U.PORTO
FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

The Hurwitz and Lipschitz Integers and Some Applications

Nikolaos Tsopanidis

UC|UP joint PhD Program in Mathematics
Tese de Doutoramento apresentada à
Faculdade de Ciências da Universidade do Porto
Departamento de Matemática

2020

The Hurwitz and Lipschitz Integers and Some Applications

Nikolaos Tsopanidis

UC|UP Joint PhD Program in Mathematics

Programa Inter-Universitário de Doutoramento em Matemática

PhD Thesis | Tese de Doutoramento

January 2021

Acknowledgements

The undertaking of a PhD in mathematics, and in particular in number theory, is a very challenging task. As a friend once said, doing a PhD just demonstrates your ability to suffer for a long period of time. During my PhD years many adversities arose to make my life difficult, and questioned my determination and therefore the outcome of my studies. The completion of this thesis was made possible, with the help of many people. First and foremost is my supervisor, António Machiavelo. From scholarship issues to pandemics, you were there for me, helping me in every possible way, suffering through my messy ways and trying to put some order into my chaos. Thank you for everything! I would also like to thank the good friends that I made during these years in Portugal. You guys know who you are, you helped me through the hardships and gave me some great moments to remember, without you all these would have been meaningless. Finally I want to thank my parents together with my brother and sister for their continuing support through the years.

I would like to acknowledge the financial support by the FCT — Fundação para a Ciência e a Tecnologia, I.P.—, through the grants with references PD/BI/143152/2019, PD/BI/135365/2017, PD/BI/113680/2015, and by CMUP — Centro de Matemática da Universidade do Porto —, which is financed by national funds through FCT under the project with reference UID/MAT/00144/2020.

Abstract

In this thesis we examine the rings of Lipschitz and Hurwitz integers, describe some of their properties, and apply those to solve certain systems of Diophantine equations. In particular, we expound the parts of the seminal works of Hurwitz and Pall on those integers that are most relevant to our purposes.

The main result of this thesis is the proof of Zhi-Wei Sun's "1-3-5 Conjecture". This conjecture states that any integer can be written as a sum of four squares, $x^2 + y^2 + z^2 + t^2$ $(x, y, z, t \in \mathbb{N})$, in such a way that $x + 3y + 5z$ is also a square. We present a proof that uses basic arithmetic on the ring of Lipschitz integers, together with an idea that combines metacommutation and conjugation by Lipschitz primes of norm $3, 5$, and 7.

Moreover, we prove a similar result for many systems of equations with a form analogous to the 1-3-5 conjecture. We also present a result about the cycle structure of the permutation induced by the metacommutation map for prime quaternions, and present a generalization of this map for semiprime quaternions. Finally, we propose a way to attack similar open problems by using a method that uses this generalization, and show how one can get, at least, partial results using this method.

Resumo

Nesta tese, examinamos os anéis dos inteiros de Lipschitz e de Hurwitz, descrevemos algumas das suas propriedades e usamos essas propriedades na resolução de certos sistemas de equações Diofantinas. Em particular, expomos as partes dos trabalhos seminais de Hurwitz e Pall relativos a esses inteiros que são mais relevantes para os nossos propósitos.

O principal resultado desta tese é a demonstração da "Conjetura 1-3-5" de Zhi-Wei Sun. Esta conjetura afirma que qualquer número inteiro pode ser escrito como uma soma de quatro quadrados, $x^2+y^2+z^2+t^2$ $(x,y,z,t \in \mathbb{N})$, de tal maneira que $x+3y+5z$ seja também um quadrado. Apresentamos uma demonstração que usa a aritmética básica do anel de números inteiros de Lipschitz, juntamente com uma ideia que combina metacomutação e conjugação por números primos de Lipschitz de norma igual a $3, 5$ e 7.

Demonstramos ainda um resultado semelhante para outros sistemas de equações com uma forma análoga à do sistema da conjetura 1-3-5. Também apresentamos um resultado sobre a estrutura da decomposição em ciclos da permutação induzida pela aplicação de metacomutação para quaterniões primários e uma generalização desta aplicação para quaterniões semiprimos. Por fim, propomos uma maneira de atacar problemas abertos semelhantes, usando um método que usa essa generalização e mostramos como é possível obter, pelo menos, resultados parciais com tal método.

Table of contents

1 Introduction

The main study of this thesis is the investigation of the rings of Lipschitz and Hurwitz integers. We prove some of the key properties of them, and apply those to solve certain systems of Diophantine equations. These rings are subrings of the ring of **Hamilton Quaternions**, that is denoted by $\mathbb{H}$, and is defined to be

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

which is actually a division algebra over $\mathbb{R}$. The multiplication in $\mathbb{H}$ is determined by

$$i^2 = j^2 = k^2 = ijk = -1.$$

Let $\alpha = a + bi + cj + dk \in \mathbb{H}$. The quaternion $\bar{\alpha} = a - bi - cj - dk$ is called the **conjugate** of α. The **Norm** of $\alpha \in \mathbb{H}$ is defined to be

$$\mathrm{N}(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2.$$

Definition 1.1. *The ring of* ***Lipschitz integers*** *is denoted by $\mathcal{L}$ and is defined to be*

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

Definition 1.2. *The ring of* ***Hurwitz integers*** *is denoted by* $\mathcal{H}$ *and is defined to be*

$$\mathcal{H} = \left\{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z} \text{ or, } a, b, c, d \in \frac{1}{2} + \mathbb{Z} \right\}.$$

Let $a, b \in \mathcal{H}$. We say that a **divides** b **from the left** and write $a \rceil b$, if there is $c \in \mathcal{H}$ such that $ac = b$. Similarly we say that a **divides** b **from the right** and write $a \lceil b$, if there is $c \in \mathcal{H}$ such that $ca = b$. Division on the left and on the right in $\mathcal{L}$ are defined the same way.

The elements in $\mathcal{L}$ of norm equal to a rational prime are called **Lipschitz primes**. We say that a Lipschitz prime $P \in \mathcal{L}$ of norm p, **lies above** p. A **Hurwitz prime** is similarly an element in $\mathcal{H}$ with rational prime norm.

On the second chapter, after some preiliminaries, we will prove some of the major properties of these rings. In particular we will see that both of them constitute an order in the quaternion algebra

$$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk \mid (a, b, c, d) \in \mathbb{Q}^4\},$$

with $\mathcal{H}$ being a maximal one. Moreover, we will present the proofs of [3, Theorem 2, p. 57] and of [15, Theorem 1], which establish that both of these rings have a kind of unique factorization into prime elements, albeit a much weaker one than the unique factorization of the integers, due to the lack of commutativity. We finish the second chapter with an exposition of the ideals in the ring of Lipschitz integers.

In chapter 3, we will present some of the work that has been done by Adolf Hurwitz and Gordon Pall on these rings. Using the arithmetic on the ring of Lipschitz integers, we will present Hurwitz's very natural way to prove **Jacobi's 4 square theorem**:

Theorem 1.3 (Jacobi)**.** *The number of ways to represent* n *as the sum of four squares is eight times the sum of the divisors of* n*, if* n *is odd, and 24 times the sum of the odd divisors of* n*, if* n *is even.*

This proof can be found in [7], in German. Moreover we will prove a particular case of the above theorem, which is the following.

Theorem 1.4. *Let $p \in \mathbb{Z}$ be a prime. There are $p+1$ Lipschitz primes up to associates that lie above p.*

We will finish chapter 3 by exposing some major results of Gordon Pall papers [15] and [16] on the arithmetic of quaternions.

In chapter 4 we will demonstrate the main result of this thesis, which is a proof of the **Zhi-Wei Sun's "1-3-5 Conjecture"**, that states the following:

Theorem 1.5. *Any $m \in \mathbb{N}$ can be written as a sum of four squares, $x^2 + y^2 + z^2 + t^2$ with $x, y, z, t \in \mathbb{N}_0$, in such a way that $x + 3y + 5z$ is a perfect square.*

There have been some advances towards a proof of this conjecture in the past, namely Y.-C. Sun and Z.-W. Sun in [18] proved that any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + t^2$ with $x, y, 5z, 5t \in \mathbb{Z}$ such that $x + 3y + 5z$ is a square (cf. Theorem 1.8 of their paper). Moreover, H.-L. Wu and Z.-W. Sun in [22] showed that any sufficiently large $n \in \mathbb{N}$ with $16 \nmid n$ can be written as $x^2 + y^2 + z^2 + t^2$ with $x, y, z, t \in \mathbb{Z}$ such that $x + 3y + 5z \in \{1, 4\}$ (cf. Theorem 1.3(i) of their paper).

While the previous attempts to attack the conjecture used the theory of quadratic forms, we use the arithmetic of the ring of Lipschitz integers. At first we will utilize the "unique factorization" that takes place in the ring of Lipschitz integers to prove the following:

Theorem 1.6. *Let $\zeta \in \mathcal{L}$ and $m, n \in \mathbb{N}$ be such that $\mathrm{N}(\zeta)m - n^4$ is non-negative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}_0$. If $\zeta = a + bi + cj + dk \in \mathcal{L}$, then the system*

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

has integer solutions for all $a, b, c, d \in \mathbb{Z}$ *such that*

$$\mathrm{N}(\zeta) = \begin{cases} 1, 3, 5, 7, 11, 15, 23 \\ 2^m \\ 3 \cdot 2^m \\ 7 \cdot 2^m \end{cases}$$

where m *is odd and positive.*

This happens due to the fact that if the norm of a given $\zeta \in \mathcal{L}$ is equal to one of the values in the above list, then ζ has just one decomposition, up to signs and order, as a sum of 4 squares. In the particular case of the "1-3-5 conjecture", $\zeta = 1 + 3i + 5j$ and $\mathrm{N}(\zeta) = 35$. It turns out that 35 has two distinct decompositions as a sum of 4 squares, namely the $1, 3, 5, 0$ and the $1, 3, 3, 4$. This realization yielded the following result:

Proposition 1.7. *Let* $n \leq \sqrt[4]{35\,m}$ *be such that* $35m - n^4$ *is not of the form* $4^r(8s + 7)$*, for any* $r, s \in \mathbb{N}_0$*. Then either the system*

$$\begin{cases} m &= x^2 + y^2 + z^2 + t^2 \\ n^2 &= x + 3y + 5z. \end{cases} \tag{1.1}$$

has integer solutions, or the system

$$\begin{cases} m &= x^2 + y^2 + z^2 + t^2 \\ n^2 &= x + 3y + 3z + 4t. \end{cases} \tag{1.2}$$

has integer solutions.

For a fixed m, computational data has shown a pattern for the n's that the system

$$\begin{cases} m &= x^2 + y^2 + z^2 + t^2 \\ n^2 &= x + 3y + 5z. \end{cases} \tag{1.3}$$

has a solution in $\mathbb{Z}$. Henceforth a new idea was necessary in order to prove the conjecture. The first step was to assume that the second system has a solution in $\mathbb{Z}$, and then find a way to show that the first one has a solution

as well. Using primes above $3, 5$ and 7, and some brand new ideas and techniques, consisting of a combination of conjugation and metacommuation in $\mathcal{L}$ (see below), it was made possible to jump from a solution of the second system to a solution for the first system.

After the proof of the integer case of the conjecture it remained to prove the natural case. This part was done using elementary number theory tools and it was an adjustment of a similar thing that was done by Legendre in [10].

The natural case was then reduced to the computational verification of the conjecture up to a certain constant. This part was done with the major contribution of Rogério Reis, a colleague at the Computer Science department, who helped to implement a very efficient algorithm in C, that checked the conjecture up to the desired constant. For more details on these computations please read [12].

In chapter 5 we will take a closer look at the **metacommutation problem**, which was first introduced in [3, p.61], and that can be described as follows. Let p be a rational prime and Q a Hurwitz prime of norm $q \neq p$, then from "unique factorization" in $\mathcal{H}$, we have that for every Hurwitz prime P of norm p, we can find primes $Q', P' \in \mathcal{H}$ of norms q, p respectively, satisfying

$$PQ = Q'P' \tag{1.4}$$

and the pair (Q', P') is unique up to unit-migration. This process of swapping two primes is called metacommutation, which yields the map :

$$\begin{aligned} \mu_Q : \Pi_p &\to \Pi_p. \\ [P] &\mapsto [P'], \end{aligned}$$

where P' is obtained from P as in (1.4) and Π_p is the set of left associate classes above p. The map is called the metacommutation map of the primes of norm p by Q, and is a permutation of the $p+1$ primes lying above p.

There are two papers that examine this permutation, namely [2] and [6], and they both prove, using different methods, the following:

Theorem 1.8. *The sign of the permutation induced by the metacommutation map μ_Q is the quadratic character $\left(\frac{q}{p}\right)$ of q modulo p.*

If $p = 2$, or if Q is congruent to a rational integer modulo p, then μ_Q is the identity permutation. Otherwise it has $1 + \left(\frac{\mathrm{Tr}(Q)^2 - 4q}{p}\right)$ fixed points.

Examining the proof of [2] we were able to provide a proof of the following result that shades some more light on the cycles of μ_Q.

Proposition 1.9. *The nontrivial cycles of μ_Q have length 2 if and only if Q is pure modulo p, and they have length 3 if and only if $\mathrm{N}(Q) \equiv \mathrm{Tr}(Q)^2 \pmod{p}$.*

After that, we will define a generalization of the metacommutation map. Moreover we will see how one can use this generalization in order to attack problems like the "1-3-5 conjecture", and get at least some partial results about their solvability in the process. We will close this thesis with some easy consequences of metacommutation on the ring of Lipschitz integers, and state some open problems that can be the subject of future work.

2

Hurwitz and Lipschitz Integers

The aim of this chapter is to expound the main properties of the rings of Hurwitz and Lipschitz integers. In particular, after some preliminaries, we will see that both of these rings are an order in the quaternion algebra $\mathbb{H}(\mathbb{Q})$ with $\mathcal{H}$ being a maximal one. Moreover, we will prove a factorization property, that both of these rings possess, and finish the chapter with some results about their ideals. Most of the properties of these rings, that will be proved here, can be found in the literature, and if so we will state where. Some other properties, even though they are not very difficult to deduce, could not be found in the literature.

2.1 Preliminaries

We have already defined the rings of Lipschitz and Hurwitz integers in the introduction. Moreover, for $x \in \mathcal{H}$, we have defined the norm of a quaternion to be equal to $\mathrm{N}(x) = \bar{x}x$, where $\bar{x}$ is the conjugate of the quaternion x. The **trace** of the quaternion $x \in \mathcal{H}$ is defined to be $\mathrm{Tr}(x) = x + \bar{x} = 2\Re(x)$, where $\Re(x)$ is the **real part** of x. Notice that $\mathrm{Tr}(x) \in \mathbb{Z}$. A quaternion $x \in \mathcal{H}$ is called **pure** if its real part is equal to zero, and is called **pure modulo** m, where m is a rational integer, if $m \mid \Re(x)$.

Notice that the real part of a product of two quaternions can be written as

$$\Re(uv) = \bar{u} \cdot v = u \cdot \bar{v},$$

where, the dot denotes the usual inner product on $\mathbb{R}^4$.

Moreover, from the above one can easily get

$$u \cdot v = \Re(u\bar{v}) = \frac{1}{2}(u\bar{v} + v\bar{u}).$$

In the particular case $v = u$, we get

$$u \cdot u = u\bar{u} = \mathrm{N}(u).$$

The **units** in $\mathcal{H}$ and in $\mathcal{L}$ are the elements that have norm equal to 1. We can easily see that the units in $\mathcal{H}$ are the elements

$$\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2},$$

while the units in $\mathcal{L}$ are the elements

$$\pm 1, \pm i, \pm j, \pm k.$$

2.2 Orders in $\mathbb{H}(\mathbb{Q})$

The Propositions presented in this section, as well as their proofs, can be found on many textbooks on Abstract Algebra in the context of Number Fields and their Rings of Integers, see for example [14, Chapter 2], and they might have been slightly altered on some occasions in order to fit our purposes.

Definition 2.1. *Let R be a ring. An R-module M is **torsion-free** if for each $m \in M$ and each nonzero $r \in R$ we have that $rm \neq 0$.*

Definition 2.2. *Let R be a ring. An R-module M is a **lattice** if M is finitely generated over R and is R-torsion-free.*

Definition 2.3. *Let A be a ring that is a finite-dimensional algebra over the field $\mathbb{Q}$ of rational numbers. An **order** is a subring $\mathcal{O}$ of A, such that $\mathcal{O}$ spans A over $\mathbb{Q}$ and $\mathcal{O}$ is a $\mathbb{Z}$ -lattice in A.*

By the above definitions we see that the rings $\mathcal{H}, \mathcal{L}$ are both $\mathbb{Z}$-orders in $\mathbb{H}(\mathbb{Q})$. Since $\mathcal{L} \subset \mathcal{H}$, $\mathcal{L}$ is not a maximal order in $\mathbb{H}(\mathbb{Q})$. The best candidate for the maximal $\mathbb{Z}$-order in $\mathbb{H}(\mathbb{Q})$ is the integral closure of $\mathbb{Z}$ in $\mathbb{H}(\mathbb{Q})$, and it turns out that the integral closure of $\mathbb{Z}$ in $\mathbb{H}(\mathbb{Q})$ is precisely $\mathcal{H}$. This section will be dedicated for the proof of this fact.

Definition 2.4. *Let R be a subring of $\mathbb{H}(\mathbb{Q})$. An element $\alpha \in \mathbb{H}(\mathbb{Q})$ is called **integral** over R if and only if it is a root of some monic polynomial in $R[x]$. The set of elements of $\mathbb{H}(\mathbb{Q})$ that are integral over $\mathbb{Z}$ is called the **integral closure** of $\mathbb{Z}$ in $\mathbb{H}(\mathbb{Q})$, and we will denote it by $\mathbb{O}_{\mathbb{H}(\mathbb{Q})}$.*

Proposition 2.5. *An element α in $\mathbb{H}(\mathbb{Q})$ is integral over $\mathbb{Z}$ if and only if α is integral over $\mathbb{Q}$ and its minimal polynomial $m_{\alpha,\mathbb{Q}}(x)$ (the monic polynomial of least degree in $\mathbb{Q}[x]$ having α as a root) has integer coefficients.*

Proof. If α is integral over $\mathbb{Q}$ with $m_{a,\mathbb{Q}}(x) \in \mathbb{Z}[x]$, then by definition α is integral over $\mathbb{Z}$. Conversely, let α be integral over $\mathbb{Z}$, and $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ of minimum degree having α as a root. If f were reducible in $\mathbb{Q}[x]$, then by Gauss's Lemma $f(x) = g(x)h(x)$ for some monic polynomials $g(x), h(x)$ in $\mathbb{Z}[x]$ of degree smaller than the degree of f. But then α would be a root of either g or h, contradicting the minimality of f. Hence f is irreducible in $\mathbb{Q}[x]$, so $f(x) = m_{\alpha,\mathbb{Q}}(x)$ and so the minimal polynomial for α has coefficients in $\mathbb{Z}$. □

Proposition 2.6. *Let $\alpha \in \mathbb{H}(\mathbb{Q})$. The following are equivalent:*

(i) α is integral over $\mathbb{Z}$;

(ii) the additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated;

(iii) $\alpha A \subset A$ for some finitely generated non-zero additive subgroup $A \subseteq \mathbb{H}(\mathbb{Q})$.

Proof. $(i) \Rightarrow (ii)$: If α is a root of a monic polynomial over $\mathbb{Z}$ of degree n, then in fact the additive group of $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{n-1}$.
$(ii) \Rightarrow (iii)$ trivially.
$(iii) \Rightarrow (i)$ Let $a_1, \ldots, a_n$ generate A. Expressing each αa_i as a linear combination of $a_1, \ldots, a_n$ with coefficients in $\mathbb{Z}$, we obtain

$$\begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_{n-1} \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_{n-1} \end{pmatrix},$$

where m is an $n \times n$ matrix over $\mathbb{Z}$. Equivalently,

$$(\alpha I - M) \begin{pmatrix} a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = 0.$$

Since not all a_i are zero, we must have that $\det(\alpha I - M) = 0$. Expressing this determinant in terms of powers of α, we see that α is a zero of a monic polynomial of degree n with integer coefficients, hence it is integral over $\mathbb{Z}$. □

Corollary 2.7. *If α and β are integral over $\mathbb{Z}$, then so are $\alpha + \beta$ and $\alpha\beta$.*

Proposition 2.8. *The ring of Hurwitz integers $\mathcal{H}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{H}(\mathbb{Q})$, and since it is an order in $\mathbb{H}(\mathbb{Q})$, it is the maximal one.*

Proof. Let $\alpha \in \mathcal{H}$. Since α is a root of the polynomial

$$x^2 - \mathrm{Tr}(\alpha)x + \mathrm{N}(\alpha),$$

and $\mathrm{Tr}(\alpha), \mathrm{N}(\alpha) \in \mathbb{Z}$, we have that $\mathcal{H} \subseteq \mathbb{O}_{\mathbb{H}(\mathbb{Q})}$. In order to show that this is the full integral closure, take $\beta = b_0 + b_1 i + b_2 j + b_3 k \in \mathbb{H}(\mathbb{Q})$ and assume that β is integral over $\mathbb{Z}$. If $b_1 = b_2 = b_3 = 0$ then $\beta = b_0 \in \mathbb{Q}$, and by Proposition 2.5 we get that $b_0 \in \mathbb{Z}$ and so $\beta \in \mathcal{H}$. If $(b_1, b_2, b_3) \neq (0, 0, 0)$,

then the minimal polynomial of β is

$$m_{\beta,\mathbb{Q}}(x) = x^2 - 2b_0x + b_0^2 + b_1^2 + b_2^2 + b_3^2.$$

By Proposition 2.5 we get that $2b_0 \in \mathbb{Z}$, and $b_0^2 + b_1^2 + b_2^2 + b_3^2 \in \mathbb{Z}$. Now, if we use corollary 2.7, we get that $\beta i, \beta j, \beta k$ are integral as well. Applying the same argument, we get that $2b_1, 2b_2, 2b_3 \in \mathbb{Z}$. Then $b_0^2 + b_1^2 + b_2^2 + b_3^2 \in \mathbb{Z}$, from which it is easy to see that either all of the b_i's are integers, or all of them are half integers, i.e. $\beta \in \mathcal{H}$, and therefore $\mathcal{H} = \mathbb{O}_{\mathbb{H}(\mathbb{Q})}$. □

2.3 "Unique factorization" and Euclidean division in $\mathcal{H}$.

A Hurwitz integer is called **irreducible** if it is not 0 or a unit and is not a product of non-units. As a convention we will call the irreducible quaternions, prime quaternions, in accordance to the literature, even though they are not primes in the usual sense of commutative algebra: it is possible for an irreducible quaternion q, to divide from the left a product ab, $\rceil\, ab$, without having either $q \rceil\, a$ or $q \rceil\, b$. The same of course holds for right division. This is a consequence of the non unique factorization, e.g. let $d = (1+k)(1+i+j) = 1+2j+k$, and $q = 1-i+j$, then $q \rceil\, d$, since we can write $d = q(1+k)$, but we do not have either $d \rceil\, 1+k$, or $d \rceil\, 1+i+j$.

Let us now see some nice properties of $\mathcal{H}$.

Proposition 2.9. *The ring $\mathcal{H}$ is right (and left) norm-Euclidean.*

Proof. Given $\alpha, \beta \in \mathcal{H}$, let $\delta = \beta^{-1}\alpha = (\bar{\beta}\alpha)/\,\mathrm{N}(\beta)$, and let ρ be the quaternion built from δ by taking the integers closer to its coordinates. Put $\epsilon = \delta - \rho$. One has then $\mathrm{N}(\epsilon) \leq 4(1/2)^2 = 1$ and $\mathrm{N}(\epsilon) = 1 \iff \epsilon = \pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$. Moreover, in the case $\mathrm{N}(\epsilon) = 1$ we may assume that $\epsilon = \frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k$, by building ρ from δ, appropriately. Put also $\tau = \beta\epsilon = \beta(\delta - \rho) = \alpha - \beta\rho \in \mathcal{H}$. One then has that $\alpha = \beta\rho + \tau$, with $\mathrm{N}(\tau) = \mathrm{N}(\beta)\,\mathrm{N}(\epsilon) \leq N(\beta)$.

If $\mathrm{N}(\epsilon) = 1$ then $\epsilon = \delta - \rho \in \mathcal{H}$, so $\beta^{-1}\alpha = \delta = \rho + \epsilon \in \mathcal{H}$, which means that $\beta \mid \alpha$ on the left, and if $\mathrm{N}(\epsilon) < 1$ then $\mathrm{N}(\tau) < \mathrm{N}(\beta)$. Therefore, the norm is a left-euclidean function in $\mathcal{H}$. □

Corollary 2.10. *The ring $\mathcal{H}$ is a right (left) principal ideal domain.*

Contrary to $\mathcal{H}$, we have that

$\mathcal{L}$ is not a right (or left) principal ideal domain.

Indeed, consider the right ideal $(1+i, 1-j)$. We will show that it is not principal. Suppose that $(1+i, 1-j) = x\mathcal{L}$, for some $x \in \mathcal{L}$. Then, there is $\ell_1, \ell_2 \in \mathcal{L}$ such that $1+i = x\ell_1$ and $1-j = x\ell_2$. Taking norms, we have the following two cases:

- If $\mathrm{N}(x) = 1$, i.e. x is a unit, then $(1+i, 1-j) = \mathcal{L}$. Thus, there must exist $\alpha_1, \alpha_2 \in \mathcal{L}$ such that $(1+i)\alpha_1 + (1-j)\alpha_2 = 1$. We then would have that

$$\begin{aligned} 1 &= (1+i)\alpha_1 + (1+i)(1/2 - 1/2i - 1/2j + 1/2k)\alpha_2 \\ &= (1+i)[\alpha_1 + (1/2 - 1/2i - 1/2j + 1/2k)\alpha_2], \end{aligned}$$

  which is absurd.

- If $\mathrm{N}(x) = 2$, then $\mathrm{N}(\ell_1) = \mathrm{N}(\ell_2) = 1$, and therefore x would be a right associate of both $1+i$ and $1-j$, hence $1+i$ would be a right associate of $1-j$, which is not the case.

