{m,n}(1,3,3,4)$ into another different solution of the same system, but those were not necessary in solving the conjecture. In the original proof of the conjecture, this process continues for $N(\rho) = 5$ and $N(\rho) = 7$, where there were also equations that did not yield new solutions for

$S_{m,n}(1,3,5,0)$, only transforming the ones of $S_{m,n}(1,3,3,4)$. However, with the congruences that were obtained for $N(\rho) = 3$ and the newly obtained ones in higher norms, these equations helped in completing the lattice of congruences covering all solutions of $S_{m,n}(1,3,3,4)$, producing the following result (see [8] for the full extent of the proof):

Theorem 7. *Let $m, n \in \mathbb{N}$ be such that $35m - n^4 \geq 0$, and not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$. Then*

i) If $m \equiv 0 \pmod 3$, then $S_{m,n}(1,3,5,0)$ has integer solutions whenever $n \not\equiv 0 \pmod 3$ and $n \not\equiv 0 \pmod 5$, in other words, $(n, 15) = 1$.

ii) If $m \equiv 1 \pmod 3$, then $S_{m,n}(1,3,5,0)$ has integer solutions whenever $n \equiv 0 \pmod 3$ and $n \not\equiv 0 \pmod 5$.

iii) If $m \equiv -1 \pmod 3$, then $S_{m,n}(1,3,5,0)$ has integer solutions whenever $n \not\equiv 0 \pmod 3$, $n \not\equiv 0 \pmod 5$ and $n \not\equiv 0 \pmod 7$, in other words, $(n, 105) = 1$.

We still have no information on whether or not for every m we can find an n such that $35m - n^4$ can be written as the sum of three squares. If that was a certainty, then we could improve Theorem 7, which is exactly our next goal. Set $S_m = \{n \in \mathbb{N} : 35m - n^4 \geq 0\}$ and $T_m = \{n \in \mathbb{N} : 35m - n^4 \text{ can be written as the sum of 3 squares}\}$, and note that T_m is always contained in S_m. The perfect situation would be that for every $m \in \mathbb{N}$, T_m is not the empty set, meaning that there would exist an $n \in \mathbb{N}$ such that $35m - n^4$ is non negative and not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$. So we will fix m's and try to find such n's.

Lemma 3. *If $m \not\equiv 0 \pmod{16}$, then T_m contains either all odd numbers of S_m, or all even numbers of S_m.*

Proof. Take $n = 2t \in S_m$, where $t \in \mathbb{N}$, in which case $n^4 = 16t^4 \equiv 0 \pmod 8$. We will calculate $35m - n^4$ modulo 8 and want to avoid $0, 4$ and 7, since if $35m - n^4 \equiv 7 \pmod 8$ then it is of the form $8s + 7$, for some $s \in \mathbb{N}$, and therefore cannot be written as the sum of three squares; if $35m - n^4 \equiv 0, 4 \pmod 8$ we can still factor out more powers of 4 until we get $4^r(8s + k)$ where $r, s, k \in \mathbb{N}$ and $k \not\equiv 4 \pmod 8$, and only then can we conclude whether or not $35m - n^4$ can be written as the sum of three squares.

i) $m \equiv 1 \pmod 8$: $35m - n^4 \equiv 3 \pmod 8$.

ii) $m \equiv 2 \pmod 8$: $35m - n^4 \equiv 6 \pmod 8$.

iii) $m \equiv 3 \pmod 8$: $35m - n^4 \equiv 1 \pmod 8$.

iv) $m \equiv 6 \pmod 8$: $35m - n^4 \equiv 2 \pmod 8$.

v) $m \equiv 7 \pmod 8$: $35m - n^4 \equiv 5 \pmod 8$.

vi) $m \equiv 8 \pmod{16}$: $35m - n^4 \equiv 0 \pmod 8$. Considering that $m = 16k + 8$, for some $k \in \mathbb{N}$, we have $35m - n^4 = 560k + 280 - 16t^4 = 4(140k + 70 - 4t^4)$, and because 70 is not a multiple of four, we can no longer factor out any more fours, and so we are left with checking the congruence:

$$\begin{aligned} 140k + 70 - 4t^4 \equiv 4k + 6 - 4t^4 &\equiv 4(k - t^4) + 6 \pmod 8 \\ &\equiv 2 \pmod 4. \end{aligned}$$

We can then conclude that, for $m \equiv 1, 2, 3, 6, 7 \pmod 8$ and for $m \equiv 8 \pmod{16}$, we have that $2\mathbb{N} \cap S_m \subseteq T_m$.

From now on we will consider $n = 2t + 1 \in S_m$ where $t \in \mathbb{N}$. Remember that the square of an odd number is always congruent to 1 modulo 8.

i) $m \equiv 2 \pmod 8$: $35m - n^4 \equiv 5 \pmod 8$.

ii) $m \equiv 4 \pmod 8$: $35m - n^4 \equiv 3 \pmod 8$.

iii) $m \equiv 5 \pmod 8$: $35m - n^4 \equiv 6 \pmod 8$.

iv) $m \equiv 6 \pmod 8$: $35m - n^4 \equiv 1 \pmod 8$.

Summarizing it gives us the following:

$$\begin{aligned} m &\equiv 1, 2, 3, 6, 7 \pmod 8 && \Longrightarrow 2\mathbb{N} \cap S_m \subseteq T_m \\ m &\equiv 2, 4, 5, 6 \pmod 8 && \Longrightarrow (1 + 2\mathbb{N}) \cap S_m \subseteq T_m \\ m &\equiv 8 \pmod{16} && \Longrightarrow 2\mathbb{N} \ \cap \ S_m \subseteq T_m. \end{aligned}$$

□

Note that this means that $m \equiv 2, 6 \pmod 8 \implies S_m = T_m$.

If $35m - n^4$ can be expressed as the sum of 3 squares, then we can look to Theorem 7 to find more information on whether our system has solutions. We just concluded that T_m either contains all even numbers of S_m or all odd numbers of S_m, but we need to guarantee that there is at least one $n \in T_m$ for every possible case of Theorem 7. What this means is that we need a certain number of consecutive integers in S_m such that it includes an n_1 such that $(n_1, 15) = 1$, an n_2 such that n_2 is a multiple of 3 but not of 5, and an n_3 such that $(n_3, 105) = 1$. Moreover, we need these three cases in both parities in order to apply the last Lemma.

Let us focus first on the classes modulo 15. Let us write all the classes in a line, imagining that the last number is connected to the first, and coloring a number if it is coprime with 15, red if odd, blue if even, and not coloring it if it shares some divisor with 15. It is important to remember that since 15 is an odd number, two elements in the same class do not necessarily share the same parity, for example $3 \equiv 18 \pmod{15}$ but one is odd and one is even, and due to this, we work modulo 30. Thus we have:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29.$$

Now, the goal is to find the smallest number of consecutive integers necessary in order to ensure that, by starting at any integer, we have two numbers coprime with 15, one of each parity. For example, if we start at 0, we need 3 consecutive integers $(0, 1, 2)$ in order to have a blue and a red number. The worst case scenario is by starting at $2, 9, 17(= 2+15), 24(= 9+15)$, where we need 6 consecutive integers.

Now we will repeat the process but instead of considering numbers coprime with 15, we want numbers that are multiples of 3 but not multiples of 5. Coloring the odd ones and the even ones by the same rules as before, we have:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29.$$

This time, we need 12 consecutive integers (from 10 until 21) to guarantee that we have a red and a blue number, with the properties we need, in S_m.

For numbers coprime with 105, since 105 is odd we have the same problem we had modulo 15, so we have to consider a few more numbers after 104 in order to guarantee that there is not any problem when changing the parity.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69	70	71	72	73	74
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99	100	101	102	103	104
105	106	107	$\cdots$											

One can see that 10 consecutive numbers are enough to guarantee at least one blue and one red number, the worst possible cases being: starting at 2 and ending at 11, and starting at 95 and ending at 104. Note that there was no problem when the switch of parity occurred.

So we need 12 consecutive integers, that is, we need m to be such that $|S_m| \geq 12$, to guarantee that all the necessary values of n are contained in S_m, which gives us:

$$35m - 12^4 \geq 0 \iff m \geq \frac{12^4}{35} = \frac{20736}{35} \iff m \geq 593.$$

So if $m \not\equiv 0 \pmod{16}$ and $m \geq 593$, $S_{m,n}(1,3,5,0)$ will have integer solutions. For $m \equiv 0 \pmod{16}$, m is of the form $16^s m'$, with $m, s \in \mathbb{N}$ and $m' \not\equiv 0 \pmod{16}$. This mean that there exists a solution $x_0, y_0, z_0, t_0 \in \mathbb{Z}$ for $S_{m',n}(1,3,5,0)$, and we can easily see that $4^s x_0, 4^s y_0, 4^s z_0, 4^s t_0$ is a solution for $S_{m,n'}(1,3,5,0)$, for some $n' \in \mathbb{N}$:

$$\begin{cases} (4^s x_0)^2 + (4^s y_0)^2 + (4^s z_0)^2 + (4^s t_0)^2 = 16^s(x_0^2 + y_0^2 + z_0^2 + t_0^2) = 16^s m' = m \\ (4^s x_0) + 3(4^s y_0) + 5(4^s z_0) = 4^s(x_0 + 3y_0 + 5z_0) = 4^s n^2 = (2^s n)^2, \end{cases}$$

and since values of $m \leq 593$ can easily be checked by computer, we have:

Theorem 8. *Any $m \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + t^2$, with $x, y, z, t \in \mathbb{Z}$ such that $x + 3y + 5z$ is a square.*

We can further improve this by giving information about the values that $x + 3y + 5z$ can take. If $6 \in S_m$, that is, if $35m - 6^4 \geq 0$, which is equivalent to $m \geq 38$, then we know that T_m either contains $\{1,3,5\}$ or $\{2,4,6\}$. If $m \equiv 0, -1 \pmod 3$ then, by Theorem 7, n can be either 1 or 2, due to both being coprime with 15 and 105. If $m \equiv 1 \pmod 3$, then n needs to be a multiple of 3 that is not a multiple of 5, so the options are $n = 3$ and $n = 6$. For $m < 38$, the result can be easily verified by computer.