A consequence of the above is that

$\mathcal{L}$ is not right (or left) Euclidean.

Due to the lack of commutativity in $\mathcal{H}$, there is no unique factorization as we know it from the rational integers, but there is a similar result, significantly weaker though, that is the following.

Theorem 2.11. *To any factorization of the norm q of a primitive Hurwitz integer Q (i.e not divisible by any natural number $n > 1$) into a product $p_0 p_1 \cdots p_s$ of rational primes, there is a factorization $Q = P_0 P_1 \cdots P_s$ of Q into a product of Hurwitz primes with $\mathrm{N}(P_0) = p_0, \ldots, \mathrm{N}(P_s) = p_s$. We shall say that "the factorization $P_0 P_1 \cdots P_s$ of Q is modelled on the factorization $p_0 p_1 \cdots p_s$ of $\mathrm{N}(Q)$." Moreover, if $Q = P_0 P_1 \cdots P_s$ is any one factorization modelled on $p_0 p_1 ... p_s$, then the others have the form*

$$Q = P_0 U_1 \cdot U_1^{-1} P_1 U_1 \cdot U_1^{-1} P_2 \cdots U_s^{-1} P_s,$$

i.e., "the factorization on a given model is unique up to unit-migration."

The proof of this theorem can be found on [3], which we reproduce here with some slight modifications.

Proof. Let $Q \in \mathcal{H}$ be primitive with $\mathrm{N}(Q) = q = p_0 p_1 \cdots p_s$, and consider the right ideal $p_0\mathcal{H} + Q\mathcal{H}$. It must be principal, since $\mathcal{H}$ is left euclidean, so there is a unique Hurwitz integer P_0, up to right multiplication by units, such that:

$$p_0\mathcal{H} + Q\mathcal{H} = P_0\mathcal{H} \tag{2.1}$$

Then, there is $a \in \mathcal{H}$ such that

$$p_0 = P_0 a. \tag{2.2}$$

Taking norms, we see that $\mathrm{N}(P_0)$ must divide $\mathrm{N}(p_0) = p_0^2$. Therefore, $\mathrm{N}(P_0)$ is equal to $1, p_0$ or p_0^2.

If $\mathrm{N}(P_0) = 1$, then $p_0\mathcal{H} + Q\mathcal{H}$ would be the whole ring, and this cannot happen because an arbitrary element $h = p_0 a + Qb$ of this ideal has norm

$$\mathrm{N}(h) = (p_0 a + Qb)\overline{(p_0 a + Qb)} = \mathrm{N}(p_0)\,\mathrm{N}(a) + p_0[a\overline{Qb} + Qb\overline{a}] + \mathrm{N}(Q)\,\mathrm{N}(b)$$

$$= p_0^2\,\mathrm{N}(a) + p_0[a\overline{Qb} + Qb\overline{a}] + p_0 p_1 \cdots p_s N(b), \text{ which is divisible by } p_0.$$

Now, if $\mathrm{N}(P_0) = p_0^2$, then by (2.2) we must have that a is a unit, so $P_0 = p_0 a^{-1}$, which means that $p_0 \mid P_0$, and thus $p_0 \mid Q$ by (2.1), which does not happen since Q is assumed primitive.

Therefore, we must have $\mathrm{N}(P_0) = p_0$. Thus, P_0 is a Hurwitz prime which is unique up to right multiplication by units, and that by (2.1) divides Q. So there exists $Q_1 \in \mathcal{H}$ such that $Q = P_0 Q_1$, with $\mathrm{N}(Q_1) = p_1 p_2 \cdots p_s$.

Repeating the argument for the ideal $p_1\mathcal{H} + Q_1\mathcal{H} = P_1\mathcal{H}$, we can show that $Q_1 = P_1 Q_2$, with $\mathrm{N}(Q_2) = p_2 \cdots p_s$. Doing the same for all the remaining Q_i's we show that there is a factorization $Q = P_0 P_1 \cdots P_s Q'$, where from a norm argument Q' must be a unit, so P_s can absorb it. So, there exists a factorization of Q modeled on its norm, and it is unique up to right multiplication by a unit, since all the P_i's are unique up to right multiplication by a unit.

□

Proposition 2.12. *An element of $\mathcal{H}$ is prime if and only if its norm is a rational prime.*

Proof. Let $h \in \mathcal{H}$. If h is not a Hurwitz prime then it must be a product of two non units, and so its norm cannot be a rational prime.

If $\mathrm{N}(h)$ is not a rational prime, then it has a prime factorization of at least two primes which would correspond to at least two Hurwitz primes in the factorization of h, and so h is not a Hurwitz prime. □

2.4 Automorphisms and bilateral ideals of $\mathcal{H}$.

In this section we will at first study the automorphisms in $\mathcal{H}$ which is based on the work of Hurwitz, see [7, Vorrlesung 5]. We will present Hurwitz's proof of the fact that the only automorphisms in $\mathcal{H}$ are the conjugation maps, by some specific elements in $\mathcal{H}$. A corollary of this result, about bilateral ideals in $\mathcal{H}$, will be proved to finish of this section.

Define the conjugation map in the Hamilton quaternions

$$\begin{aligned} \varphi_\alpha : \mathbb{H} &\to \mathbb{H} \\ \gamma &\mapsto \alpha\gamma\alpha^{-1} \end{aligned}$$

We would like to see for which elements $\alpha \in \mathcal{H}$, do we have $\varphi_\alpha(\mathcal{H}) = \mathcal{H}$. We notice that if α is a rational integer or a unit, then for any $\gamma \in \mathcal{H}$, we have $\alpha\gamma\alpha^{-1} \in \mathcal{H}$. We also see that for $\gamma = h_1 + h_2 i + h_3 j + h_4 k$, and $1 + i$ (the unique, up to associates, prime above 2 in $\mathcal{H}$) one has

$$(1+i)\gamma(1+i)^{-1} = h_1 + h_2 i - h_4 j + h_3 k.$$

Moreover, conjugation by any finite product of these kind of elements preserves $\mathcal{H}$. For these values of α, φ_α induces an $\mathcal{H}$-automorphism.

Proposition 2.13. *The only possible automorphisms of $\mathcal{H}$ are the ones induced by φ_α on $\mathcal{H}$, for $\alpha \in \mathcal{H}$ of the form $\varepsilon(1+i)^n r^m$, where $\varepsilon \in \mathcal{H}^*$, $r \in \mathbb{Z}$ and $n, m \in \mathbb{N}_0$.*

Proof. Let $\psi : \mathcal{H} \to \mathcal{H}$ be an automorphism.

For any of the units $\varepsilon \in U = \{\pm i, \pm j, \pm k\}$, $\psi(\varepsilon)$ must be a unit as well since $\psi(\varepsilon)^2 = \psi(\varepsilon^2) = -1$, and so $\mathrm{N}(\psi(\varepsilon)) = 1$. Now, $\psi(\varepsilon)$ can not be any of the units in $\mathcal{H} \setminus \mathcal{L}$ because the equation $\psi(\varepsilon)^2 = -1$ is satisfied only for the units in U. Therefore, we have that the image of each unit $\varepsilon \in U$ is again in U, and ψ is completely determined by what it does to the units in U. This leads to the question: *how many possible automorphisms ψ can exist?* There are $3! \times 2^3 = 48$ possible combinations of the image of i, j and k under ψ. From those 48 we are interested in the ones that also fulfill the condition $\psi(ijk) = \psi(i)\psi(j)\psi(k) = -1$. It is easy to see that exactly half of them do. Note that if a given map ψ' in $\mathcal{H}$ is such that $\psi'(U) = U$, $\psi'(1) = 1, \psi'(-1) = -1$ and $\psi'(i)\psi'(j)\psi'(k) = 1$, then ψ' is an anti-automorphism in $\mathcal{H}$. The last remark means that there are 24 anti-automorphisms in $\mathcal{H}$ as well.

Let $\varepsilon_0, \varepsilon_1 \in \mathcal{H}^*$ be two different units in $\mathcal{H}$. Then if we had $\varepsilon_0\gamma\varepsilon_0^{-1} = \varepsilon_1\gamma\varepsilon_1^{-1}$ for all $\gamma \in \mathcal{H}$, this would imply that $\varepsilon_1^{-1}\varepsilon_0\gamma = \gamma\varepsilon_1^{-1}\varepsilon_0$, and since $\varepsilon_1^{-1}\varepsilon_0 \in \mathcal{H}^*$ we would have that the equality $\varepsilon\gamma = \gamma\varepsilon$ holds for all $\gamma \in \mathcal{H}$ and for some unit $\varepsilon \in \mathcal{H}^*$. This can only happen when $\varepsilon = \pm 1$, which means that $\varepsilon_1 = \pm\varepsilon_0$, and since $\varepsilon_1, \varepsilon_0$ were assumed to be different to each other we have that $\varepsilon_1 = -\varepsilon_0$. This means that the 24 units $\in \mathcal{H}^*$ induce 12 different automorphisms φ_α. Now, if in the above argument we replace ε_1 by $1+i$, we get that the equality $\varepsilon\gamma\varepsilon^{-1} = (1+i)\gamma(1+i)^{-1}$, $\forall\gamma \in \mathcal{H}$ implies that $(1+i)^{-1}\varepsilon\gamma = \gamma(1+i)^{-1}\varepsilon$ and this can only happen when $(1+i)^{-1}\varepsilon \in \mathbb{R}$, which does not happen. Therefore, $1+i$ and its associates determine 12 more different automorphisms φ_α. Hence, we have 24 in total, different automorphisms for $\alpha = \varepsilon(1+i)$ or $\alpha = \varepsilon$, with $\varepsilon \in \mathcal{H}^*$. Now, it is easy to see that if $\alpha = \varepsilon(1+i)$ or $\alpha = \varepsilon$, for some $\varepsilon \in \mathcal{H}^*$, then $r\alpha$, $r \in \mathbb{Z}$, induces the same automorphism as α, since $\alpha\gamma\alpha^{-1} = r\alpha\gamma(r\alpha)^{-1}$ $\forall\gamma \in \mathcal{H}$.

Therefore, since there can be only 24 automorphisms in $\mathcal{H}$, and the ones induced by φ_α for α of the form $\varepsilon(1+i)^n r^m$ are 24 as well, it follows that those φ_α are the only automorphisms in $\mathcal{H}$.

□

Corollary 2.14. *The only two-sided ideals in $\mathcal{H}$ are the ones generated by elements of the form $(1+i)^n r^m$, where $r \in \mathbb{Z}$ and $n, m \in \mathbb{N}_0$.*

Proof. Let a be of the form $(1+i)^n r^m$, and consider the left ideal $a\mathcal{H} \trianglelefteq \mathcal{H}$. From Proposition 2.13, we know that for any $h \in \mathcal{H}$ there exists an $\ell \in \mathcal{H}$ such that $ah = \ell a$, and vice-versa. Therefore, the left ideal $a\mathcal{H}$ is equal to the right ideal $\mathcal{H}a$, which means that $a\mathcal{H}$ is a two-sided ideal.

On the other hand, assume we have a two sided ideal in $\mathcal{H}$, and since $\mathcal{H}$ is left (right) Euclidean, it is principal as a left and as a right ideal. We will start by showing that all two sided ideals have the same generator as a left and as a right ideal. Assume that its left ideal generator is different than its right ideal generator, meaning that there are $a, b \in \mathcal{H}$ such that $a\mathcal{H} = \mathcal{H}b$. We have that $a \in \mathcal{H}b$, therefore there exists $h_1 \in \mathcal{H}$ such that $a = h_1 b$. Also there exists $h_2 \in \mathcal{H}$ such that $b = ah_2$. Taking norms, we can see that h_1, h_2

are units, and so a, b are associates, say $a = ub$, $u \in \mathcal{H}^*$. The last equality implies that $\mathcal{H}b = \mathcal{H}a$.

Therefore the two sided ideals in $\mathcal{H}$ have the form $a\mathcal{H} = \mathcal{H}a$ for some $a \in \mathcal{H}$. It follows that if a is a generator of a two sided ideal in $\mathcal{H}$, then for all $h \in \mathcal{H}$, $aha^{-1} \in \mathcal{H}$. By Proposition 2.13 we know that a must be of the form $\varepsilon(1+i)^n r^m$, for some unit $\varepsilon \in \mathcal{H}$ and $m, n \in \mathbb{Z}$. The unit can be omitted since we are talking about two sided ideals. □

2.5 Right divisors in $\mathcal{L}$

In this section we will take a look at a particular result from Gordon Pall's 1940 work ([15] and [16]) on the ring of Lipschitz integers. This result is similar to Theorem 2.11 about "Unique factorization", but for the ring of Lipschitz integers. Notice from the statement below that it is actually stronger than 2.11.

Theorem 2.15. *Let $v = v_0 + v_1 i + v_2 j + v_3 k \in \mathcal{L}$ be primitive modulo m, where $m \mid \mathrm{N}(v)$, m odd and positive. Then there is a unique, up to left multiplication by units, right divisor of v of norm m.*

Firstly, we observe that if $t \in \mathcal{L}$ is a right divisor of $x \in \mathcal{L}$, that is $x = ut$ for some $u \in \mathcal{L}$, then the left-associates $\pm t$ $\pm it$,$\pm jt$,$\pm kt$ of t, are also right divisors of x of the same norm.

We are going to need some lemmas to help prove Theorem 2.15.

Lemma 2.16. *Let $x, y \in \mathcal{L}$, $m \in \mathbb{Z}$ odd. If $x \equiv y \pmod{m}$, then x and y have the same right divisors of norm m.*

Proof. Let $t \in \mathcal{L}$ be a right divisor of x with $\mathrm{N}(t) = m$, so that there exists $u \in \mathcal{L}$, such that $x = ut$. Now $x \equiv y \pmod{m} \Rightarrow \exists k \in \mathcal{L}$, such that $x = km + y$. Therefore we have $ut = k\bar{t}t + y$, hence $y = (u - k\bar{t})t$, which means that t is a right divisor of y. □

Lemma 2.17. *Let $x, v \in \mathcal{L}$, $m \in \mathbb{Z}$ odd. If $\mathrm{N}(x)$ is relatively prime to m then v and xv have the same right divisors of norm m.*

Proof. If t is a right divisor of v, then clearly is a right divisor of xv as well.

On the other hand, let t be a right divisor of xv, of norm m. Then we will have $xv = ut$, for some $u \in \mathcal{L}$. We multiply by $\bar{x}$ on the left to get $\bar{x}xv = \bar{x}ut$, so $\mathrm{N}(x)v = \bar{x}ut$. Now, since $(\mathrm{N}(x), m) = 1$, there are $b, c \in \mathbb{Z}$, such that $b\,\mathrm{N}(x)+cm = 1$. So $b\,\mathrm{N}(x) \equiv 1 \pmod{m}$. Multiplying the equation $\mathrm{N}(x)v = \bar{x}ut$ by b on the left, and reducing modulo m yields

$$v \equiv b\,\mathrm{N}(x)v \equiv b\bar{x}ut \pmod{m}.$$

It now follows from Lemma 2.17 that t is a right divisor of v as well. □

Lemma 2.18. *If Theorem 2.15 holds for every odd rational integer that is a product of at most $r-1$ primes (not necessarily distinct) with $r > 1$, it holds for any odd number that is a product of r primes.*

Proof. Let $m = p_1 p_2 \cdots p_{r-1}$, where $p_i, i = 1, \cdots, r-1$, are odd primes, and let p be some other odd prime. Let $v \in \mathcal{L}$ be primitive modulo pm, $pm \mid \mathrm{N}(v)$ and t be a right divisor of v of norm m, i.e. $v = ut$, for some $u \in \mathcal{L}$. We are looking for the right divisors of v of norm pm. We have $pm \mid N(v) = N(u)N(t)$, so $p \mid N(u)$. Since we assume that $r > 1$, u can be written $u = wz$, $z, w \in \mathcal{L}$, and $N(z) = p$. Then, $v = wzt$ and $N(zt) = N(z)N(t) = pm$, hence zt is a right divisor of v of norm pm.

Now, let $x, y \in \mathcal{L}$ be two right divisors of v of norm pm, i.e. $v = ax = by$, $a, b \in \mathcal{L}$. Since $N(x) = N(y) = pm$, we can write $x = ct$, $y = dt'$ with $N(c) = N(d) = p$, $N(t) = N(t') = m$. By hypothesis t, t' are left associates. By letting c, d absorb the unit that distinguish t from t', we can assume $t = t'$. Therefore, $ac = bd$, and again by hypothesis, c and d must be left associates. Finally, $x = ct$, $y = dt$ are left associates too, and therefore all the right divisors of v of norm pm are left associates. □

Lemma 2.19. *Let $v \in \mathcal{L}$ and $p \in \mathbb{Z}$ be an odd prime. If v is primitive modulo p, we can choose a pure quaternion $x \in \mathcal{L}$ of norm relatively prime to p, such that xv is pure modulo p.*

Proof. Since $v = v_0 + v_1 i + v_2 j + v_3 k$ is primitive modulo p, then at least one of v_i, for $i \in 0, 1, 2, 3$, is such that $(p, v_i) = 1$. We may assume that $(p, v_1) = 1$, i.e. $\exists a, b \in \mathbb{Z}$, such that $ap + bv_1 = 1$, and thus $v_1 b \equiv 1 \pmod{p}$. We need to find $x = x_1 i + x_2 j + x_3 k \in \mathcal{L}$, with $(N(x), p) = 1$, such that xv is pure modulo p, i.e. $x_1 v_1 + x_2 v_2 + x_3 v_3 \equiv 0 \pmod{p}$. We multiply the last equation with b and we get $x_1 \equiv x_2 e + x_3 f \pmod{p}$, where $e \equiv -v_2 b \pmod{p}$ and $f \equiv -v_3 b \pmod{p}$. From $(N(x), p) = 1 \Rightarrow x_1^2 + x_2^2 + x_3^2 \not\equiv 0 \pmod{p}$ and $x_1 \equiv x_2 e + x_3 f \pmod{p}$ we get

$$(1 + e^2)x_2^2 + 2efx_2x_3 + (1 + f^2)x_3^2 \not\equiv 0 \pmod{p}$$

Now, the coefficients of the quadratic form in the above equivalence are not all zero modulo p, so we can always find $x_2, x_3 \in \mathbb{Z}$ that satisfies it. From $x_1 \equiv x_2 e + x_3 f \pmod{p}$, we can get an $x_1 \in \mathbb{Z}$ such that xv is pure modulo p. □

Now we are ready to prove Theorem 2.15.

Proof of Theorem 2.15. By lemmas 2.16, 2.17, 2.18, and 2.19, we just need to prove the claim when m is an odd prime p, and v is a pure quaternion such that

$$v = i + v_2 j + v_3 k \pmod{p} \quad \text{and} \quad p \mid Nv.$$

We have $p \mid \mathrm{N}(v)$, therefore $1 + v_2^2 + v_3^2 = pb$, for some $b \in \mathbb{Z}$.

We need to find the right divisors of v of norm p, i.e. we need to find the quaternions $t = t_0 + t_1 i + t_2 j + t_3 k \in \mathcal{L}$ that satisfy $v = ut$ and $N(t) = p$, for some $u \in \mathcal{L}$. Now, multiply the equation $v = ut$ by $\bar{t}$ on the right to get $v\bar{t} = up \equiv 0 \pmod{p}$. From $v\bar{t} \equiv 0 \pmod{p}$ we get four congruencies:

$$\begin{aligned}
t_0 &\equiv v_2 t_3 - v_3 t_2 \pmod{p} \\
t_1 &\equiv -v_2 t_2 - v_3 t_3 \pmod{p} \\
t_2 &\equiv v_2 t_1 + v_3 t_0 \pmod{p} \\
t_3 &\equiv v_3 t_1 - v_2 t_0 \pmod{p}
\end{aligned}$$

We notice that if the first two congruences hold, the next two will hold as well. Let $x_0, x_1, x_2, x_3 \in \mathbb{Z}$ be such that $t_0 = v_2t_3 - v_3t_2 + px_0$, $t_1 = -v_2t_2 - v_3t_3 + px_1$, $t_2 = x_2$, and $t_3 = x_3$. Substituting this into $\mathrm{N}(t) = t_0^2 + t_1^2 + t_2^2 + t_3^2 = p$, we get

$$p(x_0^2 + x_1^2) + b(x_2^2 + x_3^2) + 2v_2(x_0x_3 - x_1x_2) - 2v_3(x_1x_3 + x_0x_2) = 1. \quad (2.3)$$

Therefore v has as many right divisors of norm p as there are solutions of this equation. So we just need to determine when the quadratic form

$$p(x_0^2 + x_1^2) + b(x_2^2 + x_3^2) + 2v_2(x_0x_3 - x_1x_2) - 2v_3(x_1x_3 + x_0x_2). \quad (2.4)$$

represents 1. We have that (2.3) can be written as

$$XAX^T = 1,$$

where

$$X = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \end{pmatrix},$$

and

$$A = \begin{pmatrix} p & 0 & -v_3 & v_2 \\ 0 & p & -v_2 & -v_3 \\ -v_3 & -v_2 & b & 0 \\ v_2 & -v_3 & 0 & b \end{pmatrix}$$

The quadratic form (2.4) is positive, being derived from $\sum_{i=1}^{4} t_i^2$, and one can check that that $\det(A) = 1$, i.e. the discriminant of (2.4) is equal to 1. Therefore, by [17, Corollary, p. 154] it is equivalent to $\sum_{i=1}^{4} x_i^2$. Now, the 8 units of $\mathcal{L}$ are the only solutions of $\sum_{i=1}^{4} x_i^2 = 1$, thus the quadratic form 2.3 has 8 solutions as well. Hence, there are 8 right divisors of v of norm p. The 8 left-associates of a given right divisor t must be the ones we are looking for. □

Corollary 2.20. *Theorem 2.15 holds with $m \in \mathbb{Z}$ even, provided $v \in \mathcal{L}$ is primitive and $\mathrm{N}(v)/m$ is odd.*

Proof. It is clear that Theorem 2.15 holds for left divisors as well. Since $\mathrm{N}(v)/m$ is odd and v is primitive, Theorem 2.15 applies, hence there is a unique up to right associates left divisor of v of norm $\mathrm{N}(v)/m$. Call this left divisor t. So we have that $v = tu$, for some $u \in \mathcal{L}$, with $\mathrm{N}(u) = m$, and since t is unique up to right associates, u must be unique up to left associates. □

Corollary 2.21. *Let $x, z \in \mathcal{L}$, $m \in \mathbb{Z}$ odd. If z and xz are both primitive modulo m, and $m \mid Nz$, then z and xz have the same right divisors of norm m.*

Proof. Let t be a right divisor of xz of norm m, and t' be a right divisor of z of norm m. Then, clearly t' is a right divisor of norm m of xz as well. Therefore, by Theorem 2.15, t and t' are left associates. The claim follows. □

2.6 The ideals in $\mathcal{L}$

Another consequence of Theorem 2.15 is the following.

Proposition 2.22. *Let $x, y \in \mathcal{L}$. There exists $x', y' \in \mathcal{L}$, such that*

$$x'y = y'x,$$

where $\mathrm{N}(x') = \mathrm{N}(x)$ and $\mathrm{N}(y') = \mathrm{N}(y)$.

Proof. For a proof of this we direct the reader to the proof of the fact that the metacommutation map is a permutation, see Chapter 5, Proposition 5.2. In our case $x, y \in \mathcal{L}$ are not primes, but the proof still works. □

Define now the equivalence relation between ideals in $\mathcal{L}$ as follows: for two right ideals $I_1, I_2 \in \mathcal{L}$ we write $I_1 \sim I_2$ if and only if there exist $x_1, x_2 \in \mathcal{L}$ such that $x_1 I_1 = x_2 I_2$. This is indeed an equivalence relation, since obviously

- $I_1 \sim I_1$,
- if $I_1 \sim I_2$ then $I_2 \sim I_1$,
- if $I_1 \sim I_2$ and $I_2 \sim I_3$, then there exists x_1, x_2, x_3, x_4 such that $x_1 I_1 = x_2 I_2$ and $x_3 I_2 = x_4 I_3$. Now, Proposition 2.22 implies that there exists $x_3' \in \mathcal{L}$, such that $x_3' x_2 = x_2' x_3$, for some $x_2' \in \mathcal{L}$. But then $x_3' x_1 I_1 = x_2' x_4 I_3$, which means that $I_1 \sim I_3$.

The set of non-zero right ideals in $\mathcal{L}$ modulo this equivalence relation forms the set of right ideal classes $\mathcal{C}\ell_R(\mathcal{L})$, of $\mathcal{L}$. Note that for ideals in an integral domain, the operation $[I][J] = [IJ]$ of multiplication of classes is well defined and commutative. Moreover, every ideal in an integral domain is invertible. Therefore the set of classes together with multiplication forms a group (the identity element is the class of principal ideals), the well known ideal class group. For more details see [4, Chapter 16] and [14, Chapters 3 and 5]. In our case the multiplication of two right ideals is not a right ideal, therefore we can only speak of the right ideal class set. Now it is easy to see the following.

Proposition 2.23. *Each ideal in $\mathcal{L}$ is either principal, or can be generated by two elements.*

Proof. Let $I \trianglelefteq \mathcal{L}$, and let S be a set of its generators. Now, since $\mathcal{L} \cong \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$, is finitely generated as an abelian group, and therefore finitely generated as a $\mathbb{Z}$-module. The integers being a principal ideal domain implies that I as a submodule of $\mathcal{L}$ is finitely generated, therefore S is finite. Let $\alpha, \beta \in S$. From the proof of Proposition 2.9, we know that there is $\rho, \epsilon \in \mathcal{L}$ such that $\alpha = \beta\rho + \beta\epsilon$, where $\mathrm{N}(\epsilon) \leqslant 1$, and $\mathrm{N}(\epsilon) = 1$ if and only if $\epsilon = \frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k$, which is a unit that will play an important role soon, and we call it ω.

Then do the following:

- If $\epsilon = 0$ i.e. $\beta \mid \alpha$, so we remove α from S.

- If $0 < \mathrm{N}(\epsilon) < 1$, then we replace α and β by β and the remainder $\beta\epsilon$ in S.
- If $\mathrm{N}(\epsilon) = 1$, then we replace α, β by $\beta, \beta\omega$ in S.