Remark 3. *In Theorem 8, for m not divisible by 16, $n^2 = x + 3y + 5z$ can be chosen to be one of $1, 4, 9,$ or 36.*

All that remains is going from integer solutions to natural solutions. And to do that we will need the following result (for a proof, see [9, Theorem 1.35]):

Proposition 2 (Cauchy-Schwarz Inequality in $\mathbb{R}^n$)**.** *Take $u_1, ..., u_n \in \mathbb{R}^+$ and $v_1, ..., v_n \in \mathbb{R}$. We have the following inequality:*

$$\left(\sum_{i=1}^{n} u_i v_i\right)^2 \leq \left(\sum_{i=1}^{n} u_i^2\right)\left(\sum_{i=1}^{n} v_i^2\right).$$

We shall now prove the following theorem:

Theorem 9. *For sufficiently large $m \in \mathbb{N}$ ($m \geq 217\,942\,742\,279$), not divisible by 16, there exists at least one $n \in [\sqrt[4]{34m}, \sqrt[4]{35m}]$ such that $S_{m,n}(1,3,5,0)$ has natural solutions.*

Proof. We know that for m sufficiently large, there will be an $n \in \mathbb{N}$ such that $35m - n^4$ can be written as the sum of three squares. Then there exist $A, B, C \in \mathbb{Z}$ such that $35m = n^4 + A^2 + B^2 + C^2$, and so, for some $\gamma = x - yi - zj - tk \in \mathcal{L}$ where $N(\gamma\alpha) = N(\delta) = 35m$, we have:

$$\delta = \gamma\alpha = n^2 + Ai + Bj + Ck,$$

and multiplying γ by α yields:

$$\delta = (x + 3y + 5z) + (3x - y + 5t)i + (5x - z - 3t)j + (-5y + 3z - t)k,$$

This means that we have:

$$\begin{cases} n^2 = & x + 3y + 5z \\ A = & 3x - y + 5t \\ B = & 5x - z - 3t \\ C = & -5y + 3z - t. \end{cases}$$

Solving for x, y, z, t, yields

$$\begin{cases} x = & \frac{3A+5B+n^2}{35} \\ y = & \frac{-A-5C+3n^2}{35} \\ z = & \frac{-B+3C+5n^2}{35} \\ t = & \frac{5A-3B-C}{35}. \end{cases}$$

Considering that the second line of $S_{m,n}(1,3,5,0)$ does not depend on t, and on the first line t is squared, if (x, y, z, t) is a solution for $S_{m,n}(1,3,5,0)$ then so is $(x, y, z, -t)$, so we can assume t to be positive. For x, y, z to be positive we need

$$\begin{cases} n^2 \geq & -3A - 5B \\ 3n^2 \geq & A + 5C \\ 5n^2 \geq & B - 3C. \end{cases}$$

Setting $(u_1, u_2) = (3, 5)$ and $(v_1, v_2) = (|A|, |B|)$, we can use the Cauchy-Schwarz inequality to get:

$$(3|A|+5|B|)^2 \leq (3^2+5^2)(A^2+B^2) \leq 34(A^2+B^2+C^2) = 34(35m-n^4).$$

If $n^2 \geq \sqrt{34(35m-n^4)} \geq 3|A|+5|B|$, then the first condition is verified, and we get $x \geq 0$. For the last two conditions we have to change the vectors used in the Cauchy-Schwarz inequality. Setting $(u_1, u_2) = (1, 5)$ and $(v_1, v_2) = (|A|, |C|)$ gets us:

$$(|A|+5|C|)^2 \leq (1^2+5^2)(A^2+C^2) \leq 26(A^2+B^2+C^2) = 26(35m-n^4).$$

If $3n^2 \geq \sqrt{26(35m-n^4)} \geq |A|+5|C|$, then the second condition is verified, and we get $y \geq 0$. Lastly, setting $(u_1, u_2) = (1, 3)$ and $(v_1, v_2) = (|B|, |C|)$ leaves us with:

$$(|B|+3|C|)^2 \leq (1^2+3^2)(B^2+C^2) \leq 10(A^2+B^2+C^2) = 10(35m-n^4).$$

If $5n^2 \geq \sqrt{10(35m-n^4)} \geq |B|+3|C|$, then the third condition is verified, and we get $z \geq 0$.

If the first inequality we obtain from this process holds, then that will also be the case for both the second and third inequalities, and so a sufficient condition for $x, y, z, t \in \mathbb{N}$ is that $n^2 \geq \sqrt{34(35m-n^4)}$, which is equivalent to $n \geq \sqrt[4]{34m}$.

Now we need to guarantee that there are at least 12 consecutive integers in S_m, noting that if $n \in S_m$, then $n \leq \sqrt[4]{35m}$.

Knowing this, we need to find $c \in \mathbb{R}$ such that for $m \geq c$, there are at least 12 consecutive integers in $[\sqrt[4]{34m}, \sqrt[4]{35m}]$. We then have a natural solution for $S_{m,n}(1, 3, 5, 0)$ if and only if

$$\begin{aligned} & \sqrt[4]{35m} - \sqrt[4]{34m} \geq 12 \\ \iff & \sqrt[4]{m}(\sqrt[4]{35} - \sqrt[4]{34}) \geq 12 \\ \iff & m \geq \left(\frac{12}{\sqrt[4]{35} - \sqrt[4]{34}}\right)^4 \approx 217\,942\,742\,279. \end{aligned}$$

□

By verifying, with the help of a computer, that for every m up to 217 942 742 278, there exists $n \in \mathbb{N}$, such that $S_{m,n}(1, 3, 5, 0)$ has natural solutions , the "m not divisible by 16" part of the theorem disappears because, when factoring out all powers of 16 from any number, the result is either bigger than 217 942 742 279, meaning that the theorem applies, or smaller, meaning that it was verified to have a solution, and then we can generate, as we have done before, a solution for the original system.

During the writing of this thesis, it was found that the proof to the 1-3-5 conjecture is incomplete due to a mistake in obtaining the number of necessary consecutive integers contained in S_m. The change of parity was overlooked while working modulo 15, reaching 10 as the answer, instead of 12. For example, starting at 10 and ending at 20 (11 numbers), there is not a single number that is odd, multiple of 3 but not multiple of 5.

This meant that, in the original proof, Machiavelo and Tsopanidis, with the help of Rogério Reis, only checked that for all values of m up to 105 103 560 126, there exists $n \in \mathbb{N}$ such that $S_{m,n}(1,3,5,0)$ has natural solutions, reported in [7].

As of submitting this thesis, the proof was completed, having checked that for all values of m up to 217 942 742 278, there exists $n \in \mathbb{N}$ such that $S_{m,n}(1,3,5,0)$ has natural solutions.

Chapter 3

Numbers with 2 Decompositions as Sums of 4 Squares

The objective now is to use the method that was described in the previous chapter to try to solve other systems, and possibly to get an idea of how to generalize the method for all cases, remembering that some, if not most, of the systems will not have natural solutions for all $m \in \mathbb{N}$, which goes to show that there will have to be differences in applying the method to find which solutions the systems actually have.

The previous method worked so well due to the fact that the norm of $1+3i+5j$ is 35, which has exactly two ways of being factored into the sum of 4 squares, $(1,3,5,0)$ and $(1,3,3,4)$, so knowing that we have an integer solution of at least one of them, even while under the restrictions of theorem 5, it was only necessary to convert the solutions of $S_{m,n}(1,3,3,4)$ into the solutions we wanted, and afterwards proving that we indeed could restrict the solutions for the natural numbers.

This lead us to investigate what numbers had exactly 2 ways of being factored into the sum of four squares, which we calculated using Python. This is the code in Python to obtain our results:

```
from math import *

def sum4sq(x):
        a=0
        b=[]
        for i in range(x+1):
                x1=x-i**2
                if x1<0:
                        break
                for j in range(x1+1):
                        x2=x1-j**2
                        if x2<0:
                                break
                        for k in range(x2+1):
                                x3=x2-k**2
                                if x3<0:
                                        break
                                if x3==isqrt(x3)**2:
                                        c=[i,j,k,int(sqrt(x-i**2-j**2-k**2))]
                                        o=list.sort(c)
                                        if c not in b:
                                                b.append(c)
                                                a=a+1
    return (b,a)
```

This computation gave us the following numbers, from 0 to 100:

$$4, 9, 10, 12, 13, 16, 17, 19, 20, 21, 22, 29, 30, 31, 35, 39, 40, 44, 46, 47, 48, 64, 71, 80, 88.$$

Out of these ones, we decided to tackle the first three, in order to get a rough understanding of what to expect before trying to generalize the argument.

We will start by analyzing the systems that originate from quaternions of norm 10, leaving 4 and 9 for later, both of them perfect squares, which means that one of the ways of writing them as the sum of 4 squares is composed by their square roots and three zeros.

Note that we will be using the same notations as in the $(1, 3, 5, 0)$ case; the quaternion that defines the system whose solution we are trying to find will be denoted by α, while the other one will be β. Before doing these calculations it is possible to know which system behaves better, that is, which one had the least amount of exceptions, those being values of m that do not have an integer or natural solution tied to them, by using PARI/GP.

3.1 Systems 1-1-2-2 and 1-3-0-0

The two ways of writing 10 as the sum of four squares give us the following systems:

$$\begin{cases} x^2 + y^2 + z^2 + t^2 = m \\ x + 3y = n^2. \end{cases} \qquad \begin{cases} x^2 + y^2 + z^2 + t^2 = m \\ x + y + 2z + 2t = n^2 \end{cases}$$

Using PARI-GP, we found that both system have integer solutions for every m up to 10000, and we decided to try to find solutions for $S_{m,n}(1,1,2,2)$ from solutions of $S_{m,n}(1,3,0,0)$. So, we set $\alpha = 1 + i + 2j + 2k$ and $\beta = 1 + 3i$, and working with the quaternion primes of norm 3, we obtain:

$$\begin{aligned} \beta(1+i+j) &= (1+i+j)(1+i+2j+2k) \\ \beta(1+i-j) &= (1+i-j)(1+i-2j-2k) \\ \beta(1-i+j) &= (1-i+j)(1+i-2j+2k) \\ \beta(1-i-j) &= (1-i-j)(1+i+2j-2k), \end{aligned}$$

then, the four congruences obtained from the condition $\rho^{-1}\gamma_0\sigma \in \mathcal{L}$ are the following:

Proposition 3. *Let $m, n \in \mathbb{N}$ be such that $10m - n^4 > 0$ and not of the form $4^r(8s + 7)$ for any $r, s \in \mathbb{N}$. If a solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ of the system $S_{m,n}(1,3,0,0)$ verifies any one of the following conditions:*

i) $y_0 - z_0 + t_0 \equiv 0 \pmod 3$;

ii) $y_0 + z_0 - t_0 \equiv 0 \pmod 3$;

iii) $y_0 + z_0 + t_0 \equiv 0 \pmod 3$;

iv) $y_0 - z_0 - t_0 \equiv 0 \pmod 3$;

then the system $S_{m,n}(1,1,2,2)$ has an integer solution.

The objective now is to find if, for any integer solution of $S_{m,n}(1,3,0,0)$, at least one of these congruence holds. Taking $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ as an arbitrary solution of $S_{m,n}(1,3,0,0)$, we know that $n^2 = x_0 + 3y_0 \equiv x_0 \pmod 3$.

Considering we only want to find one n such that the system has a solution, we can add restrictions to it in order to find more information, noticing that a square number can only be congruent to 0 or 1 modulo 3.

Proposition 4. *Let $m, n \in \mathbb{N}$ be such that $10m - n^4 \geq 0$ and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. Then the system $S_{m,n}(1,1,2,2)$ has integer solutions in each of the following situations:*

i) $m \equiv 0 \pmod 3$,

ii) $m \equiv 1 \pmod 3 \wedge n \not\equiv 0 \pmod 3$,

iii) $m \equiv -1 \pmod 3 \wedge n \equiv 0 \pmod 3$.

Proof. Let's first start by considering $n^2 \equiv x_0 \equiv 1 \pmod 3$, which is equivalent to $n \not\equiv 0 \pmod 3$. Then:

i) $m \equiv 0 \pmod 3 \implies x_0^2 + y_0^2 + z_0^2 + t_0^2 \equiv 0 \pmod 3 \implies y_0^2 + z_0^2 + t_0^2 \equiv -1 \pmod 3$.

If $y_0 \equiv 0 \pmod 3$, we have $z_0^2 + t_0^2 \equiv -1 \pmod 3$, which implies that neither z_0 nor t_0 can be congruent to 0 modulo 3. This gives us the following table, where the top line represents the coordinates y, z, t of a solution modulo 3, because only those coordinates affect the congruences obtained previously, which can be found in the first column of the table. Note that the cells are all in modulo 3.

	(0,1,1)	(0,1,-1)	(0,-1,1)	(0,-1,-1)
$y_0 + z_0 + t_0$	-1	0	0	1
$y_0 + z_0 - t_0$	0	-1	1	0
$y_0 - z_0 + t_0$	0	1	-1	0
$y_0 - z_0 - t_0$	1	0	0	-1

We can see that each column has at least one 0, meaning that at least one congruence of Proposition 3 holds in all of these solutions.

If $y_0 \not\equiv 0 \pmod 3$, we have $z_0^2 + t_0^2 \equiv 1 \pmod 3$, and thus one and only one of z_0 and t_0 can, and must, be congruent to 0 modulo 3, giving us the following table:

	(1,0,1)	(1,0,-1)	(1,1,0)	(1,-1,0)	(-1,0,1)	(-1,0,-1)	(-1,1,0)	(-1,-1,0)
$y_0 + z_0 + t_0$	-1	0	-1	0	0	1	0	1
$y_0 + z_0 - t_0$	0	-1	-1	0	1	0	0	1
$y_0 - z_0 + t_0$	-1	0	0	-1	0	1	1	0
$y_0 - z_0 - t_0$	0	-1	0	-1	1	0	1	0

Again, we have at least one 0 in each column, always satisfying at least one congruence of Proposition 3.

ii) $m \equiv 1 \pmod 3 \implies x_0^2 + y_0^2 + z_0^2 + t_0^2 \equiv 1 \pmod 3 \implies y_0^2 + z_0^2 + t_0^2 \equiv 0 \pmod 3$.

If $y_0 \equiv 0 \pmod 3$, we have $z_0^2 + t_0^2 \equiv 0 \pmod 3$, meaning that $z_0 \equiv t_0 \equiv 0 \pmod 3$, making all the three coordinates congruent to 0 modulo 3, trivially verifying all the congruences of Proposition 3 at the same time.

If $y_0 \not\equiv 0 \pmod 3$, we have $z_0^2 + t_0^2 \equiv -1 \pmod 3$ implying that neither z_0 nor t_0 can be congruent to 0 modulo 3, and since

	(1,1,1)	(1,1,-1)	(1,-1,1)	(1,-1,-1)	(-1,1,1)	(-1,1,-1)	(-1,-1,1)	(-1,-1,-1)
$y_0 + z_0 + t_0$	0	1	1	-1	1	-1	-1	0
$y_0 + z_0 - t_0$	1	0	-1	1	-1	1	0	-1
$y_0 - z_0 + t_0$	1	-1	0	1	-1	0	1	-1
$y_0 - z_0 - t_0$	-1	1	1	0	0	-1	-1	1

we have at least one 0 in each column, always satisfying at least one congruence of Proposition 3.

iii) $m \equiv -1 \pmod 3 \implies x_0^2 + y_0^2 + z_0^2 + t_0^2 \equiv -1 \pmod 3 \implies y_0^2 + z_0^2 + t_0^2 \equiv 1 \pmod 3$.

If $y_0 \equiv 0 \pmod 3$, we have $z_0^2 + t_0^2 \equiv 1 \pmod 3$, meaning that one and only one of z_0 and t_0 is congruent to 0 modulo 3. But, then, if exactly two out of the three elements on the congruences of Proposition 3 are 0, then the congruence is never going to equal 0, which means that none of the congruences holds in this case.

If $y_0 \not\equiv 0 \pmod 3$, we have $z_0^2 + t_0^2 \equiv 0 \pmod 3$, which means that both z_0 and t_0 are congruent to 0 modulo 3, which again leaves us with two elements being 0 and y not being congruent to 0, so none of the congruences of Proposition 3 hold in this case either.

This was assuming that $n^2 \equiv 1 \pmod 3$, and so we conclude that if m is either congruent to 0 or 1 modulo 3, then at least one of the congruences holds, and so we have an integer solution for $S_{m,n}(1, 1, 2, 2)$. The problem now is finding if we can conclude anything in regards to values of m congruent to -1 modulo 3.

Let us now assume that $n^2 \equiv x_0 \equiv 0 \pmod 3$.

i) $m \equiv 0 \pmod 3 \implies x_0^2 + y_0^2 + z_0^2 + t_0^2 \equiv 0 \pmod 3 \implies y_0^2 + z_0^2 + t_0^2 \equiv 0 \pmod 3$.

As we are only interested in the y, z and t coordinates, the last line gives us every information we need, which is the same as in the case where $n^2 \equiv 1$, $m \equiv 1 \pmod 3$, which was already checked above that at least one of the congruences always holds.

ii) $m \equiv 1 \pmod 3 \implies x_0^2 + y_0^2 + z_0^2 + t_0^2 \equiv 1 \pmod 3 \implies y_0^2 + z_0^2 + t_0^2 \equiv 1 \pmod 3$.

This time the situation is the same as in $n^2 \equiv 1$, $m \equiv -1 \pmod 3$, where it was verified that no congruences hold.

iii) $m \equiv -1 \pmod 3 \implies x_0^2 + y_0^2 + z_0^2 + t_0^2 \equiv -1 \pmod 3 \implies y_0^2 + z_0^2 + t_0^2 \equiv -1 \pmod 3$.

Finally, we have the same situation as in $n^2 \equiv 1$, $m \equiv 0 \pmod 3$, where we checked that at least one of the congruences will always hold.

$\square$

Now we need to find out, whether or not, for every m we can find an n such that $10m - n^4$ can be written as the sum of three squares. Set $S_m = \{n \in \mathbb{N} : 10m - n^4 \geq 0\}$ and $T_m = \{n \in \mathbb{N} : 10m - n^4 \text{ can be written as the sum of 3 squares}\}$, where the goal again is to prove that for every $m \in \mathbb{N}$, T_m is not the empty set, meaning that there would exist an $n \in \mathbb{N}$ such that $10m - n^4$ is non negative and not of the form $4^r(8s + 7)$ for any $r, s \in \mathbb{N}$. We will fix m, and try to find such values of n.

Lemma 4. *If $m \not\equiv 0, 8 \pmod{16}$, then T_m contains either all odd numbers of S_m, or all even numbers of S_m.*

Proof. Take $n = 2t \in S_m$, where $t \in \mathbb{N}$. One has, if:

i) $m \equiv 1 \pmod 8$: $10m - n^4 \equiv 2 \pmod 8$, proving that $10m - n^4$ can be written as the sum of three squares.

ii) $m \equiv 3 \pmod 8$: $10m - n^4 \equiv 6 \pmod 8$.

iii) $m \equiv 4 \pmod 8$: $10m - n^4 \equiv 0 \pmod 8$. Considering that $m = 8k + 4$, for some $\in \mathbb{N}$, we have $10(8k + 4) - (2t)^4 = 80k + 40 - 16t^4 = 4(20k + 10 - 4t^4)$. We can no longer factor out any more fours, and so we are only left with checking the congruence:

$$20k + 10 - 4t^4 \equiv 4k + 2 - 4t^4 \equiv 4(k - t^4) + 2 \pmod 8.$$

Since $4(k - t^4) + 2$ can never be congruent to 7 modulo 8 nor is a multiple of 4, we have what we wanted.

iv) $m \equiv 5 \pmod 8$: $10m - n^4 \equiv 2 \pmod 8$.

v) $m \equiv 7 \pmod 8$: $10m - n^4 \equiv 6 \pmod 8$.