We do the same with all the possible pairs of generators, and after a finite number of steps S becomes a set that all of its elements have the same norm. If then, there is a $\beta \in S$, by our division algorithm, all the rest may be replaced by $\beta\omega$. □

Corollary 2.24. *The right ideal class set $\mathcal{C}\ell_R(\mathcal{L})$ consists of 2 elements, the equivalence class of principal ideals and the equivalence class of all ideals of the form $(a, a\omega)$, where $a \in \mathcal{L}$ is a Lipschitz integer of even norm and $\omega = \frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k$.*

Proof. We have that for $a, b \in \mathcal{L}$, $(a, a\omega) \sim (b, b\omega)$, since by Proposition 2.22 there exists a', b' such that $b'a = a'b$. By Proposition 2.23, we therefore have that there are two equivalence classes in $\mathcal{C}\ell_R(\mathcal{L})$, the class of principal ideals and the class of the ideals of the form $(a, a\omega)$, for some $a \in \mathcal{L}$. The ideals in $\mathcal{L}$ that are of the form $(a, a\omega)$, implies that $\mathrm{N}(a)$ is necessarily even, since $a\omega \in \mathcal{L} \iff \mathrm{N}(a)$ is even. □

Below we list some other general properties of the rings $\mathcal{H}$ and $\mathcal{L}$, that are generally easy to deduce.

Proposition 2.25. *The following hold.*

(i) The rings $\mathcal{H}$, $\mathcal{L}$ are right (left) Noetherian but not right (left) Artinian.

(ii) Let $J(\mathcal{H}), J(\mathcal{L})$ be the Jacobson radicals of $\mathcal{H}, \mathcal{L}$ respectively. Then $J(\mathcal{H}) = J(\mathcal{L}) = 0$.

(iii) The rings $\mathcal{H}$, $\mathcal{L}$ are semiprimitive.

(iv) The rings $\mathcal{H}$, $\mathcal{L}$ are not semisimple.

(v) The only two sided maximal ideals in $\mathcal{H}$ are $(1+i)$ and (p), where p is a rational prime.

(vi) The rings $\mathcal{H}$, $\mathcal{L}$ are not perfect.

Proof. (i) The ring $\mathcal{L}$ is right Noetherian since every right ideal in $\mathcal{L}$ is finitely generated.

On the other hand, it is easy to see that for $p_i \in \mathbb{Z}$ primes, the chain of right ideals

$$(p_1) \supseteq (p_1 p_2) \cdots \supseteq (p_1 p_2 \cdots p_n) \supseteq \cdots$$

does not terminate, therefore $\mathcal{L}$ is not right Artinian. Same for $\mathcal{H}$.

(ii) Let $y \in J(\mathcal{H})$, $y \neq 0$, then from [8, p. 53] we know that $1 - xy$ is left invertible for all $x \in \mathcal{H}$. Therefore, $1 - xy$ is a unit for all $x \in \mathcal{H}$, which is absurd. Same for $\mathcal{L}$.

(iii) By definition, since $J(\mathcal{H}) = J(\mathcal{L}) = 0$.

(iv) It follows from the fact that a left semisimple ring is both left Artinian and left Noetherian.

(v) Direct consequence of Corollary 2.14 and the definition of a maximal ideal.

(vi) We have that $\mathcal{H}/J(\mathcal{H}) = \mathcal{H}$ and $\mathcal{H}$ is not semisimple, therefore $\mathcal{H}$ is not perfect. Same for $\mathcal{L}$.

□

3 Hurwitz and Pall on Integral Quaternions

To the extend of our knowledge, there are only two authors that described in some depth the properties of the rings of Hurwitz and Lipschitz integers. The first one is Adolf Hurwitz, who wrote in [7] a series of lectures about these two rings, in German. From his work we have already showed the result about automorphisms in $\mathcal{H}$. The second author is Gordon Pall, who wrote a series of articles mostly about the ring of Lipschitz integers, namely [15] and [16], from which we have already proved Theorem 2.15.

3.1 The work of Hurwitz

Apart from the result on automorphisms of $\mathcal{H}$, Hurwitz had some other interesting results in the rings of Hurwitz and Lipschitz integers, which he called the integral Quaternions. We will present some of them here on this section. In particular we will look into his elegant proof of Jacobi's four-square theorem. The main reason for that was that we could not find any textbook or article containing his work in English. Therefore we went through 1918's Hurwitz original paper and translated the old German text to English. We will not be completely faithful to the original text, we will try to capture the essence of the arguments instead. Many times instead of Hurwitz or Lipschitz integer we may just say quaternion, when the Hurwitz or Lipschitz integer is implied by the context.

Let $m \in \mathbb{N}$, the idea behind the Hurwitz's proof of Jacobi's four square theorem, is to create the Quotient ring $\mathcal{H}/m\mathcal{H}$ and count all the elements in there that have norm zero. For that reason we will try to create this Quotient ring for m being odd and see how the result on the automorphisms of $\mathcal{H}$ can be used to get a result for even m as well. First let us see what happens if we mod out by an even Hurwitz integer.

3.1.1 The Hurwitz integers modulo an even Hurwitz

We have seen in Proposition 2.14 which ideals in $\mathcal{H}$ are two sided. Therefore, we can create the quotient ring $\mathcal{H}/v\mathcal{H}$, where $v = (1+i)^n r^m$, for $r \in \mathbb{Z}$ and $n, m \in \mathbb{N}_0$.

Note that for v as above, and any $a, b \in \mathcal{H}$, when we write $a \equiv b \pmod{v}$,we mean $v \mid a - b$ from the left and from the right. Since $\overline{(1+i)} = (1+i)i = i(1+i)$, if $a \equiv b \pmod{v}$, then $\bar{a} \equiv \bar{b} \pmod{v}$.

We would like to examine more closely what happens in the particular cases : $v = 1+i$, $v = 2$, and $v = 2(1+i)$.

The quotient ring $\mathcal{H}/(1+i)\mathcal{H}$

We observe that

$$i - 1 = i(1+i),$$
$$1 - j = \frac{1-i-j-k}{2}(1+i),$$
$$1 - k = \frac{1-i+j-k}{2}(1+i),$$

that is

$$i \equiv j \equiv k \equiv 1 \pmod{1+i}.$$

We have mentioned earlier that we denote the unit $\frac{1+i+j+k}{2}$ by ω. It is easy to see that a $\mathbb{Z}$-basis for $\mathcal{H}$ is $\{\omega, i, j, k\}$. Therefore any $h \in \mathcal{H}$ can be written as

$$h = \lambda_1\omega + \lambda_2 i + \lambda_3 j + \lambda_4 k,$$

where $\lambda_i \in \mathbb{Z}$, for $i = 1, 2, 3, 4$. Since all even numbers are congruent 0 modulo $(1 + i)$, one has that the possible remainders modulo $(1 + i)$ are

$$0, 1, \omega, \omega + 1,$$

depending on λ_1 and $\lambda_2 + \lambda_3 + \lambda_4$ been odd or even. Notice that $\omega^2 = \omega - 1$, and if we subtract any two of the non-zero possible remainders we end up with a unit in $\mathcal{H}$, which is clearly not divisible by $(1 + i)$, hence $\{0, 1, \omega, \omega^2\}$ is a set of representatives of all the equivalence classes modulo $(1 + i)$.

One can see that $h \in \mathcal{H}$ is relatively prime to $(1+i)$ if and only if $\mathrm{N}(h)$ is odd. If r is the highest power of 2 that divides $\mathrm{N}(h)$, then h can be written in the form

$$h = (1 + i)^r h_1,$$

where $h_1 \in \mathcal{H}$ is of odd norm. From now on a hurwitz integer will be called ***odd*** if it has odd norm, it will be called ***even*** if for r as above, we have that $r \geqslant 2$, and it will be called ***half even*** if $r = 1$.

Moreover, we remark that $h \in \mathcal{L}$ if and only if $h \equiv 0$ or $1 \pmod{1 + i}$.

The quotient rings $\mathcal{H}/2\mathcal{H}$, $\mathcal{H}/(2 + 2i)\mathcal{H}$ and primary quaternions

In this subsection we describe the equivalence classes in the rings $\mathcal{H}/2\mathcal{H}$, $\mathcal{H}/2(1 + i)\mathcal{H}$, and we define the notion of a primary quaternion, which plays a central role in the proof of Jacobi's four-square theorem.

Let $h = \lambda_1\omega + \lambda_2 i + \lambda_3 j + \lambda_4 k$ be some quaternion in $\mathcal{H}$. Letting λ_i take the values 0 and 1, we get all the possible remainders modulo 2.

We notice that $1 + i + j = 2\omega - k \equiv k \pmod 2$. Similarly all sums of 3 of the terms $1, i, j, k$ will result in a Hurwitz integer congruent to some unit modulo 2. Also, $1 + i = 2\omega - j - k \equiv j + k \pmod 2$, and similarly for all sums of two terms of $1, i, j, k$. What remains are the units

$$1, i, j, k, \frac{1 \pm i \pm j \pm k}{2}$$

and

$$0, 1+i, 1+j, 1+k.$$

Now let $b \in \mathcal{H}$ be odd. Then we have that b must be congruent to one of the units $1, i, j, k, \frac{1 \pm i \pm j \pm k}{2}$ modulo 2. Thus, there exists a unit $\epsilon \in \mathcal{H}$ such that $b\epsilon \equiv 1 \pmod 2$. Clearly $b(-\epsilon) \equiv 1 \pmod 2$ as well, but none of the remaining units $u \in \mathcal{H}$ can yield $bu \equiv 1 \pmod 2$, since they are not congruent modulo 2.

For those odd Hurwitz integers that are congruent to 1 modulo 2, we want to further reduce them modulo $(1+i)$. We have that if $h \equiv 1 \pmod 2$, then there exists $g \in \mathcal{H}$ such that $h = 1 + 2g$. Now, g must be congruent to one of $0, 1, \omega, \omega^2$ modulo $(1+i)$, so it can be written in one of the forms

$$g = g_1(1+i), g_1(1+i)+1, g_1(1+i)+\omega, g_1(1+i)+\omega^2,$$

for some $g_1 \in \mathcal{H}$. That means that every Hurwitz integer that is congruent to 1 modulo 2 is also congruent to one of

$$1, 1+2 \equiv -1, 1+2\omega, 1+2\omega^2 \equiv -1-2\omega$$

modulo $2+2i$.

Therefore, by putting everything together, we can see that for every odd Hurwitz integer b, there is a unit ϵ such that

$$b\epsilon \equiv 1 \text{ or } 1+2\omega.$$

Definition 3.1. *An odd Hurwitz integer is called* ***primary*** *if it is congruent to* 1 *or* $1+2\omega$ *modulo* $2+2i$.

The discussion above has proved the following.

Proposition 3.2. *Let* $b \in \mathcal{H}$ *be odd, then exactly one of its right (left) associates is primary.*

Note that $(1+2\omega)^2 \equiv 1 \pmod{2+2i}$. Hence the product of two primary Hurwitz integers is again primary. Also, if $b \equiv 1 \pmod{2+2i}$ then obviously $\bar{b} \equiv 1 \pmod{2+2i}$, and if $b \equiv 1+2\omega \pmod{2+2i}$ then $\bar{b} \equiv -1-2\omega \pmod{2+2i}$, meaning that if b is primary then either $\bar{b}$ is primary or $-\bar{b}$ is primary. Moreover, since $1+2\omega \equiv 1 \pmod{1+i}$, we can see that a primary Hurwitz integer is actually in $\mathcal{L}$.

3.1.2 The Hurwitz integers modulo an odd rational integer

Let $h = \lambda_1\omega + \lambda_2 i + \lambda_3 j + \lambda_4 k$ be as before, an arbitrary Hurwitz integer, and $m \in \mathbb{Z}$ be odd. Then since

$$h \equiv \lambda_1(1+m)\omega + \lambda_2 i + \lambda_3 j + \lambda_4 k \pmod{m}$$

and $1+m$ is even, we conclude that a Hurwitz integer is congruent to a Lipschitz integer modulo any odd rational integer. Moreover we see that any Hurwitz integer is congruent to

$$\kappa_1 + \kappa_2 i + \kappa_3 j + \kappa_4 k$$

modulo m, where κ_i, $i = 1, 2, 3, 4$ are rational integers that take values from 0 to $m-1$. Therefore, the m^4 different quaternions $\kappa_1 + \kappa_2 i + \kappa_3 j + \kappa_4 k$ form a complete system of residues modulo m.

An interesting isomorphism

Proposition 3.3. *Let $m \in \mathbb{Z}$ be odd. Then, $\mathcal{H}/m\mathcal{H} \cong \mathcal{M}_2(\mathbb{Z}/m\mathbb{Z})$*

Proof. Let

$$\varphi : \mathcal{H}/m\mathcal{H} \to \mathcal{M}_2(\mathbb{Z}/m\mathbb{Z})$$

$$\gamma_1 + \gamma_2 i + \gamma_3 j + \gamma_4 k \mapsto \begin{pmatrix} \gamma_1 + \gamma_2 a + \gamma_4 b & \gamma_3 + \gamma_4 a - \gamma_2 b \\ -\gamma_3 + \gamma_4 a - \gamma_2 b & \gamma_1 - \gamma_2 a - \gamma_4 b \end{pmatrix}$$

where $a^2 + b^2 \equiv -1 \pmod{m}$. We start by showing that such a, b always exist. First, we show this for $m = p$, a prime number. Consider the sets

$$A = \left\{ 1 + a^2 \mid a = 0, 1, \ldots, \frac{p-1}{2} \right\},$$

$$B = \left\{ -b^2 \mid b = 0, 1, \ldots, \frac{p-1}{2} \right\}.$$

Both sets contain $\frac{p+1}{2}$ incongruent numbers modulo p, and if we assume that their intersection is empty, then there would exist $p+1$ incongruent numbers modulo p, which is of course absurd.

Now, using Hensel's Lemma, see [5], for the two variable polynomial

$$f(x, y) = x^2 + y^2 + 1$$

we can see that $a^2 + b^2 \equiv -1 \pmod{p^k}$, $k \in \mathbb{N}$, always has a solution as well. This together with an application of the Chinese remainder theorem yield our claim that $a^2 + b^2 \equiv -1 \pmod{m}$ has a solution for any $m \in \mathbb{N}$.

It is easy to check that φ is indeed a homomorphism. It is also not very hard to check that $\varphi(v) = 0$ if and only if $v = 0$, therefore φ is injective, and since it is defined on a finite set to a finite set of the same cardinality, it is an isomorphism.

□

Corollary 3.4. *If* $\gamma \in \mathcal{H}/m\mathcal{H}$, *then* $\mathrm{N}(\gamma) = \det(\phi(\gamma))$ *and* $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\phi(\gamma))$, *where* det *and* Tr *are the usual matrix determinant and trace.*

3.1.3 Primitive Hurwitz integers of zero norm in $\mathcal{H}/m\mathcal{H}$

As we mentioned earlier, on our way to prove the Jacobi's four square theorem, we will need to count the number of zero norm elements in $\mathcal{H}/m\mathcal{H}$, for $m \in \mathbb{Z}$, an odd number. First we will do that for a particular type of Hurwitz integers, that we call ***primitive modulo*** m.

Definition 3.5. *A Hurwitz integer* $h = \lambda_1 + \lambda_2 i + \lambda_3 j + \lambda_4 k$, *is called* ***primitive*** *if the greatest common divisor* $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ *is* 1 *and is called* ***primitive modulo*** m *if* $(\lambda_1, \lambda_2, \lambda_3, \lambda_4, m) = 1$.

From the isomorphism in Proposition 3.3, if A_h is the image of h under φ then it is clear that h is primitive modulo m if and only if the entries of A_h and m have greatest common divisor equal to 1. Let

$$\mathcal{P}_m = \{A \in M_2(\mathbb{Z}/m\mathbb{Z}) \mid \det A = 0 \text{ and the entries of } A \text{ and } m \text{ have } g.c.d = 1\}.$$

Denote the number of Hurwitz integers of zero norm in $\mathbb{Z}/m\mathbb{Z}$ that are primitive modulo m by $\psi(m)$. By Proposition 3.3 this number is equal to the cardinality of $\mathcal{P}_m$. Therefore, $\psi(m)$ is the number of solutions of the equation $ad - bc \equiv 0 \pmod{m}$ with $(a, b, c, d, m) = 1$.

Lemma 3.6. *Let* $m \in \mathbb{N}$ *be odd and* $m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ *its prime factorization, where* p_i *are distinct primes and* $a_i \in \mathbb{N}_0$, *for* $i = 1, 2, \ldots, n$. *Then*

$$\psi(m) = \prod_{i=1}^{n} \psi(p_i^{a_i})$$

Proof. This is a direct consequence of the Chinese remainder theorem. □

Lemma 3.7. *Let* ψ *be as above, then*

$$\psi(p^{k+1}) = p^{3k}\psi(p)$$

Proof. This is again an application of the multivariate version of Hensel's lemma. This time, since we do not just need to know that we have a solution for highest powers of p, but we need to know the exact number of solutions, we will perform the actual calculation. We have that $\psi(p^k)$ is the number of primitive solutions of $ad - bc \equiv 0 \pmod{p^k}$. Let a_0, b_0, c_0, d_0 be a particular solution of it, i.e. $a_0 d_0 - b_0 c_0 = \lambda p^k$, for some $\lambda \in \mathbb{Z}$. Then, for $x, y, z, w \in \mathbb{Z}$, consider

$$a = a_0 + p^k x,\ b = b_0 + p^k y,\ c = c_0 + p^k z,\ d = d_0 + p^k w.$$

Since

$$\begin{aligned} ad - bc &= (a_0 + p^k x)(d_0 + p^k w) - (b_0 + p^k y)(c_0 + p^k z) \\ &= \lambda p^k + p^k(xd_0 + wa_0 - b_0 z - c_0 y). \end{aligned}$$

We see that $ad - bc \equiv 0 \pmod{p^{k+1}}$ if and only if

$$\lambda + (a_0 w - b_0 z - c_0 y + d_0 x) \equiv 0 \pmod{p}. \tag{3.1}$$

Since we only care about primitive solutions, we know that at least one of a_0, b_0, c_0, d_0 is not divisible by p. Without loss of generality, let us assume that $a_0 \not\equiv 0 \pmod{p}$. Then, if we let x, y, z run from 0 to $p-1$ the congruence (3.1) is satisfied for a unique $w \in \mathbb{F}_p$, for each triple (x, y, z). Consequently, each solution of $ad - bc \equiv 0 \pmod{p^k}$ gives rise to p^3 solutions of $ad - bc \equiv 0 \pmod{p^{k+1}}$, meaning that

$$\psi(p^{k+1}) = p^3 \psi(p^k).$$

Repeating this argument k times yields the claim. □

Let us now calculate $\psi(p)$. We are looking for the number of solutions of $ad - bc \equiv 0 \pmod{p}$ such that $(a, b, c, d, p) = 1$. So let us break them into p groups, as follows:

$$ad \equiv bc \equiv 0,\ ad \equiv bc \equiv 1, \ldots, ad \equiv bc \equiv p - 1 \pmod{p}.$$

We can easily see that each of the $p - 1$ groups, except for the first one, has $(p-1)^2$ solutions, while the first one has $(2p-1)^2 - 1 = 4p^2 - 4p$ solutions, since the solution $(0, 0, 0, 0)$ must be excluded. Putting everything together, we have that

$$\psi(p) = (p-1)^3 + 4p^2 - 4p = (p^2 - 1)(p + 1).$$

We therefore have that

$$\psi(p^k) = p^{3k}\left(1-\frac{1}{p^2}\right)\left(1+\frac{1}{p}\right).$$

Using Lemma 3.6 we have proved the following.

Proposition 3.8. *Let $m \in \mathbb{N}$ be odd. The number of different Hurwitz integers of zero norm in $\mathcal{H}/m\mathcal{H}$ that are primitive modulo m is equal to*

$$\psi(m) = m^3 \prod_{p|m}\left(1-\frac{1}{p^2}\right)\left(1+\frac{1}{p}\right).$$

3.1.4 Counting Hurwitz integers of norm one in $\mathcal{H}/m\mathcal{H}$

Now let us see how many Hurwitz integers have norm equal to 1 in $\mathbb{Z}/m\mathbb{Z}$. Denote their number by $\chi(m)$. We just need to check the solutions of the equation $ad - bc \equiv 1 \pmod{m}$. Similarly to the previous section for $m = p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$, where p_i are distinct primes, and $a_i \in \mathbb{N}_0$, for $i = 1, 2, \ldots, n$, we have

$$\chi(m) = \prod_{i=1}^{n} \chi(p_i^{a_i}) \tag{3.2}$$

and

$$\chi(p^k) = p^{3(k-1)}\chi(p) \tag{3.3}$$

Now, in order to calculate $\chi(p)$, we again break it down to the p-groups

$$\begin{cases} ad \equiv 2 \\ bc \equiv 1 \end{cases}, \begin{cases} ad \equiv 3 \\ bc \equiv 2 \end{cases}, \ldots, \begin{cases} ad \equiv 0 \\ bc \equiv p-1 \end{cases}, \begin{cases} ad \equiv 1 \\ bc \equiv 0 \end{cases} \pmod{p}.$$

Each of the first $p-2$ groups has $(p-1)^2$ solutions, while each of the last two groups has $(p-1)(2p-1)$ solutions. Adding them all together yields

$$\chi(p) = p(p^2-1)$$

Using this together with (3.2) and (3.3) we get the following

Proposition 3.9. *Let $m \in \mathbb{N}$ be odd. The number of different Hurwitz integers of norm one in $\mathbb{Z}/m\mathbb{Z}$ is equal to*

$$\chi(m) = m^3 \prod_{p|m} \left(1 - \frac{1}{p^2}\right).$$

3.1.5 Number of primary primes above a rational prime

Let $h \in \mathcal{L}$ be a representative of some class of the $\psi(p)$ classes of Hurwitz integers (ψ from Proposition 3.8) of zero norm in $\mathcal{H}/p\mathcal{H}$ that are primitive modulo an odd prime p. Assume that h is such that $p^2 \mid \mathrm{N}(h)$, then for $h' = h + pt$ with $t \in \mathcal{H}$, we have

$$\mathrm{N}(h') \equiv \mathrm{N}(h) + 2pt \pmod{p^2}.$$

We then can choose t appropriately so that $p^2 \nmid \mathrm{N}(h')$. Therefore we may choose representatives of all those classes in $\mathcal{H}/p\mathcal{H}$ that have norm divisible by p but not p^2.

Since $\mathrm{N}(h)$ is divisible by p, by Theorem 2.11 we know that there exists $\pi \in \mathcal{H}$ with $\mathrm{N}(\pi) = p$, such that $h = a\pi$, for some $a \in \mathcal{H}$. Moreover, since there is a unique unit in $\mathcal{H}$ that makes π primary, we may assume that π is primary by letting a absorb this unit. Note that a can be assumed to be a Lipschitz integer according to the initial comments of Section 3.1.2.

Observe also that if we have two distinct primary primes π_1 and π_2 above p, then $a\pi_1 \not\equiv b\pi_2 \pmod{p}$ for all $a, b \in \mathcal{L}/p\mathcal{L}$, except for the case $a\pi_1 \equiv b\pi_2 \equiv 0 \pmod{p}$. Indeed, assume that there exists $a, b \in \mathcal{L}/p\mathcal{L}$, such that $a\pi_1 \equiv b\pi_2 \not\equiv 0 \pmod{p}$. Then $a\pi_1\overline{\pi}_2 \equiv 0 \pmod{p}$, and therefore there exists $c \in \mathcal{L}$ such that $a\pi_1\overline{\pi}_2 = cp = c\pi_2\overline{\pi}_2$. Hence, we have that $a\pi_1 = c\pi_2$, and thus, since $a\pi_1 \not\equiv 0 \pmod{p}$, by Theorem 2.15 we have that $\pi_1 = u\pi_2$ for some unit $u \in \mathcal{L}$, a contradiction.

Therefore each one of the $\psi(p)$ classes of Hurwitz integers of zero norm in $\mathbb{Z}/p\mathbb{Z}$ that are primitive modulo p has a representative of the form $a\pi$, where $a, \pi \in \mathcal{L}$, and π is a primary prime.

We will show that for π a primary prime, there are p^2-1 different residues modulo p of the form $a\pi$, $a \in \mathcal{L}$, in the list of the representatives of the $\psi(p)$ quaternions of zero norm in $\mathcal{H}/p\mathcal{H}$ that are primitive modulo p.

Multiply a given primary prime π on the left with all the p^4 different quaternions modulo p. Then, the number of elements of the form $b\pi$, that are congruent to a given one $a\pi$, modulo p, is equal to the number of solutions of the congruence $x\pi \equiv 0 \pmod{p}$ in $\mathcal{L}/p\mathcal{L}$.

Lemma 3.10. *Let $\pi \in \mathcal{H}$ have norm equal to the odd prime p. Then the equation*

$$x\pi \equiv 0 \pmod{p}$$

has p^2 solutions in $\mathcal{L}/p\mathcal{L}$.

Proof. Let $A_\pi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be the matrix in $\mathcal{M}_2(\mathbb{F}_p)$ that corresponds to π under the isomorphism in Proposition 3.3. The number of solutions in $\mathcal{H}/p\mathcal{H}$ of $x\pi \equiv 0 \pmod{p}$ is equal to the number of solutions of

$$A_\pi X \equiv 0 \pmod{p}$$

for $X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \in \mathcal{M}_2(\mathbb{F}_p)$. Now the last congruence is equivalent to

$$\begin{cases} x_1 a + x_2 c \equiv 0 \\ x_1 b + x_2 d \equiv 0 \end{cases} \pmod{p} \quad \text{and} \quad \begin{cases} x_3 a + x_4 c \equiv 0 \\ x_3 b + x_4 d \equiv 0 \end{cases} \pmod{p}.$$

Since π is a Hurwitz prime, it is primitive, and therefore $A_\pi \in \mathcal{P}_\pi$. Hence at least one of a, b, c, d is not divisible by p. Without loss of generality we may assume that $p \nmid a$. Thus, looking at the first system

$$\begin{cases} x_1 a + x_2 c \equiv 0 \\ x_1 b + x_2 d \equiv 0 \end{cases} \pmod{p},$$

we have that $x_1 \equiv -x_2 c a^{-1} \pmod{p}$. The second equation is fulfilled automatically from the first, since

$$a(x_1 b + x_2 d) = b(x_1 a + x_2 c) + (ad - bc)x_2 \pmod{p}.$$

Therefore, choosing x_2 arbitrarily, uniquely determines x_1, meaning that there are p solutions of the first system. The same is true for x_3 and x_4, which yields the claim. □

A direct consequence of the above lemma is that there are $p^4/p^2 = p^2$ left multiples of π that are incongruent modulo p. Removing the zero one, we conclude that there are $p^2 - 1$ different left multiples of a given primary prime π in the totality of $\psi(p) = (p^2 - 1)(p + 1)$ different Hurwitz primes of zero norm in $\mathcal{H}/p\mathcal{H}$ that are primitive modulo p.