Other values of m fail for n even, so now we will consider n to be odd, and so $n = 2t+1 \in S_m$ where $t \in \mathbb{N}$. Since then $n^4 \equiv 1 \pmod 8$, one has:

i) $m \equiv 2 \pmod 8$: $10m - n^4 \equiv 3 \pmod 8$.

ii) $m \equiv 6 \pmod 8$: $10m - n^4 \equiv 3 \pmod 8$.

We unfortunately cannot conclude anything in regards to $m \equiv 8 \pmod{16}$. Summarizing everything gives us the following:

$$\begin{aligned} m &\equiv 1,3,4,5,7 \pmod 8 && \Longrightarrow 2\mathbb{N} \cap S_m \subseteq T_m \\ m &\equiv 2,6 \pmod 8 && \Longrightarrow (1+2\mathbb{N}) \cap S_m \subseteq T_m. \end{aligned}$$

□

If $10m - n^4$ can be expressed as the sum of 3 squares, then we can look to Proposition 4 to find more information on whether our system has solutions. We just concluded that T_m either contains all even numbers of S_m or all odd numbers of S_m but we need to guarantee that there is at least one even and one odd $n \not\equiv 0 \pmod 3) \in S_m$ and the same for $n \equiv 0 \pmod 3) \in S_m$ in order to satisfy the proposition 4. For that to be true we need 6 consecutive integers, that is, $|S_m| \geq 6$, meaning that $10m - 6^4 \geq 0$, which is equivalent to $m \geq 130$.

Therefore, if $m \not\equiv 0, 8 \pmod{16}$ and $m \geq 130$, $S_{m,n}(1,1,2,2)$ will have integer solutions. We have already seen, in the 1-3-5 case, how we can take one solution for $S_{m,n}(a,b,c,d)$ and generate solutions for $S_{16^s m, 2^s n}(a,b,c,d)$ for every $s \in \mathbb{N}$. Values of $m \leq 130$ can easily be checked by computer, so we have:

Theorem 10. *Any $m \in \mathbb{N}$, not of the form $16^s m'$, for $s, m' \in \mathbb{N}$, such that $m' \equiv 8 \pmod{16}$, can be written as $x^2 + y^2 + z^2 + t^2$, with $x, y, z, t \in \mathbb{Z}$ such that $x + y + 2z + 2t$ is a square.*

The next step is going from integer solutions for natural solutions. For sufficiently large m, there will be an $n \in \mathbb{N}$, such that $10m - n^4$ can be written as the sum of three squares. Then there exist $A, B, C \in \mathbb{Z}$ such that $10m = n^4 + A^2 + B^2 + C^2$, and so, for some $\gamma = x - yi - zj - tk \in \mathcal{L}$ where $N(\gamma\alpha) = N(\delta) = 10m$, we have:

$$\delta = \gamma\alpha = n^2 + Ai + Bj + Ck,$$

and multiplying γ by α yields:

$$\delta = (x + y + 2z + 2t) + (x - y - 2z + 2t)i + (2x + 2y - z - t)j + (2x - 2y + z - t)k.$$

This means that we have:

$$\begin{cases} n^2 = & x+y+2z+2t \\ A = & x-y-2z+2t \\ B = & 2x+2y-z-t \\ C = & 2x-2y+z-t. \end{cases}$$

Solving for x, y, z, t yields

$$\begin{cases} x = & \frac{A+2B+2C+n^2}{10} \\ y = & \frac{-A+2B-2C+n^2}{10} \\ z = & \frac{-2A-B+C+2n^2}{10} \\ t = & \frac{2A-B-C+2n^2}{10}, \end{cases}$$

and for all of the coordinates to be positive we need

$$\begin{cases} n^2 \geq & -A-2B-2C \\ n^2 \geq & A-2B+2C \\ 2n^2 \geq & 2A+B-C \\ 2n^2 \geq & -2A+B+C. \end{cases}$$

Setting $(u_1, u_2, u_3) = (1, 2, 2)$ and $(v_1, v_2, v_3) = (|A|, |B|, |C|)$, we can use the Cauchy-Schwarz inequality to get:

$$(|A| + 2|B| + 2|C|)^2 \leq (1^2 + 2^2 + 2^2)(A^2 + B^2 + C^2) = 9(10m - n^4).$$

If $n^2 \geq \sqrt{9(10m - n^4)} \geq |A| + 2|B| + 2|C|$, then the first two conditions are verified, and we get $x \geq 0$ and $y \geq 0$. For the last two conditions we need to change (u_1, u_2, u_3) to be equal to $(2, 1, 1)$, getting:

$$(2|A| + |B| + |C|)^2 \leq (2^2 + 1^2 + 1^2)(A^2 + B^2 + C^2) = 6(10m - n^4).$$

If $2n^2 \geq \sqrt{6(10m - n^4)} \geq 2|A| + |B| + |C|$, then the last two conditions are verified and we get $z \geq 0$ and $t \geq 0$. Hence, a sufficient condition for $x, y, z, t \in \mathbb{N}$ is that $n^2 \geq \sqrt{9(10m - n^4)}$, which is equivalent to $n \geq \sqrt[4]{9m}$.

Now we need to guarantee that there are at least 6 consecutive integers in S_m bigger than $\sqrt[4]{9m}$, but first we need to know the maximum value $n \in S_m$ can take. If $10m - n^4 \geq 0$, then

$n \leq \sqrt[4]{10m}$, and knowing this, we need to find $c \in \mathbb{R}$ such that for $m \geq c$ there are at least 6 consecutive integers in $[\sqrt[4]{9m}, \sqrt[4]{10m}]$.

Since $\sqrt[4]{10m} - \sqrt[4]{9m} \geq 6$, we get:

$$\sqrt[4]{m}\left(\sqrt[4]{10} - \sqrt[4]{9}\right) \geq 6 \iff m \geq \left(\frac{6}{\sqrt[4]{10} - \sqrt[4]{9}}\right)^4 \simeq 283\,767\,035.628,$$

and therefore, for $m \geq 283\,767\,036$, there is a natural solution for $S_{m,n}(1,1,2,2)$.

Recall that we cannot conclude anything in regards to numbers that are multiples of 16 or congruent to 8 modulo 16, due to them being excluded of Lemma 4.

Theorem 11. *For sufficiently large $m \in \mathbb{N}$ $(m \geq 283\,767\,036)$, and $m \not\equiv 0, 8 \pmod{16}$, there exists at least one $n \in [\sqrt[4]{9m}, \sqrt[4]{10m}]$ such that $S_{m,n}(1,1,2,2)$ has natural solutions.*

3.2 Systems 2-0-0-0 and 1-1-1-1

The quaternions of norm equal to 4 are: 2 and $1 + i + j + k$, which are associated with the following systems, of which, as we know from Theorem 5, for each $m \in \mathbb{N}$, one of them will have an integer solution if $4m - n^4$ non-negative and not of the form $4^r(8s + 7)$:

$$\begin{cases} x^2 + y^2 + z^2 + t^2 = m \\ 2x = n^2, \end{cases} \qquad \begin{cases} x^2 + y^2 + z^2 + t^2 = m \\ x + y + z + t = n^2. \end{cases}$$

We first set $\alpha = 2, \beta = 1 + i + j + k$, and so will try to create a solution for $S_{m,n}(2,0,0,0)$ from a solution of $S_{m,n}(1,1,1,1)$. Using prime quaternions in $\mathcal{L}$ we were unable to find useful results, and so had to resort, without loss of generality, to prime quaternions in $\mathcal{H}$ of norm 3, thus obtaining the following equations:

$$\begin{aligned}
\beta\left(-\frac{3}{2} - \frac{1}{2}i - \frac{1}{2}j - \frac{1}{2}k\right) &= (-i - j - k)(2) \\
\beta\left(-\frac{1}{2} + \frac{1}{2}i + \frac{3}{2}j - \frac{1}{2}k\right) &= (1 + j + k)(2j) \\
\beta\left(\frac{1}{2} + \frac{1}{2}i - \frac{1}{2}j - \frac{3}{2}k\right) &= (-1 - j + k)(-2) \\
\beta\left(-\frac{1}{2} + \frac{3}{2}i - \frac{1}{2}j + \frac{1}{2}k\right) &= (1 - i + k)(-2).
\end{aligned}$$

Using the first equation, we have

$$\begin{aligned}\rho^{-1}\gamma_0\sigma =& \frac{1}{2}x_0+\frac{1}{2}y_0+\frac{1}{2}z_0+\frac{1}{2}t_0+\left(\frac{1}{2}x_0+\frac{1}{6}y_0-\frac{5}{6}z_0+\frac{1}{6}t_0\right)i\\ &+\left(\frac{1}{2}x_0+\frac{1}{6}y_0+\frac{1}{6}z_0-\frac{5}{6}t_0\right)j+\left(\frac{1}{2}x_0-\frac{5}{6}y_0+\frac{1}{6}z_0+\frac{1}{6}t_0\right)k,\end{aligned}$$

and $\rho^{-1}\gamma_0\sigma \in \mathcal{L}$ if and only if:

$$\begin{cases} x_0+y_0+z_0+t_0 & \equiv 0 \pmod 2 \\ 3x_0+y_0-5z_0+t_0 & \equiv 0 \pmod 6, \end{cases}$$

which is equivalent to:

$$\begin{cases} x_0+y_0+z_0+t_0 & \equiv 0 \pmod 2 \\ y_0+z_0+t_0 & \equiv 0 \pmod 3. \end{cases}$$

Since $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ is a solution for $S_{m,n}(1,1,1,1)$, then any permutation of x_0, y_0, z_0 and t_0 is still a solution, and so from one single equation, we obtain 4 congruences. By repeating the process for the other equations, we can see that the congruence $x_0+y_0+z_0+t_0 \equiv 0 \pmod 2$ is common to all of them, and considering that $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ is a solution for $S_{m,n}(1,1,1,1)$ and the fact that $a^2 \equiv a \pmod 2$, for every $a \in \mathbb{N}$, we have:

$$n^2 = x_0^2+y_0^2+z_0^2+t_0^2 \equiv x_0+y_0+z_0+t_0 \equiv 0 \pmod 2,$$

and therefore n is even. The congruences modulo 3 we obtain from the other equations are the ones we already had from permuting the coordinates of the solution. Thus we get:

Proposition 5. *Let $m, n \in \mathbb{N}$ be such that n is even, $4m-n^4 \geq 0$ and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. If a solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ of the system $S_{m,n}(1,1,1,1)$ verifies any one of the following conditions:*

i) $y_0+z_0+t_0 \equiv 0 \pmod 3$,

ii) $x_0+z_0+t_0 \equiv 0 \pmod 3$,

iii) $x_0+y_0+t_0 \equiv 0 \pmod 3$,

iv) $x_0+y_0+z_0 \equiv 0 \pmod 3$,

then the system $S_{m,n}(2,0,0,0)$ has an integer solution.

Proposition 6. *Let $m, n \in \mathbb{N}$ be such that $4m - n^4 \geq 0$ and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. Then the system $S_{m,n}(2,0,0,0)$ has integer solutions if one of the following congruence holds:*

i) $m \equiv 0 \pmod 3 \wedge n \not\equiv 0 \pmod 3 \wedge n \equiv 0 \pmod 2$,

ii) $m \equiv -1 \pmod 3 \wedge n \equiv 0 \pmod 3 \wedge n \equiv 0 \pmod 2$,

iii) $m \equiv 1 \pmod 3 \wedge n \not\equiv 0 \pmod 3 \wedge n \equiv 0 \pmod 2$.

Proof. It can be easily checked with the help of a computer that, in each situation, at least one of the congruences from Proposition 5 holds. $\square$

In order to improve the above proposition, set $S_m = \{n \in \mathbb{N} : 4m - n^4 \geq 0\}$ and $T_m = \{n \in \mathbb{N} : 4m - n^4 \text{ can be written as the sum of 3 squares}\}$, where the goal is to prove that for every $m \in \mathbb{N}$, T_m is not the empty set, meaning that there would exist an $n \in \mathbb{N}$ such that $4m - n^4$ is non negative and not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$. We will fix m and try to find such values of n.

Lemma 5. *If* $m \not\equiv 0 \pmod{16}$*, then:*

$$\begin{aligned}
m \equiv 1,2,5,6 \pmod 8 &\implies 2\mathbb{N} \cap S_m \subseteq T_m,\\
m \equiv 3 \pmod 8 &\implies 4\mathbb{N} \cap S_m \subseteq T_m,\\
m \equiv 7 \pmod 8 &\implies (2+4\mathbb{N}) \cap S_m \subseteq T_m,\\
m \equiv 4,8 \pmod{16} &\implies 4\mathbb{N} \cap S_m \subseteq T_m,\\
m \equiv 12 \pmod{16} &\implies (2+4\mathbb{N}) \cap S_m \subseteq T_m.
\end{aligned}$$

Proof. Since n is even, $n = 2t$ for some $t \in \mathbb{N}$. Let us first consider the cases modulo 8:

i) $m \equiv 1 \pmod 8$: $4m - n^4 = 4(8k+1) - (2t)^4 = 4(8k+1-4t^4)$ for some $k \in \mathbb{N}$. For every value of t, $8k+1-4t^4 \equiv 1 \pmod 4$, and so it is not a multiple of four and it cannot be congruent to 7 modulo 8;

ii) $m \equiv 2 \pmod 8$: $4m - n^4 = 4(8k+2) - (2t)^4 = 4(8k+2-4t^4)$ for some $k \in \mathbb{N}$. For every value of t, $8k+2-4t^4 \equiv 2 \pmod 4$, again not a multiple of four and it cannot be congruent to 7 modulo 8;

iii) $m \equiv 3 \pmod 8$: $4m - n^4 = 4(8k+3) - (2t)^4 = 4(8k+3-4t^4)$ for some $k \in \mathbb{N}$. For t even, then $8k+3-4t^4 \equiv 3 \pmod 4$;

iv) $m \equiv 5 \pmod 8$: $4m - n^4 = 4(8k+5) - (2t)^4 = 4(8k+5-4t^4)$ for some $k \in \mathbb{N}$. For every value of t, $8k+5-4t^4 \equiv 1 \pmod 4$;

v) $m \equiv 6 \pmod 8$: $4m - n^4 = 4(8k+6) - (2t)^4 = 4(8k+6-4t^4)$ for some $k \in \mathbb{N}$. For every value of t, $8k+6-4t^4 \equiv 2 \pmod 4$;

vi) $m \equiv 7 \pmod 8$: $4m - n^4 = 4(8k+7) - (2t)^4 = 4(8k+7-4t^4)$ for some $k \in \mathbb{N}$. For t odd, then $8k+7-4t^4 \equiv 3 \pmod 4$.

Now we shall analyze the remaining cases modulo 16:

i) $m \equiv 4 \pmod{16}$: $4m - n^4 = 4(16k+4) - (2t)^4 = 16(4k+1-t^4)$ for some $k \in \mathbb{N}$. For t even, $4k+1-t^4 \equiv 1, 5 \pmod 8$, it is not a multiple of four and it cannot be congruent to 7 modulo 8;

i) $m \equiv 8 \pmod{16}$: $4m - n^4 = 4(16k+8) - (2t)^4 = 16(4k+2-t^4)$ for some $k \in \mathbb{N}$. For t even, $4k+2-t^4 \equiv 2, 6 \pmod 8$;

i) $m \equiv 12 \pmod{16}$: $4m - n^4 = 4(16k+12) - (2t)^4 = 16(4k+3-t^4)$ for some $k \in \mathbb{N}$. For t odd, $4k+3-t^4 \equiv 2, 6 \pmod 8$.

$\square$

For $m \not\equiv 0 \pmod{16}$, we need 12 consecutive integers in S_m in order to guarantee that there exists at least one value of n for each of the following conditions:

i) $n \equiv 0 \pmod 3 \wedge n \equiv 0 \pmod 4$;

ii) $n \equiv 0 \pmod 3 \wedge n \equiv 2 \pmod 4$;

iii) $n \not\equiv 0 \pmod 3 \wedge n \equiv 0 \pmod 4$;

iv) $n \not\equiv 0 \pmod 3 \wedge n \equiv 2 \pmod 4$.

If $|S_m| \geq 12$, i.e, $m \geq 5184$, $S_{m,n}(2,0,0,0)$ has integers solutions for $m \not\equiv 0 \pmod{16}$, but we have already seen how to generate solutions for those cases. The cases $m \leq 5184$ can easily be checked by computer to always have a solution.

Also, if we take a solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ of $S_{m,n}(2,0,0,0)$, then $(x_0, \pm y_0, \pm z_0, \pm t_0)$ will also be a solution, and since $2x_0 = n^2$, we have $x_0 \in \mathbb{N}$. We can then conclude that:

Theorem 12. *Any $m \in \mathbb{N}$ can be written as $x^2+y^2+z^2+t^2$ with $x, y, z, t \in \mathbb{N}$ such that $2x$ is a square.*

On the other hand, for most values of m, there do not exist any values of n such that $S_{m,n}(1,1,1,1)$ has solutions, making it unfeasible to have a fruitful study of the system.

3.3 Systems 3-0-0-0 and 1-2-2-0

Now we shall analyze the quaternions of norm equal to 9, which are: 3 and $1 + 2i + 2j$, which produce the following systems:

$$\begin{cases} x^2 + y^2 + z^2 + t^2 = m \\ 3x = n^2, \end{cases} \qquad \begin{cases} x^2 + y^2 + z^2 + t^2 = m \\ x + 2y + 2z = n^2. \end{cases}$$

Let us start by setting $\alpha = 1 + 2i + 2j, \beta = 3$, where the goal is to find a solution for $S_{m,n}(1, 2, 2, 0)$, for some $n \in \mathbb{N}$. Note that, for $\beta = 3$ and ρ a prime quaternion of norm 3, when trying to find the greatest common denominator between 9 and $\beta\rho$, which is the first step in our process, the answer is $\beta\rho$ itself because it divides 9 and is obviously the greatest divisor of itself.

This forced us into a manual approach, where Luis Roçadas wrote a function in pariGP which, for all possible values of ρ (all four non-associated primes of norm 3), went through all possible primes of norm 3, including associates, and divided 3ρ by them on the left hand side. This gives out the following equalities:

$$\begin{array}{rlrl}
\text{i)} & 3(1 + i - j) = (-1 + j + k)(-2 - 2i - j) & \text{vii)} & 3(1 + i + j) = (-1 - j - k)(-2 - 2i + j) \\
\text{ii)} & 3(1 + i - j) = (-1 - i + k)(-2 - i - 2k) & \text{viii)} & 3(1 + i + j) = (-1 + j + k)(-2 - i + 2k) \\
\text{iii)} & 3(1 + i - j) = (-i + j + k)(-2 - 2j - k) & \text{ix)} & 3(1 + i + j) = (-i - j - k)(-2 + 2j + k) \\
\text{iv)} & 3(1 - i - j) = (i + j + k)(-2 - 2i - k) & \text{x)} & 3(1 - i + j) = (i - j - k)(-2 - 2i + k) \\
\text{v)} & 3(1 - i - j) = (-1 + i + k)(-2 - i + 2j) & \text{xi)} & 3(1 - i + j) = (-1 + i - k)(-2 - i - 2j) \\
\text{vi)} & 3(1 - i - j) = (-1 + j + k)(-2 + j - 2k) & \text{xii)} & 3(1 - i + j) = (-1 - j - k)(-2 - j + 2k).
\end{array}$$

where the congruences obtained from the condition $\rho^{-1}\gamma_0\sigma \in \mathcal{L}$ can be found in the following proposition:

Proposition 7. *Let $m, n \in \mathbb{N}$ such that $9m - n^4 \geq 0$ and not of the form $4^r(8s + 7)$, for any $r, s \in \mathbb{N}$. If a solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ of the system $S_{m,n}(3, 0, 0, 0)$ verifies any one of the following conditions:*

i) $x_0 - z_0 - t_0 \equiv 0 \pmod 3$ *iii)* $x_0 - y_0 + z_0 \equiv 0 \pmod 3$ *v)* $x_0 + y_0 + z_0 \equiv 0 \pmod 3$

ii) $x_0 + y_0 + t_0 \equiv 0 \pmod 3$ *iv)* $x_0 - z_0 + t_0 \equiv 0 \pmod 3$ *vi)* $x_0 - y_0 - t_0 \equiv 0 \pmod 3$

vii) $x_0 + z_0 + t_0 \equiv 0 \pmod 3$ *ix)* $x_0 - y_0 - z_0 \equiv 0 \pmod 3$ *xi)* $x_0 - y_0 + t_0 \equiv 0 \pmod 3$

viii) $x_0 + y_0 - t_0 \equiv 0 \pmod 3$ *x)* $x_0 + z_0 - t_0 \equiv 0 \pmod 3$ *xii)* $x_0 + y_0 - z_0 \equiv 0 \pmod 3$.

then the system $S_{m,n}(1,2,2,0)$ *has an integer solution.*

As we did previously, we want to prove that for every solution of the system $S_{m,n}(3,0,0,0)$ at least one of the congruences holds, and therefore we would have solutions for the system $S_{m,n}(1,2,2,0)$. One detail that makes this task a lot easier is the fact that, since we have a solution of $S_{m,n}(3,0,0,0)$, then we know that $3x_0 = n^2$, which implies that $x_0 \equiv 0 \pmod 3$, therefore removing x_0 from all congruences. Here are the non-equivalent congruences that remain:

i) $z_0 + t_0 \equiv 0 \pmod 3$ iii) $y_0 + t_0 \equiv 0 \pmod 3$ v) $y_0 + z_0 \equiv 0 \pmod 3$

ii) $z_0 - t_0 \equiv 0 \pmod 3$ iv) $y_0 - t_0 \equiv 0 \pmod 3$ vi) $y_0 - z_0 \equiv 0 \pmod 3$.

If at least two of y_0, z_0, t_0 are congruent to each other, then one of ii), iv) or vi) will hold. Now, considering we only have three options for residues modulo 3, those being $0, 1$ and 2, in case all coordinates are different, one of the coordinates will be congruent to 1 and one will be congruent to 2, so at least one of i), iii) or v) will hold. Therefore we have:

Proposition 8. *Let* $m, n \in \mathbb{N}$ *such that* $9m - n^4 \geq 0$ *and not of the form* $4^r(8s+7)$*, for any* $r, s \in \mathbb{N}$*. Then the system* $S_{m,n}(1,2,2,0)$ *has an integer solution.*

The next part focuses on finding out whether or not for every m we can find an n such that $9m - n^4$ can be written as the sum of three squares. To do that we set $S_m = \{n \in \mathbb{N} : 9m - n^4 \geq 0\}$ and $T_m = \{n \in \mathbb{N} : 9m - n^4 \text{ can be written as the sum of 3 squares}\}$. We want to prove that for every $m \in \mathbb{N}$, T_m is not the empty set.

Lemma 6. *If* $m \not\equiv 0 \pmod{16}$*, then* T_m *contains either all odd numbers of* S_m*, or all even numbers of* S_m*.*

Proof. Take $n = 2t \in S_m$, where $t \in \mathbb{N}$.

i) $m \equiv 1 \pmod 8 \implies 9m - n^4 \equiv 1 \pmod 8$.

ii) $m \equiv 2 \pmod 8 \implies 9m - n^4 \equiv 2 \pmod 8$.

iii) $m \equiv 3 \pmod 8 \implies 9m - n^4 \equiv 3 \pmod 8$.

iv) $m \equiv 5 \pmod 8 \implies 9m - n^4 \equiv 5 \pmod 8$.

v) $m \equiv 6 \pmod 8 \implies 9m - n^4 \equiv 6 \pmod 8$.

vi) $m \equiv 8 \pmod{16} \implies 9m - n^4 = 9(16k+8) - (2t)^4 = 144k + 72 - 16t^4 = 4(36k + 18 - 4t^4)$, where $k \in \mathbb{N}$. We can no longer factor out any more fours, and we can observe that $36k + 18 - 4t^4 \equiv 2 \pmod 4$, which can never be congruent to 7 modulo 8, and thus we have what we wanted.

Other values of m fail for n even, so from now on we will consider $n = 2t + 1 \in S_m$ where $t \in \mathbb{N}$.

i) $m \equiv 4 \pmod 8 \implies 9m - n^4 \equiv 3 \pmod 8$.

ii) $m \equiv 7 \pmod 8 \implies 9m - n^4 \equiv 6 \pmod 8$.

Summarizing, we have obtained:

$$\begin{aligned}
m &\equiv 1, 2, 3, 5, 6 \pmod 8 && \implies 2\mathbb{N} \cap S_m \subseteq T_m \\
m &\equiv 4, 7 \pmod 8 && \implies (1 + 2\mathbb{N}) \cap S_m \subseteq T_m \\
m &\equiv 8 \pmod{16} && \implies 2\mathbb{N} \cap S_m \subseteq T_m.
\end{aligned}$$

□

In order to have an integer solution, the only requirement from the previous Proposition was that $n \equiv 0 \pmod 3$. Adding the fact that we need to have one such n to be odd and another such n to be even, in order to guarantee that at least one of them is contained in T_m, we see that we need 6 consecutive integers to guarantee the existence of an integer solution, that is, $|S_m| \geq 6$, which is equivalent to $9m - 6^4 \geq 0$, meaning that $m \geq 144$

So if $m \not\equiv 0 \pmod{16}$ and $m \geq 144$, $S_{m,n}(1, 2, 2, 0)$ will have integer solutions, and we know from previous cases how to derive a solution for $m \equiv 0 \pmod{16}$. Values of $m \leq 144$ can easily be checked by computer, so we have:

Theorem 13. *Any $m \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + t^2$, with $x, y, z, t \in \mathbb{Z}$ such that $x + 2y + 2z$ is a square.*

Let us focus now on natural solutions. For sufficiently large values of m, there will be an $n \in \mathbb{N}$ such that $9m - n^4$ can be written as the sum of three squares. From this, and recalling that $\alpha = 1 + 2i + 2j$, we know that there exist $A, B, C \in \mathbb{Z}$ such that:

$$\delta = \gamma\alpha = n^2 + Ai + Bj + Ck,$$

for some $\delta = x - yi - zj - tk \in \mathcal{L}$ with $N(\delta) = 9m$. Multiplying γ by α yields:

$$\delta = (x + 2y + 2z) + (2x - y + 2t)i + (2x - z - 2t)j + (-2y + 2z - t)k.$$

This means that we have:

$$\begin{cases} n^2 = & x + 2y + 2z \\ A = & 2x - y + 2t \\ B = & 2x - z - 2t \\ C = & -2y + 2z - t, \end{cases}$$

and solving for x, y, z, t we get

$$\begin{cases} x = & \frac{2A+2B+n^2}{9} \\ y = & \frac{-A-2C+2n^2}{9} \\ z = & \frac{-B+2C+2n^2}{9} \\ t = & \frac{2A-2B-C}{9}. \end{cases}$$

Note that if (x, y, z, t) is a solution for $S_{m,n}(1, 2, 2, 0)$, then so is $(x, y, z, -t)$, and so we can assume t to be positive. For x, y, z to be positive we need:

$$\begin{cases} n^2 \geq & -2A - 2B \\ 2n^2 \geq & A + 2C \\ 2n^2 \geq & B - 2C. \end{cases}$$

Setting $(u_1, u_2) = (2, 2)$ and $(v_1, v_2) = (|A|, |B|)$, we can use the Cauchy-Schwarz inequality to get:

$$(2|A| + 2|B|)^2 \leq (2^2 + 2^2)(A^2 + B^2) \leq 8(A^2 + B^2 + C^2) = 8(9m - n^4).$$

If $n^2 \geq \sqrt{8(9m - n^4)} \geq 2|A| + 2|B|$, then the first condition is verified and we get $x \geq 0$. Similarly, one can prove that if $2n^2 \geq \sqrt{5(9m - n^4}$, then both the second and third conditions are verified and we get $y \geq 0$ and $z \geq 0$. Hence a sufficient condition for $x, y, z, t \in \mathbb{N}$ is that $n^2 \geq \sqrt{8(9m - n^4)}$, which is equivalent to $n \geq \sqrt[4]{8m}$. Considering that for $n \in S_m$ we have $9m - n^4 \geq 0$, then $n \leq \sqrt[4]{9m}$.

Knowing this, we need to find $c \in \mathbb{R}$ such that for $m \geq c$, there are at least 6 consecutive integers in $[\sqrt[4]{8m}, \sqrt[4]{9m}]$. With such c, we have a natural solution for $S_{m,n}(1,2,2,0)$

$$\begin{aligned}\sqrt[4]{9m} - \sqrt[4]{8m} \geq 6 &\iff \sqrt[4]{m}\left(\sqrt[4]{9} - \sqrt[4]{8}\right) \geq 6 \\ &\iff m \geq \left(\frac{6}{\sqrt[4]{9} - \sqrt[4]{8}}\right)^4 \simeq 203\,135\,106.62731\ldots\ .\end{aligned}$$

Theorem 14. *For sufficiently large $m \in \mathbb{N}$ ($m \geq 203135107$) not divisible by 16 there exists at least one $n \in [\sqrt[4]{8m}, \sqrt[4]{9m}]$ such that $S_{m,n}(1,2,2,0)$ has natural solutions.*

Having finished this case, let us try solving $S_{m,n}(3,0,0,0)$. In order to do that, set $\alpha = 3, \beta = 1 + 2i + 2j$, and we obtain the following equations:

$$\begin{aligned}\beta(1+i+j) &= (-1+i+j)(3) \\ \beta(1+i-j) &= (1+j-k)(2+2i+j) \\ \beta(1-i+j) &= (1+i+k)(2+i+2j) \\ \beta(1-i-j) &= (-1+i+j)(-1-2i-2j).\end{aligned}$$

This time, while the method has not been completely fruitless, we only obtain one equation that is helpful, granting us only one congruence. Unfortunately, when moving to primes of higher norms, we do not obtain any useful equation; if you have a solution for $S_{m,n}(1,2,2,0)$ you cannot manipulate it using remark 2 to get a solution for $S_{m,n}(1,3,3,0)$. For that to happen we would need to solve $(1+2i+2j)\rho = \sigma 3$, where ρ and σ are primes of norm p, with $p \geq 5$, but then:

$$(1+2i+2j)\rho = \sigma 3 \iff (1-i-j)(-1+i+j)\rho = (1-i-j)(1+i+j)\sigma \iff (-1+i+j)\rho = (1+i+j)\sigma.$$

On both sides of the equation, we have the product of primes of different norms, which is primitive, and so the factorization of the product is unique in the model corresponding to the ordered prime factorization of the norm: $3p$. This implies that $(-1+i+j)$ and $(1+i+j)$ are associated, which is not true, leaving us with an contradiction.