Therefore, since for every primary prime π of norm p, we may choose a representative of the form $a\pi$, for some $a \in \mathcal{L}$, for all $\psi(p)$ classes, and there are $p^2 - 1$ different Hurwitz integers of the form $a\pi$, we conclude the following.

Theorem 3.11. *There are $p + 1$ primary primes with norm p.*

3.1.6 Primary Hurwitz integers of norm m

Now let b be an odd primary Hurwitz integer, that is $b \equiv 1$ or $1 + 2\omega \pmod{2 + 2i}$, and let $m \in \mathbb{Z}$ be the largest integer that divides it. Then $b = mc$ for some primitive quaternion $c \in \mathcal{H}$. Note that both m and $-m$ divide b, so if we set m to be whichever one is congruent to 1 modulo 4, then since $2(1 + i) \mid 4$, it follows that c is primary. Therefore, a primary quaternion that is not primitive can be written as a rational integer times a primary and primitive quaternion. Note that a Lipschitz prime is always primitive.

Proposition 3.12. *Let $m > 1$ be an odd integer. The number of primary and primitive Lipschitz integers of norm m is equal to*

$$Q(m) = m \prod_{p|m} \left(1 + \frac{1}{p}\right). \tag{3.4}$$

Proof. Letting $m = p^k q^n \ldots$, since we are looking for primitive and primary Lipschitz integers h of norm m, by Theorem 2.11 it suffices to look at all possible products of the form

$$\pi_1 \pi_2 \cdots \pi_k \rho_1 \rho_2 \cdots \rho_n \cdots$$

with $\mathrm{N}(\pi_i) = p$, $\mathrm{N}(\rho_j) = q, \ldots$, for $i = 1, \ldots, k$, $j = 1, \ldots, n$, and so on, and such that no two consecutive factors in the product are conjugates.

Now, π_1 can be any of the $p + 1$ different primary primes of norm p, π_2 can be any of the $p + 1$ primes of norm p except $\bar{\pi}_1$, and so on. Hence

$$Q(m) = (p+1)p^{k-1}(q+1)q^{n-1} \cdots$$

which is equal to

$$Q(m) = m \left(1 + \frac{1}{p}\right)\left(1 + \frac{1}{q}\right) \cdots$$

□

From the above proof it follows that if m_1 and m_2 are relatively prime, then

$$Q(m_1 m_2) = Q(m_1)Q(m_2). \tag{3.5}$$

Now, let us look at the number of all the primary Hurwitz integers of norm m. Let $b \in \mathcal{H}$ be primary but not primitive. There exists $d \in \mathbb{Z}$ such that $b = dc$, with $d \equiv 1 \pmod 4$ and c primitive and primary. We have that $\mathrm{N}(b) = d^2 \mathrm{N}(c) = m$. Hence, if we let d go through all the numbers congruent to 1 modulo 4 whose square divides m, and count all the primary and primitive quaternions of norm $c = m/d^2$, for each d, then adding everything together will yield the number of all primary quaternions of norm m. The

number of all primary and primitive quaternions of norm m/d^2 is $Q(m/d^2)$, thus the number of all primary quaternions of norm m is

$$f(m) = \sum_{d^2|m} Q\left(\frac{m}{d^2}\right), \tag{3.6}$$

where the sum runs through all d that their square divide m. Now for $m = p^k q^n \ldots$, let $d^2 = p^{2a}q^{2b}$, where $a, b, \ldots$ are all non-negative numbers such that $2a \leqslant k$, $2b \leqslant n$. Then, we have

$$f(m) = \sum_{d^2|m} Q\left(\frac{m}{d^2}\right) = \sum_{a=0}^{k/2} Q\left(p^{k-2a}\right) \cdot \sum_{b=0}^{n/2} Q\left(q^{n-2b}\right) \cdots$$

By (3.4) we have

$$\begin{aligned} \sum_{a=0}^{k/2} Q\left(p^{k-2a}\right) &= Q\left(p^k\right) + Q\left(p^{k-2}\right) + Q\left(p^{k-4}\right) + \ldots + \\ &= p^{k-1}(p+1) + p^{k-3}(p+1) + p^{k-5}(p+1) + \ldots \\ &= p^k + p^{k-1} + \ldots + p + 1. \end{aligned}$$

This proves the following result.

Proposition 3.13. *Let $m \in \mathbb{Z}$ be odd. The number of primary Hurwitz integers of norm m is equal to the divisor function*

$$\sigma(m) = \prod_p \sum_{i=1}^{\nu_p(m)} p^i = \sum_{d|m} d, \tag{3.7}$$

where $\nu_p(m)$ is the p-adic valuation of m.

3.1.7 Jacobi's four-square Theorem

On this section we look at the number of ways that a given positive integer n can be represented as a sum of four squares i.e. the number of solutions of the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n,$$

with $x_1, x_2, x_3, x_4 \in \mathbb{N}$. This number is usually denoted by $r_4(n)$.

We can write the above equation in the form

$$\mathrm{N}(x) = n$$

for

$$x = x_1 + x_2 i + x_3 j + x_4 k.$$

The number we are looking for is, thus, equal to the number of Lipschitz integers of norm $n \in \mathbb{N}$.

Let 2^r be the highest power of 2 that divides n. Hence we can write $n = 2^r m$, where m is odd. We can see the two cases

- If $r = 0$, then $n = m$ is odd. By Proposition 3.2, out of the 24 right (left) associates of any Hurwitz integer of odd norm there is a unique one that is primary, and therefore in $\mathcal{L}$. The number of primary quaternions of odd norm m, by Proposition 3.13, is equal to

  $$f(n) = \sum_{d|n} d$$

  Each primary quaternion is a Lipschitz integer and multiplying it by the units $\pm 1, \pm i, \pm j, \pm k$ yields again a quaternion in $\mathcal{L}$. On the other hand, multiplying a primary quaternion by the remaining units in $\mathcal{H}$, yields elements not in $\mathcal{L}$. We therefore have that there are

  $$r_4(n) = 8 \cdot \sum_{d|n} d.$$

  Lipschitz integers of norm n, when n is odd.

- If $r \geqslant 1$, then we have that

  $$\mathrm{N}(x) = 2^r m,$$

and, as we have seen before, we can write

$$x = (1+i)^r \cdot y,$$

where $y \in \mathcal{H}$ is odd.

For any quaternion y, we have that $x = (1+i)^r y\ \epsilon \in \mathcal{L}$ for all 24 units ϵ of $\mathcal{H}$. Moreover, using the fact that exactly one of the right associates of a given quaternion of odd norm is primary, and that there are $f(m) = \sum_{d|m} d$ primary quaternions of norm m, we get that there are

$$r_4(n) = 24 \cdot \sum_{\substack{d|n \\ d\ odd}} d,$$

Lipschitz integers of norm n, when n is even.

We have proved:

Theorem 3.14 (Jacobi's four-square Theorem)**.** *The number $r_4(n)$ of ways that a given positive integer n can be represented as the sum of four squares is equal to*

$$r_4(n) = \begin{cases} 8 \cdot \sum_{d|n} d, & \text{if } n \text{ is odd} \\ 24 \cdot \sum_{\substack{d|n \\ d\ odd}} d, & \text{if } n \text{ is even} \end{cases}$$

3.2 Gordon Pall's results

In this section we will take a look at some more results from Gordon Pall's 1940 work [15] on the ring of Lipschitz integers. His work sheds some light into the factorization of Lipschitz integers. Almost all propositions, theorems and corollaries can be found on [15]. We adjusted the notations and proofs to make the readers job easier. Some of these results will be used in the proof of the "1-3-5 Conjecture".

3.2.1 Left multiples

For a primitive Lipschitz integer, we will describe the different left multiples modulo a rational prime power. Moreover, we will see how many of them there are. We also look at its left multiples that are pure modulo a prime power, and show that they are proportional modulo this prime power.

Lemma 3.15. *Let $t = t_0 + t_1 i + t_2 j + t_3 k$ be primitive, p is an odd rational prime and $p \nmid t_0^2 + t_\alpha^2$ for some $\alpha \in \{1, 2, 3\}$. No two of the following p^{2r} quaternions are congruent modulo p^r:*

$$(e + fu)t, \qquad e, f = 0, 1, \dots, p^r - 1, \tag{3.8}$$

where $u = i$, if $p \nmid t_0^2 + t_1^2$; $u = j$, if $p \nmid t_0^2 + t_2^2$; and $u = k$, if $p \nmid t_0^2 + t_3^2$.

Proof. Assume $p \nmid t_0^2 + t_1^2$, and suppose that $(e_1 + f_1 i)t \equiv (e_2 + f_2 i)t \pmod{p^r}$. Putting $t = t_0 + t_1 i + t_2 j + t_3 k$, this is equivalent to

$$\begin{aligned}(e_1 - e_2)t_0 - (f_1 - f_2)t_1 &\equiv 0 \pmod{p^r} \\ (e_1 - e_2)t_1 + (f_1 - f_2)t_0 &\equiv 0 \pmod{p^r}.\end{aligned}$$

Multiplying the first by t_0, the second by t_1, and adding the two congruencies yields

$$(e_1 - e_2)(t_0^2 + t_1^2) \equiv 0 \pmod{p^r}.$$

Since $p \nmid t_0^2 + t_1^2$, we get $e_1 \equiv e_2 \pmod{p^r}$. Similarly we get $f_1 \equiv f_2 \pmod{p^r}$. The proof is similar if $p \nmid t_0^2 + t_2^2$ or $p \nmid t_0^2 + t_3^2$. □

The following is a generalization of Lemma 3.10.

Theorem 3.16. *Let p be an odd rational prime, and $t \in \mathcal{L}$ be primitive, such that $p^r \mid \mathrm{N}(t)$. If $u \in \mathcal{L}$ runs through all p^{4r} remainders modulo p^r, then ut takes precisely p^{2r} values modulo p^r, and each one of these values is taken precisely p^{2r}.*

Proof. We will show that $\exists \alpha \in \{1, 2, 3\}$ such that $p \nmid t_0^2 + t_\alpha^2$. Suppose $p \mid t_0^2 + t_\alpha^2$, $\forall \alpha = 1, 2, 3$. Then it should divide their sum too, so $p \mid 3t_0^2 + t_1^2 +$

$t_2^2 + t_3^2 = 2t_0^2 + \mathrm{N}(t)$. But $p^r \mid \mathrm{N}(t)$, so $p \mid \mathrm{N}(t)$, hence we must have $p \mid t_0^2$, and therefore, $p \mid t_0$. Now from $p \mid t_0^2 + t_\alpha^2$, we get $p \mid t_\alpha$, $\alpha = 1, 2, 3$, which is impossible since t is primitive.

Let λ denote the number of solutions of $xt \equiv 0 \pmod{p^r}$, and μ denote the number of possible values of ut modulo p^r. The number of solutions $xt \equiv wt$, for a given representative w, is the same as that of $(x - w)t \equiv 0$, hence equals λ. Therefore $\mu\lambda = p^{4r}$. By lemma 3.15, $\mu \geq p^{2r}$, and since $x = (e + fi_\alpha)\bar{t}$, e, f from 3.15, satisfies $xt \equiv 0$, we get that $\lambda \geq p^{2r}$. Thus, finally $\lambda = \mu = p^{2r}$. □

Corollary 3.17. *If $p^n \mid Nt$, the residues (3.8) in lemma 3.15 represent a complete set of left multiples of t modulo p^n.*

Proof. This is obvious from the proof of Theorem 3.16. □

Corollary 3.18. *Precisely p^r of the p^{2r} left multiples of t modulo p^r are pure modulo p^r.*

Proof. Let α from lemma 3.15 be equal to 1. Then, a left multiple of t will have the form

$$(e + fi)t = (et_0 - ft_1) + (et_1 + ft_0)i + (et_2 - ft_3)j + (et_3 + ft_2)k, \quad (3.9)$$

and it is pure modulo p^r if and only if $(et_0 - ft_1) \equiv 0 \pmod{p^r}$. Now, since either t_0 or t_1 is not divisible by p, and assuming without loss of generality that $t_1 \not\equiv 0 \pmod{p}$, then for each $e \in \{0, 1, ..., p^r - 1\}$ there is exactly one $f \in \{0, 1, ..., p^r - 1\}$ such that $(et_0 - ft_1) \equiv 0 \pmod{p^r}$. Therefore p^r of the left multiples of t pure. The cases for $\alpha = 2, 3$ are similar. □

Theorem 3.19. *Let t be primitive, and $m \mid \mathrm{N}(t)$. Then, all left-multiples ut, which are pure modulo m, are proportional modulo m.*

Proof. By the Chinese Remainder Theorem we can reduce the proof to the case where $m = p^r$, a prime power. By the first paragraph of the proof of Theorem 3.16, there is an $\alpha \in \{1, 2, 3\}$ such that $p \nmid t_0^2 + t_\alpha^2$. Without loss of

generality, we may assume $\alpha = 1$. By Corollary 3.18, we get that the pure modulo p^r left multiples of t, are of the form

$$\lambda_{e,f} \equiv (et_1 + ft_0)i + (et_2 - ft_3)j + (et_3 + ft_2)k \pmod{p^r},$$

where

$$et_0 - ft_1 \equiv 0 \pmod{p^r}.$$

Assuming, again without loss of generality, that $t_1 \not\equiv 0 \pmod{p}$, we have

$$\begin{aligned}\lambda_{e,f} &\equiv e(t_1 i + t_2 j + t_3 k) + f(t_0 i - t_3 j + t_2 k) \\ &\equiv e(t_1 i + t_2 j + t_3 k) + et_0/t_1(t_0 i - t_3 j + t_2 k) \\ &\equiv e\left[(t_1 i + t_2 j + t_3 k) + t_0/t_1(t_0 i - t_3 j + t_2 k)\right] \pmod{p^r}.\end{aligned}$$

Hence for e running through $0, p^r - 1$, we obtain all the p^r pure left multiples of t, and they are clearly proportional modulo p^r. □

Corollary 3.20. *Let v be primitive and pure modulo m, $m \mid \mathrm{N}(v)$, and let wv be pure modulo m. Then, there exists an integer λ such that $wv \equiv \lambda v \pmod{m}$.*

Proof. From the proportionality of the pure left multiples v modulo m, and the fact that v itself is pure. □

3.2.2 Right and left divisors

The aim of this chapter is to examine when two quaternions have the same divisors of a given integer norm. We will give necessary and sufficient conditions for them to have the same right divisors, the same left divisors and the same left and right divisors. The result yielding a necessary and sufficient condition for two quaternions to have the same right and left divisors of a given norm, will be used in the proof of the 1-3-5 conjecture. Throughout this section m is an odd integer.

Lemma 3.21. *Let x and y be primitive modulo m, where $m \in \mathbb{Z}$, $m \mid \mathrm{N}(x)$, $m \mid \mathrm{N}(y)$. If x and y have the same right divisors of norm p^r, for every p^r dividing m, then x and y have the same right divisors of norm m.*

Proof. Let us first prove the claim for $m = pq$, where p, q are distinct rational primes. Therefore, we are assuming that x and y have the same right divisors of norm p and q. Let P be the common right divisor of x and y of norm p, then we can write $x = L_1P$ and $y = L_2P$ for some $L_1, L_2 \in \mathcal{L}$. Now, $q \mid \mathrm{N}(L_1), \mathrm{N}(L_2)$, hence, by Theorem 2.15, we can write $L_1 = L_1'Q_1$ and $L_2 = L_2'Q_2$, for some unique up to left associates Q_1, Q_2 of norm q, and $L_1', L_2' \in \mathcal{L}$. Then, we will have that

$$x = L_1'Q_1P$$

and

$$y = L_2'Q_2P.$$

Each of the quaternions Q_1P, Q_2P have a unique, up to left unit multiplication, right divisor of norm q, call them Q_1', Q_2'. Then, Q_1', Q_2' are right divisors of x, y of norm q as well, and since x and y have the same right divisors of q we must have that Q_1' and Q_2' are left associates.

Therefore we can write

$$Q_1P = P_1Q$$

and

$$Q_2P = P_2Q$$

for some $P_1, P_2 \in \mathcal{L}$ of norm p, and $Q \in \mathcal{L}$ of norm q, a left associate of Q_1' and Q_2'. From these two equalities we get that

$$Q\bar{P} = \bar{P}_1Q_1 = \bar{P}_2Q_2.$$

By Theorem 2.15, we get that Q_1 and Q_2 are left associates, which means that Q_1P and Q_2P are left associates. Therefore we have proven that if x

and y have the same right divisors of norm p and q, then they have the same right divisors of norm pq.

To finish the proof notice that the whole argument works fine if, instead of primes, we have powers of primes. This together with a simple induction argument yields the claim. □

Lemma 3.22. *The largest rational integer factor of m dividing $z \in \mathcal{L}$ is not changed if z is replaced by yz, or zy, for any $y \in \mathcal{L}$, where $\mathrm{N}(y)$ is coprime to m.*

Proof. Let k be the largest rational integer factor of m that divides z. Then obviously $k \mid yz$. Moreover let $k_0 > k$ be the largest integer factor of yz, with $k_0 \mid m$. Then, $k_0^2 \mid \mathrm{N}(yz) = \mathrm{N}(y)\,\mathrm{N}(z)$, and since $k_0 \nmid \mathrm{N}(z)$, then $\frac{k_0}{k} \mid \mathrm{N}(y)$, which cannot happen, since $(\mathrm{N}(y), m) = 1$.

On the other hand let k be the largest integer factor of yz that divides m. Then $k \mid \bar{y}yz = \mathrm{N}(y)z$, therefore we must have $k \mid z$, since $\mathrm{N}(y)$ is coprime to m. It is clear that k is the largest divisor of z that divides m, because otherwise we would have a divisor of yz larger than k. □

Lemma 3.23. *Let $t_1, t_2, \ldots, t_f \in \mathcal{L}$ have odd prime norm p. Then*

$$t = t_1 t_2 \cdots t_f \text{ is primitive} \iff t_i t_{i+1} \text{ is primitive } \forall i = 1, 2, \ldots, f-1.$$

Proof. ($\Rightarrow$) let $t = t_1 t_2 \cdots t_f$ be primitive, and assume that there exists a $j \in \{1, 2, \ldots, f-1\}$ such that $t_j t_{j+1} = qr$, for some rational prime q, and some $r \in \mathcal{L}$. Then, we have

$$\begin{aligned} t =& t_1 t_2 \cdots t_f \\ =& t_1 t_2 \cdots t_j t_{j+1} \cdots t_f \\ =& t_1 t_2 \cdots t_{j-1}\, qr\, t_{j+2} \cdots t_f \\ =& q t_1 t_2 \cdots t_{j-1}\, r\, t_{j+2} \cdots t_f, \end{aligned}$$

hence t is not primitive, a contradiction.

($\Leftarrow$) For $f = 2$, t is primitive trivially. Assume that $t_i t_{i+1}$ is primitive for $i = 1, 2, \ldots, f$, and assume that $t = t_1 t_2 \cdots t_f$ is primitive as well. We will show that $x = t t_{f+1}$ is primitive.

Assume that x is non-primitive. Then, it can be written as $x = yq$, where $y \in \mathcal{L}$ and q a rational prime. Taking norms, we have $\mathrm{N}(x) = q^2 \mathrm{N}(y)$. We also have that $\mathrm{N}(x) = \mathrm{N}(t)\,\mathrm{N}(t_{f+1}) = p^{f+1}$, so we must have that $q = p$. Therefore, we have that $x = yp$, so $t t_{f+1} = y\overline{t_{f+1}} t_{f+1}$, which yields $t = y\overline{t_{f+1}}$. Hence $t^{(f)}$ and $\overline{t^{(f+1)}}$ are both right divisors of t of norm p, and thus, by Theorem 2.15, we must have that $t_f = u\overline{t_{f+1}}$ for some unit u. Thus $t^{(f)} t^{(f+1)} = up$, which means that it is not primitive, and contradicts our assumption. □

Remark. Let $t_1, t_2, \ldots, t_f \in \mathcal{L}$ have odd prime norm p. If any $t_i t_{i+1}$ is not primitive, then it is of the form up, u a unit; we can remove the factor p from $t = t_1 t_2 \cdots t_f$, absorb the unit u into t^{i-1} or t^{i+2}, and proceed with the remaining product of $f - 2$ factors. We finally obtain $t = p^r t_1 t_2 \cdots t_h$, where $t_1, t_2, \ldots, t_h \in \mathcal{L}$ primitive as in the previous lemma, and $h = f - 2r$.

Lemma 3.24. *If x and y are primitive modulo p, and $xy \equiv 0 \pmod{p^r}$, then $p^r \mid \mathrm{N}(x)$ and $\mathrm{N}(y)$, and x and $\bar{y}$ have the same right divisors of norm p^r.*

Proof. We have $p^r \mid xy$, so $p^r \mid \bar{x}xy$ and $p^r \mid xy\bar{y}$, and since $p \nmid x, y$, we get that $p^r \mid \mathrm{N}(x), \mathrm{N}(y)$. Hence, by Theorem 2.15, there exists z, z', v, v', t, t' $x = zz't$, $\bar{y} = \bar{v}\bar{v}'\bar{t}'$, where $\mathrm{N}(t) = \mathrm{N}(t') = p^r$, $\mathrm{N}(z') = p^e$, $\mathrm{N}(v') = p^f$ $(e, f \geqslant 0)$ and $\mathrm{N}(z)\,\mathrm{N}(v) \not\equiv 0 \pmod{p}$. Then we have that

$$xy = zz'tt'v'v \equiv 0 \pmod{p^r}$$

Now, since x and y are primitive modulo p, it follows that zz', $z't$ and $t'v'$, $v'v$ are primitive $\pmod{p}$. Therefore, by Lemmas 3.22 and the above remark, we must have that $tt' \equiv 0 \pmod{p^r}$. Since $\mathrm{N}(t) = \mathrm{N}(t') = p^r$, that means that t and $\bar{t}'$ must be left associates. □

Theorem 3.25. *Let x and y be primitive modulo m. Then,*

$$x \text{ and } y \text{ have the same right divisors of norm } m \iff x\bar{y} \equiv 0 \pmod{m}.$$

Proof. ($\Rightarrow$) If $x = ut, y = vt$, for some $t \in \mathcal{L}$, with $\mathrm{N}(t) = m$, then $x\bar{y} = ut\bar{t}\bar{v} = muv \equiv 0 \pmod{m}$.
($\Leftarrow$) By Lemma 3.24, we know that x and y have the same right divisors of norm p^r for all the prime powers p^r dividing m. Corollary 3.21 finishes the proof. □

Theorem 3.26. *Let x and y be primitive modulo m, $m \mid \mathrm{N}(x), \mathrm{N}(y)$. Then, there exists a factorization $m = m_1 m_2$, in odd positive integers, such that x and y have the same left divisors of norm m_1, and the same right divisors of norm m_2, if and only if*

$$x \cdot y \equiv 0 \pmod{m},$$

where the dot denotes the usual inner product on $\mathbb{R}^4$.

Proof. ($\Rightarrow$) Let t' and t'' be left and right divisors of x of norm m_1 and m_2, respectively. Then $x = ut''$, where $m_1 \mid \mathrm{N}(u)$, and by the uniqueness in Theorem 2.15 the left divisor of norm m_1 of u, must be t'. Hence there is $a \in \mathcal{L}$, such that $x = t'at''$. Similarly, there is $b \in \mathcal{L}$, such that $y = t'bt''$, and $\mathrm{N}(t') = m_1$, $\mathrm{N}(t'') = m_2$. We need to show that $x \cdot \bar{y} = \frac{1}{2}(x\bar{y} + y\bar{x}) \equiv 0 \pmod{m}$. We have

$$\begin{aligned} x\bar{y} + y\bar{x} &= t'at''\bar{t}''\bar{b}\bar{t}' + t'bt''\bar{t}''\bar{a}\bar{t}' \\ &= t'am_1\bar{b}\bar{t}' + t'bm_1\bar{a}\bar{t}' \\ &= m_1t'(a\bar{b} + b\bar{a})\bar{t}' = m_1t'(2a \cdot \bar{b})\bar{t}' \\ &= 2(a \cdot \bar{b})m_1t'\bar{t}' = 2(a \cdot \bar{b})m_1m_2 \\ &= 2(a \cdot \bar{b})m \equiv 0 \pmod{m}. \end{aligned}$$

($\Leftarrow$) Let $x \cdot y \equiv 0 \pmod{m}$, therefore $x\bar{y} + y\bar{x} \equiv 0 \pmod{m}$. Multiplying by x on the right yields $x\bar{y}x \equiv 0 \pmod{m}$.