We will try solving $S_{m,n}(3,0,0,0)$ with a different approach in the next chapter.

Chapter 4

The a-0-0-0 problem

In the previous chapter we tried to apply the method developed by Tsopanidis and Machiavelo to systems $S_{m,n}(a,b,c,d)$ where the norm of $a+bi+cj+dk$ was either $4, 9$ or 10, those being the 3 smallest numbers with only 2 ways of being represented as sums of four squares. However, there were difficulties to apply it to $\alpha' = 2$, having to resort to Hurwitz primes, and $\alpha'' = 3$, where it was impossible to apply the method at all. What both systems have in common is the fact that α' and α'' are quaternions that are real numbers.

The objective now is finding some alternative methodology that works in such cases, which led us to consider the systems of the form $S_{m,n}(a,0,0,0)$, where $a \in \mathbb{N}$, that is, we want to find out, for fixed $a \in \mathbb{N}$, for what values of $m \in \mathbb{N}$ there exists at least one $n \in \mathbb{N}$ such that the following system:

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

has solutions $x, y, z, t \in \mathbb{N}$.

Before continuing, we can consider a to be square-free because if $a = a_1 a_2^2$, where a_1 is the square free part of a, then $ax = a_1 a_2^2 x = n^2$, which is equivalent to $a_1 x = \left(\frac{n}{a_2}\right)^2$. This means that a solution of $S_{m,n}(a,0,0,0)$ is a solution of $S_{m,\frac{n}{a_2}}(a_1,0,0,0)$, and vice-versa.

The problem is trivial for m not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$, because then m can be written as the sum of three squares, and if $y^2 + z^2 + t^2 = m$ we can just take $x = 0$.

So, we assume from now on that m is of the form $4^r(8s+7)$, and we can use a similar approach to the one used in the trivial case above; by passing x^2 to the other side of the expression, we obtain the following equation: $y^2 + z^2 + t^2 = m - x^2$, which will have natural solutions when $m - x^2 \geq 0$ and not of the form $4^r(8s+7)$ for $r, s \in \mathbb{N}$.

Since ax has to be a perfect square, it means that $x = ab^2$, for some $b \in \mathbb{N}$. We can set

$a = 2^u c$ and $b = 2^v d$, $u, v, c, d \in \mathbb{N}$, where $u \in \{0, 1\}$ because a is assumed to be square free, and c and d are odd numbers. Remember that u, c are fixed and that we are looking v, d. Thus, we have:

$$m - x^2 = m - (ab^2)^2 = 4^r(8s+7) - a^2b^4 = 4^r(8s+7) - 4^{u+2v}c^2d^4.$$

Let us tackle this by separating the problem into two cases, when a is odd and when a is even.

4.1 a odd

If a is odd, then $u = 0$, which leads us to $m - x^2 = 4^r(8s+7) - 4^{2v}c^2d^4$. Our goal is to find a solution, and so we only need to find values of v, d that give us an adequate solution. Thus, we can define v according to our needs in each case.

We have two situations depending on the parity of r. If r is even, then setting $v = \frac{r}{2}$ we get:

$$4^r(8s+7) - 4^{2v}c^2d^4 = 4^r(8s+7-c^2d^4),$$

and because c,d, and consequently d^2, are odd numbers, so is the product cd^2; and therefore

$$8s+7-c^2d^4 \equiv 7 - c^2d^4 \equiv 7 - 1 \equiv 6 \pmod 8,$$

which means that $m - x^2$ is not of the form $4^r(8s+7)$, and we now only need to check if $8s+7-c^2d^4 \geq 0$. To maximize the values where this inequality is valid, we set $d = 1$, the smallest of the odd numbers. Since a is odd, then $a = c$ and we get:

$$8s+7 \geq a^2.$$

Thus we conclude that, for a odd and for $m = 4^r(8s+7)$, for some $r, s \in \mathbb{N}$, where r is even, if $8s+7 \geq a^2$, we have a solution for $S_{m,n}(a,0,0,0)$, with $n^2 = ax = (ab)^2 = a^2 2^r$.

We can go even further, and prove the reciprocal of this result. Let a and m be as above, and suppose that we have a solution (x_0, y_0, z_0, t_0) of $S_{m,n}(a,0,0,0)$. Then, we know that $m - x_0^2 = 4^r(8s+7) - 4^{2v}c^2d^4$, for some $v, d \in \mathbb{N}$, can be written as the sum of three squares. If $v = \frac{r}{2}$ we have a solution, as seen above, and so we have to consider the remaining two possibilities:

If $v < \frac{r}{2}$, then:

$$4^r(8s+7) - 4^{2v}c^2d^4 = 4^{2v}(4^{r-2v}(8s+7) - c^2d^4),$$

and, considering that $r-2v$ is a even number, greater than zero, we know that 4^{r-2v} is a multiple of 16, and consequently, a multiple of 8. We are left with the following congruence:

$$4^{r-2v}(8s+7)-c^2d^4 \equiv -c^2d^4 \equiv -1 \equiv 7 \pmod 8,$$

a contradiction, since $m-x^2$ can be written as a sum of three squares.

If $v>\frac{r}{2}$, then:

$$4^r(8s+7)-4^{2v}c^2d^4 = 4^r(8s+7-4^{2v-r}c^2d^4),$$

which, considering that $2v-r$ is a even number, greater than zero, leaves us with with following congruence:

$$(8s+7)-4^{2v-r}c^2d^4 \equiv 7 \pmod 8,$$

again, a contradiction, since $m-x^2$ can be written as a sum of three squares. We have just proved that every solution of $S_{m,n}(a,0,0,0)$, for a odd and $m=4^r(8s+7)$ for some $r,s\in\mathbb{N}$, where r is even, has to respect the congruence obtained by setting $v=\frac{r}{2}$, which is $8s+7\geq a^2$.

Let us now consider that r is odd, and set $v=\frac{r-1}{2}$. We have:

$$4^r(8s+7)-4^{2v}c^2d^4 = 4^{r-1}(4(8s+7)-c^2d^4),$$

and

$$4(8s+7)-c^2d^4 \equiv 28-c^2d^4 \equiv 3 \pmod 8,$$

which means that $m-x^2$ is not of the form $4^r(8s+7)$. We now are left with checking if $32s+28-c^2d^4\geq 0$. To maximize the values where this inequality is valid, we again set $d=1$. Knowing that $a=c$, we then get the following:

$$32s+28\geq a^2,$$

which is equivalent to $8s+7\geq \left(\frac{a}{2}\right)^2$. Therefore we can conclude that, for a odd and for $m=4^r(8s+7)$, for some $r,s\in\mathbb{N}$, where r is odd, if $32s+28\geq a^2$, we have a solution for $S_{m,n}(a,0,0,0)$, with $n^2=ax=(ab)^2=a^2 2^{r-1}$.

The reciprocal result can be obtained with an approach analogous to what was used in the case where r was even. With this we have the following result:

Proposition 9. *Let $m, A \in \mathbb{N}$, where $A = ab^2$, for some $a, b \in \mathbb{N}$ where a is the square free part of A, and assume a is odd. If $m \neq 4^r(8s+7)$, for any $r, s \in \mathbb{N}$, then there exists $n \in \mathbb{N}$ such that $S_{m,n}(A,0,0,0)$ has natural solutions for all $A \in \mathbb{N}$. Assume now that $m = 4^r(8s+7)$ for some $r, s \in \mathbb{N}$, then:*

i) When r is even, there exists $n \in \mathbb{N}$ such that $S_{m,n}(A,0,0,0)$ has natural solutions if and only if $8s+7 \geq a^2$;

ii) When r is odd, there exists $n \in \mathbb{N}$ such that $S_{m,n}(A,0,0,0)$ has natural solutions if and only if $8s+7 \geq \left(\frac{a}{2}\right)^2$.

4.2 a even

Let's now look into the situation where a is even. This time $u = 1$, and so $m - x^2 = 4^r(8s+7) - 4^{2v+1}c^2d^4$.

We will start by considering r to be odd this time, and again setting $v = \frac{r-1}{2}$, yields the following:

$$4^r(8s+7) - 4^{2v+1}c^2d^4 = 4^r((8s+7) - c^2d^4),$$

and $8s+7-c^2d^4 \equiv 6 \pmod 8$, meaning that we only need to focus on the inequality $8s+7 > c^2d^4$. Again considering d to be equal to 1, and knowing that this time we have $c = \frac{a}{2}$, the inequality we get is:

$$32s + 28 \geq a^2,$$

equivalent to $8s+7 \geq \left(\frac{a}{2}\right)^2$. Thus we conclude that, for a even and for $m = 4^r(8s+7)$, for some $r, s \in \mathbb{N}$, where r is odd, if $32s+28 \geq a^2$, we have a solution for $S_{m,n}(a,0,0,0)$, with $n^2 = ax = (ab)^2 = a^2 2^{r-1}$.

Finally, let's consider r to be even. Let us begin by considering only $r = 0$. Setting $v = 0$ and $d = 1$, we have:

$$4^r(8s+7) - 4^{2v+1}c^2d^4 = 8s+7-4c^2 = 8s+7-(2c)^2 = 8s+7-a^2.$$

Remember that a is even and that it is square-free, so $a \equiv 2 \pmod 4$, which implies that $a^2 \equiv 4 \pmod 8$. Therefore:

$$8s+7-a^2 \equiv 7-4 \equiv 3 \pmod 8,$$

meaning that if a is even and $r = 0$, $m - x^2$ will not be of the form $4^r(8s+7)$, and we are only left with the inequality:

$$8s + 7 \geq a^2.$$

We then conclude that, for a even and for $m = (8s + 7)$, for some $s \in \mathbb{N}$, if $8s + 7 \geq a^2$, we have a solution for $S_{m,n}(a, 0, 0, 0)$, with $n^2 = ax = (ab)^2 = a^2$.