We will first prove the claim for $m = p^r$, so $p^r \mid \bar{y}x$. Let p^s be the highest power of p such that $p^s \mid x\bar{y}$. By Theorem 3.25, x and y have the same right divisors of norm p^s. If $s = r$, then the claim holds trivially. If $r > s$, let t be the common right right divisor of x and y with $\mathrm{N}(t) = p^s$. Then we can write $x = ut$, $y = vt$. We see that $x\bar{y} = p^s u\bar{v}$, and since p^s is the highest power of p that divides $x\bar{y}$, we get that $p \nmid u\bar{v}$. Moreover, we have that $x\bar{y}x = p^s u\bar{v}x$ and $p^r \mid x\bar{y}x$, hence $p^{r-s} \mid u\bar{v}x$. By Theorem 3.25 we have that $v\bar{u}$ and x have the same left divisors of norm p^{r-s}. These must be the same as the left divisors of v of norm p^{r-s}, and therefore with those of y. This proves the theorem if m is a prime power. Corollary 3.21 then, yields the result for any $m \in \mathbb{Z}$. □

If $x = x_0 + x_1 i + x_2 j + x_3 k$ and $y = y_0 + y_1 i + y_2 j + y_3 k$, then $x\bar{y} \equiv 0 \pmod{p^r}$ is, of course, equivalent to

$$x_0 y_0 + x_1 y_1 + x_2 y_2 + x_3 y_3 \equiv 0 \pmod{p^r} \tag{3.10}$$

together with

$$\begin{cases} (x_0 y_1 - x_1 y_0) + (x_2 y_3 - x_3 y_2) \equiv 0 \pmod{p^r} \\ (x_0 y_2 - x_2 y_0) + (x_3 y_1 - x_1 y_3) \equiv 0 \pmod{p^r} \\ (x_0 y_3 - x_3 y_0) + (x_1 y_2 - x_2 y_1) \equiv 0 \pmod{p^r} \end{cases} \tag{3.11}$$

Theorem 3.27. *Let $m \mid \mathrm{N}(y)$, $y \in \mathcal{L}$ primitive modulo m, and $x \in \mathcal{L}$. The right divisors of y are right divisors of x if and only if, for each prime-power p^r that divides m, (3.10) holds together with (3.11$_\alpha$), where α, like Lemma 3.15, is such that $p \nmid y_0^2 + y_\alpha^2$. An analogous result holds for left divisors, with the $+$'s in (3.11) changed to $-$'s.*

Proof. Let $p^r \mid m$. From the proof of theorem 3.16 we know that $p \nmid y_0^2 + y_\alpha^2$, for some $\alpha = 1, 2$ or 3. We may assume that $\alpha = 1$. Since $p^r \mid \mathrm{N}(y)$, we can

verify that, modulo p^r the following equations hold

$$\begin{aligned}(-y_0y_2+y_1y_3)L(3.10)-(y_0y_3+y_1y_2)L(3.11_1)+(y_0^2+y_1^2)L(3.11_2)=0\\ -(y_0y_3+y_1y_2)L(3.10)+(y_0y_2-y_1y_3)L(3.11_1)+(y_0^2+y_1^2)L(3.11_3)=0.\end{aligned} \tag{3.12}$$

Where $L(*)$ is the left hand side of the congruence $*$. It is easy to see now that the congruences (3.12) yield that (3.10) together with (3.11_α) implies (3.11) for $\alpha = 1, 2$ or 3. □

Corollary 3.28. *Let x be pure and primitive modulo m, and $d^2+\mathrm{N}(x) \equiv 0 \equiv e^2+\mathrm{N}(x) \pmod m$, for some $d, e \in \mathbb{Z}$. Then $d+x$ and $e+x$ have the same right divisors of norm m if and only if $d \equiv e \pmod m$.*

Proof. ($\Rightarrow$) Assume $d+x$ and $e+x$ have the same right divisors of norm m. By Theorem 3.25, we have that $(d+x)(e+\bar{x}) \equiv 0 \pmod m$. Therefore $de+d\bar{x}+ex+\mathrm{N}(x) \equiv 0 \pmod m$. We also have that $\bar{x} = -x$, which together with $\mathrm{N}(x)+e^2 \equiv 0 \pmod m$, yields $de-dx+ex-e^2 \equiv 0 \pmod m$, which is equivalent to $(d-e)(e-x) \equiv 0 \pmod m$. Since x is primitive modulo m, $e-x$ is primitive mod m as well, and therefore we must have that $d \equiv e \pmod m$.

($\Leftarrow$) Assume that $d \equiv e \pmod m$. We need to show that $(d+x)(e+\bar{x}) \equiv 0 \pmod m$. We have $(d+x)(e+\bar{x}) \equiv de+ex-dx-e^2 \equiv (x-e)(e-d) \equiv 0 \pmod m$. □

Corollary 3.29. *Let x, y be pure and primitive modulo m, and assume that $d^2+\mathrm{N}(x) \equiv 0 \equiv d^2+\mathrm{N}(y) \pmod m$, for some $d \in \mathbb{Z}$. Then $d+x$ and $d+y$ have the same right divisors of norm m if and only if $x \equiv y \pmod m$.*

Proof. ($\Rightarrow$) Let $d+x$ and $d+y$ have the same right divisors of norm m. By Theorem 3.25, we have that $(d+x)(d+\bar{y}) \equiv 0 \pmod m$. Therefore $d^2+d(x+\bar{y})+x\bar{y} \equiv -\mathrm{N}(x)+d(x+\bar{y})+x\bar{y} \equiv 0 \pmod m$. We have that $\bar{y} = -y$, and from $\mathrm{N}(x)+d^2 \equiv 0 \pmod m$ and $\mathrm{N}(x) = -x^2$, we get $x^2+d(x-y)-xy \equiv 0 \pmod m$, and so $(d+x)(x-y) \equiv 0 \pmod m$. Since x is primitive mod m, $d+x$ is primitive mod m as well, and therefore we must have that $x \equiv y \pmod m$.

($\Leftarrow$) Let $x \equiv y \pmod{m}$. We need to show that $(d+x)(d+\bar{y}) \equiv 0 \pmod{m}$. We have $(d+x)(d+\bar{y}) \equiv d^2+d(x-y)-xy \equiv d^2-xy \equiv x^2-xy \equiv x(x-y) \equiv 0 \pmod{m}$. □

Corollary 3.30. *Let $x = x_1i + x_2j + x_3k$ be pure, $v = v_1i + v_2j + v_3k$ be pure and primitive modulo m, $m \mid \mathrm{N}(v)$, and $m \mid \sum_{i=1}^{3} x_iv_i$. Then there exists an integer x_0 such that $x_0 + x$ and v has the same right divisors of norm m.*

Proof. By Theorem 3.27, and the Chinese Remainder Theorem, it is enough, for every prime power p^r dividing m, to find an $x_0 \in \mathbb{Z}$ that satisfies one of the following congruences

$$\begin{cases} x_0v_1 + x_2v_3 - x_3v_2 & \equiv 0 \pmod{p^r} \\ x_0v_2 + x_3v_1 - x_1v_3 & \equiv 0 \pmod{p^r} \\ x_0v_3 + x_1v_2 - x_2v_1 & \equiv 0 \pmod{p^r}. \end{cases}$$

This always happens because v is primitive, and therefore $p \nmid v_\alpha$ for some $\alpha = 1, 2$ or 3. □

Corollary 3.31. *If $y \in \mathcal{L}$ is primitive modulo m, $m \mid \mathrm{N}(y)$, and $x \in \mathcal{L}$, then x has the right divisors of norm m of y, and the left divisors of norm m of y, if and only if $x \equiv ky \pmod{m}$ for some $k \in \mathbb{Z}$.*

Proof. Let $x = x_0 + x_1i + x_2j + x_3k$ and $y = y_0 + y_1i + y_2j + y_3k$. By Theorem 3.27 we get that x has the right divisors of norm m of y, and the left divisors of norm m of y, if and only if $x_fy_g \equiv x_gy_f \pmod{p^r}$, for all $f, g \in \{0, 1, 2, 3\}$ for every prime that divides m with multiplicity r. Since y is primitive modulo m, there exists $\alpha \in \{0, 1, 2, 3\}$ such that $p \nmid y_\alpha$. Then $x_g \equiv (x_\alpha/y_\alpha)y_g \pmod{p^r}$, for all $g \in \{0, 1, 2, 3\}$, and therefore $x \equiv (x_\alpha/y_\alpha)y \pmod{p^r}$. □

Corollary 3.32. *If $x, y \in \mathcal{L}$ are primitive modulo m, $m \mid \mathrm{N}(x), m \mid \mathrm{N}(y)$ and $m \mid \sum_{i=1}^{4} x_i y_i$, then there is a factorization $m = m_1 m_2$ such that*

$$\begin{aligned}(x_0y_1 - x_1y_0) &\equiv \pm(x_2y_3 - x_3y_2)\\ (x_0y_2 - x_2y_0) &\equiv \pm(x_3y_1 - x_1y_3)\\ (x_0y_3 - x_3y_0) &\equiv \pm(x_1y_2 - x_2y_1)\end{aligned}$$

with all the signs $\pm$ taken as $+$ for modulus m_1 and as $-$ for modulus m_2.

Proof. Direct consequence of Theorems 3.26 and 3.27. □

4

The 1-3-5 Conjecture and Related Problems

In this chapter, using quaternion arithmetic in the ring of Lipschitz integers, we present a proof of Zhi-Wei Sun's "1-3-5 conjecture" for all integers, and for all natural numbers greater than a specific constant. This, together with the computations in [12], which checked the validity of the conjecture up to that constant, completely proves the 1-3-5 conjecture. We also establish some variations of this conjecture. This whole chapter is essentially contained in [13].

Lagrange's four-square theorem states that any $m \in \mathbb{N} = \{0, 1, 2, \ldots\}$ can be written as the sum of four integer squares. In the paper [19, Conjecture 4.3], Zhi-Wei Sun made the following conjecture.

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

We present here a proof of that conjecture for all $m \in \mathbb{N}$ with $x, y, z, t \in \mathbb{Z}$, and a proof for all $m \not\equiv 0 \pmod{16}$ greater than a specific constant, with $x, y, z, t \in \mathbb{N}$. This, together with computations done by the authors and Rogério Reis in [12], which checked the validity of the conjecture up to that constant, completely proves the 1-3-5 conjecture. Moreover, we establish some general results that correspond to variations of this conjecture.

While the previous attempts to attack the conjecture used the theory of quadratic forms, we use the arithmetic of the ring of Lipschitz integers, $\mathcal{L}$

As we have seen in (2.15) and (2.20) Gordon Pall has proven in [15] that for a Lipschitz integer v which is primitive modulo m, where $m \mid N(v)$, m is odd and positive, there is a unique, up to left multiplication by units, right divisor of v of norm m. This also holds for even m, provided v is actually primitive and $\frac{\mathrm{N}(v)}{m}$ is odd.

For our purposes, uniqueness of factorization is not required. We only need existence, which means that we may drop the condition for a Lipschitz integer to be primitive, and we will still have a factorization modeled on any factorization of its norm, including even factors, because the only primes dividing 2 in $\mathcal{L}$ are, up to associates, $1+i$, $1+j$, and $1+k$, and $(1+i)(a+bi+cj+dk) = (a+bi-dj+ck)(1+i)$, with similar relations holding for $1+j$ and $1+k$. Moreover, by Jacobi's 4-square theorem, factors of powers of 2 are reduced to the factorization of 2 and $\pm 1 \pm i \pm j \pm k$, which can easily be checked to be, up to associates, products of two of the numbers $1+i$, $1+j$, or $1+k$.

4.1 The general setting

Let $a, b, c, d \in \mathbb{Z}$, and $m, n \in \mathbb{N}$ be given. Let us start by describing conditions under which one can guarantee the existence of $x, y, z, t \in \mathbb{Z}$ such that

$$\begin{cases} x^2+y^2+z^2+t^2 &= m \\ ax+by+cz+dt &= n^2. \end{cases} \tag{4.1}$$

Putting $\gamma = x+yi+zj+tk, \zeta = a+bi+cj+dk \in \mathcal{L}$, these equations are equivalent to

$$\mathrm{N}(\gamma) = m \tag{4.2}$$

$$\gamma \cdot \zeta = \Re(\bar{\gamma}\zeta) = n^2, \tag{4.3}$$

where the dot denotes here the usual inner product on $\mathbb{R}^4$. If one sets $\delta = \bar{\gamma}\zeta$, it follows from (4.3) that $\delta = n^2 + Ai + Bj + Ck$, for some $A, B, C \in \mathbb{Z}$, and $m\,\mathrm{N}(\zeta) - n^4 = A^2 + B^2 + C^2$. By Legendre's three-square theorem, see [9,

pp. 293–295], or for more recent proofs see [21] and [1], a necessary condition for the solvability of (4.1) is that one has

$$n \leq \sqrt[4]{m\ \mathrm{N}(\zeta)}, \tag{4.4}$$

and that

$$m\ \mathrm{N}(\zeta) - n^4 \text{ is not of the form } 4^r(8s+7) \text{ for any } r, s \in \mathbb{N}. \tag{4.5}$$

Assume now, conversely, that conditions (4.4) and (4.5) are satisfied. Then, again by Legendre's three-square theorem, there exist $A, B, C \in \mathbb{Z}$ such that $m\ \mathrm{N}(\zeta) - n^4 = A^2 + B^2 + C^2$. Setting $\delta = n^2 + Ai + Bj + Ck$, one has $\mathrm{N}(\delta) = m\ \mathrm{N}(\zeta)$. It then follows, by the existence of factorizations modeled on factorizations of the norm in the ring of Lipschitz integers, that there exists $\xi, \gamma \in \mathcal{L}$ such that $\delta = \bar{\gamma}\xi$ and $\mathrm{N}(\xi) = \mathrm{N}(\zeta)$, $\mathrm{N}(\gamma) = m$. It follows that γ is a solution of

$$\begin{aligned} \mathrm{N}(\gamma) &= m & (4.6)\\ \gamma \cdot \xi = \Re(\bar{\gamma}\xi) &= n^2. & (4.7) \end{aligned}$$

This proves the following.

Theorem 4.1. *Let $m, n, \ell \in \mathbb{N}$ be such that $n \leq \sqrt[4]{m\ell}$, and assume that $m\ell - n^4$ is not of the form $4^r(8s+7)$ for any $r, s \in \mathbb{N}$. Then, for some $a, b, c, d \in \mathbb{N}$ such that $\mathrm{N}(a + bi + cj + dk) = \ell$, the system*

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

has integer solutions.

Proof. This follows from all that was written above, together with the fact that one can change the signs of x, y, z, t so as to make a, b, c, d non-negative, if they are not already so. □

A direct consequence of Theorem 4.1 is the following.

Theorem 4.2. *Let $\zeta \in \mathcal{L}$ and $m, n \in \mathbb{N}$ be such that $\mathrm{N}(\zeta)m - n^4$ is non-negative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. If $\zeta = a + bi + cj + dk \in \mathcal{L}$, then the system*

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

has integer solutions whenever

$$\mathrm{N}(\zeta) = \begin{cases} 1, 3, 5, 7, 11, 15, 23 \\ 2^g \\ 3 \cdot 2^g \\ 7 \cdot 2^g \end{cases}$$

where g is odd and positive.

Proof. Let $\ell \in \mathbb{N}$, define the *partition number* $P_4(\ell)$ of ℓ into 4 squares to be

$$P_4(\ell) = \left| \{a_1, a_2, a_3, a_4\} \in \mathbb{N}^4 \mid a_1 \geqslant a_2 \geqslant a_3 \geqslant a_4, \sum_{i=1}^{4} a_i^2 = \ell \right|$$

By Theorem 4.1, it suffices to guarantee that $P_4(\mathrm{N}(\zeta)) = 1$, for all $\zeta \in \mathcal{L}$, with $\mathrm{N}(\zeta)$ running through all the values in the statement, which is true by [11, Theorem 1]. □

4.2 The 1-3-5 conjecture

Let us now consider the existence of integer solutions for the system:

$$\begin{cases} m &= x^2 + y^2 + z^2 + t^2 \\ n^2 &= x + 3y + 5z. \end{cases} \tag{1-3-5}$$

Since the only possible Lipschitz integers of norm 35, up to the signs and the order of the coefficients, are $1+3i+5j$ and $1+3i+3j+4k$, Theorem 4.1 immediately yields the following result.

Proposition 4.3. *Let $n \leq \sqrt[4]{35\,m}$ be such that $35m - n^4$ is not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. Then either the system (1-3-5) has integer solutions, or the system*

$$\begin{cases} m &= x^2+y^2+z^2+t^2 \\ n^2 &= x+3y+3z+4t. \end{cases} \tag{1-3-3-4}$$

has integer solutions.

Define $\mathcal{R}(P)$ to be the set of all Lipschitz integers obtained from $P \in \mathcal{L}$, by permuting and changing the signs of its coordinates. For $\alpha, \alpha' \in \mathcal{L}$, we say that α' is in the same *decomposition class* as α, and write $\alpha' \sim \alpha$, if $\mathcal{R}(\alpha') = \mathcal{R}(\alpha)$.

From now on, we set $\alpha = 1+3i+5j$ and $\beta = 1+3i+3j+4k$. In sections $4, 5, 6$ and 7 we will prove that the system (1-3-5) always has a solution for all $m \in \mathbb{N}$ with $x, y, z, t \in \mathbb{Z}$. The natural solution case will be handled in the last section. The biggest part of this paper will be focused on proving the following theorem.

Theorem 4.4. *Let $m, n \in \mathbb{N}$ be such that $35m - n^4$ is non-negative 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 the system (1-3-5) has integer solutions whenever $n \not\equiv 0 \pmod 3$ and $n \not\equiv 0 \pmod 5$, i.e. $(n, 15) = 1$.

ii) If $m \equiv 1 \pmod 3$, then the system (1-3-5) has integer solutions whenever $n \equiv 0 \pmod 3$ such that $n \not\equiv 0 \pmod 5$.

iii) If $m \equiv -1 \pmod 3$, then the system (1-3-5) has integer solutions whenever $n \not\equiv 0 \pmod 3$, $n \not\equiv 0 \pmod 5$ and $n \not\equiv 0 \pmod 7$, i.e. $(n, 105) = 1$.

Since the condition "$35m - n^4$ is not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$" holds often enough, this theorem shows more than what the integer case of the 1-3-5 conjecture asserts. As it is suggested from the statement of the theorem, we need to work modulo $3, 5$ and 7.

Let us now establish the framework within which we are going to work. We assume that $m, n \in \mathbb{N}$ are such that $35m - n^4$ is non-negative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. Like in the first section, this implies that there exist $A, B, C \in \mathbb{N}$ such that $35m - n^4 = A^2 + B^2 + C^2$. Letting $\delta = n^2 + Ai + Bj + Ck \in \mathcal{L}$, we have that $\mathrm{N}(\delta) = 35m$, and therefore there exist $\zeta, \gamma \in \mathcal{L}$ with $\mathrm{N}(\zeta) = 35$ and $\mathrm{N}(\gamma) = m$, such that $\delta = \gamma\zeta$. Then $\mathrm{N}(\zeta) = 35$, and so $\zeta \sim \beta$ or $\zeta \sim \alpha$.

If $\zeta \in \mathcal{R}(\alpha)$ then the system (1-3-5) has integer solutions and we are done. If $\zeta \in \mathcal{R}(\beta)$, then there exist a γ', obtained from appropriate sign and coefficient changes of γ, with $\mathrm{N}(\gamma') = \mathrm{N}(\gamma) = m$, such that $\Re(\gamma'\beta) = \Re(\gamma\zeta) = n^2$. Therefore, we may assume, without loss of generality, that $\zeta = \beta$. Let $\gamma = x - yi - zj - tk$. Performing the multiplication $\gamma\beta$ yields

$$\delta = (x+3y+3z+4t)+(3x-y-4z+3t)i+(3x+4y-z-3t)j+(4x-3y+3z-t)k,$$

so we have, for future reference:

$$\begin{cases} n^2 &= x + 3y + 3z + 4t \\ A &= 3x - y - 4z + 3t \\ B &= 3x + 4y - z - 3t \\ C &= 4x - 3y + 3z - t. \end{cases} \tag{4.8}$$

We now point out the main idea behind what is going to be done in the next sections.

Remark 4.1. *For any $\rho \in \mathcal{L}\backslash\{0\}$, one has $\Re(\rho^{-1}\delta\rho) = \Re(\delta)$ and $\mathrm{N}(\rho^{-1}\gamma\rho) = \mathrm{N}(\gamma)$. Since, for any $\sigma \in \mathcal{L} \setminus \{0\}$,*

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

we see that if one can find $\rho, \sigma \in \mathcal{L}\backslash\{0\}$ such that $\sigma^{-1}\beta\rho = \alpha'$ and $\rho^{-1}\gamma\sigma \in \mathcal{L}$, with $\alpha' \in \mathcal{R}(\alpha)$ and $\mathrm{N}(\rho) = \mathrm{N}(\sigma)$, then from a solution $(x, y, z, t) \in \mathbb{Z}^4$ for (1-3-3-4) one can obtain a solution in $\mathbb{Z}^4$ for (1-3-5).

We will be using this in the case where $\mathrm{N}(\rho) = \mathrm{N}(\sigma) = p$, an odd prime, and in order to apply this remark, we will need conditions on γ that guarantee $\rho^{-1}\gamma\sigma \in \mathcal{L}$, which is the same as $\bar{\rho}\gamma\sigma \equiv 0 \pmod{p}$. Those conditions can be obtained by using Corollary 8 in [15], which will be here applied in the following way. Since $\bar{\rho}\gamma\sigma$ and $\bar{\rho}\sigma$ have the same right and left divisors of norm p, **when $\bar{\rho}\sigma$ is primitive modulo** p, Pall's result implies that there is a $k_\gamma \in \mathbb{Z}$ such that $\bar{\rho}\gamma\sigma \equiv k_\gamma\bar{\rho}\sigma \pmod{p}$. But then, taking the conjugate congruence, adding both, and using the fact that $\Re(rs) = \Re(sr)$ for all $r, s \in \mathcal{L}$, one gets

$$\gamma \cdot \rho\bar{\sigma} \equiv k_\gamma\, \rho \cdot \sigma \pmod{p}.$$

When $\rho \cdot \sigma \not\equiv 0 \pmod{p}$, which is the same as $p \nmid \Re(\bar{\rho}\sigma)$, then one has $k_\gamma \equiv \frac{\gamma\cdot\rho\bar{\sigma}}{\rho\cdot\sigma} \pmod{p}$, and one concludes that

$$\bar{\rho}\gamma\sigma \equiv \frac{1}{\rho \cdot \sigma}\,(\gamma \cdot \rho\bar{\sigma})\,\bar{\rho}\sigma \pmod{p}, \text{ for all } \gamma \in \mathcal{L}. \tag{4.9}$$

If $\rho \cdot \sigma \equiv 0 \pmod{p}$, then $\gamma \cdot \rho\bar{\sigma} \equiv 0 \pmod{p}$ for all $\gamma \in \mathcal{L}$, and in particular $\rho\bar{\sigma} \equiv 0 \pmod{p}$. Hence $\sigma = u\rho$, for some $u \in \mathcal{L}^*$. Before dealing with this possibility, consider the case **when $\bar{\rho}\sigma$ is not primitive modulo** p. This means that σ is a right associate of ρ, and so we can assume, without loss of generality, that $\sigma = \rho$. Using coordinates, we can explicitly see that, also in this case, $\bar{\rho}\gamma\rho$ has proportional coordinates modulo p, and thus, as above, there are $\varepsilon, \delta \in \mathcal{L}$ such that $\bar{\rho}\gamma\rho \equiv (\gamma \cdot \varepsilon)\,\delta \pmod{p}$, for all $\gamma \in \mathcal{L}$. If $\rho = a + bi + cj + dk$, with $c^2 + d^2 \neq 0$, it can be seen that one can take

$\delta = (a^2 + b^2)i + (bc - ad)j + (ac + bd)k$, and ε can then be easily computed for any given ρ. Finally, if $\rho = a + bi$, with $b \neq 0$, one can take $\delta = 2aj - 2bk$ and $\varepsilon = aj + bk$.

Finally, for the case $\sigma = u\rho$, with $u \in \mathcal{L}^*$, one applies what we just saw to γu, to obtain ε, δ such that $\bar{\rho}\gamma\sigma = \bar{\rho}\gamma u\rho \equiv (\gamma u \cdot \varepsilon)\,\delta \equiv (\gamma \cdot \varepsilon\bar{u})\,\delta \pmod{p}$.

Thus, the following holds:

Proposition 4.5. *Let p be an odd rational prime. Given $\rho, \sigma \in \mathcal{L}$ with norm p, then there are $\varepsilon, \delta \in \mathcal{L}$ such that $\bar{\rho}\gamma\sigma \equiv (\gamma \cdot \varepsilon)\,\delta \pmod{p}$, for all $\gamma \in \mathcal{L}$. Moreover, for any ρ, σ, one can easily compute ε, which then yields the following criterion:*

$$\rho^{-1}\gamma\sigma \in \mathcal{L} \iff \gamma \cdot \varepsilon \equiv 0 \pmod{p}.$$

From now on, we assume that $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ is a solution of the system (1-3-3-4), we set $\gamma_0 = x_0 - y_0 i - z_0 j - t_0 k$, and we are going to show that from this solution one can construct a solution for the (1-3-5) system, by using Remark 4.1 and Proposition 4.5.

4.3 Using primes in $\mathcal{L}$ with norm 3

Let $\rho = 1 + i - j$. One can easily check that

$$\beta\rho = \sigma\alpha', \tag{4.10}$$

where $\sigma = 1 + i + j$, $\alpha' = 5 + 3i + j \in \mathcal{R}(\alpha)$, and that

$$\rho^{-1}\gamma_0\,\sigma \in \mathcal{L} \iff x_0 - z_0 - t_0 \equiv 0 \pmod{3}.$$

Thus, since $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ is a solution of (1-3-3-4), it follows by Remark 4.1 that when this congruence holds, $\rho^{-1}\gamma_0\,\sigma$ yields a solution of (1-3-5).

Now, there are 4 right non-associated primes above 3, and for the ones other than $\rho_1 = 1 + i - j$, multiplying by β on the left yields:

$$\beta(1 - i - j) = (1 + j + k)(3 - 5j + k) \tag{4.11}$$

$$\beta(1 + i + j) = (1 - j + k)(-3 + 4i + j + 3k) \tag{4.12}$$

$$\beta(1 - i + j) = (1 + i + k)(3 - i + 4j + 3k). \tag{4.13}$$

Using (4.11) instead of (4.10), and repeating the same argument, we get that, if $x_0 - y_0 - t_0 \equiv 0 \pmod 3$, then the system (1-3-5) has an integer solution; using (4.12) for $x_0 + y_0 - t_0 \equiv 0 \pmod 3$, one obtains yet another integer solution for the system (1-3-3-4); and using (4.13) for $x_0 + z_0 - t_0 \equiv 0 \pmod 3$, one gets again another integer solution for the system (1-3-3-4). In the last two cases we obtain no direct information for the solvability of the system (1-3-5), but the extra solutions we get, using (4.12) and (4.13), for the system (1-3-3-4) are going to prove instrumental for our proof. Later on we will need to write these extra solutions in terms of x_0, y_0, z_0, t_0. For now, we note that the above discussion has proved the following.

Proposition 4.6. *Let $m, n \in \mathbb{N}$ be such that $35m - n^4$ is non-negative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. For a solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ of the system (1-3-3-4), if either of the following holds:*

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

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

then the system (1-3-5) has an integer solution.

4.4 Using primes in $\mathcal{L}$ with norm 5

Much like as we did in the previous section, where we used the primes above 3 to see that a solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ for the system (1-3-3-4) either yields conditions for the solvability of the system (1-3-5), or another solution of the system (1-3-3-4), here we will use the primes above 5 to do something

analogous, and we will actually calculate the new solutions for the system (1-3-3-4), since we will need to use those explicit expressions.

Taking representatives of all the six primes of norm 5, up to right associates, and multiplying by β on the left, we get

$$\begin{aligned}
\beta(1+2i) &= (j-2k)(3-4i+3j-k)\\
\beta(1+2j) &= (2+i)(-3-i+4j+3k)\\
\beta(1-2k) &= (1-2i)(3+3i+j+4k)\\
\beta(1-2i) &= (2+i)(3-i+5k)\\
\beta(1-2j) &= (-1+2i)(3-5i-j)\\
\beta(1+2k) &= (j-2k)(-3+5j-k).
\end{aligned}$$

For $\delta = \gamma_0\beta$, we then see that

$$\begin{aligned}
(1+2i)^{-1}\delta(1+2i) &= [(1+2i)^{-1}\gamma_0(j-2k)](3-4i+3j-k)\\
(1+2j)^{-1}\delta(1+2j) &= [(1+2j)^{-1}\gamma_0(2+i)](-3-i+4j+3k)\\
(1-2k)^{-1}\delta(1-2k) &= [(1-2k)^{-1}\gamma_0(1-2i)](3+3i+j+4k)\\
(1-2i)^{-1}\delta(1-2i) &= [(1-2i)^{-1}\gamma_0(2+i)](3-i+5k)\\
(1-2j)^{-1}\delta(1-2j) &= [(1-2j)^{-1}\gamma_0(-1+2i)](3-5i-j)\\
(1+2k)^{-1}\delta(1+2k) &= [(1+2k)^{-1}\gamma_0(j-2k)](-3+5j-k).
\end{aligned} \tag{4.14}$$

Denoting the expressions in the brackets by γ_i, $i = 1,\ldots,6$, respectively, one sees that if any of $\gamma_4, \gamma_5, \gamma_6$ is in $\mathcal{L}$, then the system (1-3-5) would have integer solutions by Remark 4.1, and we are done. One has, using (4.8) and Proposition 4.5,

$$\begin{aligned}
&\gamma_4 \in \mathcal{L} \iff t_0 \equiv 3z_0 \pmod 5 \iff n^2 \equiv 2A \pmod 5\\
&\gamma_5 \in \mathcal{L} \iff x_0 - 2y_0 + 2z_0 + t_0 \equiv 0 \pmod 5 \iff A \equiv 0 \pmod 5\\
&\gamma_6 \in \mathcal{L} \iff x_0 - 2y_0 + z_0 - 2t_0 \equiv 0 \pmod 5 \iff n^2 \equiv -A \pmod 5.
\end{aligned}$$

Therefore, we just proved the following.

Proposition 4.7. *Let $m, n \in \mathbb{N}$ be such that $35m - n^4$ is non-negative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. If $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ is a solution of the system (1-3-3-4), and $A = 3x_0 - y_0 - 4z_0 + 3t_0$ satisfies any one of the following congruences:*

(i) $A \equiv 0 \pmod 5$,

(ii) $n^2 \equiv 2A \pmod 5$,

(iii) $n^2 \equiv -A \pmod 5$,

then the system (1-3-5) has an integer solution.

We notice that if (x_0, y_0, z_0, t_0) is a solution of the system (1-3-3-4), then (x_0, z_0, y_0, t_0) is a solution of it as well. Therefore we also have:

Corollary 4.8. *Let $m, n \in \mathbb{N}$ be such that $35m - n^4$ is non-negative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. If $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ is a solution of the system (1-3-3-4) such that any of the following congruences hold:*

(i) $t_0 \equiv 3y_0 \pmod 5$,

(ii) $x_0 + 2y_0 - 2z_0 + t_0 \equiv 0 \pmod 5$,

(iii) $x_0 + y_0 - 2z_0 - 2t_0 \equiv 0 \pmod 5$,

then the system (1-3-5) has an integer solution.

Let us look at $\gamma_1, \gamma_2, \gamma_3$ now. Using once more (4.8) and Proposition 4.5, one gets:

$$\begin{aligned}
\gamma_1 \in \mathcal{L} &\iff y_0 \equiv 3x_0 \pmod 5 \iff n^2 \equiv -2A \pmod 5 \\
\gamma_2 \in \mathcal{L} &\iff x_0 - 2y_0 - 2z_0 - t_0 \equiv 0 \pmod 5 \iff n^2 \equiv 0 \pmod 5 \\
\gamma_3 \in \mathcal{L} &\iff x_0 - 2y_0 - z_0 + 2t_0 \equiv 0 \pmod 5 \iff n^2 \equiv A \pmod 5.
\end{aligned}$$

Note that for $n^2 \not\equiv 0 \pmod 5$, either $n^2 \equiv \pm A \pmod 5$, $n^2 \equiv \pm 2A \pmod 5$ or $A \equiv 0 \pmod 5$. We have seen what happens if $n^2 \equiv -A \pmod 5$, $n^2 \equiv 2A \pmod 5$ and $A \equiv 0 \pmod 5$, hence we just need to see what happens on the other two remaining cases:

- If $n^2 \equiv A \pmod 5$, then $x_0 - 2y_0 - z_0 + 2t_0 \equiv 0 \pmod 5$, so $\gamma_3 \in \mathcal{L}$. Since

$$\gamma_3 = \tfrac{x_0-2y_0+4z_0+2t_0}{5} - \tfrac{2x_0+y_0-2z_0+4t_0}{5}i - \tfrac{4x_0+2y_0+z_0-2t_0}{5}j + \tfrac{2x_0-4y_0-2z_0-t_0}{5}k,$$

and, according to (4.14), γ_3 yields the element $\beta^* = 3 + 3i + j + 4k \in \mathcal{R}(\beta)$, it follows that

$$\gamma^* = \tfrac{4x_0+2y_0+z_0-2t_0}{5} - \tfrac{2x_0+y_0-2z_0+4t_0}{5}i - \tfrac{x_0-2y_0+4z_0+2t_0}{5}j + \tfrac{2x_0-4y_0-2z_0-t_0}{5}k$$

satisfies $\Re(\gamma^*\beta) = \Re(\gamma_3\beta^*) = \Re(\gamma_0\beta)$, and thus γ^* yields a solution of (1-3-3-4).

If we denote the coordinates of the conjugate of γ^* by x_1, y_1, z_1, t_1, using the fact that $x_0 - 2y_0 - z_0 + 2t_0 = 5\kappa$, for some $\kappa \in \mathbb{Z}$, we have

$$\begin{cases} x_1 &= x_0 - \kappa \\ y_1 &= y_0 + 2\kappa \\ z_1 &= z_0 + \kappa \\ t_1 &= t_0 - 2\kappa. \end{cases} \tag{4.15}$$

- If $n^2 \equiv -2A \pmod 5$, then $y_0 \equiv 3x_0 \pmod 5$, and so $\gamma_1 \in \mathcal{L}$. One then sees, as above, that

$$\Re\left[\left(\frac{-4x_0+3y_0}{5} - \frac{3x_0+4y_0}{5}i - z_0j - t_0k\right)\beta\right] = \Re(\gamma\beta),$$

and therefore

$$(x_2, y_2, z_2, t_2) = \left(\frac{-4x_0+3y_0}{5}, \frac{3x_0+4y_0}{5}, z_0, t_0\right)$$

is another integer solution of the system (1-3-3-4) obtained from the solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$. We have $y_0 = 3x_0 + 5\lambda$, for some $\lambda \in \mathbb{Z}$,

and thus

$$\begin{cases} x_2 &= x_0 + 3\lambda \\ y_2 &= y_0 - \lambda \\ z_2 &= z_0 \\ t_2 &= t_0. \end{cases} \tag{4.16}$$

is another integer solution of (1-3-3-4).

Now we are ready to prove the following:

Proposition 4.9. *Let $m, n \in \mathbb{N}$ be such that $35m - n^4$ is non-negative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. The following holds:*

i) If $m \equiv 0 \pmod 3$, then the system (1-3-5) has integer solutions for all $n \in \mathbb{N}$ with $(n, 15) = 1$.

ii) If $m \equiv 1 \pmod 3$, then the system (1-3-5) has integer solutions for all $n \equiv 0 \pmod 3$ with $5 \nmid n$.

Proof. As above, we may assume the existence of a solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ of the system (1-3-3-4). Note that if $m \equiv 0 \pmod 3$ and $n^2 \equiv 1 \pmod 3$, or if $m \equiv 1 \pmod 3$ and $n^2 \equiv 0 \pmod 3$, then $35m - n^4 \equiv -1 \pmod 3$. Therefore $A^2 + B^2 + C^2 \equiv -1 \pmod 3$, and since the squares modulo 3 are 0 and 1, we have that exactly one of the A, B, C is 0 modulo 3, and the other two are ± 1 modulo 3. From (4.8) and for a solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ of (1-3-3-4), we see that

$$\begin{cases} n^2 &\equiv x_0 + t_0 \pmod 3 \\ A &\equiv -y_0 - z_0 \pmod 3 \\ B &\equiv y_0 - z_0 \pmod 3 \\ C &\equiv x_0 - t_0 \pmod 3. \end{cases}$$

We now consider all possibilities for the congruence classes of A, B, C modulo 3. In each one of the following cases, one sees that one can use Proposition 4.6 to show that the system (1-3-5) has integer solutions:

- If $A \equiv 0 \pmod 3$ and $B \equiv C \pmod 3$, then it is easy to see that $x_0 + 2z_0 + 2t_0 \equiv 0 \pmod 3$.

- If $A \equiv 0 \pmod 3$ and $B \equiv -C \pmod 3$, then $x_0 + 2y_0 + 2t_0 \equiv 0 \pmod 3$.

- If $C \equiv 0 \pmod 3$ and $A \equiv B \pmod 3$, then $x_0 + 2y_0 + 2t_0 \equiv 0 \pmod 3$.

- If $C \equiv 0 \pmod 3$ and $A \equiv -B \pmod 3$, then $x_0 + 2z_0 + 2t_0 \equiv 0 \pmod 3$.

- If $B \equiv 0 \pmod 3$ and $A \equiv C \pmod 3$, then $x_0 + 2y_0 + 2t_0 \equiv 0 \pmod 3$.

There is only one remaining case:

- If $B \equiv 0 \pmod 3$ and $A \equiv -C \pmod 3$, then we have that $x_0 + y_0 + 2t_0 \equiv x_0 + z_0 + 2t_0 \equiv 0 \pmod 3$. Proposition 4.6 does not yield the claim this time. Instead, we are going to use the results from the previous section. For $n^2 \not\equiv 0 \pmod 5$, we have the following cases:

  - If we have that $A \equiv 0 \pmod 5$ or $n^2 \equiv 2A \pmod 5$ or $n^2 \equiv -A \pmod 5$, by Proposition 4.7, the system (1-3-5) has integer solutions.

  - If $n^2 \equiv A \pmod 5$ then the solution (4.15) of the system (1-3-3-4) satisfies $x_1 + 2y_1 + 2t_1 \equiv 2(x_0 + z_0 + 2t_0) \equiv 0 \pmod 3$. Therefore, Proposition 4.6 yields the claim.

  - If $n^2 \equiv -2A \pmod 5$, then the solution (4.16) of the system (1-3-3-4) satisfies $x_2 + 2y_2 + 2t_2 \equiv x_0 + y_0 + 2t_0 \equiv 0 \pmod 3$. Therefore, Proposition 4.6 yields the claim again.

□

The case $m \equiv -1 \pmod 3$ of (4.4) is the only one left to be treated. For that case, similarly to the above, we can show the following:

Proposition 4.10. *Let $m, n \in \mathbb{N}$, $m \equiv -1 \pmod 3$, $n \not\equiv 0 \pmod 3$, be such that $35m - n^4$ is non-negative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. Then, either the system (1-3-5) has integer solutions, or if $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ is a solution of the system (1-3-3-4), we must have either $x_0 + y_0 + 2t_0 \equiv 0 \pmod 3$ and $z_0 \equiv 0 \pmod 3$, or $x_0 + z_0 + 2t_0 \equiv 0 \pmod 3$ and $y_0 \equiv 0 \pmod 3$.*

Proof. Let $m \equiv -1 \pmod 3$ and $n \not\equiv 0 \pmod 3$, which means that $n^2 \equiv 1 \pmod 3$, then $35m - n^4 \equiv 0 \pmod 3$, so that $A^2 + B^2 + C^2 \equiv 0 \pmod 3$. Therefore $A^2 \equiv B^2 \equiv C^2 \not\equiv 2 \pmod 3$, and

- If $A \equiv B \equiv C \pmod 3$, then $x_0 + z_0 + 2t_0 \equiv 0 \pmod 3$ and $y_0 \equiv 0 \pmod 3$.
- If $A \equiv -B \equiv -C \pmod 3$, then $x_0 + 2y_0 + 2t_0 \equiv 0 \pmod 3$, and Proposition 4.6 applies.
- If $A \equiv B \equiv -C \pmod 3$, then $x_0 + 2z_0 + 2t_0 \equiv 0 \pmod 3$, and again Proposition 4.6 applies.
- If $A \equiv -B \equiv C \pmod 3$, then $x_0 + y_0 + 2t_0 \equiv 0 \pmod 3$ and $z_0 \equiv 0 \pmod 3$.

□

In order to complete the proof of the case $m \equiv -1 \pmod 3$ of Theorem 4.4, we need to work modulo 7 as well, since the above methods are not enough to cover every possibility.

4.5 Using primes in $\mathcal{L}$ with norm 7

Let $\rho_1 = 1+i+j+2k$, $\rho_2 = 1-i-j-2k$, $\rho_3 = 1-i+j-2k$, $\rho_4 = 1+i-j+2k$, $\rho_5 = 1+i+j-2k$, $\rho_6 = 1-i-j+2k$, $\rho_7 = 1+i-j-2k$, and , $\rho_8 = 1-i+j+2k$ be representatives of all the 8 right non-associate primes of norm 7. Multiplying

them all by β on the left, as we did before for the primes of norm 3 or 5, we get:

$$\begin{aligned}
\beta\rho_1 &= (1-i+2j-k)(-3-3i+4j+k)\\
\beta\rho_2 &= (1-i+2j-k)(3+i-4j+3k)\\
\beta\rho_3 &= (2-i-j+k)(4+i+3j+3k)\\
\beta\rho_4 &= (1+i-j-2k)(1+3i+3j-4k)\\
\beta\rho_5 &= (-2+i+j-k)(-i-5j-3k)\\
\beta\rho_6 &= (-1-2i-j-k)(-3+j-5k)\\
\beta\rho_7 &= (-2+i+j-k)(-3i-5j+k)\\
\beta\rho_8 &= (1+i-j-2k)(-3+5i+j).
\end{aligned}$$

Denoting by σ_i the corresponding prime above 7 that shows up on the right side, and setting $\hat{\gamma}_i = \rho_i^{-1}\gamma_0\sigma_i$, one has

$$\begin{aligned}
\rho_1^{-1}\gamma_0\beta\rho_1 &= \hat{\gamma}_1\,(-3-3i+4j+k)\\
\rho_2^{-1}\gamma_0\beta\rho_2 &= \hat{\gamma}_2\,(3+i-4j+3k)\\
\rho_3^{-1}\gamma_0\beta\rho_3 &= \hat{\gamma}_3\,(4+i+3j+3k)\\
\rho_4^{-1}\gamma_0\beta\rho_4 &= \hat{\gamma}_4\,(1+3i+3j-4k)\\
\rho_5^{-1}\gamma_0\beta\rho_5 &= \hat{\gamma}_5\,(-i-5j-3k)\\
\rho_6^{-1}\gamma_0\beta\rho_6 &= \hat{\gamma}_6\,(-3+j-5k)\\
\rho_7^{-1}\gamma_0\beta\rho_7 &= \hat{\gamma}_7\,(-3i-5j+k)\\
\rho_8^{-1}\gamma_0\beta\rho_8 &= \hat{\gamma}_8\,(-3+5i+j).
\end{aligned} \tag{4.17}$$

If any of the $\hat{\gamma}_i$ for $i = 5, 6, 7, 8$ is in $\mathcal{L}$, then the system (1-3-5) would have integer solutions, and we are done. Using (4.8) and Proposition 4.5, one deduces

$$\begin{aligned}
\hat{\gamma}_5 \in \mathcal{L} &\iff x_0+2y_0+z_0+t_0 \equiv 0 \pmod 7 \iff A \equiv 0 \pmod 7\\
\hat{\gamma}_6 \in \mathcal{L} &\iff x_0-2y_0+3t_0 \equiv 0 \pmod 7 \iff n^2 \equiv A \pmod 7\\
\hat{\gamma}_7 \in \mathcal{L} &\iff y_0+2z_0+3t_0 \equiv 0 \pmod 7 \iff n^2 \equiv -2A \pmod 7\\
\hat{\gamma}_8 \in \mathcal{L} &\iff x_0+y_0-z_0-2t_0 \equiv 0 \pmod 7 \iff n^2 \equiv -4A \pmod 7.
\end{aligned}$$

Therefore, we have proved the following.

Proposition 4.11. *Let $m, n \in \mathbb{N}$ be such that $35m - n^4$ is non-negative and not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. If $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ is a solution of the system (1-3-3-4), and if any of the following holds:*

(i) $A \equiv 0 \pmod 7$

(ii) $n^2 \equiv A \pmod 7$

(iii) $n^2 \equiv -2A \pmod 7$

(iii) $n^2 \equiv -4A \pmod 7$

then the system (1-3-5) has an integer solution.

Now, let us look at $\hat{\gamma}_i$, for $i = 1, 2, 3, 4$. Applying once more (4.8) and Proposition 4.5, one has:

$$\begin{aligned}
\hat{\gamma}_1 \in \mathcal{L} &\iff x_0 + 4z_0 + 2t_0 \equiv 0 \pmod 7 \iff n^2 \equiv 4A \pmod 7 \\
\hat{\gamma}_2 \in \mathcal{L} &\iff x_0 - y_0 + 2z_0 - t_0 \equiv 0 \pmod 7 \iff n^2 \equiv 2A \pmod 7 \\
\hat{\gamma}_3 \in \mathcal{L} &\iff x_0 + 4y_0 - 2z_0 \equiv 0 \pmod 7 \iff n^2 \equiv -A \pmod 7 \\
\hat{\gamma}_4 \in \mathcal{L} &\iff x_0 + 3y_0 + 3z_0 + 4t_0 \equiv 0 \pmod 7 \iff n^2 \equiv 0 \pmod 7.
\end{aligned}$$

If any of the $\hat{\gamma}_i$ for $i = 1, 2, 3, 4$ is in $\mathcal{L}$, then we will have another solution for the system (1-3-3-4). We do not care for $\hat{\gamma}_4$, as the statement of Theorem 4.4 suggests, and we will examine each of the cases $\hat{\gamma}_1, \hat{\gamma}_2, \hat{\gamma}_3 \in \mathcal{L}$ separately. Note that if $n \not\equiv 0 \pmod 7$, then we have either $n^2 \equiv \pm A \pmod 7$, $n^2 \equiv \pm 2A \pmod 7$, $n^2 \equiv \pm 4A \pmod 7$, or $A \equiv 0 \pmod 7$.

- If $\hat{\gamma}_1 \in \mathcal{L}$, then $n^2 \equiv 4A \pmod 7$ and $x_0 + 4z_0 + 2t_0 \equiv 0 \pmod 7$, which means that $x_0 + 4z_0 + 2t_0 = 7\mu$, for some $\mu \in \mathbb{Z}$. Looking at the coordinates of $\hat{\gamma}_1$, rearranging them and changing signs accordingly, one sees that for

$$\gamma_1^* = \frac{6x_0 + 3z_0 - 2t_0}{7} - \frac{3x_0 - 2z_0 + 6t_0}{7} i - y_0 j + \frac{2x_0 - 6z_0 - 3t_0}{7} k$$

one has $\Re(\gamma_1^*\beta) = \Re(\gamma\beta)$, and hence

$$(\hat{x}_1, \hat{y}_1, \hat{z}_1, \hat{t}_1) = \left(\frac{6x_0 + 3z_0 - 2t_0}{7}, \frac{3x_0 - 2z_0 + 6t_0}{7}, y_0, \frac{-2x_0 + 6z_0 + 3t_0}{7}\right)$$

is another integer solution of the system (1-3-3-4), which we can write as:

$$\begin{cases} \hat{x}_1 &= x_0 + z_0 - \mu \\ \hat{y}_1 &= -2z_0 + 3\mu \\ \hat{z}_1 &= y_0 \\ \hat{t}_1 &= 2z_0 + t_0 - 2\mu. \end{cases} \tag{4.18}$$

- If $\hat{\gamma}_2 \in \mathcal{L}$, then $n^2 \equiv 2A \pmod 7$, and $x_0 - y_0 + 2z_0 - t_0 \equiv 0 \pmod 7$, i.e. $x_0 - y_0 + 2z_0 - t_0 = 7\nu$, for some $\nu \in \mathbb{Z}$. As in the previous case, one shows that for $\gamma_2^* = \frac{5x_0+2y_0-4z_0+2t_0}{7} - \frac{2x_0+5y_0+4z_0-2t_0}{7}i + \frac{4x_0-4y_0+z_0-4t_0}{7}j - \frac{2x_0-2y_0+4z_0+5t_0}{7}k$ we have that $\Re(\gamma_2^*\beta) = \Re(\gamma\beta)$. Thus, the conjugate of γ_2^* provides another integer solution of the system (1-3-3-4). Denoting its coordinates by $\hat{x}_2, \hat{y}_2, \hat{z}_2, \hat{t}_2$, one can see that:

$$\begin{cases} \hat{x}_2 &= x_0 - 2\nu \\ \hat{y}_2 &= y_0 + 2\nu \\ \hat{z}_2 &= z_0 - 4\nu \\ \hat{t}_2 &= t_0 + 2\nu. \end{cases} \tag{4.19}$$

- If $\hat{\gamma}_3 \in \mathcal{L}$, then $n^2 \equiv -A \pmod 7$, and $x_0 + 4y_0 - 2z_0 \equiv 0 \pmod 7$, i.e. $x_0 + 4y_0 - 2z_0 = 7\xi$, for some $\xi \in \mathbb{Z}$. As in the previous cases,

$$\gamma_3^* = \frac{-2x_0 + 6y_0 - 3z_0}{7} + \frac{3x_0 - 2y_0 - 6z_0}{7}i - \frac{6x_0 + 3y_0 + 2z_0}{7}j - t_0k,$$

satisfies $\Re(\gamma_3^*\beta) = \Re(\gamma\beta)$. Hence, the coordinates of its conjugate,

$\hat{x}_3, \hat{y}_3, \hat{z}_3, \hat{t}_3$, furnish another integer solution of the system (1-3-3-4), and one has:

$$\begin{cases} \hat{x}_3 &= 2y_0 - z_0 - 2\xi \\ \hat{y}_3 &= 2y_0 - 3\xi \\ \hat{z}_3 &= -3y_0 + 2z_0 + 6\xi \\ \hat{t}_3 &= t_0. \end{cases} \tag{4.20}$$

Now we have everything that we need to prove the following result.

Proposition 4.12. *Let $m, n \in \mathbb{N}$ be such that $35m - n^4$ is non-negative not of the form $4^r(8s+7)$, for any $r, s \in \mathbb{N}$. When $m \equiv -1 \pmod 3$ the system (1-3-5) has integer solutions for all $n \in \mathbb{N}$ with $(n, 105) = 1$.*

Proof. Let $A \in \mathbb{Z}$ from (4.8). We see that for all $n \in \mathbb{N}$ such that $n^2 \not\equiv 0 \pmod 7$, we necessarily have one of the following: $n^2 \equiv \pm A \pmod 7$, $n^2 \equiv \pm 2A \pmod 7$, $n^2 \equiv \pm 4A \pmod 7$, or $A \equiv 0 \pmod 7$. Therefore, we have:

- If either $A \equiv 0 \pmod 7$, $n^2 \equiv A \pmod 7$, $n^2 \equiv -2A \pmod 7$, or $n^2 \equiv -4A \pmod 7$, then Proposition 4.11 says that the system (1-3-5) has an integer solution.

- If $n^2 \equiv -A \pmod 7$, then the solution $\hat{x}_3, \hat{y}_3, \hat{z}_3, \hat{t}_3$ from (4.20) satisfies $\hat{x}_3 + 2\hat{z}_3 + 2\hat{t}_3 \equiv x_0 + z_0 + 2t_0 \pmod 3$, and $\hat{x}_3 + 2\hat{y}_3 + 2\hat{t}_3 \equiv x_0 + y_0 + 2t_0 \pmod 3$, therefore, Proposition 4.10 and Proposition 4.6 yield the result.

- If $n^2 \equiv 4A \pmod 7$, then the solution $\hat{x}_1, \hat{y}_1, \hat{z}_1, \hat{t}_1$ from (4.18) satisfies $\hat{x}_1 + 2\hat{y}_1 + 2\hat{t}_1 \equiv 2(x_0 + z_0 + 2t_0) \pmod 3$, and $\hat{x}_1 + 2\hat{z}_1 + 2\hat{t}_1 \equiv 2(x_0 + y_0 + 2t_0) \pmod 3$, so again Proposition 4.10 and Proposition 4.6 yield the result.