Now, for $r \geq 2$, setting $v = \frac{r-2}{2}$, which is equivalent to $r = 2v + 2$, makes it possible to factor out all powers of 4 of $x^2 = 4^{2v+1}c^2d^4$. This yields:

$$4^r(8s + 7) - 4^{2v+1}c^2d^4 = 4^{r-1}(4(8s + 7) - c^2d^4),$$

and

$$4(8s + 7) - c^2d^4 \equiv 28 - c^2d^4 \equiv 3 \pmod 8.$$

By setting $d = 1$, we can get the final inequality which is $32s + 28 \geq c^2$. Remembering that $c = \frac{a}{2}$ we have

$$128s + 112 \geq a^2,$$

which is equivalent to $8s + 7 \geq \left(\frac{a}{4}\right)^2$. Therefore, for a even and for $m = 4^r(8s + 7)$, for some $r, s \in \mathbb{N}$, where r is even and non-zero, if $128s + 112 \geq a^2$, we have a solution for $S_{m,n}(a, 0, 0, 0)$, with $n^2 = ax = (ab)^2 = a^2 2^{r-2}$.

The reciprocal result for all three cases, can be obtained using an analogous approach to the one used for a odd. Organizing what was seen above, in the case where a is even, we get:

Proposition 10. *Let $m, A \in \mathbb{N}$, where $A = ab^2$, for some $a, b \in \mathbb{N}$, where a is the square free part of A, and assume a is even. If $m \neq 4^r(8s + 7)$, for $r, s \in \mathbb{N}$, then there exists $n \in \mathbb{N}$ such that $S_{m,n}(A, 0, 0, 0)$ has natural solutions for all $A \in \mathbb{N}$. If $m = 4^r(8s + 7)$ for some $r, s \in \mathbb{N}$, then:*

i) When $r = 0$, there exists $n \in \mathbb{N}$ such that $S_{m,n}(A, 0, 0, 0)$ has natural solutions if and only if $8s + 7 \geq a^2$;

ii) When r is odd, there exists $n \in \mathbb{N}$ such that $S_{m,n}(A, 0, 0, 0)$ has natural solutions if and only if $8s + 7 \geq \left(\frac{a}{2}\right)^2$;

iii) When $r > 0$ is even, there exists $n \in \mathbb{N}$ such that $S_{m,n}(A, 0, 0, 0)$ has natural solutions if and only if $8s + 7 \geq \left(\frac{a}{4}\right)^2$.

This concludes all the cases, and so we can organize them into the following theorem:

Theorem 15. *Let $m, A \in \mathbb{N}$, where $A = ab^2$, for some $a, b \in \mathbb{N}$, where a is the square free part of A. If $m \neq 4^r(8s+7)$, for $r, s \in \mathbb{N}$, then there exists $n \in \mathbb{N}$ such that $S_{m,n}(A,0,0,0)$ has natural solutions for all $A \in \mathbb{N}$. If $m = 4^r(8s+7)$ for some $r, s \in \mathbb{N}$, then:*

i) When a is odd and r is even, or when a is even and $r = 0$, there exists $n \in \mathbb{N}$ such that $S_{m,n}(A,0,0,0)$ has natural solutions if and only if $8s+7 \geq a^2$;

ii) When r is odd, there exists $n \in \mathbb{N}$ such that $S_{m,n}(A,0,0,0)$ has natural solutions if and only if $8s+7 \geq (\frac{a}{2})^2$;

iii) When a and r are both even, and $r > 0$, there exists $n \in \mathbb{N}$ such that $S_{m,n}(A,0,0,0)$ has natural solutions if and only if $8s+7 \geq (\frac{a}{4})^2$.

Example 1: Let $A = 12$ which is equal to 3×2^2 and therefore behaves in the same way as $a = 3$. Since a is odd, iii) and the second part of i) from Theorem 15 do not need to be considered. The inequality in ii) always holds, considering that $\left(\frac{3}{2}\right)^2 = 2.25$ is smaller than 7, the smallest possible value of $8s+7$, for s natural.

Looking into the first part of i), we have $8s+7 \geq 3^2 = 9$, and the inequality is only invalid when $s = 0$, telling us that $S_{m,n}(3,0,0,0)$ (and consequently, $S_{m,n}(12,0,0,0)$) does not have natural solutions if and only if $m = 4^r \times 7$, where r is even, meaning that 7×16^k, for $k \in \mathbb{N}$ are the only exceptions.

Example 2: Let $A = 14 = 2 \times 7$, which is square free. Considering that $A = a$ is even, we can ignore the first part of i) and examine the rest of the inequalities:

i) $8s+7 \geq 14^2 = 196 \iff 8s \geq 189 \iff s \geq 23.625$, which results in all m's of the form $8s+7$, for $s \in$ [0,23] not having natural solutions for $S_{m,n}(14,0,0,0)$.

ii) $8s+7 \geq \left(\frac{14}{2}\right)^2 = 7^2 = 49 \iff 8s \geq 42 \iff s \geq 5.25$, which results in all m's of the form $4^r(8s+7)$, for $s \in$ [0,5] and r odd not having natural solutions for $S_{m,n}(14,0,0,0)$, meaning that $28, 60, 92, 124, 156, 188$ and all its multiples by powers of 16 are exceptions.

iii) $8s+7 \geq \left(\frac{14}{4}\right)^2 = (3.5)^2 = 12.25 \iff 8s \geq 5.25 \iff s \geq 0.65625$, which results in all m's of the form $16^s 7$, for $s > 0$, not having a solution for $S_{m,n}(14,0,0,0)$.

We can conclude that there exists $n \in \mathbb{N}$ such that $S_{m,n}(14,0,0,0)$ has natural solutions if and only if m is not of the following form:

$$15, 23, 31, 39, 47, 55, 63, 71, 79, 87, 95, 103, 111, 119, 127, 135, 143, 151, 159, 167, 175, 183, 191$$

$$7 \times 16^k, 28 \times 16^k, 60 \times 16^k, 92 \times 16^k, 124 \times 16^k, 156 \times 16^k, 188 \times 16^k, k \in \mathbb{N}.$$

Chapter 5

Conclusion

In the beginning of this thesis, a brief, but necessary, exposure of the basic of quaternions was made, with a particular focus on Lipschitz and Hurwitz quaternions. Their useful connecting bridges to the natural numbers, in the way of the theorem of four squares and their unique model factorization, were essential in the proof of the 1-3-5 conjecture, of which we present a sketch, with an added correction.

Afterwards, applying the methods used to prove the conjecture, we were able to successfully solve other problems, completely analyzing the systems $S_{m,n}(1,1,2,2)$, $S_{m,n}(2,0,0,0)$ and $S_{m,n}(1,2,2,0)$.

We were also able to fully describe the solutions of the systems $S_{m,n}(a,0,0,0)$ for all $a \in \mathbb{N}$, with an alternative methodology, inspired by the difficulties observed in the previous sections with the systems $S_{m,n}(2,0,0,0)$ and $S_{m,n}(3,0,0,0)$.

While still very isolated results, they are a great step toward fully understanding the systems of this form, not forgetting that the research of Diophantine equations is older than most mathematics, and the knowledge obtained in the pursuit of their solutions is invaluable. One should not forget that the tools developed throughout this research, and the new found familiarization with quaternions, could lead into more results, possibly unrelated to Diophantine equations, down the line.

Going forward, a major problem that we are faced with lies in the fact that the approach used in solving the 1-3-5 conjecture is only applicable case by case; trying to generalize it seems too hard of a problem, if not an impossible one, due to every system behaving in vastly different ways. That being said, I truly believe that, by separating all of them into certain families of systems, like we did in the last chapter of this thesis, some more general results might be possible in the future. Another evident limitation is the time factor, too many tests have to be run and too many approaches have to be tested in order to find more results, and I wish I had the opportunity to continue this research for a longer period of time.

Finishing this thesis, one cannot help but be overjoyed when looking backwards. It was the most pleasant of experiences to be able to finally do research in a area that is so close to my heart as number theory is, while being supported by the best of guidances. Lastly, my hope is that these pages fuel in someone the urge to pick up these pieces and dive into problems of this nature, firmly believing that the more people work in number theory, the better mathematics gets as a whole.

Bibliography

[1] NC Ankeny. Sums of Three Squares. *Proceedings of the American Mathematical Society*, 8(2):316–319, 1957.

[2] Boyd Coan and Cherng-tiao Perng. Factorization of Hurwitz Quaternions. In *Int. Math. Forum*, volume 7, pages 2143–2156, 2012.

[3] Henry Cohn and Abhinav Kumar. Metacommutation of Hurwitz Primes. *Proceedings of the American Mathematical Society*, 143(4):1459–1469, 2015.

[4] John H Conway and Derek A Smith. *On Quaternions and Octonions*. CRC Press, 2003.

[5] Adrien Marie Legendre. *Essai sur la Theorie des Nombres*. Courcier, 1808.

[6] Derrick H Lehmer. On the Partition of Numbers into Squares. *The American Mathematical Monthly*, 55(8):476–481, 1948.

[7] António Machiavelo, Rogério Reis, and Nikolaos Tsopanidis. Report on Zhi-Wei Sun's 1-3-5 Conjecture and Some of Its Refinements. *Journal of Number Theory*, 222:21–29, 2021.

[8] António Machiavelo and Nikolaos Tsopanidis. Zhi-Wei Sun's 1-3-5 Conjecture and Variations. *Journal of Number Theory*, 222:1–20, 2021.

[9] Walter Rudin. *Principles of Mathematical Analysis*. 1953.

[10] Zhi-Wei Sun. Refining Lagrange's Four-Square Theorem. *Journal of Number Theory*, 175:167–190, 2017.

[11] John Voight. *Quaternion Algebras*. Springer, 2021.