- If $n^2 \equiv 2A \pmod 7$, then $x_0 - y_0 + 2z_0 - t_0 \equiv 0 \pmod 7$, so $x_0 - y_0 + 2z_0 - t_0 = 7\nu$, for some $\nu \in \mathbb{Z}$. We are going to check when the solution (4.19) satisfies the solvability conditions modulo 5 of Proposition 4.7 and Corollary 4.8. Let $\hat{A} = 3\hat{x}_2 - \hat{y}_2 - 4\hat{z}_2 + 3\hat{t}_2$ be the corresponding A for the solution $\hat{x}_2, \hat{y}_2, \hat{z}_2, \hat{t}_2$. If either $\hat{A} \equiv 0 \pmod 5$,

$n^2 \equiv 2\hat{A} \pmod 5$, or $n^2 \equiv -\hat{A} \pmod 5$ holds, then, by Proposition 4.7, we are done. So we just need to check the following two cases:

- If $n^2 \equiv \hat{A} \pmod 5$, then $\hat{x}_2 - 2\hat{y}_2 - \hat{z}_2 + 2\hat{t}_2 \equiv 0 \pmod 5$. Therefore, $x_0 - 2y_0 - z_0 + 2t_0 \equiv -2\nu \pmod 5$. We also have that $x_0 - y_0 + 2z_0 - t_0 = 7\nu \equiv 2\nu \pmod 5$, and therefore we obtain $x_0 + y_0 - 2z_0 - 2t_0 \equiv 0 \pmod 5$. Corollary 4.8 then yields the result.
- If $n^2 \equiv -2\hat{A} \pmod 5$, then $\hat{y}_2 \equiv 3\hat{x}_2 \pmod 5$, which implies that $y_0 + 2x_0 \equiv 2\nu \pmod 5$. This together with $x_0 - y_0 + 2z_0 - t_0 \equiv 2\nu \pmod 5$ yields $x_0 + 2y_0 - 2z_0 + t_0 \equiv 0 \pmod 5$. Therefore, Corollary 4.8 yields the result again.

□

Proposition 4.9 and Propostion 4.12 combined make for Theorem 4.4.

4.6 Integer solutions

For $m \in \mathbb{N}$, we set $S_m = \{n \in \mathbb{N} : 35m - n^4 \geqslant 0\}$, and it will also be convenient to set $T_m = \{n \in S_m : 35m - n^4 \text{ is a sum of 3 squares}\}$.

Lemma 4.13. *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.*

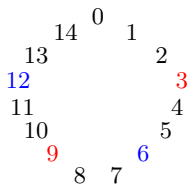
Proof. Simple congruence arguments easily show the following:

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

□

Lemma 4.14. *If $m \not\equiv 0 \pmod{16}$ and if A is a subset of S_m containing at least 10 consecutive numbers, then there is at least one $n \in A \cap T_m$ that satisfies $3 \mid n$ and $5 \nmid n$, and another $n \in A \cap T_m$ such that $(n, 105) = 1$.*

Proof. Consider the classes modulo 15 written in a circle as follows.



The colors have the following meaning: red and blue represent different parities, but not necessarily the parity of the number in the figure — if one adds a multiple of 15, the parities either remain the same or switch —, and only residues that are divisible by 3 but not by 5 are colored. Then, in order to apply the previous lemma to guarantee that in a certain set of consecutive numbers there is at least one divisible by 3 but not by 5, one just needs to ensure that the set must contain both a blue and a red residue. By inspection of the figure, one sees that, actually, one only needs 9 consecutive numbers (the worst cases are the sequences starting at 10 and ending at 3, and starting at 13 and ending at 6).

For the second statement, one must work modulo 105. Again, imagine all the classes modulo 105 in a circular, or periodic arrangement. Here we represent them in five lines, and the reader should imagine the number 104 connected back to the beginning, and only the residues that are coprime to 105 are shown, the other being represented by a dot.

·	1	2	·	4	·	·	·	8	·	·	11	·	13	·	·	16	17	·	19	·
·	22	23	·	·	26	·	·	29	·	31	32	·	34	·	·	37	38	·	·	41
·	43	44	·	46	47	·	·	·	·	52	53	·	·	·	·	58	59	·	61	62
·	64	·	·	67	68	·	·	71	·	73	74	·	76	·	·	79	·	·	82	83
·	·	86	·	88	89	·	·	92	·	94	·	·	97	·	·	·	101	·	103	104

Again, a simple inspection shows that 10 consecutive numbers suffice to guarantee at least a blue and a red residue (the worst cases are the sequences starting at 2 and ending at 11, and starting at 95 and ending with 104). □

We have that $|S_m| \geqslant 10$ if $\sqrt[4]{35m} \geqslant 10$, which is equivalent to $m \geqslant 286$. Therefore, from Theorem 4.4, it follows that the system (1-3-5) has

integer solutions for all $m \not\equiv 0 \pmod{16}$ and $m \geqslant 286$. Since it is easy to check that this system has solutions for all m up to 286, and since a solution $(x_0, y_0, z_0, t_0) \in \mathbb{Z}^4$ for that system for some m, yields the solution $(4x_0, 4y_0, 4z_0, 4t_0) \in \mathbb{Z}^4$ for $16m$, a simple descent argument establishes the following result.

Theorem 4.15. *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. Moreover, for $m \in \mathbb{N}$, with $16 \nmid m$ one can choose this square to be one of $1, 4, 9$, or 36.*

Proof. It only remains to prove the last statement, which follows from the fact that, when $6 \in S_m$, i.e. when $m \geq 38$, by Lemma 4.13, T_m either contains $\{1, 3, 5\}$ or $\{2, 4, 6\}$. Thus, for $m \equiv 0, -1 \pmod{3}$ one can choose, in Theorem 4.4, either $n = 1$ or $n = 2$; for $m \equiv 1 \pmod{3}$, either $n = 3$ or $n = 6$. □

Note that if we do not require $16 \nmid m$ then the square will be on the set

$$\{4^r s^2 : r \in 2\mathbb{N} \ \& \ s \in \{1, 2, 3, 6\}\}.$$

In Conjecture 4.5(ii) of the paper [20], Zhi-Wei Sun conjectured that any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + t^2$ with $x, y, z, t \in \mathbb{N}$ such that $| x + 3y - 5z | \in \{4^r : r \in \mathbb{N}\}$. Theorem 4.15 provides an advance towards this conjecture.

4.7 Natural Solutions

Theorem 4.16. *For $m \in \mathbb{Z}$ not divisible by 16 and sufficiently large (namely $m \geqslant 1.05104 \times 10^{11}$), there exists at least one $n \in \left[\sqrt[4]{34\, m}, \sqrt[4]{35\, m}\right]$ such that the system (1-3-5) has solutions in $\mathbb{N}$.*

Proof. Firstly, we note that there is a constant $c \in \mathbb{R}$ such that for $m \geq c$ the interval $\left[\sqrt[4]{34\,m}, \sqrt[4]{35\,m}\right]$ contains at least 10 consecutive integers. We can easily calculate c:

$$\sqrt[4]{35\,m} - \sqrt[4]{34\,m} \geq 10 \iff m \geq \left(\frac{10}{\sqrt[4]{35} - \sqrt[4]{34}}\right)^4 \simeq 105\,103\,560\,126.8026.$$

From Lemma 4.14 we know that, for $m \geqslant c$, the interval contains an $n \in \mathbb{N}$ such that $35m - n^4$ is a sum of 3 squares and m, n satisfy the conditions of Theorem 4.4. It then follows that there exist $A, B, C \in \mathbb{Z}$ such that $\delta = \gamma\alpha = n^2 + Ai + Bj + Ck \in \mathcal{L}$, for some $\gamma = x - yi - zj - tk \in \mathcal{L}$, with $\alpha = 1 + 3i + 5j$, and $\mathrm{N}(\delta) = 35\,m$. We then have that

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

Therefore we must have that

$$\begin{cases} n^2 &= x + 3y + 5z \\ A &= 3x - y + 5t \\ B &= 5x - z - 3t \\ C &= -5y + 3z - t. \end{cases} \tag{4.21}$$

Solving (4.21) yields

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

Note that if (x, y, z, t) is a solution of (1-3-5), then $(x, y, z, -t)$ is a solution of it as well. Therefore a sufficient condition to have a solution of (1-3-5) in $\mathbb{N}$ is:

$$\begin{cases} n^2 &\geqslant -3A - 5B \\ 3n^2 &\geqslant A + 5C \\ 5n^2 &\geqslant B - 3C. \end{cases} \tag{4.22}$$

Now, from the Cauchy-Schwartz inequality we can see that

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

If $n^2 \geqslant \sqrt{34\,(35m - n^4)}$, then $n^2 \geqslant -3A - 5B$, and so $x \geqslant 0$. Similarly one can show that if $3n^2 \geqslant \sqrt{26\,(35m - n^4)}$, then $y \geqslant 0$, and if $5n^2 \geqslant \sqrt{10\,(35m - n^4)}$, then $z \geqslant 0$. Hence $n^2 \geqslant \sqrt{34\,(35m - n^4)}$ is a sufficient condition for $x, y, z \in \mathbb{N}$. The last condition is equivalent to $n \geqslant \sqrt[4]{34\,m}$. □

Finally, Rogério Reis, from the department of Computer Science of the University of Porto, and a researcher at CMUP, wrote a very efficient C program, implementing ideas by the authors and suggestions made by Zhi-Wei Sun, that checked that all natural numbers up to 105 103 560 126, except for the multiples of 16, do have a 1-3-5 representation. These verification is reported in [12]. Qing-Hu Hou computation mentioned in [22] was also rechecked, i.e. it was verified that Sun's 1-3-5 Conjecture holds for all numbers up to 10^{10}. Since $\frac{105\,103\,560\,126}{16} < 10^{10}$, a simple decent argument completes the proof of the 1-3-5 conjecture. Therefore, we can now state the following.

Main Theorem. 4.1. *Any natural number can be written as a sum of four squares, $x^2 + y^2 + z^2 + t^2$ with $x, y, z, t \in \mathbb{N}$, in such a way that $x + 3y + 5z$ is a perfect square.*

As a final remark, we note that what one would naturally call the 1-3-3-4 conjecture is not true. That is, it is not true that every natural number m can be written as a sum of four squares, $m = x^2+y^2+z^2+t^2$, so that $x+3y+3z+4t$ is a perfect square. For example the numbers 3, 4, 7, 8, 22, 23, 31, 42, 61, 95, 148, 157 and 376 do not have such a representation. Computations seem to suggest that, except for these thirteen numbers and all its multiples by powers of 16, all other numbers do have a 1-3-3-4 representation.

5

Metacommutation in $\mathcal{H}$ and $\mathcal{L}$

Although the rings of Hurwitz and Lipschitz integers are not commutative, they do nevertheless have a very interesting property, called metacommutation, that is directly linked with Theorems 2.11 and 2.15. In this chapter we will define metacommutation and its generalization in the ring of Hurwitz integers, but everything works in the ring of Lipschitz integers as well.

We remind the reader that Theorem 2.11 implies that if we want to investigate all possible prime factorizations of a Hurwitz quaternion, then we need to look at all possible factorizations of its norm. Let us focus on the particular case of a Hurwitz integer that is a product of two Hurwitz primes.

Let p and q be rational primes and Q a Hurwitz prime of norm q. Then from Theorem 2.11, we have that for every Hurwitz prime P of norm p, we can find primes $Q', P' \in \mathcal{H}$ of norms q, p, respectively, satisfying

$$PQ = Q'P', \tag{5.1}$$

and the pair (Q', P') is unique up to unit-migration. This process of swapping the primes is called **metacommutation**.

Given $P_1, P_2 \in \mathcal{H}$, define an equivalence relation $\sim$ by

$$P_1 \sim P_2 \text{ if and only if } \exists u \in \mathcal{H}^* : P_1 = uP_2.$$

Denote the equivalence class of P, which is the set of left associates of P, by $[P]$. This class contains 24 elements, since there are 24 units in $\mathcal{H}$. Let Π_p be the set of these left associate classes of Hurwitz primes lying above the prime p. By Theorem 3.11, there are exactly $p+1$ of these classes that correspond to the $p+1$ primary primes of norm p.

Definition 5.1. *Let P, P' be two Hurwitz primes of norm p. The map*

$$\begin{aligned} \mu_Q : \Pi_p &\to \Pi_p \\ [P] &\mapsto [P'], \end{aligned}$$

*where P' is obtained from P as in (5.1), is called the **metacommutation map** by Q of the primes of norm p.*

Proposition 5.2. *Let P, P' be two Hurwitz primes of norm p. Then,*

$$\mu_Q : \Pi_p \to \Pi_p$$

is a permutation of the $p+1$ primes lying above p.

Proof. We know that P' is unique up to left multiplication by a unit. Also, from (5.1), is obvious that replacing P with a left associate has no effect on P', therefore μ_Q is well defined.

Now, assume that there is $P_1, P_2 \in \mathcal{H}$ such that $P_1 Q = Q' P$ and $P_2 Q = Q'' P$, then $\bar{Q}' P_1 = P \bar{Q} = \bar{Q}'' P_2$. By Theorem 2.11, we have that P_1 and P_2 are left associates, and therefore μ_Q is injective, and since it is defined on a finite set, it is a permutation.

□

The main result on the metacommutation map is the following theorem.

Theorem 5.3 (Cohn and Kumar)**.** *The sign of the metacommutation map μ_Q is the quadratic character $\left(\frac{q}{p}\right)$ of q modulo p.*

If $p = 2$, or if Q is congruent to a rational integer modulo p, then μ_Q is the identity permutation. Otherwise it has $1 + \left(\frac{\mathrm{Tr}(Q)^2 - 4q}{p}\right)$ fixed points.

There are two papers that prove the above theorem, namely the papers [2] and [6].

From now on we will call the cycles of μ_Q that have length greater than 1, i.e. that are not made by a single fixed point, **nontrivial cycles**. Using results of the above papers it is not very hard to prove the following.

Proposition 5.4. *The nontrivial cycles of μ_Q have length 2 if and only if Q is pure modulo p.*

Proof. Let $Q = a + bi + cj + dk$ and $q = \mathrm{N}(Q)$. From [2], we know that we can think of μ_Q as the left action of the matrix

$$\phi_Q = \frac{1}{q}\begin{pmatrix} a^2+b^2-c^2-d^2 & 2ad+2bc & -2ac+2bd \\ -2ad+2bc & a^2-b^2+c^2-d^2 & 2ab+2cd \\ 2ac+2bd & -2ab+2cd & a^2-b^2-c^2+d^2 \end{pmatrix}$$

on the points of the conic $C_p = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_p) \mid x^2 + y^2 + z^2 = 0\}$.

If Q is pure modulo p, then $a \equiv 0 \pmod{p}$, therefore ϕ_Q becomes symmetric, and since it is orthogonal as well, we must have that $\phi_Q^2 = I$ in $\mathbb{F}_p$. This means that μ_Q can not have a nontrivial cycle of length greater than 2.

If the nontrivial cycles of μ_Q have length 2, then ϕ_Q^2 fixes every point of C_p, or to put it differently we have that

$$(\phi_Q^2 - I)v = 0,$$

for all $v \in C_p$. Now if C_p contains three linearly independent vectors then this would mean that $\phi_Q^2 - I = 0$ in $\mathbb{F}_p$.

Choose $a, b \in \mathbb{F}_p$ such that $a^2 + b^2 + 1 \equiv 0 \pmod{p}$, and notice that $(1, a, b), (b, 1, a)$, and $(a, b, 1)$ are 3 distinct points in C_p. The determinant of the matrix that has these vectors as columns equals $D_1 = a^3 + b^3 - 3ab + 1$. If one considers the vectors $(1, a, b), (b, -1, a), (a, b, -1)$, that are also in C_p then the respective determinant is $D_2 = a^3 + b^3 + ab + 1$. Then, we claim that at

least one of D_1 and D_2 is non-zero in $\mathbb{F}_p$. Indeed, let $D1 \equiv D2 \equiv 0 \pmod{p}$, then $2ab \equiv 0 \pmod{p}$, and so either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. We can assume, without loss of generality, that $b \equiv 0 \pmod{p}$. Then $a^2 + 1 \equiv 0 \pmod{p}$. But, $D_1 \equiv 0$ implies $a^3 + 1 \equiv 0 \pmod{p}$, from which it follows that $a^3 \equiv a^2 \pmod{p}$, and so $a \equiv 1 \pmod{p}$, and then $2 \equiv 0 \pmod{p}$, a contradiction. Therefore $(D_1, D_2) \not\equiv (0,0) \pmod{p}$, and therefore $\phi_Q^2 = I$ in $\mathbb{F}_p$..

The characteristic polynomial ofϕ_Q is

$$\chi_{\phi_Q} = x^3 - \mathrm{Tr}(\phi_Q)x^2 + \mathrm{Tr}(\phi_Q)x - 1,$$

and since ϕ_Q satisfies it, we have that

$$\phi_Q^3 - \mathrm{Tr}(\phi_Q)\phi_Q^2 + \mathrm{Tr}(\phi_Q)\phi_Q - I = 0$$

using that $\phi_Q^2 = I$, we get that

$$(\phi_Q - I)(\mathrm{Tr}(\phi_Q) + 1) = 0$$

in $\mathbb{F}_p$. Therefore, either $\phi_Q = I$ in $\mathbb{F}_p$ or $\mathrm{Tr}(\phi_Q)+1 \equiv 0 \pmod{p}$. If $\phi_Q = I$ in $\mathbb{F}_p$, then all the points are fixed, so all the cycles have length 1, a contradiction since we are assuming that nontrivial cycles exist. Hence we must have that $\mathrm{Tr}(\phi_Q) + 1 \equiv 0 \pmod{p}$, and since $\mathrm{Tr}(\phi_Q) \equiv \frac{4a^2}{q} - 1 \pmod{p}$, we finally get that $a \equiv 0 \pmod{p}$. □

Proposition 5.5. *The nontrivial cycles of μ_Q have length 3 if and only if* $\mathrm{N}(Q) \equiv \mathrm{Tr}(Q)^2 \pmod{p}$.

Proof. Let again $Q \equiv a + bi + cj + dk \pmod{p}$, $\mathrm{N}(Q) = q$ and ϕ_Q from the above proof.
($\Leftarrow$) If $\mathrm{N}(Q) \equiv \mathrm{Tr}(Q)^2 \pmod{p}$ then $3a^2 \equiv b^2+c^2+d^2 \pmod{p} \iff 4a^2 \equiv q \pmod{p} \iff \mathrm{Tr}(\phi_Q) = 0$ in $\mathbb{F}_p$. Since ϕ_Q satisfies its characteristic

polynomial we have that

$$\phi_Q^3 - \mathrm{Tr}(\phi_Q)\phi_Q^2 + \mathrm{Tr}(\phi_Q)\phi_Q - \det(\phi_Q) = 0,$$

therefore $\phi_Q^3 = I$ in $\mathbb{F}_p$. From Theorem 5.3 in [6] we know that all the nontrivial cycles have the same length, if this length were equal to 2, then from the above proposition we would have that $\phi_Q^2 = I$, hence $\phi_Q = I$ in $\mathbb{F}_p$. This would mean that there is no cycle with length greater than one, a contradiction. Therefore we must have that all the nontrivial cycles have length 3.

($\Rightarrow$) If the nontrivial cycles of μ_Q have length 3, then ϕ_Q^3 fixes every point of C_p, therefore like in the previous proof, since there are 3 linearly independent vectors in C_p, ϕ_Q^3 is the identity operator, i.e. $\phi_Q^3 = I$ in $\mathbb{F}_p$. Since ϕ_Q satisfies its characteristic polynomial we have that

$$\phi_Q^3 - \mathrm{Tr}(\phi_Q)\phi_Q^2 + \mathrm{Tr}(\phi_Q)\phi_Q - \det(\phi_Q) = 0$$

using that $\phi_Q^3 = I$, we get that

$$\mathrm{Tr}(\phi_Q)(\phi_Q^2 - \phi_Q) = 0$$

in $\mathbb{F}_p$. Therefore, either $\phi_Q^2 = \phi_Q$ or $\mathrm{Tr}(\phi_Q) = 0$ in $\mathbb{F}_p$. If $\phi_Q^2 = \phi_Q$ then since $\phi_Q^3 = I$, we have that $\phi_Q = I$ in $\mathbb{F}_p$, which means that all the points are fixed, a contradiction. Hence we must have that $\mathrm{Tr}(\phi_Q) \equiv 0 \pmod{p}$, and since $\mathrm{Tr}(\phi_Q) = \frac{4a^2}{q} - 1$, we get that $3a^2 \equiv b^2 + c^2 + d^2 \pmod{p}$. □

5.1 Generalization of the metacommutation map

In this section we will define a generalization of the metacommutation map, in the sense that we will look at metacommutation by a fixed prime $R \in \mathcal{H}$ as a permutation of the Hurwitz *integers* of semiprime norm pq. Remember that in the previous section we have defined metacommutation as a right

action, meaning that we multiplied the primes above $p \in \mathbb{Z}$ on the right with a certain prime above Q.

From now on, we will call **right metacommutation** by the prime $R \in \mathcal{H}$, the map:

$$\begin{aligned} \mu_R : \Pi_p^L &\longrightarrow \Pi_p^L \\ P &\longmapsto P', \end{aligned}$$

where P, P' satisfy

$$P\,R = R'\,P' \tag{5.2}$$

for some $R' \in \mathcal{H}$ above $r = \mathrm{N}(R)$, and Π_p^L is the set of left associate classes of the Hurwitz primes above p.
We can similarly define the left metacommutation map. Let Π_q^R be the set of right associate classes of the Hurwitz primes above q. Define now **left metacommutation** as the map

$$\begin{aligned} {}_R\mu : \Pi_q^R &\longrightarrow \Pi_q^R \\ Q &\longmapsto Q', \end{aligned}$$

where $Q, Q' \in \mathcal{L}$ above the rational prime q, R is from (5.2), and they satisfy

$$R\,Q = Q'\,R'' \tag{5.3}$$

for some $R'' \in \mathcal{L}$ above $r \in \mathbb{Z}$.

Observe that

$$P\,R = R'\,P' \iff \bar{R}'\,P\,R\bar{R} = \bar{R}'\,R'\,P'\bar{R} \iff \bar{R}'\,P = P'\bar{R}$$

Which means that

$$\mu_{\bar{R}}(P') = P \tag{5.4}$$

Moreover

$$P\,R = R'\,P' \iff R\bar{P}' = \bar{P}R'.$$

Therefore we have that

$$P \overset{\mu_R}{\longmapsto} P' \iff \bar{P}' \overset{{}_R\mu}{\longmapsto} \bar{P}.$$

Hence μ_R and ${}_R\mu$ have the same cycle structure, since whenever $(P_1, P_2, \cdots, P_n)$ is a cycle of μ_R, then $(\bar{P}_n, \bar{P}_{n-1} \cdots, \bar{P}_1)$ is a cycle of ${}_R\mu$.

Putting (5.2) and (5.3) together, we get

$$R'\,P'\,Q = P\,R\,Q = P\,Q'\,R'' \tag{5.5}$$

The metacommutation maps μ_R, ${}_R\mu$ induce a permutation of the Hurwitz integers above pq, that is defined by

$$\begin{aligned} {}_R\mu_R : \Pi_{pq} &\longrightarrow \Pi_{pq} \\ P'\,Q &\longmapsto P\,Q', \end{aligned}$$

where $P, P'Q, Q'$ from (5.5) and $\Pi^R_{pq} = \left\{PQ \,|\, P \in \Pi^L_p,\, Q \in \Pi^R_q\right\}$.
Equivalently, we may define ${}_R\mu_R$ as the map ${}_R\mu_R : \Pi^R_{pq} \longrightarrow \Pi^R_{pq}$ such that

$${}_R\mu_R(P'\,Q) = \mu_{\bar{R}}(P')\ {}_R\mu(Q)$$

${}_R\mu_R$ is indeed a permutation of the integers above pq because:

- ${}_R\mu_R$ is well defined since by the above, $P'Q$ and any of its right associates will have the same image under ${}_R\mu_R$.
- ${}_R\mu_R$ is injective because

$$\begin{aligned} {}_R\mu_R(P'_0\,Q_0) = {}_R\mu_R(P'_1\,Q_1) &\iff \\ \mu_{\bar{R}}(P'_0)\ {}_R\mu(Q_0) = \mu_{\bar{R}}(P'_1)\ {}_R\mu(Q_1). & \end{aligned}$$

  Now we know that $\mu_{\bar{R}}(P'_0), \mu_{\bar{R}}(P'_1)$ are both quaternions of norm p, and again from Theorem 2.11 we must have $\mu_{\bar{R}}(P'_0) = \mu_{\bar{R}}(P'_1)$ up to left associates. Now since $\mu_{\bar{R}}$ is a permutation we have that $P'_0 = P'_1$. Similarly we have that $Q_0 = Q_1$, hence $P'_0\,Q_0 = P'_1\,Q_1$.

We can generalize the metacommutation map in another way as well. It is not hard to see that metacommutation by a Hurwitz *integer* of the primes above some prime $r \in \mathbb{Z}$, is just a composition of metacommutation maps. Let $P, Q, R \in \mathcal{H}$ be Hurwitz primes, then by Theorem 2.11 we have that there exists $P', Q', R', R'' \in \mathcal{H}$, such that

$$RPQ = P'R'Q = P'Q'R''$$

Therefore we may define

$$\begin{aligned} \mu_{PQ} : \Pi_r^L &\longrightarrow \Pi_r^L \\ R &\longmapsto R'', \end{aligned}$$

And since

$$\mu_{PQ}(R) = R'' = \mu_Q(\mu_P(R)),$$

We have that

$$\mu_{PQ} = \mu_Q \circ \mu_P.$$

Note that everything that we did in this section hold in the ring of Lipschitz integers as well, as it is mentioned at the end of [6].

5.2 A partial answer to the 1-3-5 conjecture

In this section we are going to demonstrate a way to attack problems like the "1-3-5 conjecture" using metacommutation. In connection to the "1-3-5 conjecture", we will look at the particular case that a Hurwitz integer has norm 35, to prove the following.

Proposition 5.6. *For all primes $r \in \mathbb{Z}$, there exist $R, R' \in \mathcal{L}$ of norm equal to r, such that*

$$R\zeta = \zeta' R',$$

for some $\zeta, \zeta' \in \mathcal{L}$, with $\mathrm{N}(\zeta) = \mathrm{N}(\zeta') = 35$, and $\zeta \not\sim_d \zeta'$.

We remind the reader that for $\alpha, \beta \in \mathcal{L}$, we have $\alpha \sim_d \beta$ if and only if a can be obtained by b with sign and coefficient changes. Before trying to prove the above we are going to need a couple of technical lemmas.

Lemma 5.7. *Let $r \in \mathbb{Z}$ be a prime greater than 289. Then, there exist $R = R_0 + R_1 i + R_2 j + R_3 k \in \mathcal{L}$, with $\mathrm{N}(R) = r$ and R_0 satisfying any combination of $R_0^2 \equiv \pm 1 \pmod 5$ and $R_0^2 \equiv 1, 2, 4 \pmod 7$.*

Proof. For $R_0^2 \equiv 1 \pmod 5$ and $R_0^2 \equiv 1 \pmod 7$ it is easy to see that at least one of $r-1$, $r-36$ can not be of the form $4^k(8s+7)$. Hence, there exists $b, c, d \in \mathbb{Z}$ such that $r - R_0^2 = b^2 + c^2 + d^2$, where $R_0 = 1$, or $R_0 = 36$. The rest of the cases are handled analogously, but for the sake of completeness, we write the values of R_0 that make the argument work.

- $R_0^2 \equiv 1 \pmod 5$ and $R_0^2 \equiv 2 \pmod 7$ take $R_0^2 = 16$ or $R_0^2 = 121$
- $R_0^2 \equiv 1 \pmod 5$ and $R_0^2 \equiv 4 \pmod 7$ take $R_0^2 = 81$ or $R_0^2 = 256$
- $R_0^2 \equiv -1 \pmod 5$ and $R_0^2 \equiv 1 \pmod 7$ take $R_0^2 = 64$ or $R_0^2 = 169$
- $R_0^2 \equiv -1 \pmod 5$ and $R_0^2 \equiv 2 \pmod 7$ take $R_0^2 = 9$ or $R_0^2 = 289$
- $R_0^2 \equiv -1 \pmod 5$ and $R_0^2 \equiv 4 \pmod 7$ take $R_0^2 = 4$ or $R_0^2 = 144$.

□

Lemma 5.8. *Let $r > 289$ be a prime, and let $\mu_R : \Pi_5^L \longrightarrow \Pi_5^L$, ${}_R\mu : \Pi_7^R \longrightarrow \Pi_7^R$ be the (right and left) metacommutation maps for the Lipschitz primes above 5 and 7 respectively. We can always find an $R = R_0 + R_1 i + R_2 j + R_3 k \in \mathcal{L}$, with $\mathrm{N}(R) = r$, such that*
(α)μ_R and ${}_R\mu$ both have 1 fixed point and one cycle of 5 and 7 respectively, whenever $\left(\frac{r}{5}\right) = \left(\frac{r}{7}\right) = 1$.
(β)μ_R has 1 fixed point and a cycle of 5 and ${}_R\mu$ has no fixed points and a cycle of 8, whenever $\left(\frac{r}{5}\right) = 1$ and $\left(\frac{r}{7}\right) = -1$.
(γ)μ_R has two fixed points and a cycle of 4 and ${}_R\mu$ has 1 fixed point and a cycle of 7, whenever $\left(\frac{r}{5}\right) = -1$ and $\left(\frac{r}{7}\right) = 1$.

(δ) μ_R has two fixed points and a cycle of 4 and ${}_R\mu$ has no fixed points and a cycle of 8, whenever $\left(\frac{r}{5}\right) = \left(\frac{r}{7}\right) = -1$.

Proof. Note that by [2] the number of fixed points under metacomutation by R is equal to $1 + \left(\frac{R_0^2 - r}{p}\right)$, and its sign is $\left(\frac{r}{p}\right)$. In our case p is either 5 or 7.

(α) If $\left(\frac{r}{5}\right) = \left(\frac{r}{7}\right) = 1$ then μ_R and ${}_R\mu$ both having 1 fixed point and one cycle of 5 and 7 respectively, is equivalent to $R_0^2 = r \pmod 5$ and $R_0^2 = r \pmod 7$.

(β) If $\left(\frac{r}{5}\right) = 1$ and $\left(\frac{r}{7}\right) = -1$ then μ_R having 1 fixed point and a cycle of 5 and ${}_R\mu$ having no fixed points and a cycle of 8, is equivalent to $R_0^2 = r \pmod 5$ and $R_0^2 \equiv r-1, r-2$ or $r-4 \pmod 7$.

(γ) If $\left(\frac{r}{5}\right) = -1$ and $\left(\frac{r}{7}\right) = 1$ then μ_R having two fixed points and a cycle of 4 and ${}_R\mu$ has 1 fixed point and a cycle of 7 is equivalent to $R_0^2 = r \pm 1 \pmod 5$ and $R_0^2 \equiv r \pmod 7$.

(δ) If $\left(\frac{r}{5}\right) = \left(\frac{r}{7}\right) = -1$ then μ_R having two fixed points and a cycle of 4 and ${}_R\mu$ having no fixed points and a cycle of 8, is equivalent to $R_0^2 = r \pm 1 \pmod 5$ and $R_0^2 \equiv r-1, r-2$ or $r-4 \pmod 7$.
By the previous lemma we have that in any of these cases there exists an $R \in \mathcal{L}$, with $\mathrm{N}(R) = r$ that can make the argument work.

In all the cases and depending on the value of r modulo 5 and 7 we get 1 or 2 possible values for R_0^2. The previous lemma yields the result. □

Proof of Proposition 5.6. From [2] we know that the signs of the permutations $\mu_R, {}_R\mu$ are equal to the Legendre symbols $\left(\frac{r}{5}\right)$, $\left(\frac{r}{7}\right)$, respectively. Moreover we know from [2] that we have at most 2 fixed points, and from [6] that all the nontrivial cycles have the same length. Depending on the signs of these permutations, we have the following cases:

- $\left(\frac{r}{5}\right) = \left(\frac{r}{7}\right) = 1$. We can easily see that both signs being positive can happen only when some combination of the following occurs:

μ_R	${}_R\mu$
0 fixed points and 2 cycles of 3	0 fixed points and 2 cycles of 4
1 fixed point and a cycle of 5	0 fixed points and 4 cycles of 2
2 fixed points and 2 cycles of 2	1 fixed point and a cycle of 7
	2 fixed points and 2 cycles of 3

By the previous lemmas we know that there exists $R \in \mathcal{L}$ such that μ_R and ${}_R\mu$ both have 1 fixed point.

Then

$$(P_0), (P_1, P_2, \ldots, P_5)$$

is the cycle structure of μ_R for the primes above 5 and

$$(Q_0), (Q_1, Q_2, \ldots, Q_7)$$

is the cycle structure of ${}_R\mu$ for the primes above 7. It is easy to see now from the above cycle structures and (5.5) that under ${}_R\mu_R$:

- P_0Q_0 is a fixed point
- $(P_0Q_1, P_0Q_2, \ldots, P_0Q_7)$ is a cycle of length 7
- $(P_5Q_0, P_4Q_0, \ldots, P_1Q_0)$ is a cycle of length 5
- $(P_1Q_1, P_5Q_2, P_4Q_3, P_3Q_4, P_2Q_5, \ldots, P_3Q_6, P_2Q_7)$ is a cycle of length 35

A cycle of length 35 implies that there must exist P_i, P_j, Q_k, Q_l such that $P_iQ_k \nsim P_jQ_l$, because there are 48 integers in Π_{35}, 24 in the class of $\alpha = 1 + 3i + 5j$, and 24 in the class of $\beta = 1 + 3i + 3j + 4k$.

- $\left(\frac{r}{5}\right) = -1$ and $\left(\frac{r}{7}\right) = 1$. We have the following possibilities

μ_R	${}_R\mu$
0 fixed points and 2 cycles of 3	0 fixed points and a cycle of 8
1 fixed point and a cycle of 5	2 fixed points and a cycle of 6
2 fixed points and 2 cycles of 2	2 fixed point and 3 cycles of 2

We know that there exists $R \in \mathcal{L}$ such that μ_R has 1 fixed point and ${}_R\mu$ has no fixed points and a cycle of 8. This would yield a cycle of length 40 for ${}_R\mu_R$ and the result follows.

- $\left(\frac{r}{5}\right) = -1$ and $\left(\frac{r}{7}\right) = 1$. We have the following possibilities

μ_R	${}_R\mu$
0 fixed points and 3 cycles of 2	0 fixed points and 2 cycles of 4
0 fixed points and a cycle of 6	0 fixed points and 4 cycles of 2
2 fixed points and 1 cycle of 4	1 fixed point and a cycles of 7
	2 fixed points and 2 cycles of 3

There exists $R \in \mathcal{L}$ such that μ_R has 2 fixed points and ${}_R\mu$ has one fixed point and a cycle of 7. This would yield a cycle of length 28 for ${}_R\mu_R$ and the result follows.

- $\left(\frac{r}{5}\right) = \left(\frac{r}{7}\right) = -1$. We have the following possibilities

μ_R	${}_R\mu$
0 fixed points and 3 cycles of 2	0 fixed points and a cycles of 8
0 fixed points and a cycle of 6	2 fixed points and a cycles of 6
2 fixed points and a cycle of 4	2 fixed points and 3 cycles of 2

In this case, there is no way we can have a cycle with length greater than 24, but we know that if we multiply any given prime above 5 with the 8 primes above 7 (up to right associates), we get that 4 products are equivalent to α and 4 are equivalent to β.

Now, we know that there exists $R \in \mathcal{L}$, such that μ_R has 2 fixed points, and ${}_R\mu$ has no fixed points and a cycle of 8. This would yield 2 cycles of length 8 for ${}_R\mu_R$ that are $(Q_0P_0, Q_0P_1, ..., Q_0P_8)$ and $(Q_1P_0, Q_1P_1, \cdots, Q_1P_8)$, where Q_0, Q_1 are the fixed points under μ_R and $(P_0, P_1, \cdots, P_8)$ is the length 8 cycle of ${}_R\mu$. On each of these cycles we have elements of both classes, therefore the result follows.

Note that this proof covers all the primes above 289, but is is easy to check computationally the validity of the claim for all the primes below 289 as well. □

We will see now, how can one use Proposition 5.6 to attack the "1-3-5 conjecture". First we will need the following auxiliary lemma. We remind the reader that

$$S_m = \left\{ n \in \mathbb{N} : \, 35m - n^4 \geqslant 0 \right\}$$

and

$$T_m = \left\{ n \in S_m : \, 35m - n^4 \text{ is a sum of 3 squares} \right\}.$$

Lemma 5.9. *Let p be any odd prime $L \in \mathbb{N}_0$. Then the following*

(i) L is of the form $4^r(8s+7)$ for some $r, s \in \mathbb{N}_0$

(ii) $p^2\, L$ is of the form $4^r(8s+7)$ for some $r, s \in \mathbb{N}_0$

are equivalent.

Proof. Let $p^2\, L = 4^r(8s+7)$ for some $r, s \in \mathbb{N}_0$. We have $4^r \mid L$, therefore $L = 4^r L'$ for some $L' \in \mathbb{Z}$. So $p^2 L' = 8s+7 \Rightarrow p^2 L' = 7 \pmod 8$. We also have that $p^2 \equiv 1 \pmod 8$, for all odd primes $p \in \mathbb{Z}$, therefore $L' \equiv 7 \pmod 8$, hence L is of the form $4^r(8s+7)$ for some $r, s \in \mathbb{N}_0$.

Conversely, assume that $L = 4^r(8s+7)$ for some $r, s \in \mathbb{N}_0$. Then $p^2 L = p^2 4^r(8s+7) = 4^r[p^2(8s+7)]$. What is inside the brackets is clearly congruent to $7 \pmod 8$, which yields the result. □

Let us demonstrate now an interesting consequence of Proposition 5.6 and of the above lemma.

Proposition 5.10. *Let p be any odd prime. The system*

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

has solutions in $\mathbb{Z}$ for all $m, n \in \mathbb{N}$, such that $p^2 \mid m, p \mid n$, and $n \in T_m$.

Proof. From $p^2 \mid m$ and $p \mid n$ we have that there exist $m', n' \in \mathbb{N}$ such that $m = p^2\, m'$ and $n = p\, n'$. Therefore we have that $35\, m - n^4 = 35\, p^2\, m' - (p\, n')^4$ and therefore, by the previous lemma we have that

$$35\, m' - p^2\, n'^4 \text{ is not of the form } 4^r(8s+7) \text{ for any } r, s \in \mathbb{N}_0. \tag{5.6}$$

Hence there exists $A, B, C \in \mathbb{Z}$ such that

$$35m' - p^2 n'^4 = A^2 + B^2 + C^2.$$

Let $\delta = pn'^2 + Ai + Bj + Ck$ then $\mathrm{N}(\delta) = 35m'$, therefore there exist $\zeta, \gamma \in \mathcal{L}$ such that $\delta = \zeta\gamma$ and $\mathrm{N}(\zeta) = 35$, $\mathrm{N}(\gamma) = m'$.

- If $\zeta \sim_d \alpha$, the system

$$\begin{cases} m' &= x^2 + y^2 + z^2 + t^2 \\ p\, n'^2 &= x + 3y + 5z. \end{cases}$$

  has solutions in $\mathbb{Z}$, which since $m = p^2 m'$, $n = pn'$ implies that the system

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

  has solutions in $p\,\mathbb{Z}$.

- If If $\zeta \sim_d \beta$, the system

$$\begin{cases} m' &= x^2 + y^2 + z^2 + t^2 \\ p\, n'^2 &= x + 3y + 3z + 4t. \end{cases}$$

  has solutions in $\mathbb{Z}$. The above system, with the appropriate sign changes for the coordinates of γ, can be written

$$\begin{cases} m' &= \mathrm{N}(\gamma) \\ p\, n'^2 &= \Re(\beta\bar{\gamma}). \end{cases}$$

Now by Proposition (5.6), we know that there exists primes $P, P' \in \mathcal{L}$ above $p \in \mathbb{Z}$ such that $P\beta = \alpha' P'$, for some $\alpha' \sim_d \alpha$. We can see that

$$P\beta\bar{\gamma}P^{-1} = \alpha' P'\bar{\gamma}P^{-1}.$$

Let $\gamma' = P'\bar{\gamma}P^{-1}$. Since $\mathrm{N}(\gamma) = \mathrm{N}(\gamma')$ and $\Re(\beta\bar{\gamma}) = \Re(P\beta\bar{\gamma}P^{-1})$, we have that the system

$$\begin{cases} m' &= \mathrm{N}(\gamma') \\ p\,n'^2 &= \Re(\alpha'\gamma'). \end{cases}$$

has solutions in $\frac{1}{p}\mathbb{Z}$. Multiplying γ' by p yields the result.

□

A completely analogous result is the following

Corollary 5.11. *Let p be any odd prime. Then the system*

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

has solutions in $\mathbb{Z}$ for all $m, n \in \mathbb{N}_0$, such that $p^2 \mid m, p \mid n$, and $n \in T_m$.

5.3 A more general approach

Let $m, n \in \mathbb{N}_0$ be such that $35m - n^4 \in T_m$. On top of that, let us assume this time that there is an odd prime p such that $p^2 \mid 35m - n^4$. Note that this is a more general assumption than the result in Proposition 5.10. Then we have that that there exist $A, B, C \in \mathbb{N}_0$ such that

$$\begin{aligned} \frac{35m - n^4}{p^2} &= A^2 + B^2 + C^2 \Rightarrow \\ 35m - n^4 &= (pA)^2 + (pB)^2 + (pC)^2. \end{aligned}$$

Let $\delta = n^2 + pAi + pBj + pCk$, then $\mathrm{N}(\delta) = 35\,m$. Therefore, $\exists \zeta, \gamma \in \mathcal{L}$, with $\mathrm{N}(\zeta) = 35$, $\mathrm{N}(\gamma) = m$, such that $\delta = \zeta\gamma$. Then we can see the following two cases:

- If $\zeta \sim_d \alpha$, then the system (1-3-5) has integer solutions.

- If $\zeta \sim_d \beta$, then there are two cases.

  If $p = 5$ or $p = 7$, then Propositions 4.7 and 4.11 say that the system (1-3-5) has integer solutions.

  If $p \neq 5, 7$, then for $\lambda_1 = Ai + Bj + Ck$, we have

$$\zeta\gamma = n^2 + p\lambda_1. \tag{5.7}$$

  Taking norms, we get $35m = n^4 + p^2\,\mathrm{N}(\lambda_1)$, from which it is easy to see that $n^2 = 35t \pmod p \Rightarrow n^2 = 35t + p\lambda_2$ for some $t, \lambda_2 \in \mathbb{Z}$. Multiplying (5.7) by $\bar{\zeta}$ on the left we get:

$$\begin{aligned} 35\gamma &= \bar{\zeta}n^2 + p\bar{\zeta}\lambda_1 \\ &= \bar{\zeta}(35t + p\lambda_2) + p\bar{\zeta}\lambda_1 \\ &= 35\bar{\zeta}t + p\bar{\zeta}(\lambda_1 + \lambda_2) \end{aligned}$$

  Then $35 \mid \bar{\zeta}(\lambda_1 + \lambda_2) \Rightarrow \bar{\zeta}(\lambda_1 + \lambda_2) = 35\lambda$, for some $\lambda \in \mathcal{L}$. Hence

$$\gamma = t\,\bar{\beta} - p\lambda. \tag{5.8}$$

  Furthermore, we know that $\exists P, P' \in \mathcal{L}$, with $\mathrm{N}(P) = \mathrm{N}(P') = p$, such that

$$P\zeta = \zeta' P' \tag{5.9}$$

for some $\zeta' \sim_d \alpha$. Now if we conjugate $\delta = \zeta\gamma$ by P we get

$$\begin{aligned} \delta' &= P\delta P^{-1} \\ &= P\zeta\gamma P^{-1} \\ &= P\zeta P'^{-1}P'\gamma P^{-1} \\ &= \zeta' P'\gamma P^{-1} \end{aligned}$$

Let $\gamma' = P'\gamma P^{-1}$ and from (5.8) we get that

$$\begin{aligned} \gamma' &= P'(t\,\bar{\zeta} - p\lambda)P^{-1} \\ &= t\,P'\bar{\zeta}P^{-1} - P'p\lambda P^{-1} \\ &= t\,P'\bar{\zeta}P^{-1} - P'\lambda\bar{P} \end{aligned}$$

Therefore, a sufficient condition for $\gamma' \in \mathcal{L}$ is $P'\bar{\zeta}P^{-1} \in \mathcal{L}$. From (5.9) we have that $\bar{\zeta} = \bar{P}'\bar{\zeta}'\bar{P}^{-1}$, so we have

$$\begin{aligned} P'\bar{\zeta}P^{-1} &= P'\bar{P}'\bar{\zeta}'\bar{P}^{-1}P^{-1} \\ &= p\zeta'\frac{P}{p}P^{-1} = \zeta' \in \mathcal{L}. \end{aligned}$$

Let $\gamma' = a - bi - cj - dk$ and $\zeta' = \alpha = 1 + 3i + 5j$ (again we may assume this) we have that the system:

$$\begin{cases} \mathrm{N}(\gamma') &= \mathrm{N}(\gamma) = m \\ \Re(\zeta'\gamma') &= \Re(P\delta P^{-1}) = \Re(\delta) = n^2 \end{cases} \iff \begin{cases} m &= a^2 + b^2 + c^2 + d^2 \\ n^2 &= a + 3b + 5c \end{cases}$$

has solutions in $\mathbb{Z}$.

Therefore we have proven that

Proposition 5.12. *Let $m, n \in \mathbb{N}_0$ be such that $n \in T_m$. Moreover, assume that there is an odd prime p, such that $p^2 \mid 35m - n^4$. Then, the system (1-3-5) has solutions in $\mathbb{Z}$.*

5.4 Metacommutation and Lipschitz integers

A very interesting thing to prove would be a more general version of Proposition 5.6. We managed to get some partial results to this direction, but there is still no answer to the general case of this proposition. It is a potential subject of a future work, since this would shed some light as to how the decomposition classes behave, and help attack similar problems to the "1-3-5 conjecture". We remind the reader that two quaternions belong to the same decomposition class if they can be obtained from one another by coefficient and sign changes. The number of decompositions of a natural number, is the number of ways it can be written as a sum of 4 squares up to sign and coefficient changes. Denote this number by $\mathcal{DC}(m)$, for $m \in \mathbb{N}$. We believe that the following holds.

Conjecture 5.1. *For all primes $p, q \in \mathbb{Z}$, with $\mathcal{DC}(p) \geqslant 2$, there are $Q, Q', P, P' \in \mathcal{L}$, such that $PQ = Q'P'$ and $P \not\sim_d P'$, where $\mathrm{N}(Q) = \mathrm{N}(Q') = q$ and $\mathrm{N}(P) = \mathrm{N}(P') = p$.*

A special case of the above can be easily proved.

Proposition 5.13. *Conjecture 5.1 holds provided that there exists a prime $Q \in \mathcal{L}$ above q such that $\mathrm{Tr}(Q)^2 \equiv 4q \pmod{p}$.*

Proof. If there exists $Q \in \mathcal{L}$ such that $\mathrm{Tr}(Q)^2 \equiv 4q \pmod{p}$, then μ_Q has a unique fixed point. Therefore since all the nontrivial cycles of μ_Q have the same length, the remaining p primes above p must permute in a cycle of length p, yielding that there must exist primes P, P' such that $\mu_Q(P) = P'$ and $P \not\sim_d P'$. □

Another interesting result is the following.

Proposition 5.14. *Let $p \equiv q \equiv 1 \pmod{4}$ be primes. Then there exists $P, Q \in \mathcal{L}$ with $\mathrm{N}(P) = p$ and $\mathrm{N}(Q) = q$, such that $PQP^{-1} \in \mathcal{L}$.*

Proof. If $q \equiv 1 \pmod 4$ then it can be written as a sum of 2 squares, therefore there exist $Q_0, Q_1 \in \mathbb{Z}$ such that

$$q = Q_0^2 + Q_1^2.$$

Then we look at metacommutation by $Q = Q_0 + Q_1 i$, of the primes above p. We know that μ_Q has $1 + \left(\frac{\mathrm{Tr}(Q)^2 - 4q}{p}\right)$ fixed points. This can be written as

$$1 + \left(\frac{Q_0^2 - q}{p}\right) = 1 + \left(\frac{-Q_1^2}{p}\right) = 1 + \left(\frac{-1}{p}\right) = 2,$$

since $p \equiv 1 \pmod 4$. Therefore, there exists $P \in \mathcal{L}$ such that $PQP^{-1} \in \mathcal{L}$, in fact there are two different primes above p for any non pure prime Q' above q with $Q' \sim_d Q$, that satisfy $PQ'P^{-1} \in \mathcal{L}$. □

Now it would be nice to prove the above proposition for any primes p and q, but computational data seem to suggest that it is not always true. They did seem to suggest though that the following, which was too difficult to prove, is always true.

Conjecture 5.2. *Let p, q be primes with $p < q$. Then Proposition 5.14 holds for all pairs (p, q) except for the following*

$$\{(3, 23), (17, 31), (41, 71), (89, 151), (569, 647)\}.$$

Bibliography

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

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

[3] Conway, J. H. and Smith, D. A. (2003). *On Quaternions and Octonions*. AK Peters/CRC Press.

[4] Dummit, D. S. and Foote, R. M. (2004). *Abstract Algebra*, volume 3. Wiley Hoboken.

[5] Fisher, B. (1997). A Note on Hensel's Lemma in Several Variables. *Proceedings of the American Mathematical Society*, 125(11):3185–3189.

[6] Forsyth, A., Gurev, J., and Shrima, S. (2016). Metacommutation as a Group Action on the Projective Line over $\mathbb{F}_p$. *Proceedings of the American Mathematical Society*, 144(11):4583–4590.

[7] Hurwitz, A. (2013). *Vorlesungen über die Zahlentheorie der Quaternionen*. Springer-Verlag.

[8] Lam, T.-Y. (2013). *A First Course in Noncommutative Rings*, volume 131. Springer Science & Business Media.

[9] Legendre, A.-M. (1808). *Essai sur La Théorie des Nombres*. Courcier.

[10] Legendre, A. M. (1816). *Supplément à l'Essai sur la Théorie des Nombres*. De l'Imprimerie de Mme Ve Courcier.

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

[12] Machiavelo, A., Reis, R., and Tsopanidis, N. (2020). Report on Zhi-Wei Sun's 1-3-5 Conjecture and Some of Its Refinements.

[13] Machiavelo, A. and Tsopanidis, N. (2020). Zhi-Wei Sun's 1-3-5 Conjecture and Variations. *arXiv:2003.02592*.

[14] Marcus, D. A. and Sacco, E. (1977). *Number Fields*, volume 2. Springer.

[15] Pall, G. (1940). On the Arithmetic of Quaternions. *Transactions of the American Mathematical Society*, 47(3):487–500.

[16] Pall, G. et al. (1938). On the Factorization of Generalized Quaternions. *Duke Math. J*, 4:696–704.

[17] Scharlau, W. and Opolka, H. (2013). *From Fermat to Minkowski: Lectures on the Theory of Numbers and its Historical Development*. Springer Science & Business Media.

[18] Sun, Y.-C. and Sun, Z.-W. (2018). Some Variants of Lagrange's Four Squares Theorem. *Acta Arith.*, 183:339–356.

[19] Sun, Z.-W. (2017). Refining Lagrange's Four-Square Theorem. *Journal of Number Theory*, 175:167–190.

[20] Sun, Z.-W. (2019). Restricted Sums of Four-Squares. *Int. J. Number Theory*, 15(9):1863–1893.

[21] Wójcik, J. (1971). On Sums of Three Squares. In *Colloquium Mathematicum*, volume 1, pages 117–119.

[22] Wu, H.-L. and Sun, Z.-W. (2020). On the 1-3-5 Conjecture and Related Topics. *Acta Arith.*, 193:253–268.